Naše zn. 60299/2026-SŽ-GŘ-O25

ZADÁVACÍ DOKUMENTACE

k nadlimitní sektorové veřejné zakázce na dodávky zadávané v otevřeném řízení podle § 56 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „***ZZVZ***"), s názvem

„Realizace systému Zabezpečeného úložiště v prostředí Správy železnic"

(dále jen „***Zadávací dokumentace***" a/nebo „***ZD***")

Identifikační údaje Zadavatele a osoby zastupující Zadavatele:

Název:	Správa železnic, státní organizace
Sídlo:	Dlážděná 1003/7, Praha 1 – Nové Město, PSČ 110 00
IČO:	709 94 234
DIČ:	CZ 70994234

Zapsaný v obchodním rejstříku vedeném Městským soudem v Praze oddílu A, vložce 48384

Zastoupen:	Ing. Mojmírem Nejezchlebem, zástupcem generálního ředitele pověřeným správní radou řízením organizace
	a
	Ing. Tomášem Čočkem, Ph.D., náměstkem generálního ředitele pro ekonomiku
Profil Zadavatele:	https://zakazky.spravazeleznic.cz/

1. Informace o osobě, která zpracovala část Zadávací dokumentace

Zadavatel označuje následující části Zadávací dokumentace, na jejichž zpracování se podílela osoba odlišná od Zadavatele:

Část Zadávací dokumentace	Identifikace osoby
Přílohy č. 1, 2, 3, 9 a 10 Přílohy č. 5 Zadávací dokumentace - *Závazný vzor smlouvy*	s-boost s.r.o., IČO: 23037539, se sídlem Senovážné náměstí 978/23, Nové Město, 110 00 Praha 1

Příloha č. 1, 2, 3, 4, 5, 6, 7 a 8 Zadávací dokumentace Přílohy č. 5 a 8 Přílohy č. 5 Zadávací dokumentace – *Závazný vzor smlouvy*	PORTOS s.r.o., advokátní kancelář, IČO: 481 18 753, se sídlem Hvězdova 1716/2b, 140 00 Praha 4

2. Informace o předběžné tržní konzultaci:

2.1. Zadavatel v souladu s § 33 ZZVZ realizoval před zahájením zadávacího řízení předběžnou tržní konzultaci (dále jen „**PTK**") s dodavateli, a to písemnou formou (informace o konání PTK byla uveřejněna na profilu zadavatele – viz Přehled - E-ZAK Správa železnic, https://zakazky.spravazeleznic.cz/contract_display_17444.html). Zadavatel v této souvislosti obeznámil neomezený okruh potenciálních dodavatelů se svým záměrem a potřebami prostřednictvím dokumentu Pozvánka k předběžné tržní konzultaci ve věci přípravy zadávacích podmínek pro veřejné zakázky s názvy „Mobilní kontejnerové datové centrum" a "Realizace systému zabezpečeného úložiště v prostředí Správy železnic", případně pro jinou veřejnou zakázku shodnou s předmětem těchto dvou zakázek (dále jen „**Pozvánka**") a zároveň zaslal Pozvánku 11 vybraným dodavatelům přímo prostřednictvím e-mailu. Dodavatelé, kteří projevili zájem účastnit se PTK, měli Zadavateli v rámci dotazovacího kola PTK zaslat odpovědi na otázky uvedené v Příloze č. 4 Pozvánky – *Otázky k zodpovězení PTK*, a to na e-mailovou adresu: cnitptk@spravazeleznic.cz.

2.2. Předběžné tržní konzultace se účastnili následující dodavatelé:

- ALTRON, a.s., se sídlem Novodvorská 994/138, Braník, 142 00 Praha 4, IČO: 64948251,
- GAPP System, spol. s r.o., se sídlem Petržílkova 2565/23, Stodůlky, 158 00 Praha 5, IČO: 60487291,
- Conteg, spol. s r.o., se sídlem Štětkova 1638/18, Nusle, 140 00 Praha 4, IČO: 25701843,
- ALTEPRO solutions a.s., se sídlem Na Maninách 1092/20, Holešovice, 170 00 Praha 7, IČO: 03665496,
- Aricoma Systems a.s., se sídlem Hornopolní 3322/34, Moravská Ostrava, 702 00 Ostrava, IČO: 04308697,
- HEWLETT-PACKARD s.r.o., se sídlem Za Brumlovkou 1559/5, Michle, 140 00 Praha 4, IČO: 17048851,
- AŽD Praha s.r.o., se sídlem Žirovnická 3146/2, Záběhlice, 106 00 Praha 10, IČO: 48029483,
- O2 IT Services s.r.o., se sídlem Za Brumlovkou 266/2, Michle, 140 00 Praha 4, IČO: 02819678,
- KABEL TRADE PRAHA s.r.o., se sídlem Praha 4 - Kunratice, Dobronická 1257, PSČ 14800, IČO: 256 13 383,
- Power Tech spol. s r.o., se sídlem Na Šutce 391/32, Troja, 182 00 Praha 8, IČO: 26196930.

2.3. Informace o předmětu a výsledku předběžné tržní konzultace:

Zadavatel seznámil dodavatele se svým záměrem realizovat veřejnou zakázku a s cílem, jehož má být prostřednictvím plnění veřejné zakázky dosaženo.

V rámci předběžné tržní konzultace Zadavatel ověřil:

a) formu dodávky, spolupráci na dokumentaci a testování řešení,

b) soulad s právními předpisy a zkušenosti dodavatelů s veřejnými zakázkami,

c) možnosti financování, rámcové ceny a výpočet celkových nákladů vlastnictví,

d) předchozí realizace, technické kompetence a schopnost provozní podpory.

Na základě informací sdělených v rámci předběžné tržní konzultace Zadavatel:

a) ověřil, že trh je připraven dodat požadované řešení v plném rozsahu a většina dodavatelů má relevantní zkušenosti, avšak že pro přesné návrhy, ceny a srovnatelnost nabídek je nezbytné upřesnit technickou specifikaci. Zadavatel proto rozpracoval dokumenty Bližší specifikace předmětu plnění a Technická specifikace, které tvoří přílohu Závazného vzoru smlouvy. Konkrétně Zadavatel na základě PTK definoval požadavky na vhodnou technologii pro Bezpečné úložiště, stanovil nižší velikost úložiště a změnil poměr rychlých a pomalých disků oproti původnímu předpokladu,

b) stanovil požadavky na významné zakázky v rámci technické kvalifikace dle čl. 12.1 této Zadávací dokumentace,

c) stanovil časový Harmonogram plnění, který tvoří Přílohu č. 9 Přílohy č. 5 této zadávací dokumentace – Závazný vzor smlouvy,

d) upravil údaj o předpokládané hodnotě veřejné zakázky,

e) rozhodl nezahrnout do této Veřejné zakázky dodávku Mobilního kontejnerového datového centra a tuto realizovat jako samostatnou veřejnou zakázku.

2.4. Shrnutí výsledku předběžné tržní konzultace tvoří Přílohu č. 9 této Zadávací dokumentace.

3. Druh veřejné zakázky a zadávacího řízení:

3.1. Hlavní předmět veřejné zakázky ve smyslu § 15 ZZVZ odpovídá veřejné zakázce na dodávky.

3.2. Zadavatel zadává veřejnou zakázku v souvislosti s výkonem své relevantní činnosti ve smyslu § 153 odst. 1. písm. f) ZZVZ. Jedná se proto o sektorovou veřejnou zakázku.

3.3. Veřejná zakázka je v souladu s § 56 a násl. ZZVZ zadávána v **otevřeném řízení** ve smyslu § 3 písm. b) ZZVZ.

4. Účel a předmět veřejné zakázky:

4.1. Předmětem veřejné zakázky je dodání, implementace a konfigurace technologie centralizovaného bezpečného datového úložiště za účelem splnění zákonných povinností Zadavatele v oblasti kybernetické a fyzické bezpečnosti. Součástí plnění je zpracování analytické části, vytvoření koncepce Bezpečného úložiště, návrh detailního implementačního postupu pro vybrané systémy, dodání HW, implementace a konfigurace technologie a napojení na vybrané systémy Zadavatele.

4.2. Podrobné vymezení předmětu veřejné zakázky je uvedeno v Příloze č. 5 Zadávací dokumentace – Závazný vzor smlouvy (dále tak jen „**smlouva**").

4.3. Klasifikace předmětu veřejné zakázky (CPV) :

Hlavní kód CPV: 30210000-4 | Stroje na zpracování dat (technické vybavení)

Doplňkové kódy CPV:

Kód CPV: 72220000-3 | Systémové a technické konzultační služby

Kód CPV: 72224000-1 | Poradenství v oblasti plánování systémů

Kód CPV: 72263000-6 | Implementace softwaru

Kód CPV: 72253200-5 | Systémová podpora

Kód CPV: 72245000-4 | Analýza systémů a programování

Kód CPV: 80533000-9 | Školení v oblasti IT

Kód CPV: 32415000-5 | Ethernetové sítě

Kód CPV: 72511000-0 | Programové vybavení pro správu sítě

Kód CPV: 50312310-1 | Údržba zařízení datové sítě

Kód CPV: 50324100-3 | Údržba systémů

Kód CPV: 72000000-5 | Informační technologie: poradenství, vývoj programového vybavení, internet a podpora

Kód CPV: 72263000-6 | Implementace programového vybavení

Kód CPV: 72261000-2 | Podpora programového vybavení.

4.4. Předmět plnění veřejné zakázky bude spolufinancován z Evropských strukturálních a investičních fondů prostřednictvím Integrovaného regionálního operačního programu (IROP) v rámci projektu „Dohled a řízení bezpečnosti", reg. č. "CZ.06.01.01/00/22_005/0000104".

4.5. Dne 17. prosince 2018 vydal Národní úřad pro kybernetickou a informační bezpečnost (dále jen „**NÚKIB**"), na základě ZoKB Varování, č. j. 3012/2018NÚKIB-E/110, kde uvedl, že: *„Použití technických nebo programových prostředků následujících společností, včetně jejich dceřiných společností, představuje hrozbu v oblasti kybernetické bezpečnosti:*

- Huawei Technologies Co., Ltd, Šen-čen, Čínská lidová republika

- ZTE Corporation, Šen-čen, Čínská lidová republika".

Dne 4. ledna 2019 vydal NÚKIB k varování ze dne 17. prosince 2018 (dále jen „**metodika**"), která stanoví mimo jiné postupy pro provádění a aktualizaci analýzy rizik v oblasti kybernetické bezpečnosti.

V souladu s touto metodikou a v návaznosti na povinnosti vyplývající ze zákona č. 264/2025 Sb., o kybernetické bezpečnosti, a z vyhlášky č. 409/2025 Sb., *o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností*, provedl Zadavatel analýzu rizik související s předmětnou veřejnou zakázkou. Na základě provedené analýzy rizik Zadavatel identifikoval rizika spojená s výše uvedenými technickými a programovými prostředky jako neakceptovatelná a současně stanovil opatření k jejich zvládání, spočívající v nepřipuštění použití těchto prostředků v rámci plnění veřejné zakázky, za účelem zajištění odpovídající úrovně kybernetické bezpečnosti.

Zadavatel tak na základě vydaného varování NÚKIB, navazující metodiky a provedené analýzy rizik, v souladu s povinnostmi vyplývajícími ze zákona č. 264/2025 Sb., o kybernetické bezpečnosti, nepřipouští v rámci plnění veřejné zakázky použití technických nebo programových prostředků společností (výrobců), které jsou uvedeny v aktuálně platném varování NÚKIB jako hrozba v oblasti kybernetické bezpečnosti.

Pokud by některý z dodavatelů ve své nabídce nerespektoval zákaz, resp. zadávací podmínku uvedenou v tomto čl. 4.5 Zadávací dokumentace, tzn. že by pro plnění veřejné zakázky navrhl použití technických nebo programových prostředků výše uvedených společností (výrobců), Zadavatel bude postupovat podle § 48 odst. 2 písm. a) ZZVZ ve spojení s § 48 odst. 8 ZZVZ a přistoupí k vyloučení takového dodavatele ze zadávacího řízení.

5. Předpokládaná hodnota

5.1. Předpokládaná hodnota veřejné zakázky se nezveřejňuje.

6. Doba plnění a místo plnění veřejné zakázky, prohlídka místa plnění:

6.1. Doba plnění veřejné zakázky

Termín zahájení plnění: Od okamžiku účinnosti smlouvy.

Termín ukončení plnění: do skončení Fáze F6.2 (Post-implementační podpora), přičemž Fáze F6.2 nebude ukončena dříve než za 60 měsíců od skončení fáze F3.3.

Podrobnosti ohledně doby plnění veřejné zakázky stanoví Harmonogram plnění, který tvoří Přílohu č. 9 smlouvy.

6.2. Místo plnění veřejné zakázky

Plnění veřejné zakázky bude probíhat na dvou místech:

- V Trianglu 2474, 190 00 Praha 9 – Libeň, a
- Cvokařská 2834/2, 301 00 Plzeň – Slovany.

6.3. Prohlídka místa plnění

Zadavatel neprovádí prohlídku místa plnění ve smyslu ustanovení § 97 ZZVZ, neboť její uskutečnění není pro účely průběhu zadávacího řízení či plnění veřejné zakázky nezbytné.

7. Sociálně a environmentálně odpovědné zadávání, inovace

7.1. Zadavatel při vytváření zadávacích podmínek, včetně pravidel pro hodnocení nabídek, a výběru dodavatele, postupoval tak, aby v co nejvyšší možné míře naplnil zásady sociálně odpovědného zadávání, environmentálně odpovědného zadávání a inovací tak jak jsou definovány v § 28 odst. 1 písm. p) až r) ZZVZ (dále jen „***odpovědné zadávání***"). Vzhledem k tomu, že jednotlivé postupy odpovědného zadávání nebyly v ZZVZ ani v jiném zákoně taxativně vymezeny a současně je odpovědné zadávání stále se velmi dynamicky vyvíjejícím institutem veřejného zadávání, Zadavatel při vytváření podmínek zvažoval použití zejména těch prvků odpovědného zadávání, které byly v době vytváření zadávacích podmínek jednoznačně vymezitelné a vymahatelné, a současně byla u nich vysoká míra jistoty, že Zadavatel jejich aplikací neporuší ostatní zásady uvedené v § 6 ZZVZ a také principy 3E vyplývající ze zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole).

7.2. Zadavatel aplikuje v zadávacím řízení prvky odpovědného zadávání podle čl. 7.3 a 7.4 této Zadávací dokumentace. Použití jiných prvků odpovědného zadávání, které byly Zadavateli známy při vytváření této Zadávací dokumentace, není vzhledem k povaze a smyslu zakázky možné z těchto důvodů:

7.2.1. V oblasti environmentálního odpovědného zadávání Zadavatel neshledal potřebu použití dílčích aspektů odpovědného zadávání, neboť činnosti, které jsou předmětem této veřejné zakázky, nezatěžují životní prostředí nad rámec běžného života a spotřeba energií, vody, surovin a produkce znečišťujících látek je minimální či žádná.

7.2.2. V oblasti inovací Zadavatel nestanovil dílčí kritéria odpovědného zadávání s ohledem na skutečnost, že v rámci předmětu plnění veřejné zakázky neidentifikoval žádná možná inovativní řešení. Z těchto důvodů jsou inovace u daného předmětu plnění fakticky vyloučeny.

7.2.3. V oblasti sociálně odpovědného zadávání Zadavatel neshledal potřebu použití dalších dílčích aspektů odpovědného zadávání, kromě těch, které jsou uvedeny v čl. 7.3 a 7.4 této Zadávací dokumentace, s ohledem na specifičnost těchto služeb, kdy předmětem služeb je specializované plnění. Vzhledem k těmto důvodům je nutné, aby se na plnění veřejné zakázky podílely osoby s vysokou kvalifikací. Nejedná se tedy o vhodnou příležitost k zaměstnání osob znevýhodněných na trhu práce.

7.3. Rovnocenné platební podmínky v rámci dodavatelského řetězce:

7.3.1. Zadavatel realizuje zakázku s ohledem na ochranu malých a středních podniků

v případném postavení poddodavatelů, a to formou:

a. umožnění přímých plateb případným poddodavatelům a

b. zajištění stejné doby splatnosti faktur pro poddodavatele jako pro vybraného dodavatele.

7.4. Dodržování pracovněprávních předpisů:

7.4.1. Zadavatel stanovuje, že vybraný dodavatel je při plnění veřejné zakázky povinen dodržovat pracovněprávní předpisy, a to zejména, nikoliv však výlučně, předpisy upravující mzdy zaměstnanců, pracovní dobu, dobu odpočinku mezi směnami, placené přesčasy, bezpečnost práce apod. Zadavatel dále vyžaduje zajistit férové pracovní podmínky a odpovídající úroveň bezpečnosti práce pro všechny osoby podílející se na plnění veřejné zakázky. Vybraný dodavatel je povinen zajistit splnění tohoto požadavku Zadavatele i u svých poddodavatelů.

7.4.2. Vybraný dodavatel bude povinen plnění těchto povinností Zadavateli doložit kdykoli do 5 pracovních dnů od výzvy Zadavatele, a to včetně všech potřebných dokladů dle aktuálních právních předpisů, resp. též s příslušnými výstupy ze mzdového a účetního systému vybraného dodavatele.

8. Požadavky Zadavatele na kvalifikaci dodavatelů

8.1. Zadavatel požaduje dle § 73 ZZVZ po účastnících zadávacího řízení předložení dokladů a informací k prokázání splnění podmínek kvalifikace.

8.2. Kritéria kvalifikace

Zadavatel požaduje, aby dodavatelé prokázali následující:

a) svou základní způsobilost dle § 74 a § 75 ZZVZ;

b) svou profesní způsobilost dle § 77 ZZVZ;

c) svou ekonomickou kvalifikaci dle § 78 ZZVZ;

d) svou technickou kvalifikaci dle § 79 ZZVZ.

8.3. Forma prokazování splnění kvalifikace

8.3.1. Dodavatel prokáže splnění kvalifikace ve všech případech příslušnými doklady.

8.3.2. Za účelem prokázání kvalifikace Zadavatel přednostně vyžaduje doklady evidované v systému, který identifikuje doklady k prokázání splnění kvalifikace (systém e-Certis).

8.3.3. Zadavatel vylučuje možnost, aby dodavatelé pro účely podání nabídky požadované doklady o kvalifikaci dle čl. 8 této ZD nahradili písemným čestným prohlášením dle § 86 ZZVZ. Tím není dotčen bod 8.3.10 ZD.

8.3.4. Dodavatel může nahradit požadované doklady jednotným evropským osvědčením pro veřejné zakázky ve smyslu § 87 ZZVZ. Vzor jednotného evropského osvědčení je stanoven prováděcím nařízením Komise (EU) 2016/7 ze dne 5. ledna 2016, kterým se zavádí standardní formulář jednotného evropského osvědčení pro veřejné zakázky (dostupný např. na internetové adrese: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0007&from=cs).

8.3.5. Dodavatel není povinen předložit Zadavateli doklady osvědčující skutečnosti obsažené v jednotném evropském osvědčení pro veřejné zakázky, pokud Zadavateli sdělí, ve kterém jiném zadávacím řízení mu je již předložil.

8.3.6. Povinnost předložit doklad může dodavatel splnit odkazem na odpovídající informace vedené v informačním systému veřejné správy ve smyslu *zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů,* nebo v obdobném systému vedeném v jiném členském státu, který umožňuje neomezený dálkový přístup. Takový odkaz musí obsahovat internetovou

adresu a údaje pro přihlášení a vyhledání požadované informace, jsou-li takové údaje nezbytné. V ČR jde zejména o výpis z obchodního rejstříku, výpis z veřejné části živnostenského rejstříku nebo výpis ze seznamu kvalifikovaných dodavatelů.

8.3.7. Dodavatel předkládá doklady prokazující splnění kvalifikace ve formě prosté kopie. Tímto není dotčeno oprávnění Zadavatele dle bodu 22.2.2 ZD a právo požadovat předložení originálu nebo úředně ověřené kopie dokladu postupem dle § 46 odst. 1 ZZVZ.

8.3.8. Doklady prokazující základní způsobilost podle § 74 ZZVZ musí prokazovat splnění požadovaného kritéria způsobilosti nejpozději v době 3 měsíců přede dnem zahájení zadávacího řízení.

8.3.9. V případech, kdy Zadavatel v rámci prokázání splnění kvalifikace požaduje předložení čestného prohlášení dodavatele, musí takové čestné prohlášení obsahovat Zadavatelem požadované údaje.

8.3.10. Pokud ZZVZ nebo Zadavatel požaduje předložení dokladu podle právního řádu České republiky, může dodavatel předložit obdobný doklad podle právního řádu státu, ve kterém se tento doklad vydává. Doklad, který je vyhotoven v jiném jazyce, než který Zadavatel určil pro podání nabídky, se předkládá s překladem do jazyka určeného Zadavatelem pro podání nabídky. Není-li v zadávacích podmínkách výslovně stanoveno jinak, platí, že Zadavatel určil pro podání nabídky český jazyk. Bude-li mít Zadavatel pochybnosti o správnosti překladu, je oprávněn si vyžádat předložení úředně ověřeného překladu dokladu tlumočníkem zapsaným do seznamu soudních tlumočníků a soudních překladatelů podle zákona č. 354/2019 Sb., o soudních tlumočnících a soudních překladatelích, ve znění pozdějších předpisů. Doklad v českém nebo slovenském jazyce a doklad o vzdělání v latinském jazyce se předkládají bez překladu; Zadavatel může povinnost předložit překlad prominout i u jiných dokladů. Pokud se podle příslušného právního řádu požadovaný doklad nevydává, může být nahrazen písemným čestným prohlášením.

8.4. **Prokázání kvalifikace prostřednictvím jiných osob dle § 83 ZZVZ**

8.4.1. Dodavatel může ekonomickou kvalifikaci, technickou kvalifikaci nebo profesní způsobilost s výjimkou kritéria podle § 77 odst. 1 ZZVZ prokázat prostřednictvím jiných osob. Dodavatel je v takovém případě povinen Zadavateli předložit:

a) doklady prokazující splnění profesní způsobilosti podle § 77 odst. 1 ZZVZ jinou osobou,

b) doklady prokazující splnění chybějící části kvalifikace prostřednictvím jiné osoby,

c) doklady o splnění základní způsobilosti podle § 74 ZZVZ jinou osobou a

d) smlouvu nebo jinou osobou podepsané potvrzení o její existenci, jejímž obsahem je závazek jiné osoby k poskytnutí plnění určeného k plnění veřejné zakázky nebo k poskytnutí věcí nebo práv, s nimiž bude dodavatel oprávněn disponovat při plnění veřejné zakázky, a to alespoň v rozsahu, v jakém jiná osoba prokázala kvalifikaci za dodavatele.

8.4.2. Nejedná-li se o situaci dle bodu 8.4.3 ZD, má se za to, že požadavek podle písm. d) je splněn, pokud z obsahu smlouvy nebo potvrzení o její existenci podle písm. d) vyplývá závazek jiné osoby plnit veřejnou zakázku společně a nerozdílně s dodavatelem.

8.4.3. Prokazuje-li dodavatel prostřednictvím jiné osoby kvalifikaci a předkládá doklady podle § 79 odst. 2 písm. a), b) nebo d) ZZVZ vztahující se k takové osobě, musí ze smlouvy nebo potvrzení o její existenci podle písm. d) vyplývat závazek, že jiná osoba bude vykonávat služby, ke kterým se prokazované kritérium kvalifikace vztahuje.

8.4.4. Dodavatelé a jiné osoby prokazují (mohou prokázat) kvalifikaci společně.

8.4.5. Dodavatel a jiná osoba, jejímž prostřednictvím dodavatel prokazuje ekonomickou kvalifikaci podle § 78 ZZVZ, nesou společnou a nerozdílnou odpovědnost za plnění

veřejné zakázky.

8.4.6. Zadavatel upozorňuje, že povinnost doložit veškeré doklady uvedené výše v tomto článku platí i v případě, kdy je část kvalifikace prokazována poddodavatelem poddodavatele (pod-poddodavatelem).

8.5. **Prokazování kvalifikace v případě společné účasti dodavatelů dle § 82 ZZVZ**

8.5.1. V případě společné účasti dodavatelů prokazuje základní způsobilost dle § 74 a § 75 ZZVZ a profesní způsobilost podle § 77 odst. 1 ZZVZ každý dodavatel samostatně.

8.6. **Prokazování kvalifikace získané v zahraničí dle § 81 ZZVZ**

8.6.1. V případě, že byla kvalifikace získána v zahraničí, prokazuje se doklady vydanými podle právního řádu země, ve které byla získána, a to v rozsahu požadovaném Zadavatelem.

8.6.2. Potvrzení pro daňové nedoplatky zahraničních dodavatelů v ČR vydává Finanční úřad pro Prahu 1 a potvrzení pro nedoplatky zahraničních dodavatelů v ČR na pojistném a na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti vydává Pražská správa sociálního zabezpečení.

8.7. **Změny kvalifikace účastníka zadávacího řízení dle § 88 ZZVZ**

8.7.1. Pokud po předložení dokladů nebo prohlášení o kvalifikaci dojde v průběhu zadávacího řízení ke změně kvalifikace účastníka zadávacího řízení, je účastník zadávacího řízení povinen tuto změnu Zadavateli do 5 pracovních dnů oznámit a do 10 pracovních dnů od oznámení této změny předložit nové doklady nebo prohlášení ke kvalifikaci. Zadavatel může tyto lhůty prodloužit nebo prominout jejich zmeškání. Povinnost podle věty první účastníku zadávacího řízení nevzniká, pokud je kvalifikace změněna takovým způsobem, že:

a) podmínky kvalifikace jsou nadále splněny,

b) nedošlo k ovlivnění kritérií hodnocení nabídek.

8.7.2. Zadavatel může vyloučit účastníka zadávacího řízení, pokud prokáže, že účastník nesplnil shora uvedenou povinnost.

8.8. **Výpis ze seznamu kvalifikovaných dodavatelů dle § 228 ZZVZ**

8.8.1. Předložení dokladu o zapsání dodavatele do seznamu kvalifikovaných dodavatelů vedeného Ministerstvem pro místní rozvoj dle § 226 až § 232 ZZVZ nahrazuje v souladu s § 228 ZZVZ doklad prokazující profesní způsobilost podle § 77 ZZVZ v tom rozsahu, v jakém údaje ve výpisu ze seznamu kvalifikovaných dodavatelů prokazují splnění kritérií profesní způsobilosti, a základní způsobilost podle § 74 ZZVZ v plném rozsahu. Výpis ze seznamu kvalifikovaných dodavatelů nesmí být k poslednímu dni, ke kterému má být prokázána základní způsobilost nebo profesní způsobilost, starší než tři měsíce.

8.9. **Předložení certifikátu dle § 234 ZZVZ**

8.9.1. Platným certifikátem vydaným v rámci schváleného systému certifikovaných dodavatelů lze podle § 234 ZZVZ prokázat kvalifikaci v zadávacím řízení. Má se za to, že dodavatel je kvalifikovaný v rozsahu uvedeném na certifikátu.

8.10. **Důsledek nesplnění kvalifikace**

8.10.1. Dodavatel, který nesplní kvalifikaci v rozsahu požadovaném ZZVZ a touto zadávací dokumentací, může být Zadavatelem z účasti v zadávacím řízení vyloučen. Vybraný dodavatel, který nesplní kvalifikaci v rozsahu požadovaném ZZVZ a touto zadávací dokumentací, bude Zadavatelem z účasti v zadávacím řízení vyloučen.

9. Základní způsobilost dle § 74 a § 75 ZZVZ

9.1. Zadavatel v souladu s ustanovením § 73 ZZVZ požaduje prokázání základní způsobilosti podle § 74 ZZVZ následujícím způsobem:

a) Způsobilým není dodavatel, který byl v zemi svého sídla v posledních 5 letech před zahájením zadávacího řízení pravomocně odsouzen pro trestný čin uvedený v příloze č. 3 ZZVZ nebo obdobný trestný čin podle právního řádu země sídla dodavatele; k zahlazeným odsouzením se nepřihlíží.

Dodavatel prokazuje splnění podmínek základní způsobilosti v tomto kritériu ve vztahu k České republice předložením **výpisu z evidence Rejstříku trestů**.

b) Způsobilým není dodavatel, který má v České republice nebo v zemi svého sídla v evidenci daní zachycen splatný daňový nedoplatek.

Dodavatel prokazuje splnění podmínek základní způsobilosti v tomto kritériu ve vztahu k České republice a k zemi svého sídla předložením **potvrzení příslušného finančního úřadu a písemného čestného prohlášení ve vztahu ke spotřební dani**.

c) Způsobilým není dodavatel, který má v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na veřejné zdravotní pojištění.

Dodavatel prokazuje splnění podmínek základní způsobilosti v tomto kritériu ve vztahu k České republice a k zemi svého sídla předložením **písemného čestného prohlášení**. K prokázání uvedeného kritéria je dodavatel oprávněn využít vzor čestného prohlášení uvedeného jako Příloha č. 1 této Zadávací dokumentace.

d) Způsobilým není dodavatel, který má v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti.

Dodavatel prokazuje splnění podmínek základní způsobilosti v tomto kritériu ve vztahu k České republice a k zemi svého sídla **předložením potvrzení příslušné okresní/územní správy sociálního zabezpečení**.

e) Způsobilým není dodavatel, který je v likvidaci, proti němuž bylo vydáno rozhodnutí o úpadku, vůči němuž byla nařízena nucená správa podle jiného právního předpisu nebo v obdobné situaci podle právního řádu země sídla dodavatele.

Dodavatel prokazuje splnění podmínek základní způsobilosti v tomto kritériu ve vztahu k České republice předložením **výpisu z obchodního rejstříku, nebo předložením písemného čestného prohlášení v případě, že není v obchodním rejstříku zapsán**. V případě, že dodavatel není zapsán v obchodním rejstříku, je k prokázání uvedeného kritéria oprávněn využít vzor čestného prohlášení uvedeného jako Příloha č. 1 Zadávací dokumentace.

9.2. Je-li dodavatelem právnická osoba, musí podmínku uvedenou v odstavci 9.1 písm. a) splňovat tato právnická osoba a zároveň každý člen statutárního orgánu. Je-li členem statutárního orgánu dodavatele právnická osoba, musí podmínku uvedenou shora pod písm. a) splňovat:

a) tato právnická osoba,

b) každý člen statutárního orgánu této právnické osoby a

c) osoba zastupující tuto právnickou osobu v statutárním orgánu dodavatele.

9.3. Účastní-li se zadávacího řízení pobočka závodu:

9.3.1. zahraniční právnické osoby, musí podmínku uvedenou v odstavci 9.1 písm. a) splňovat tato právnická osoba a vedoucí pobočky závodu

9.3.2. české právnické osoby, musí podmínku uvedenou shora pod písm. a) splňovat:

a) tato právnická osoba,

b) každý člen statutárního orgánu této právnické osoby a

c) osoba zastupující tuto právnickou osobu v statutárním orgánu dodavatele

d) vedoucí pobočky závodu.

9.4. Zadavatel nemusí ve smyslu § 75 odst. 2 ZZVZ uplatnit důvod pro vyloučení účastníka zadávacího řízení, i když nesplnil podmínky základní způsobilosti, pokud:

a) by vyloučení účastníka znemožnilo zadání veřejné zakázky v tomto zadávacím řízení a

b) naléhavý veřejný zájem, zejména veřejné zdraví nebo ochrana životního prostředí, vyžaduje plnění veřejné zakázky.

9.5. Účastník zadávacího řízení může v souladu s § 76 ZZVZ prokázat, že i přes nesplnění základní způsobilosti podle § 74 ZZVZ nebo naplnění důvodu nezpůsobilosti podle § 48 odst. 5 a 6 ZZVZ obnovil svou způsobilost k účasti v zadávacím řízení, pokud v průběhu zadávacího řízení Zadavateli doloží, že přijal dostatečná nápravná opatření. To neplatí po dobu, na kterou byl účastník zadávacího řízení pravomocně odsouzen k zákazu plnění veřejných zakázek nebo účasti v koncesním řízení.

9.6. Pokud Zadavatel dospěje k závěru, že způsobilost účastníka zadávacího řízení byla obnovena, ze zadávacího řízení jej nevyloučí nebo předchozí vyloučení účastníka zadávacího řízení zruší.

10. Profesní způsobilost dle § 77 ZZVZ

10.1. Zadavatel v souladu s ustanovením § 73 ZZVZ požaduje prokázání profesní způsobilosti dle § 77 ZZVZ následujícím způsobem:

10.1.1. Dodavatel prokazuje splnění profesní způsobilosti dle § 77 odst. 1 ZZVZ ve vztahu k České republice předložením výpisu z obchodního rejstříku nebo jiné obdobné evidence, pokud jiný právní předpis zápis do takové evidence vyžaduje.

Dodavatel prokazuje splnění tohoto kritéria profesní způsobilosti předložením **výpisu z obchodního rejstříku či jiné obdobné evidence**.

10.2. Doklady k prokázání profesní způsobilosti dodavatel nemusí předložit, pokud právní předpisy v zemi jeho sídla obdobnou profesní způsobilost nevyžadují.

11. Ekonomická kvalifikace dle § 78 ZZVZ

11.1. Zadavatel požaduje, aby minimální obrat dodavatele dosahoval za každé ze 3 bezprostředně předcházejících účetních období minimální úrovně 100 mil. Kč.

11.2. Jestliže dodavatel vznikl později, postačí, předloží-li údaj o svém obratu v požadované výši za všechna účetní období od svého vzniku.

11.3. Dodavatel prokazuje splnění tohoto kritéria ekonomické kvalifikace předložením **výkazu zisku a ztrát dodavatele nebo obdobného dokladu podle právního řádu země sídla dodavatele**.

11.4. V případě, že dodavatel prokazuje ekonomickou kvalifikaci podle § 78 ZZVZ prostřednictvím jiné osoby ve smyslu § 83 ZZVZ, požaduje Zadavatel, aby dodavatel a jiná osoba nesli společnou a nerozdílnou odpovědnost za plnění veřejné zakázky. V takovém případě dodavatel v nabídce doloží doklad o příslušném závazku, tj. společné a nerozdílné odpovědnosti za plnění veřejné zakázky.

12. Technická kvalifikace dle § 79 ZZVZ

12.1. Seznam významných zakázek

12.1.1. K prokázání kritéria technické kvalifikace požaduje Zadavatel doložení **Seznamu významných zakázek poskytnutých za posledních 5 let před zahájením zadávacího řízení**.

Ze seznamu významných zakázek musí vyplývat alespoň následující údaje:

a) název objednatele,

b) předmět plnění významné zakázky,

c) doba realizace významné zakázky,

d) finanční objem významné zakázky, je-li dále požadován,

e) kontaktní osoba objednatele, u které bude možné realizaci významné zakázky ověřit, vč. kontaktního e-mailu a telefonu.

Za účelem zpracování seznamu významných zakázek je dodavatel oprávněn využít dokument Příloha č. 3 této Zadávací dokumentace.

12.1.2. Ze Seznamu významných zakázek musí vyplývat, že dodavatel v uvedeném období realizoval minimálně:

- **1 významnou zakázku**, jejímž předmětem byla dodávka HW infrastruktury, zahrnující minimálně:
  - servery
  - disková pole
  - síťové prvky
  - konfigurace a implementace bezpečnostních pravidel,

  přičemž tato významná zakázka musí kumulativně zahrnovat **všechny** z uvedených položek servery/disková pole/síťové prvky/konfigurace a implementace bezpečnostních pravidel, a
- **2 významné zakázky**, jejichž předmětem byla dodávka HW infrastruktury, zahrnující:
  - servery
  - disková pole
  - síťové prvky
  - konfigurace a implementace bezpečnostních pravidel,

  přičemž každá z těchto 2 významných zakázek musí kumulativně zahrnovat **alespoň 2** z uvedených položek servery/disková pole/síťové prvky/konfigurace a implementace bezpečnostních pravidel,

a to v objemu min. 10 mil. Kč bez DPH za každou významnou zakázku.

12.1.3. Ze Seznamu významných zakázek musí dále vyplývat, že ze zakázek splňujících požadavky dle předchozího odstavce:

- alespoň jedna zakázka byla v objemu 20 mil. Kč bez DPH,
- alespoň jedna zakázka zahrnovala dvě geograficky oddělené lokality nebo primární / sekundární lokalitu,
- alespoň jedna zakázka zahrnovala analýzu data managementu, a
- alespoň jedna zakázka byla realizována pro:
  - subjekt kritické infrastruktury ve smyslu zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) nebo zákona č. 266/2025 Sb., o odolnosti subjektů kritické infrastruktury a o změně souvisejících zákonů (zákon o kritické infrastruktuře), nebo
  - velký podnik, tj. podnik s nejméně 250 zaměstnanci a ročním obratem více než 50 mil. EUR nebo bilanční sumou roční rozvahy vyšší než 43 mil.

EUR. 1,25 mld. Kč[1].

12.1.4. Doba „za posledních 5 let před zahájením zadávacího řízení" se pro účely tohoto zadávacího řízení považuje za splněnou, pokud významná zakázka byla v průběhu této doby dokončena alespoň v rozsahu odpovídajícímu požadavkům Zadavatele uvedeným výše. Významná zakázka může být uznána výhradně tehdy, pokud subjekt dokládající poskytnutí příslušné významné zakázky v jejím rámci realizoval činnosti relevantní z hlediska požadavků uplatněných Zadavatelem, přičemž tyto relevantní činnosti nebyly realizovány (ukončeny) dříve, než v posledních 5 letech před zahájením zadávacího řízení veřejné zakázky. Doba „za posledních 5 let před zahájením zadávacího řízení" se považuje za splněnou i v případě, že se jedná o významné zakázky, které probíhaly i po zahájení zadávacího řízení, nebo pokud stále probíhají, za předpokladu splnění výše uvedených parametrů ke dni konce lhůty pro prokázání kvalifikace (tj. řádné dokončení příslušné části významné zakázky, která naplňuje požadavky Zadavatele na významné zakázky). Z předložených údajů a dokladů vztahujících se k příslušné významné zakázce musí být zcela jednoznačně zřejmé, jaké činnosti, v jakém rozsahu a v jakém časovém období příslušný subjekt při plnění příslušné zakázky realizoval.

12.2. **Seznam techniků nebo technických útvarů, kteří se budou podílet na plnění veřejné zakázky (bez ohledu na to, zda jde o zaměstnance dodavatele nebo osoby v jiném vztahu k dodavateli) a osvědčení o vzdělání a odborné kvalifikaci těchto osob (realizační tým)**

12.2.1. K prokázání kritéria technické kvalifikace požaduje Zadavatel **<u>doložit jmenný seznam členů realizačního týmu</u>** a dále ve vztahu ke každému členovi realizačního týmu:

a) strukturovaný profesní životopis, z něhož bude vyplývat splnění požadavků Zadavatele (je-li požadována referenční zkušenost s projektem, uvede dodavatel rovněž údaje, z nichž bude ověřitelné splnění požadavku, včetně kontaktních údajů na objednatele příslušného projektu), jehož vzor je Přílohou č. 2 této Zadávací dokumentace,

b) údaj o tom, zda je člen realizačního týmu v pracovněprávním či jiném vztahu k dodavateli (v takovém případě uvede v jakém),

c) doklady, z nichž bude vyplývat splnění požadavků Zadavatele na vzdělání či odbornou způsobilost, je-li požadováno (vysokoškolský diplom, autorizace, osvědčení, certifikát, apod.).

12.2.2. Členové realizačního týmu budou odpovědní za činnosti, které bude dodavatel provádět v průběhu realizace veřejné zakázky. Každá osoba v realizačním týmu může zastávat i více pozic, splňuje-li požadavky na každou z těchto pozic.

12.2.3. Dodavatel předloží doklady o odborné kvalifikaci pro členy realizačního týmu na níže uvedených pozicích, kteří splňují dále uvedené požadavky:

Pracovní pozice	**Popis role a minimální požadavky na kvalifikaci člena realizačního týmu**
Architekt infrastruktury (Solution Architect)	**Popis role:** Architekt infrastruktury je odpovědný za návrh a architektonické zpracování komplexních řešení ICT infrastruktury se zaměřením na oblast síťových technologií, serverových platforem a datových úložišť dodávaného technického řešení. V rámci výkonu této role zajišťuje návrh technické koncepce infrastruktury, včetně řešení vysoké dostupnosti, bezpečnosti, škálovatelnosti a kontinuity provozu. Odpovídá za zpracování architektonické a technické dokumentace,

[1] Viz čl. 2 doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků.

	za návrh řešení pro prostředí s více lokalitami včetně geograficky oddělených datových center a za návrh mechanismů replikace dat, zálohování a disaster recovery. **Popis minimálních požadavků na kvalifikaci člena realizačního týmu:** • Minimálně **5 let** praxe na uvedené pozici (či obdobné), přičemž obsahem této praxe bylo: o návrh ICT infrastruktury v oblasti sítí a datových úložišť. • Zkušenost s o účastí na min. 2 projektech za posledních 5 let před zahájením zadávacího řízení, o minimální finanční hodnotě **10 mil. Kč** bez DPH **za každý projekt**, které zahrnovaly návrh komplexní infrastruktury (servery, úložiště, sítě), přičemž tyto zahrnovaly: ▪ alespoň 1 projekt se dvěma geograficky oddělenými lokalitami nebo primární / sekundární lokalitou, ▪ alespoň 1 projekt, který byl realizován pro: • subjekt kritické infrastruktury ve smyslu zákona č. 240/2000 Sb., krizovém řízení a o změně některých zákonů (krizový zákon) nebo zákona č. 266/2025 Sb., o odolnosti subjektů kritické infrastruktury a o změně souvisejících zákonů (zákon o kritické infrastruktuře), nebo • velký podnik, tj. podnik s nejméně 250 zaměstnanci a ročním obratem více než 50 mil. EUR nebo bilanční sumou roční rozvahy vyšší než 43 mil. EUR. 1,25 mld. Kč[2]. o **Pro vyloučení pochybností Zadavatel sděluje, že tyto předložené reference (zkušenosti) <u>nemusí</u> být vázány k nabízenému řešení.** • Certifikace: platná certifikace výrobce nabízeného řešení pro návrh/deployment.
Síťový specialista	**Popis role:** Síťový specialista je odpovědný za praktickou realizaci a implementaci dodávaného řešení na základě architektonického návrhu zpracovaného Architektem infrastruktury. V rámci výkonu této role přebírá schválené technické řešení a zajišťuje jeho detailní rozpracování do úrovně implementační dokumentace, následnou konfiguraci, nasazení a uvedení do provozu. Odpovídá za instalaci, konfiguraci a optimalizaci aktivních síťových prvků, včetně OOB přepínačů, L3 směrovačů, bezpečnostních prvků FW a dalších komponent tvořících síťovou infrastrukturu. Jeho činností je realizace řešení pro prostředí Zadavatele s vysokými nároky na dostupnost, bezpečnost a výkon, včetně implementace redundance, segmentace sítě, vysoké dostupnosti a propojení geograficky oddělených lokalit. Zajišťuje implementaci mechanismů pro bezpečný přenos dat, monitoring síťového provozu, optimalizaci

[2] Viz čl. 2 doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků.

	výkonu a řešení incidentů vzniklých v průběhu nasazení i převzetí do ostrého provozu. Odpovídá za provádění funkčních a zátěžových testů, spolupracuje při akceptačních řízeních a zajišťuje předání řešení do provozu včetně zpracování provozní a technické dokumentace. **Popis minimálních požadavků na kvalifikaci člena realizačního týmu:** • Minimálně **5 let** praxe na uvedené pozici (či obdobné), přičemž obsahem této praxe bylo: o návrh nebo správa sítí. • Zkušenost s o účastí na min. 2 projektech za posledních 5 let před zahájením zadávacího řízení, o minimální finanční hodnotě **5 mil. Kč** bez DPH **za každý projekt**, jejichž předmětem byl návrh a implementace datacentrových sítí, přičemž tyto zahrnovaly: ▪ alespoň 1 projekt s geograficky oddělenými lokalitami nebo primární/sekundární lokalitou. o **Tyto předložené reference (zkušenosti) <u>musí</u> být vázány k nabízenému řešení.** • Certifikace: o platná certifikace na úrovni professional/experta v oblasti síťových technologií, ať již se zaměřením na oblast implementace a správy datových center či v oblasti podnikových sítích. Zadavatel pro účely této certifikace uzná jak relevantní, technologicky neutrální certifikace, tak certifikace související s konkrétními technologiemi jako např.: Cisco Certified Network Professional Enterprise (CCNP Enterprise), Juniper Networks Certified Internet Professional – Enterprise Routing and Switching (JNCIP-ENT), Cisco Certified Network Professional Data Center (CCNP Data Center), Juniper Networks Certified Internet Professional – Data Center (JNCIP-DC) nebo jiné ekvivalentní či vyšší certifikace prokazující odpovídající odborné znalosti, o platná certifikace na úrovni professional/experta v oblasti síťové bezpečnosti zahrnující firewall. Zadavatel pro účely této certifikace uzná relevantní technologicky neutrální certifikace, tak certifikace související s konkrétními technologiemi jako např.: Fortinet Certified Solution Specialist (FCSS) – Network Security, Cisco Certified Network Professional Security (CCNP Security), Juniper Networks Certified Internet Professional – Security (JNCIP-SEC), Palo Alto Networks Certified Network Security Engineer (PCNSE) nebo jiné ekvivalentní či vyšší certifikace prokazující odpovídající odborné znalosti.
Bezpečnostní specialista	**Popis role:** Tato role bude vykonávat funkci architekta kybernetické bezpečnosti dle zákona č. 264/2025 Sb., o kybernetické bezpečnosti, v platném znění, resp. vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, v platném znění.

	Bezpečnostní specialista bude odpovědný za návrh, implementaci a dohled nad bezpečnostními opatřeními v oblasti dodávaného řešení s cílem zajistit důvěrnost, integritu a dostupnost informačních a komunikačních systémů na technické řešení provozovaném. V rámci své role vychází z architektonického návrhu infrastruktury a bezpečnostní koncepce organizace, které dále rozpracovává do konkrétních bezpečnostních mechanismů, technických konfigurací a provozních pravidel. Bezpečnostní specialista úzce spolupracuje s architektem infrastruktury i síťovým specialistou. Bezpečnostní specialista odpovídá za implementaci a konfiguraci bezpečnostních technologií, zejména v oblasti firewallů nové generace (NGFW), systémů pro detekci a prevenci průniků komunikace, systémů pro řízení přístupu, segmentaci sítí dle koncepce organizace, šifrování komunikace a napojení dohledových nástrojů. Podílí se na návrhu bezpečnostní architektury pro projekt bezpečného úložiště s vysokými nároky na dostupnost a odolnost, včetně řešení pro geograficky oddělené lokality a prostředí kritické infrastruktury Zadavatele. **Popis minimálních požadavků na kvalifikaci člena realizačního týmu:** • Minimálně **3 roky** praxe na uvedené pozici (či obdobné), přičemž obsahem této praxe byl: o návrh implementace bezpečnostních opatření a zajišťování bezpečné architektury v oblasti informační nebo kybernetické bezpečnosti. • Zkušenost s o účastí na min. 2 projektech za posledních 5 let před zahájením zadávacího řízení, o minimální finanční hodnotě **5 mil. Kč** bez DPH **za každý projekt**, které zahrnovaly realizaci bezpečnostního řešení spočívajícího v návrhu, dodávce, implementaci a zprovoznění HA firewallového clusteru (v režimu active/active nebo active/passive), včetně integrace řešení do datového centra, přičemž tyto zahrnovaly: ▪ alespoň 1 projekt realizovaný pro: • subjekt kritické infrastruktury ve smyslu zákona č. 240/2000 Sb., krizovém řízení a o změně některých zákonů (krizový zákon) nebo zákona č. 266/2025 Sb., o odolnosti subjektů kritické infrastruktury a o změně souvisejících zákonů (zákon o kritické infrastruktuře), nebo • velký podnik, tj. podnik s nejméně 250 zaměstnanci a ročním obratem více než 50 mil. EUR nebo bilanční sumou roční rozvahy vyšší než 43 mil. EUR. 1,25 mld. Kč[3]. o **Pro vyloučení pochybností Zadavatel sděluje, že tyto předložené reference (zkušenosti) <u>nemusí</u> být vázány k nabízenému řešení.**

[3] Viz čl. 2 doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků.

	• Certifikace:
	  ○ platná certifikace vztahující se ke kybernetické bezpečnosti informačních systémů např. Certified Ethical Hacker Practical (CEH practical), Offensive Security Certified Professional (OSCP), Comptia Pentest+, Certified Information Systems Security Professional (CISSP), CompTIA CySA+ nebo jiná ekvivalentní či vyšší certifikace prokazující odpovídající odborné znalosti, **NEBO**
	  ○ platná certifikace vztahující se k bezpečnostním řešením např. Cisco Certified Specialist – Network Security Firepower (CCNP Security), Fortinet Certified Professional (FCP)- Network Security, Fortinet Certified Solution Specialist (FCSS) - Network Security, Palo Alto Networks Certified Network Security Administrator (PCNSA) nebo Engineer (PCNSE), nebo jiná ekvivalentní či vyšší certifikace prokazující odpovídající odborné znalosti.

Datový analytik pro data storage	**Popis role:**
	Datový analytik pro data storage je role zaměřená na systematické zpracování, analýzu a interpretaci dat souvisejících s provozem bezpečného úložiště. Systém práce s daty je v kontextu bezpečnostních událostí a výkonnostních ukazatelů klíčových informačních systémů na daném úložišti. V rámci své role zajišťuje transformaci provozních, technických a bezpečnostních dat do strukturované podoby umožňující jejich další vyhodnocování, identifikaci trendů, rizik a optimalizačních či výkonových příležitostí.
	Datový analytik pro data storage odpovídá za návrh metodiky sběru dat, jejich konsolidaci z různých zdrojů relevantních pro organizaci. Provádí pokročilé analýzy zaměřené na výkonnost, dostupnost, kapacitní plánování, bezpečnostní události a efektivitu provozu úložiště. Výstupy svých analýz zpracovává do přehledných reportů, dashboardů a analytických podkladů a dokumentace.
	Popis minimálních požadavků na kvalifikaci člena realizačního týmu:
	• Minimálně **3 roky** praxe na uvedené pozici (či obdobné), přičemž obsahem této praxe bylo:
	  ○ analýza korporátních dat, mapování životního cyklu dat a potřeb jednotlivých stakeholderů,
	  ○ návrh klasifikace těchto korporátních dat a jejich systému jejich řízení,
	  ○ návrh rozložení a managementu těchto korporátních dat v rámci Enterprise tieringové storage na základě identifikovaných potřeb stakeholderů.
	• Zkušenost s
	  ○ účastí na min. 1 projektu za posledních 5 let před zahájením zadávacího řízení, o minimální finanční hodnotě **3 mil. Kč** bez DPH, který zahrnoval:
	  ▪ analýzu datových toků, zdrojů a kvality dat + návrh data managementu.
	  ○ **Pro vyloučení pochybností Zadavatel sděluje, že tyto předložené reference (zkušenosti) <u>nemusí</u> být vázány k nabízenému řešení.**

Projektový manažer	**Popis role:**

	Projektový manažer je odpovědný za komplexní řízení všech složek dodavatele v projektu Bezpečného úložiště, a to od návrhu řešení, přes jeho dodávku a implementaci až po akceptaci a předání do provozu Zadavatele. Odpovídá za plánování a koordinaci kapacit dodavatele, řízení úkolů a milníků projektu, věcnou kontrolu jednotlivých fází a včasnou identifikaci a řízení součinnosti potřebné pro řádné dokončení díla. Současně dohlíží na plnění smluvních podmínek, dodržování harmonogramu a požadovanou kvalitu plnění. V rámci své role zajišťuje vedení projektové dokumentace. Koordinuje činnost realizačního týmu dodavatele, zejména architekta, síťových a bezpečnostních specialistů a dalších odborných rolí, a zajišťuje efektivní komunikaci mezi všemi zapojenými stranami. Odpovídá za řízení rizik projektu, včasnou identifikaci problémů a návrh nápravných opatření předkládaných projektovému výboru a managementu SŽ, včetně pravidelného reportingu a organizace kontrolních dnů. Projektový manažer zároveň odpovídá za přípravu podkladů pro akceptační řízení, za soulad akceptačních protokolů se smlouvou a Zvláštními obchodními podmínkami pro Zakázky v oblasti ICT. **Popis minimálních požadavků na kvalifikaci člena realizačního týmu:** • Minimálně **6 let** praxe na uvedené pozici (či obdobné), přičemž obsahem této praxe bylo: o řízení IT/ICT projektů. • Zkušenost s o účastí na řízení min. 3 IT/ICT projektů na pozici projektového manažera, za posledních 5 let před zahájením zadávacího řízení, o minimální finanční hodnotě **15 mil. Kč** bez DPH **za každý projekt**, které zahrnovaly: ▪ alespoň 1 projekt realizovaný pro: • subjekt kritické infrastruktury ve smyslu zákona č. 240/2000 Sb., krizovém řízení a o změně některých zákonů (krizový zákon) nebo zákona č. 266/2025 Sb., o odolnosti subjektů kritické infrastruktury a o změně souvisejících zákonů (zákon o kritické infrastruktuře), nebo • velký podnik, tj. podnik s nejméně 250 zaměstnanci a ročním obratem více než 50 mil. EUR nebo bilanční sumou roční rozvahy vyšší než 43 mil. EUR. 1,25 mld. Kč[3]. ▪ alespoň 1 projekt v oblasti budování datového centra. o **Pro vyloučení pochybností Zadavatel sděluje, že tyto předložené reference (zkušenosti) <u>nemusí</u> být vázány k nabízenému řešení.** • Certifikace: platná certifikace PRINCE2 Foundation nebo jiná obdobná či vyšší certifikace.

12.3. Zadavatel uvádí, že předmětem dokládaných zkušeností člena realizačního týmu pro účely prokázání kvalifikace dle čl. 12.2.3 Zadávací dokumentace bude pouze dokončený projekt (účast na dokončeném projektu) příslušného člena realizačního týmu. Bude-li se

jednat o dosud neukončený probíhající projekt, je dodavatel povinen prokázat, že v rámci služby již byly dodavatelem provedeny a objednatelem akceptovány služby v Zadavatelem požadovaném věcném a finančním rozsahu. Pro vyloučení pochybností Zadavatel uvádí, že se může jednat rovněž o „osobní zkušenost člena realizačního týmu", tedy že předmětný projekt nemusel realizovat dodavatel podávající nabídku v daném zadávacím řízení. Tuto zkušenost tedy příslušný člen realizačního týmu mohl získat např. ve svém předchozím zaměstnání apod.

13. Požadavky Zadavatele na způsob zpracování nabídkové ceny:

13.1. Zadavatel požaduje, aby účastník uvedl nabídkovou cenu za plnění předmětu této veřejné zakázky, v české měně (Koruna česká), v členění bez daně z přidané hodnoty (DPH).

13.2. Za účelem výpočtu nabídkové ceny v Kč bez DPH vyplní účastník dokument Ceník, který tvoří Přílohu č. 3 smlouvy. Za správnost provedení výpočtu nabídkové ceny odpovídá účastník.

13.3. Zadavatel požaduje, aby účastník uvedl také dílčí ceny za části předmětu Veřejné zakázky (jednotlivé položky) v souladu s dokumentem Ceník, který tvoří Přílohu č. 3 smlouvy.

13.4. Účastník je povinen vyplnit všechna požadovaná pole v dokumentu Ceník, který tvoří Přílohu č. 3 smlouvy, která jsou označena k vyplnění dodavatelem.

13.5. Celková nabídková cena jakož i nabídková cena doplněná účastníkem do jednotlivých buněk v dokumentu Ceník, který tvoří Přílohu č. 3 smlouvy, představuje maximální výši úhrady za plnění dle Smlouvy, jakož i za jednotlivé položky a je stanovena jako cena „nejvýše přípustná" a pevná. V této ceně musí být zahrnuty veškeré náklady spojené s realizací předmětu veřejné zakázky, tj. veškeré náklady související. Zadavatel připouští překročení celkové nabídkové ceny a/nebo jednotkových cen dodavatele pouze za podmínek stanovených ve smlouvě.

14. Jiné požadavky Zadavatele na plnění veřejné zakázky:

14.1. Využití poddodavatele

14.1.1. Zadavatel požaduje, aby účastník zadávacího řízení v nabídce:

a) určil části veřejné zakázky, které hodlá plnit prostřednictvím poddodavatelů, nebo

b) předložil seznam poddodavatelů, pokud jsou dodavateli známi a uvedl, kterou část veřejné zakázky bude každý z poddodavatelů plnit.

14.1.2. Seznam poddodavatelů učiní dodavatel přílohou Smlouvy.

15. Varianty nabídky

15.1. Zadavatel nepřipouští varianty nabídky.

16. Závazný vzor smlouvy

16.1. Dodavatel je povinen využít Závazný vzor smlouvy, který tvoří dokument Příloha č. 5 Zadávací dokumentace.

16.2. Dodavatel není oprávněn činit změny či doplnění Závazného vzoru smlouvy (vč. jeho příloh), vyjma údajů, u nichž vyplývá z jejich obsahu povinnost doplnění (označené jako *„doplní dodavatel"*, *„doplní zhotovitel"* či jiným obdobným způsobem). V případě nabídky podávané společně několika dodavateli je dodavatel oprávněn upravit Závazný vzor smlouvy toliko s ohledem na tuto skutečnost; totéž platí, je-li dodavatelem fyzická osoba.

16.3. Dodavatel je povinen Závazný vzor smlouvy doplněný dle výše uvedených pokynů učinit součástí nabídky.

17. Způsob hodnocení nabídek:

17.1. Kritéria hodnocení

17.1.1. Hodnocení nabídek bude provedeno v souladu s § 114 a násl. ZZVZ podle kritéria nejnižší nabídkové ceny.

17.1.2. Celková nabídková cena musí být zpracována v souladu s čl. 13 a dokumentem Ceník, který tvoří Přílohu č. 3 smlouvy.

17.1.3. Jako ekonomicky nejvýhodnější bude vyhodnocena nabídka s nejnižší Celkovou nabídkovou cenou v Kč bez DPH.

17.1.4. V případě, že je více nabídek se shodným celkovým parametrem hodnotícího kritéria, rozhodne o pořadí nabídky čas podání těchto nabídek, přičemž platí, že lépe se umístila ta nabídka, která byla podána dříve.

18. Zadávací dokumentace:

18.1. **Uveřejnění zadávací dokumentace**

18.1.1. V souladu s § 96 odst. 1 a 2 ZZVZ je Zadávací dokumentace s výjimkou formulářů dle § 212 ZZVZ zveřejněna na profilu Zadavatele na internetové adrese: https://zakazky.spravazeleznic.cz/. Tamtéž budou uveřejňovány i vysvětlení, změny nebo doplnění zadávací dokumentace této veřejné zakázky.

18.2. **Námitky proti zadávacím podmínkám**

18.2.1. Námitky proti zadávacím podmínkám lze v souladu s § 242 odst. 5 ZZVZ podat nejpozději 72 hodin před skončením lhůty pro podání nabídek.

18.3. **Vysvětlení, změna nebo doplnění zadávací dokumentace**

18.3.1. Zadavatel může zadávací dokumentaci vysvětlit, doplnit či změnit za podmínek podrobně stanovených v § 98, § 99 a souvisejících ustanoveních ZZVZ.

18.3.2. Požádá-li o vysvětlení zadávací dokumentace dodavatel, Zadavatel při vyřízení žádosti postupuje v souladu s § 98 a souvisejícími ustanoveními ZZVZ.

19. Závaznost pokynů Zadavatele

19.1. V případě, že zadávací podmínky obsahují odkazy na specifická označení výrobků a služeb, která platí pro určitého podnikatele (osobu) za příznačná, umožňuje Zadavatel použití i jiných, kvalitativně a technicky obdobných řešení, které naplní Zadavatelem požadovanou funkcionalitu (byť jiným způsobem).

20. Komunikace mezi Zadavatelem a dodavatelem:

20.1. Veškerá komunikace mezi Zadavatelem a dodavatelem musí být v souladu s § 211 ZZVZ vedena pouze písemnou formou, a to elektronicky, s výjimkou případů vymezených v ustanovení § 211 odst. 5 ZZVZ. Nestanoví-li tato Zadávací dokumentace jinak, bude veškerá komunikace mezi Zadavatelem a dodavatelem probíhat v českém jazyce. Doručování písemností a komunikace mezi Zadavatelem a dodavatelem bude ze strany Zadavatele probíhat prostřednictvím elektronického nástroje E-ZAK (na adrese: https://zakazky.spravazeleznic.cz/), který splňuje podmínky vyhlášky č. 260/2016 Sb., o stanovení podrobnějších podmínek týkajících se elektronických nástrojů, elektronických úkonů při zadávání veřejných zakázek a certifikátu shody. Na komunikaci ze strany dodavatelů učiněnou elektronicky, avšak nikoliv prostřednictvím elektronického nástroje E-ZAK, bude tedy Zadavatel vždy odpovídat prostřednictvím elektronického nástroje.

20.2. Zpracování osobních údajů včetně jejich zvláštních kategorií případně poskytnutých v průběhu zadávacího řízení je Zadavatelem prováděno pouze za účelem zadání Veřejné zakázky, přičemž Zadavatel v celém procesu ochrany osobních údajů postupuje v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679, o ochraně

fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES, obecně závaznými právními předpisy a vnitřními předpisy zadavatele, které agendu ochrany osobních údajů upravují.

21. Požadavky Zadavatele na zpracování nabídky, způsob podání nabídek

21.1. Účastník předloží nabídku v elektronické podobě, a to s využitím elektronického nástroje E-ZAK. Způsob správného podání nabídky v elektronické podobě na veřejnou zakázku je uveden v uživatelské příručce elektronického nástroje E-ZAK pro dodavatele, která je k dispozici na internetové stránce profilu Zadavatele: https://zakazky.spravazeleznic.cz/manual.html.

21.2. Pro tyto účely a v souladu se ZZVZ systém vyžaduje registraci účastníků a elektronický podpis založený na kvalifikovaném certifikátu. Podáním nabídky účastník se stanovenou formou komunikace a doručování souhlasí a zavazuje se poskytnout veškerou nezbytnou součinnost, zejména provést registraci v elektronickém nástroji E-ZAK a pravidelně kontrolovat doručené zprávy.

21.3. Účastník je povinen přiložit ke své nabídce čestné prohlášení o tom, že v souvislosti se zadávacím řízením na předmětnou veřejnou zakázku neuzavřel a neuzavře s jinými osobami zakázanou dohodu ve smyslu zákona č. 143/2001 Sb., o ochraně hospodářské soutěže a o změně některých zákonů (zákon o ochraně hospodářské soutěže), ve znění pozdějších předpisů a že nepostupoval ve vzájemné shodě s jiným účastníkem zadávacího řízení, s nímž je spojenou osobou podle zákona č. 586/1992 Sb., o daních z příjmů, ve znění pozdějších předpisů, při přípravě částí nabídek, které mají být hodnoceny podle kritérií hodnocení. Vzor čestného prohlášení je upraven jako Příloha č. 4 této Zadávací dokumentace.

21.4. Speciální požadavky Zadavatele na zpracování nabídek:

21.4.1. Podává-li nabídku více osob společně, zejména jako společnost ve smyslu ustanovení § 2716 a násl. zákona č. 89/2012 Sb., občanský zákoník, případně jako jiné sdružení či seskupení dodavatelů (dále v textu této Zadávací dokumentace je takové seskupení dodavatelů obecně označováno zejména jako „***společnost***" dodavatelů a člen takového seskupení jako „***společník***"), musí předložit informace o takové společnosti.

21.4.2. Podává-li nabídku více osob společně, jsou povinni doložit v nabídce, že všichni tito dodavatelé budou vůči Zadavateli a jakýmkoliv třetím osobám z jakýchkoliv závazků vzniklých v souvislosti s veřejnou zakázkou, plněním předmětu veřejné zakázky či vzniklých v důsledku prodlení či jiného porušení smluvních nebo jiných povinností v souvislosti s plněním předmětu veřejné zakázky, zavázáni společně a nerozdílně. Účastník řízení tento požadavek doloží kopií smlouvy či jiného dokumentu, ze kterého bude daná skutečnost vyplývat.

21.4.3. Jeden ze společníků bude ve výše uvedené smlouvě či jiném dokumentu uveden jako vedoucí společník. Komunikace mezi Zadavatelem a společníky, kteří podávají společnou nabídku, potom bude v takovém případě probíhat prostřednictvím tohoto vedoucího společníka. Veškerá právní jednání budou považována za doručená, resp. odeslaná, okamžikem doručení, resp. odeslání, vedoucímu společníkovi.

21.5. Pro zpracování nabídky Zadavatel doporučuje níže uvedené řazení dokladů a dokumentů:

a) Obsah nabídky (včetně nabídkové ceny),

b) Čestné prohlášení ve vztahu k zakázaným dohodám - Vzor čestného prohlášení je upraven jako Příloha č. 4 této Zadávací dokumentace,

c) Čestné prohlášení o střetu zájmů - Vzor čestného prohlášení je upraven jako Příloha č. 7 této Zadávací dokumentace,

d) Čestné prohlášení o splnění podmínek v návaznosti na mezinárodní sankce - Vzor čestného prohlášení je upraven jako Příloha č. 8 této Zadávací dokumentace,

e) Čestné prohlášení k ve vztahu k zákonu o registru smluv - Vzor čestného prohlášení je upraven jako Příloha č. 6 této Zadávací dokumentace,

f) Doklady prokazující splnění základní způsobilosti,

g) Doklady prokazující splnění profesní způsobilosti,

h) Doklady prokazující splnění ekonomické kvalifikace,

i) Doklady prokazující splnění technické kvalifikace,

j) Závazný vzor smlouvy doplněný dle pokynů v této Zadávací dokumentaci – Závazný vzor smlouvy je upraven jako Příloha č. 5 této Zadávací dokumentace,

k) Jiné informace a doklady, je-li to potřebné.

21.6. Požaduje-li Zadavatel v nabídce pro účely posouzení splnění kvalifikace anebo hodnocení nabídek dle kritéria kvality předložení dokladů o rozhodné finanční hodnotě (např. finanční hodnota referenční zakázky, výše obratu) a v účastníkem předložených dokladech bude tato hodnota uvedena v jiné měně než CZK, bude částka přepočtena Zadavatelem dle posledního čtvrtletního průměrného kurzu devizového trhu příslušné měny k CZK stanoveného a zveřejněného ČNB ke dni zahájení zadávacího řízení. Postup dle předchozí věty se neuplatní pro hodnocení dle kritéria nejnižší nabídkové ceny. Nabídková cena musí být vždy uvedena v Zadavatelem požadované měně.

21.7. Nabídka musí být podána v českém jazyce nebo v souladu s ustanovením § 45 odst. 3 ZZVZ. Zadavatel nepřipouští podání nabídky v listinné podobě ani v jiné elektronické formě mimo elektronický nástroj E-ZAK. Povinnost překládat nabídku v českém jazyce se nevztahuje na certifikáty členů realizačního týmu či datasheety, tyto dokumenty mohou být předkládány rovněž v jazyce anglickém, avšak Zadavatel je oprávněn si vyžádat jejich překlad po dodavateli, bude-li to požadovat za potřebné.

21.8. Nabídky podávané v elektronické podobě účastník doručí do konce níže uvedené lhůty pro podání nabídek.

21.9. Dokumenty musí být do systému E-ZAK vkládány jako jeden soubor (ve výše uvedených formátech) nebo více zkomprimovaných souborů ve formátu zip, rar nebo 7z, bez použití hesla. Zkomprimované soubory nesmí obsahovat žádný další zkomprimovaný soubor. Zadavatel upozorňuje, že systém elektronického zadávání veřejných zakázek E-ZAK umožňuje pracovat se soubory o velikosti nejvýše 50 MB za jeden takový soubor, příp. zkomprimované soubory. Soubory většího rozsahu je nutno před jejich odesláním prostřednictvím E-ZAK vhodným způsobem rozdělit. Velikost samotné nabídky jako celku není nijak omezena.

21.10. Lhůta pro podání nabídek bude stanovena prostřednictvím elektronického nástroje E-ZAK.

22. Informace pro dodavatele a podmínky pro uzavření smlouvy:

22.1. Zadavatel si v souladu s **§ 170 ZZVZ** vyhrazuje právo zrušit zadávací řízení**.**

22.2. **Požadavky Zadavatele pro uzavření smlouvy**

22.2.1. Vybraný dodavatel je povinen Zadavateli na písemnou výzvu učiněnou dle § 122 odst. 3 ZZVZ předložit doklady či vzorky, pokud je Zadavatel požadoval a nemá je k dispozici.

22.2.2. Zadavatel je oprávněn v písemné výzvě určit další doklady, které je vybraný dodavatel povinen předložit v souladu s § 122 odst. 4 ZZVZ, tj. například originály nebo úředně ověřené kopie dokladů.

22.2.3. U vybraného dodavatele, je-li českou právnickou osobou, Zadavatel zjistí údaje o

jeho skutečném majiteli podle zákona upravujícího evidenci skutečných majitelů (dále jen „***skutečný majitel***") z evidence skutečných majitelů podle téhož zákona (dále jen „***evidence skutečných majitelů***"). Vybraného dodavatele, je-li zahraniční právnickou

osobou, Zadavatel vyzve k předložení výpisu ze zahraniční evidence obdobné evidenci skutečných majitelů nebo, není-li takové evidence,

a) ke sdělení identifikačních údajů všech osob, které jsou jeho skutečným majitelem,

a

b) k předložení dokladů, z nichž vyplývá vztah všech osob podle předchozího písmene a) k dodavateli; těmito doklady jsou zejména:

- výpis ze zahraniční evidence obdobné veřejnému rejstříku,
- seznam akcionářů,
- rozhodnutí statutárního orgánu o vyplacení podílu na zisku,
- společenská smlouva, zakladatelská listina nebo stanovy.

22.2.4. Zadavatel vyloučí vybraného dodavatele, je-li českou právnickou osobou, která má skutečného majitele, pokud nebylo možné zjistit údaje o jeho skutečném majiteli z evidence skutečných majitelů (k zápisu zpřístupněnému v evidenci skutečných majitelů po odeslání oznámení o vyloučení dodavatele se nepřihlíží). Zadavatel vyloučí vybraného dodavatele, je-li zahraniční právnickou osobou, pokud nepředložil údaje.

22.2.5. Zadavatel upozorňuje, že preferuje uzavírání smluv v elektronické podobě prostřednictvím některého druhu zaručených elektronických podpisů. V případě, že dodavatel není schopen k takovému postupu zajistit Zadavateli součinnost, žádáme, aby Zadavatele o této skutečnosti bezodkladně informoval.

22.3. **Další podmínky Zadavatele pro uzavření smlouvy (§ 104 ZZVZ)**

22.3.1. Vybraný dodavatel je povinen Zadavateli na písemnou výzvu učiněnou dle § 122 odst. 3 písm. b) ZZVZ předložit:

a) doklady a informace dle čl. 24.3 a čl. 25.7 Zadávací dokumentace;

b) kopii dokladu o pojištění odpovědnosti za škodu sjednané v rozsahu podrobně stanoveném v čl. 22. smlouvy, např. pojistná smlouva, pojistný certifikát,

22.3.2. Neposkytnutí uvedené součinnosti vybraným dodavatelem je v souladu s ustanovením § 122 odst. 8 ZZVZ důvodem pro vyloučení vybraného dodavatele ze Zadávacího řízení.

23. Registr smluv

23.1. Zadavatel je povinen uveřejňovat uzavřené smlouvy v registru smluv na základě ustanovení zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (dále jen „***ZRS***").

23.2. Zadavatel na základě výše uvedeného požaduje, aby účastník pro účely uveřejnění smlouvy v registru smluv ve smlouvě, která bude nedílnou součástí nabídky, označil její části, které jsou předmětem obchodního tajemství nebo ty části, ve kterých jsou obsaženy informace, které nemohou být v registru smluv uveřejněny na základě ustanovení § 3 odst. 1 ZRS.

23.3. Dodavatel podáním nabídky akceptuje, že nabídková cena, která je předmětem hodnocení, bude vždy uveřejněna postupem dle ZRS. Zadavatel upozorňuje, že v případě jednotkových nabídkových cen, které nejsou předmětem hodnocení, se zpravidla nebude jednat o obchodní tajemství. V případě, že dodavatel tyto jednotkové ceny označí jako obchodní tajemství, je zadavatel oprávněn přezkoumat, zda jím označené jednotkové ceny naplňují veškeré znaky obchodního tajemství, a tyto jednotkové ceny případně uveřejnit. Dodavatel je v takovém případě zadavateli povinen poskytnout součinnost, zejména je povinen k výzvě zadavatele blíže odůvodnit naplnění všech znaků obchodního tajemství ve vztahu k jím označeným jednotkovým cenám. Dodavatel podáním nabídky dále akceptuje, že i v případě, že jednotkové ceny naplní všechny znaky obchodního tajemství, je zadavatel oprávněn uveřejnit jednotkové ceny dle ZRS, je-li to nezbytné pro

účely § 9 odst. 2 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

23.4. Pokud účastník ve smlouvě, která bude nedílnou součástí nabídky, označí její části nebo určité informace dle čl. 23.2 této Zadávací dokumentace, je účastník povinen předložit Čestné prohlášení. Vzor čestného prohlášení je zpracován jako Příloha č. 6 této Zadávací dokumentace. Tímto čestným prohlášením účastník prohlašuje, že jím uvedené údaje a skutečnosti kumulativně naplňují všechny definiční znaky obchodního tajemství tak, jak je vymezeno v ustanovení § 504 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „***obchodní tajemství***") a pro případ, že by takto označené údaje a skutečnosti nenaplňovaly znaky obchodního tajemství, nese účastník veškerou odpovědnost za skutečnost, že takto znečitelněná smlouva, či rámcová dohoda byla uveřejněna způsobem odporujícím ZRS. Odpovědnost dodavatele dle předchozí věty není dotčena postupem zadavatele dle čl. 23.3 této Zadávací dokumentace

23.5. Výše uvedené čestné prohlášení dle čl. 23.4 této Zadávací dokumentace účastník nedokládá v případě, že neoznačí ve smlouvě, která bude nedílnou součástí nabídky, žádné takové části nebo informace ve smyslu čl. 23.2 této Zadávací dokumentace**.**

23.6. Účastník odpovídá za správnost a pravdivost veškerých údajů a skutečností, které jím budou uvedeny ve výše uvedeném čestném prohlášení.

23.7. Výjimkou z povinnosti uveřejnění smlouvy v registru smluv jsou důvody uvedené v ustanovení § 3 odst. 2 ZRS. Je-li účastník subjektem uvedeným v ustanovení § 3 odst. 2 písm. k) ZRS (případně je subjektem uvedeným v ustanovení § 3 odst. 2 ZRS dle jiného písmene, než je zde uvedeno), doporučuje Zadavatel, aby účastník tuto skutečnost uvedl v nabídce. V případě, že tak účastník neučiní, bude Zadavatel postupovat, jako by na smlouvu nedopadala výjimka uvedená v ustanovení § 3 odst. 2 písm. k) ZRS (případně jiná výjimka dle ustanovení § 3 odst. 2 ZRS dle jiného písmene, než je zde uvedeno) a Zadavatel neodpovídá za škodu nebo jakoukoliv jinou újmu tímto postupem vzniklou.

24. Střet zájmů dle zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů

24.1. Dle § 4b zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů (dále jen „***Zákon o střetu zájmů***"), se nesmí účastnit zadávacích řízení dle ZZVZ jako účastník zadávacího řízení nebo jako poddodavatel, prostřednictvím kterého účastník zadávacího řízení prokazuje kvalifikaci, obchodní společnost, ve které veřejný funkcionář uvedený v § 2 odst. 1 písm. c) Zákona o střetu zájmů nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti.

24.2. Zadavatel požaduje, aby dodavatel a jeho poddodavatel, prostřednictvím kterého prokazuje kvalifikaci, nebyli ve střetu zájmů dle § 4b Zákona o střetu zájmů. Skutečnost, že dodavatel a jeho poddodavatel, prostřednictvím kterého prokazuje část kvalifikace, nejsou ve střetu zájmů dle § 4b Zákona o střetu zájmů, prokáže dodavatel předložením čestného prohlášení, jehož vzorové znění je Příloha č. 7 Zadávací dokumentace, ve své nabídce.

24.3. Zadavatel je oprávněn ověřovat si splnění zadávacích podmínek dle tohoto článku. Vybraný dodavatel je povinen předložit k výzvě Zadavatele dle § 122 odst. 3 písm. b) ZZVZ doklady a informace, z nichž nepochybně vyplyne, že vybraný dodavatel i všichni poddodavatelé, jimiž vybraný dodavatel prokazuje kvalifikaci, splňují podmínku neexistence střetu zájmů ve smyslu § 4b Zákona o střetu zájmů a tohoto čl. 24 Zadávací dokumentace. V případě vybraného dodavatele nebo jeho poddodavatele, prostřednictvím kterého vybraný dodavatel prokazoval část kvalifikace, je-li zahraniční právnickou osobou, je vybraný dodavatel povinen předložit zejména doklady ve smyslu § 122 odst. 6 ZZVZ, a to i ve vztahu k příslušnému poddodavateli, prostřednictvím kterého vybraný dodavatel prokazoval část kvalifikace.

24.4. V případě postupu účastníka v rozporu s čl. 24 Zadávací dokumentace bude účastník

vyloučen ze zadávacího řízení.

25. Další zadávací podmínky v návaznosti na mezinárodní sankce, zákaz zadání veřejné zakázky

25.1. Zadavatel v tomto řízení postupuje v souladu s § 48a ZZVZ.

25.2. Dle článku 5k nařízení Rady (EU) č. 833/2014 ze dne 31. července 2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, ve znění pozdějších předpisů[4] (dále jen „***Nařízení č. 833/2014***") se zakazuje se zadat jakoukoli veřejnou zakázku nebo koncesní smlouvu spadající do oblasti působnosti směrnic o zadávání veřejných zakázek, jakož i čl. 10 odst. 1, 3, odst. 6 písm. a) až e), odst. 8, 9 a 10, článků 11, 12, 13 a 14 směrnice 2014/23/EU, čl. 7 písm. a) až d), článku 8 a čl. 10 písm. b) až f) a h) až j) směrnice 2014/24/EU, článku 18, čl. 21 písm. b) až e) a g až i) a článků 29 a 30 směrnice 2014/25/EU a čl. 13 písm. a) až d), f) až h) a j) směrnice 2009/81/ES a hlavy VII nařízení Evropského parlamentu a Rady (EU, Euratom) 2018/1046 následujícím osobám, subjektům nebo orgánům, nebo pokračovat v jejich plnění s následujícími osobami, subjekty a orgány:

a) jakýkoli ruský státní příslušník, fyzická osoba s bydlištěm v Rusku nebo právnická osoba, subjekt či orgán usazené v Rusku;

b) právnická osoba, subjekt nebo orgán, které jsou z více než 50 % přímo či nepřímo vlastněny některým ze subjektů uvedených v písmeni a) tohoto odstavce, nebo

c) fyzická nebo právnická osoba, subjekt nebo orgán, které jednají jménem nebo na pokyn některého ze subjektů uvedených v písmeni a) nebo b) tohoto odstavce,

včetně subdodavatelů, dodavatelů nebo subjektů, jejichž způsobilost je využívána ve smyslu směrnic o zadávání veřejných zakázek, pokud představují více než 10 % hodnoty zakázky.

25.3. Zadavatel požaduje, aby účastník sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti v zadávacím řízení, ani žádný z jeho poddodavatelů nebo jiných osob, jejichž způsobilost je využívána ve smyslu směrnic o zadávání veřejných zakázek, **nebyli** osobami dle odst. 2 tohoto článku a Nařízení č. 833/2014.

25.4. Dle čl. 2 nařízení Rady (EU) č. 269/2014 ze dne 17. března 2014, o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, ve znění pozdějších předpisů (dále jen „***Nařízení č. 269/2014***"), a dalších prováděcích předpisů k tomuto Nařízení č. 269/2014[5], nesmějí být žádné finanční prostředky ani hospodářské zdroje přímo ani nepřímo zpřístupněny fyzickým nebo právnickým osobám, subjektům či orgánům nebo fyzickým nebo právnickým osobám, subjektům či orgánům s nimi spojeným uvedeným v příloze I Nařízení nebo v jejich prospěch; dle čl. 2 **nařízení Rady (ES) č. 765/2006** ze dne 18. května 2006 o omezujících opatřeních vzhledem k situaci v Bělorusku a k zapojení Běloruska do ruské agrese proti Ukrajině, ve znění pozdějších předpisů, nesmějí být fyzickým nebo právnickým osobám nebo subjektům uvedeným v příloze I tohoto nařízení nebo v jejich prospěch přímo ani nepřímo zpřístupněny žádné finanční prostředky ani hospodářské zdroje; dle čl. 2 **nařízení Rady (EU) č. 208/2014** ze dne 5. března 2014 o omezujících opatřeních vůči některým osobám, subjektům a orgánům vzhledem k situaci na Ukrajině nesmějí být žádné finanční prostředky ani hospodářské zdroje přímo

[4] Zejm. Nařízení Rady (EU) 2022/576 ze dne 8. dubna 2022, kterým se mění nařízení (EU) č. 833/2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině

[5] Zejm, Prováděcí nařízení Rady (EU) 2022/581 ze dne 8. dubna 2022, kterým se provádí nařízení (EU) č. 269/2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny a prováděcí nařízení Rady (EU) 2022/658 ze dne 21. dubna 2022, kterým se provádí nařízení (EU) č. 269/2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny.

ani nepřímo zpřístupněny fyzickým nebo právnickým osobám, subjektům či orgánům uvedeným v příloze I tohoto nařízení nebo v jejich prospěch (dále společně jen „***Osoby vedené na sankčních seznamech***“).

25.5. Zadavatel dále požaduje, aby účastník sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti v zadávacím řízení, ani žádný z jeho poddodavatelů nebo jiných osob, jejichž způsobilost je využívána ve smyslu směrnic o zadávání veřejných zakázek, **nebyli** Osobami vedenými na sankčních seznamech.

25.6. Splnění zadávacích podmínek stanovených Zadavatelem dle tohoto článku prokáže účastník předložením čestného prohlášení, jehož vzorové znění je Příloha č. 8 této Zadávací dokumentace, ve své nabídce.

25.7. Zadavatel je oprávněn ověřovat si splnění zadávacích podmínek dle tohoto článku. Vybraný dodavatel je povinen předložit k výzvě Zadavatele dle § 122 odst. 3 písm. b) ZZVZ doklady a informace, z nichž nepochybně vyplyne, že vybraný dodavatel i všichni poddodavatelé nebo jiné osoby, jejichž způsobilost je využívána ve smyslu směrnic o zadávání veřejných zakázek, splňují podmínky uvedené v tomto článku Zadávací dokumentace.

25.8. V případě postupu účastníka v rozporu s čl. 25 Zadávací dokumentace bude účastník vyloučen ze zadávacího řízení.

Přílohy Zadávací dokumentace

Příloha č. 1. Čestné prohlášení k základní způsobilosti

Příloha č. 2. Vzor profesního životopisu

Příloha č. 3. Vzor seznamu významných zakázek

Příloha č. 4. Čestné prohlášení ve vztahu k zakázaným dohodám

Příloha č. 5. Závazný vzor smlouvy

Příloha č. 6. Čestné prohlášení ve vztahu k zákonu o registru smluv

Příloha č. 7. Čestné prohlášení o střetu zájmů

Příloha č. 8. Čestné prohlášení o splnění podmínek v návaznosti na mezinárodní sankce

Příloha č. 9. Výstupy z PTK

Ing. Mojmír Nejezchleb
02.04.2026 16:32
Podepsáno elektronicky

……

Ing. Mojmír Nejezchleb
zástupce generálního ředitele
pověřený správní radou řízením organizace

Ing. Tomáš Čoček
02.04.2026 15:44
Podepsáno elektronicky

……

Ing. Tomáš Čoček, Ph.D.
náměstek generálního ředitele
pro ekonomiku

SPRÁVA ŽELEZNIC

Příloha č. 1 Zadávací dokumentace

Vzor čestného prohlášení o splnění části základní způsobilosti

Účastník:

Obchodní firma/jméno	[DOPLNÍ ÚČASTNÍK]
Sídlo/místo podnikání	[DOPLNÍ ÚČASTNÍK]
IČO	[DOPLNÍ ÚČASTNÍK]
Zastoupen	[DOPLNÍ ÚČASTNÍK]

který podává žádost o účast/nabídku na nadlimitní sektorovou veřejnou zakázku s názvem „**Realizace systému Zabezpečeného úložiště v prostředí Správy železnic**", tímto čestně prohlašuje, že:

i. nemá v České republice v evidenci daní zachycen splatný daňový nedoplatek ve vztahu ke spotřební dani,
ii. nemá v České republice splatný nedoplatek na pojistném nebo na penále na veřejné zdravotní pojištění.

Pozn. zadavatele: v případě, že dodavatel není zapsán v obchodním rejstříku, je třeba, aby toto prohlášení doplnil o další bod dle § 74 odst. 1 písm. e) zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů.

Pozn. zadavatele: zahraniční dodavatel se sídlem mimo ČR doplní toto prohlášení ve vztahu k zemi svého sídla, pokud se v zemi jeho sídla příslušná skutečnost neprokazuje dokladem vydaným podle právního řádu země jeho sídla (kvalifikace získaná v zahraničí se prokazuje doklady vydanými podle právního řádu země, ve které byla získána, pokud se však podle příslušného právního řádu požadovaný doklad nevydává, může být nahrazen čestným prohlášením).

V [DOPLNÍ ÚČASTNÍK] dne [DOPLNÍ ÚČASTNÍK]

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČO: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

Příloha č. 2 Zadávací dokumentace „Realizace systému Zabezpečeného úložiště v prostředí Správy železnic“

PROFESNÍ ŽIVOTOPIS

Jméno, příjmení, titul	[DOPLNÍ DODAVATEL]
Telefon, e-mail	[DOPLNÍ DODAVATEL]

Zaměstnavatel / OSVČ	[DOPLNÍ DODAVATEL]
Telefon, e-mail	[DOPLNÍ DODAVATEL]
Kontaktní adresa zaměstnavatele / sídla	[DOPLNÍ DODAVATEL]
Vztah k dodavateli *Dodavatel doplní, zda se jedná o jeho zaměstnance, nebo o poddodavatele.*	[DOPLNÍ DODAVATEL]

PROFESNÍ A DALŠÍ CERTIFIKÁTY

Datum obdržení autorizace / osvědčení / certifikátu, případně **doba platnosti, je-li certifikát vydáván na omezenou dobu** (*ve formátu DD/MM/RRRR)*	**Název a popis certifikátu prokazujícího odbornou způsobilost**
[DOPLNÍ DODAVATEL]	[DOPLNÍ DODAVATEL]

POZICE V REALIZAČNÍM TÝMU (dle čl. 12.2.3 *zadávací dokumentace*)

[DOPLNÍ DODAVATEL]

PROFESNÍ PRAXE

Doba profesní praxe na konkrétní pozici *(ve formátu mm/rrrr - mm/rrrr)*	**Zaměstnavatel/OSVČ** *Dodavatel doplní označení zaměstnavatele či uvede, že byl OSVČ*	**Popis vykonávaných činností** *Dodavatel doplní označení pozice a rovněž stručný popis vykonávaných činností, ze kterého bude vyplývat naplnění požadavků dle čl. 12 zadávací dokumentace*
[DOPLNÍ DODAVATEL]		[DOPLNÍ DODAVATEL]
[DOPLNÍ DODAVATEL]		[DOPLNÍ DODAVATEL]
[DOPLNÍ DODAVATEL]		[DOPLNÍ DODAVATEL]

ZKUŠENOSTI PRO ÚČELY PROKÁZÁNÍ TECHNICKÉ KVALIFIKACE

Objednatel projektu *(název, IČO, sídlo, místo podnikání, kontakt k ověření realizované referenční zakázky (telefonní a e-mailový kontakt na kontaktní osobu)*	***Název a popis předmětu projektu*** *(ze kterého bude vyplývat naplnění požadavků dle čl. 12.2 zadávací dokumentace)*	***Finanční hodnota projektu*** (v Kč bez DPH)	***Doba realizace projektu*** *(datum od-do ve formátu MM/RRRR – MM/RRRR)*
[DOPLNÍ DODAVATEL]	[DOPLNÍ DODAVATEL]	[DOPLNÍ DODAVATEL]	[DOPLNÍ DODAVATEL]
[DOPLNÍ DODAVATEL]	[DOPLNÍ DODAVATEL]	[DOPLNÍ DODAVATEL]	[DOPLNÍ DODAVATEL]
[DOPLNÍ DODAVATEL]	[DOPLNÍ DODAVATEL]	[DOPLNÍ DODAVATEL]	[DOPLNÍ DODAVATEL]

Tento strukturovaný životopis je určen pro účely podání nabídky do veřejné zakázky s názvem „**Realizace systému Zabezpečeného úložiště v prostředí Správy železnic**.

Všechny údaje uvedené v tomto profesním životopisu jsou správné, úplné a pravdivé.

V [DOPLNÍ DODAVATEL] dne [DOPLNÍ DODAVATEL]

Podpis člena realizačního týmu

---

titul, jméno, příjmení
[DOPLNÍ DODAVATEL]

SPRÁVA ŽELEZNIC

Příloha č. 3 Zadávací dokumentace

Vzor seznamu významných zakázek

Účastník:

Obchodní firma/jméno	[DOPLNÍ ÚČASTNÍK]
Sídlo/místo podnikání	[DOPLNÍ ÚČASTNÍK]
IČO	[DOPLNÍ ÚČASTNÍK]
Zastoupen	[DOPLNÍ ÚČASTNÍK]

který podává nabídku na nadlimitní sektorovou veřejnou zakázku s názvem **„Realizace systému Zabezpečeného úložiště v prostředí Správy železnic"** tímto čestně prohlašuje, že za posledních 5 let před zahájením zadávacího řízení realizoval minimálně níže specifikované významné referenční zakázky, v níže uvedené hodnotě a v níže uvedeném termínu.

	Zakázka č. 1	**Zakázka č. 2**	**Zakázka č. 3**
Objednatel referenční zakázky IČO, sídlo/místo podnikaní, kontakt k ověření realizované zakázky	[DOPLNÍ ÚČASTNÍK]	[DOPLNÍ ÚČASTNÍK]	[DOPLNÍ ÚČASTNÍK]
Popis předmětu referenční zakázky, z něhož vyplyne splnění všech podmínek kvalifikace, jak jsou zadavatele požadovány v zadávacích podmínkách	[DOPLNÍ ÚČASTNÍK]	[DOPLNÍ ÚČASTNÍK]	[DOPLNÍ ÚČASTNÍK]
Finanční objem plnění ve vztahu, k němuž je kvalifikace prokazována	[DOPLNÍ ÚČASTNÍK]	[DOPLNÍ ÚČASTNÍK]	[DOPLNÍ ÚČASTNÍK]

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČ: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

Doba realizace (datum od-do, v rámci 5 let nazpět před zahájením zadávacího řízení)	[DOPLNÍ ÚČASTNÍK]	[DOPLNÍ ÚČASTNÍK]	[DOPLNÍ ÚČASTNÍK]
Předmět referenční zakázky zahrnoval analýzu data managementu	[DOPLNÍ ÚČASTNÍK]	[DOPLNÍ ÚČASTNÍK]	[DOPLNÍ ÚČASTNÍK]
Předmět referenční zakázky byl realizována pro subjekt kritické infrastruktury/velký podnik	[DOPLNÍ ÚČASTNÍK]	[DOPLNÍ ÚČASTNÍK]	[DOPLNÍ ÚČASTNÍK]
Předmět referenční zakázky zahrnoval dvě geograficky oddělené lokality nebo primární / sekundární lokalitu	[DOPLNÍ ÚČASTNÍK]	[DOPLNÍ ÚČASTNÍK]	[DOPLNÍ ÚČASTNÍK]
Předmět referenční zakázky zahrnoval dodávku serverů	[DOPLNÍ ÚČASTNÍK]	[DOPLNÍ ÚČASTNÍK]	[DOPLNÍ ÚČASTNÍK]
Předmět referenční zakázky zahrnoval dodávku diskových polí	[DOPLNÍ ÚČASTNÍK]	[DOPLNÍ ÚČASTNÍK]	[DOPLNÍ ÚČASTNÍK]
Předmět referenční zakázky zahrnoval dodávku síťových prvků	[DOPLNÍ ÚČASTNÍK]	[DOPLNÍ ÚČASTNÍK]	[DOPLNÍ ÚČASTNÍK]
Předmět referenční zakázky zahrnoval konfiguraci a implementaci bezpečnostních pravidel	[DOPLNÍ ÚČASTNÍK]	[DOPLNÍ ÚČASTNÍK]	[DOPLNÍ ÚČASTNÍK]

pozn. Účastník rozšíří tabulku dle potřeby v případě většího počtu referenčních zakázek.

V [DOPLNÍ ÚČASTNÍK] dne [DOPLNÍ ÚČASTNÍK]

SPRÁVA ŽELEZNIC

Příloha č. 4 zadávací dokumentace

Čestné prohlášení účastníka

Účastník:

Obchodní firma/jméno	[DOPLNÍ ÚČASTNÍK]
Sídlo/místo podnikání	[DOPLNÍ ÚČASTNÍK]
IČO	[DOPLNÍ ÚČASTNÍK]
Zastoupen	[DOPLNÍ ÚČASTNÍK]

který podává nabídku na nadlimitní sektorovou veřejnou zakázku s názvem **„Realizace systému Zabezpečeného úložiště v prostředí Správy železnic", č.j. 60299/2026-SŽ-GŘ-O25**, tímto čestně prohlašuje, že v souvislosti se zadávanou veřejnou zakázkou neuzavřel a neuzavře s jinými osobami zakázanou dohodu ve smyslu zákona č. 143/2001 Sb., o ochraně hospodářské soutěže a o změně některých zákonů (zákon o ochraně hospodářské soutěže), ve znění pozdějších předpisů.

Účastník si je vědom všech právních důsledků, které pro něj mohou vyplývat z nepravdivosti zde uvedených údajů a skutečností.

V [DOPLNÍ ÚČASTNÍK] dne [DOPLNÍ ÚČASTNÍK]

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČO: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

Příloha č. 5 Zadávací dokumentace – Závazný vzor smlouvy

Smlouva o dílo - Realizace systému Zabezpečeného úložiště v prostředí Správy železnic

Číslo smlouvy Objednatele: [DOPLNÍ OBJEDNATEL PŘI PODPISU SMLOUVY]
Číslo smlouvy Zhotovitele: [DOPLNÍ ZHOTOVITEL]

uzavřená podle ustanovení § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „***občanský zákoník***“)

(dále jen „***Smlouva***“)

Objednatel: **Správa železnic, státní organizace**

zapsaná v obchodním rejstříku vedeném Městským soudem v Praze pod sp. zn. A 48384

Praha 1 - Nové Město, Dlážděná 1003/7, PSČ 110 00

IČ 70994234, DIČ CZ70994234

zastoupená Ing. Mojmírem Nejezchlebem, zástupcem generálního ředitele pověřeným správní radou řízením organizace a
Ing. Tomášem Čočkem, Ph.D., náměstkem generálního ředitele pro ekonomiku

Zhotovitel: [DOPLNÍ ZHOTOVITEL *jméno osoby/název firmy*]

[DOPLNÍ ZHOTOVITEL *údaje o zápisu v evidenci*]

[DOPLNÍ ZHOTOVITEL *sídlo*]

IČO [DOPLNÍ ZHOTOVITEL], DIČ [DOPLNÍ ZHOTOVITEL]

Bankovní spojení: [DOPLNÍ ZHOTOVITEL]

Číslo účtu: [DOPLNÍ ZHOTOVITEL]

[DOPLNÍ ZHOTOVITEL *údaje o statutárním orgánu nebo jiné oprávněné osobě*]
(dále též jen „***Zhotovitel***“ nebo „***Dodavatel***“)

(Objednatel a Zhotovitel dále také jako „***Smluvní strany***“ nebo „***Strany***“)

Tato Smlouva je uzavřena na základě výsledků zadávacího řízení veřejné zakázky s názvem „Realizace systému Zabezpečeného úložiště v prostředí Správy železnic“, ev. č. veřejné zakázky ve věstníku veřejných zakázek: ..... (dále jen „***Veřejná zakázka***“). Jednotlivá ustanovení této Smlouvy tak budou vykládána v souladu se zadávacími podmínkami Veřejné zakázky.

Veřejná zakázka je spolufinancovaná z Evropských strukturálních a investičních fondů

prostřednictvím Integrovaného regionálního operačního programu (IROP) v rámci projektu „Dohled a řízení bezpečnosti", reg. č. "CZ.06.01.01/00/22_005/0000104".

Pokud nevyplývá z této Smlouvy jinak, mají pojmy s velkými počátečními písmeny význam definovaný v Příloze č. 6 – *Zvláštní obchodní podmínky pro Zakázky v oblasti ICT* (dále také jen „***ZOP***" nebo „***Zvláštní obchodní podmínky***"), nebo Příloze č. 7 – *Obchodní podmínky ke Smlouvě o dílo* (dále jen „***OOP***" nebo „***Obchodní podmínky***"). Pro vyloučení jakýchkoliv pochybností Strany uvádějí, že pokud je v této Smlouvě obsažen článek se shodným názvem jako v ZOP, OOP nebo jiném smluvním dokumentu, neznamená to, že by článek této Smlouvy plně nahrazoval příslušné články v jiných smluvních dokumentech, pokud není výslovně uvedeno jinak; obdobné platí pro vztahy mezi jinými smluvními dokumenty.

1. Účel Smlouvy

1.1. Účelem Smlouvy je realizace zákonné povinnosti Objednatele, a to posílením fyzické a kybernetické bezpečnosti a ochranou aktiv proti kybernetickým hrozbám prostřednictvím dodávky technologie pro centralizované bezpečné datové úložiště (dále také jen „***BÚ***"), implementace a konfigurace dodané technologie, odborné školení správy a údržby dodané technologie pro vybrané odborné pracovníky Objednatele.

1.2. Účelem této Smlouvy je tak zejména provedení Díla, tj. provedení Předmětu díla a poskytnutí souvisejících plnění v takovém rozsahu a takovým způsobem, aby minimálně po dobu trvání této Smlouvy došlo k naplnění bezpečnostních požadavků, jejichž naplnění je provedením Díla sledováno.

1.3. Účelem této Smlouvy je to, aby bylo Dílo Zhotovitelem provedeno a po dobu trvání této Smlouvy udržováno funkční v souladu s požadavky vyplývajícími z:

a. právních předpisů;

b. Smlouvy a jejích příloh;

c. zadávací dokumentace Veřejné zakázky;

d. Nabídky a

e. Interních předpisů SŽ (dále jen „***Interní předpisy***"), přičemž se za Interní předpisy pro účely této Smlouvy považují pouze interní předpisy SŽ, se kterými byl Zhotovitel prokazatelně seznámen.

2. Předmět Smlouvy

2.1. Předmětem této Smlouvy je závazek Zhotovitele provést na svůj náklad a nebezpečí pro Objednatele řádně a včas Dílo a závazek Objednatele Dílo převzít a zaplatit Zhotoviteli Cenu díla a příslušnou DPH, a to vše za podmínek stanovených v této Smlouvě.

2.2. Předmětem díla je dodání, implementace a konfigurace technologie centralizovaného bezpečného datového úložiště za účelem splnění zákonných povinností Objednatele v oblasti kybernetické a fyzické bezpečnosti. Součástí plnění je zpracování analytické části, vytvoření koncepce Bezpečného úložiště, návrh detailního implementačního postupu pro vybrané systémy, dodání HW, implementace a konfigurace technologie a napojení na vybrané systémy Objednatele.

2.3. Bližší požadavky na Předmět díla jsou vymezeny zejména, nikoliv však výlučně, v Příloze č. 1 Bližší specifikace předmětu plnění a v Příloze č. 2 Technická specifikace.

2.4. Provedení Díla spočívá v provedení následujících oblastí dílčích plnění ze strany Zhotovitele podrobně definovaných v Příloze č. 1 Bližší specifikace předmětu plnění a v Příloze č. 2 Technická specifikace:

a. Datový management vybraných systémů:

- Analýza současného stavu data managementu
- Návrh na změnu data managementu

b. Implementační plán Bezpečného úložiště (včetně Exit strategie)

c. Dodávka a implementace Bezpečného úložiště do primární a sekundární lokality

d. Konfigurace Bezpečného úložiště

e. Napojením na vybrané systémy

f. Post-implementační testování

g. Školení a dokumentace

h. Post-implementační a Technická podpora

i. Konzultační služby na vyžádání

(dále jen „***Plnění***").

2.5. Provedení Díla spočívá rovněž v provedení všech činností, jejichž potřeba vyplývá z účelu a obsahu této Smlouvy, jejích příloh a z dokumentů uvedených v této Smlouvě.

2.6. Bude-li určitý relevantní právní předpis v době trvání této Smlouvy nahrazen jiným právním předpisem, je Zhotovitel povinen vyvinout veškerou snahu, kterou po něm lze spravedlivě požadovat, aby Dílo bylo uvedeno do souladu s tímto novým právním předpisem tak, aby Předmět díla byl provozován v souladu s Požadavky, a to zejména s požadavky souvisejícími s povinnostmi Objednatele na zajištění odpovídající úrovně kybernetické bezpečnosti. Obdobné platí i pro změny Interních předpisů, pokud byly tyto změny provedeny v návaznosti na změny právních předpisů a Zhotovitel byl s novým zněním Interních předpisů seznámen.

3. Místo plnění

3.1. Místem plnění je V Trianglu 2474-180 00, Praha 9 a Cvokařská 2834/2-301 00 Plzeň 1.

4. Doba plnění

4.1. Doba trvání této Smlouvy činí nejméně 60 měsíců od ukončení fáze F3.3 (v této době bude plněna fáze F6.2 (Post-implementační podpora)) (dále jen „***doba trvání Smlouvy***").

4.2. Doba trvání Smlouvy nemá vliv na existenci práv a povinností Stran, která mají vzhledem ke své povaze a okolnostem trvat i po konci doby trvání Smlouvy.

4.3. Pokud není stanoveno jinak, je Zhotovitel povinen provádět Dílo a jeho části v termínech uvedených v závazném harmonogramu realizace Díla obsaženém v Příloze č. 9 této Smlouvy (dále jen „***Harmonogram***").

4.4. Žádná ze Stran není oprávněna jednostranně měnit termíny uvedené v Harmonogramu.

5. Cena díla

5.1. Celková cena za splnění závazku Zhotovitele provést Dílo v rozsahu dle této Smlouvy, tj. Cena díla, je uvedena pod položkou Nabídková cena celkem v Příloze č. 3 této Smlouvy – Ceník (dále také jen „***Příloha č. 3***").

5.2. Ceny, a to jak jednotkové ceny, tak nabídková cena celkem, obsažené v Příloze č. 3 této Smlouvy, jsou uvedeny jako maximální, nejvýše přípustné, nepřekročitelné a zahrnující veškeré náklady Zhotovitele nutné k řádnému a včasnému provedení Díla, resp. příslušného dílčího plnění (např. správní a místní poplatky, vedlejší náklady, náklady spojené s dopravou do místa plnění, včetně nákladů souvisejících s celními poplatky a s provedením všech zkoušek a testů prokazujících dodržení předepsané kvality a parametrů Předmětu plnění dle této Smlouvy, náklady na licence apod. jsou všechny zahrnuty v cenách obsažených v Příloze č. 3 této Smlouvy).

5.3. Součástí Ceny díla jsou i náklady na dodávky a služby, které v zadávací dokumentaci Veřejné zakázky, Nabídce ani v této Smlouvě a jejích přílohách nejsou výslovně uvedeny, ale Zhotovitel jakožto odborník ví nebo má vědět, že jsou nezbytné pro řádné a včasné provedení Díla. Zhotovitel nese veškeré náklady nutně nebo účelně vynaložené při plnění závazku z této Smlouvy včetně správních poplatků.

5.4. Ceny obsažené v Příloze č. 3 této Smlouvy jsou uvedeny bez DPH. V případě změny zákonné sazby DPH není třeba uzavírat dodatek k této Smlouvě, ledaže o to Objednatel požádá.

5.5. Zhotovitel odpovídá za to, že sazba DPH je stanovena v souladu s platnými právními

předpisy.

5.6. Změna Ceny díla dle části 5 odst. 19.2 OOP se nepřipouští.

6. Platební podmínky

6.1. Zhotovitel je oprávněn doručit Objednateli Výzvu k úhradě v následujících platebních milnících, v níže definovaných výších a za níže vymezených podmínek:

První platební milník (**Platební milník A**): Výzva k úhradě ve výši ceny za položky označené v Příloze č. 1 této Smlouvy takto: Fáze F1.1 (Datový management vybraných systémů), Fáze F1.2 (Implementační plán Bezpečného úložiště), Fáze F2.1 (Dodávka a implementace Bezpečného úložiště do primární lokality), Fáze F2.2 (Dodávka a implementace Bezpečného úložiště do sekundární lokality), a to nejdříve po akceptaci (bez výhrad) těchto Fází, které jsou tvořeny činnostmi blíže specifikovanými v části 5.1, 5.2, 5.3, 5.3.4 Přílohy č. 1 této Smlouvy;

Druhý platební milník (**Platební milník B**): Výzva k úhradě ve výši ceny za položky označené v Příloze č. 1 této Smlouvy takto: Fáze F3.1A (Konfigurace primární lokality, F3.1B (Konfigurace sekundární lokality), Fáze F3.2 (Napojení na vybrané systémy), Fáze F3.3 (Post-implementační testování), Fáze F4 (Školení), Fáze F5 (Dokumentace), a to nejdříve po akceptaci (bez výhrad) těchto Fází, které jsou tvořeny činnostmi uvedenými v části 5.4.1, 5.4.2, 5.4.3, 6.1 a 6.2 Přílohy č. 1 této Smlouvy;

6.2. Zhotovitel je dále oprávněn doručit Objednateli Výzvu k úhradě vždy za každý měsíc, v němž došlo k akceptaci (bez výhrad) plnění na základě Objednávky Konzultačních služeb na vyžádání dle čl. 10 této Smlouvy, a to ve výši součinu počtu MD dle Objednávky či Objednávek a ceny za jeden MD dle příslušné položky ceny Konzultační služby na vyžádání uvedené Příloze č. 3 této Smlouvy.

6.3. Zhotovitel je dále oprávněn doručit Objednateli Výzvu k úhradě za každý měsíc po akceptaci (bez výhrad) služeb Post-implementační podpory a Technické podpory, a to ve výši ceny za příslušný měsíc dle příslušné položky ceny Post-implementační podpora, ceny Technická podpora – primární lokalita a ceny Technická podpora – sekundární lokalita uvedených Příloze č. 3 této Smlouvy.

6.4. Výzva k úhradě musí být fakturou nebo daňovým dokladem. Kromě náležitostí účetního či daňového dokladu musí být Výzva k úhradě označena registračním číslem projektu: CZ.06.01.01/00/22_005/0000104. Pokud je Výzva k úhradě hrazena z více zdrojů, budou na ní uvedena všechna čísla projektů. Objednatel je oprávněn čísla projektu aktualizovat v průběhu trvání této Smlouvy a Zhotovitel je povinen tuto skutečnost akceptovat a zohlednit v rámci prováděné fakturace.

6.5. Výzvu k úhradě doručí Zhotovitel Objednateli jedním z následujících způsobů:

V listinné podobě na adresu:

Správa železnic, státní organizace

Centrální finanční účtárna Čechy

Náměstí Jana Pernera 217

530 02 Pardubice

V elektronické podobě na adresu:

ePodatelnaCFU@spravazeleznic.cz

Prostřednictvím datové schránky:

uccchjm

6.6. Splatnost každé Výzvy k úhradě se sjednává na 60 kalendářních dnů od jejího doručení Objednateli. V případě, že Výzva k úhradě nebude mít odpovídající náležitosti, je Objednatel oprávněn ve lhůtě splatnosti ji vrátit Zhotoviteli s vytknutím nedostatků, aniž by se dostal do prodlení se splatností. Lhůta splatnosti počíná běžet znovu od okamžiku doručení opravené či doplněné Výzvy k úhradě Objednateli.

6.7. Zhotovitel, poskytovatel zdanitelného plnění, je povinen bezprostředně, nejpozději do 2 pracovních dnů od zjištění svého úpadku, popř. od vydání rozhodnutí správce daně, že je Zhotovitel nespolehlivým plátcem dle § 106a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „***ZDPH***"), oznámit takovou skutečnost prokazatelně Objednateli, příjemci zdanitelného plnění. Porušení této povinnosti je Stranami považováno za podstatné porušení této Smlouvy.

6.8. Zhotovitel se zavazuje, že bankovní účet jím určený pro zaplacení jakéhokoliv závazku Objednatele na základě této Smlouvy bude od data podpisu této Smlouvy do ukončení její platnosti zveřejněn způsobem umožňujícím dálkový přístup ve smyslu § 96 odst. 2 ZDPH, v opačném případě je Zhotovitel povinen sdělit Objednateli jiný bankovní účet řádně zveřejněný ve smyslu § 96 ZDPH.

6.9. Strany se dohodly na tom, že Zhotovitel není oprávněn činit jednostranná započtení svých pohledávek vzniklých na základě této Smlouvy či v souvislosti s ní vůči jakýmkoliv pohledávkám Objednatele. Pohledávky a nároky Zhotovitele vzniklé na základě této Smlouvy či v souvislosti s ní nesmějí být Zhotovitelem postoupeny třetím osobám, zastaveny, nebo s nimi nesmí být jinak disponováno bez předchozího písemného souhlasu Objednatele (zahrnuje i zákaz Zhotovitele postoupit tuto Smlouvu). Jakýkoliv právní úkon učiněný Zhotovitelem v rozporu s tímto ustanovením bude považován za podstatné porušení této Smlouvy.

6.10. Zhotovitel se rovněž zavazuje zajistit řádné a včasné plnění finančních závazků vůči svým Poddodavatelům, prostřednictvím kterých bude realizovat Dílo, resp. jeho část dle této Smlouvy. Za řádné a včasné plnění dle předcházející věty se považuje plné uhrazení Poddodavatelem řádně vystavených faktur za předmět této Smlouvy, resp. jeho část, a to vždy do 60 kalendářních dnů od obdržení platby ze strany Objednatele za konkrétní plnění předmětu této Smlouvy, resp. jeho části.

7. Akceptační řízení

7.1. Akceptačnímu řízení dle části 8 ZOP a tohoto článku této Smlouvy podléhají všechny Fáze F1.1 až F5 dle Přílohy č. 1 této Smlouvy, přičemž každá z těchto Fází je součástí některého z platebních milníků A až B, jak stanoví část 9 Přílohy č. 1 této Smlouvy.

7.2. Fáze plnění F1.1 až F5 dle Přílohy č. 1 této Smlouvy se považují za ukončené akceptací (bez výhrad) posledního dílčího plnění, resp. výstupu uvedeného pro příslušnou Fázi v Příloze č. 1 této Smlouvy. Akceptační kritéria a způsob akceptace Fáze vyplývají z Přílohy č. 1 této Smlouvy.

7.3. Akceptačnímu řízení dle části 8 ZOP a tohoto článku této Smlouvy podléhají rovněž Konzultační služby na vyžádání dle čl. 10 této Smlouvy, které budou realizované na základě Objednávek. Akceptační kritéria budou v tomto případě vyplývat ze specifikace prací uvedených v Objednávce.

7.4. Akceptace Post-implementační a Technické podpory se řídí čl. 8.3 ZOP.

7.5. Posuzování jakýchkoliv Akceptačních kritérií je nutno provádět s ohledem na účel této Smlouvy.

8. Práva duševního vlastnictví

8.1. Pro Software, který je Autorským dílem, platí článek 6.1. ZOP.

9. Školení

9.1. Objednatel požaduje provedení školení ze strany Zhotovitele. Podrobnosti stanoví Příloha č. 1 této Smlouvy.

10. Konzultační služby na vyžádání

10.1. Zhotovitel se zavazuje poskytovat Konzultační služby na vyžádání, které jsou blíže vymezeny v části 8 Přílohy č. 1 této Smlouvy.

10.2. Maximální souhrn Konzultačních služeb na vyžádání činí 150 MD za celou dobu trvání této Smlouvy. Objednatel není povinen Konzultační služby na vyžádání čerpat.

10.3. Objednatel v případě zájmu o provedení prací v rámci Konzultačních služeb na vyžádání

doručí Zhotoviteli objednávku prostřednictvím e-mailu Kontaktních osob uvedených v čl. 12 této Smlouvy se specifikací požadovaných prací, termínem provedení těchto prací a předpokládanou časovou náročností vyjádřenou v MD (dále jen „***Objednávka***").

10.4. Zhotovitel se zavazuje bez zbytečného odkladu projednat s Objednatelem své případné připomínky k Objednávce, přičemž je povinen postupovat v souladu s principy „best practice" a s ohledem na účel této Smlouvy. Objednatel je povinen oprávněné připomínky Zhotovitele zohlednit v obsahu Objednávky.

10.5. V případě, že Zhotovitel (již) nemá žádné oprávněné připomínky k Objednávce, je povinen Objednávku nejpozději do 3 pracovních dnů písemně přijmout prostřednictvím e-mailu Kontaktních osob uvedených v čl. 12 této Smlouvy. Přijetím Objednávky vzniká Zhotoviteli povinnost provést v Objednávce specifikované práce, a to při dodržení stanovených termínů a stanovené časové náročnosti vyjádřené v MD.

10.6. Pro vyloučení všech pochybností Smluvní strany uvádí, že Objednávka nepředstavuje uzavření samostatné dílčí smlouvy na základě rámcové dohody dle § 131 ZZVZ.

10.7. Na provedení prací dle Objednávky a s tím souvisejícího práva a povinnosti Stran se v rozsahu, v jakém je to možné, použijí ustanovení této Smlouvy. Zhotovitel je tak především, nikoliv však výlučně, povinen předložit provedené práce k Akceptačnímu řízení ve smyslu čl. 7 této Smlouvy a poskytnout ve vztahu k těmto pracím Objednateli licenci či jiná práva z duševního vlastnictví v rozsahu v souladu s čl. 8 této Smlouvy.

11. Účast poddodavatelů a realizační tým

11.1. Zhotovitel je oprávněn plnit tuto Smlouvu výlučně prostřednictvím Poddodavatelů uvedených v Příloze č. 5 této Smlouvy – *Poddodavatelé*.

11.2. Před zapojením nového Poddodavatele do plnění této Smlouvy musí být Objednateli předložen nový seznam Poddodavatelů, který bude tvořit Přílohu č. 5 této Smlouvy, a tento seznam musí být Objednatelem písemně schválen. Tím nejsou dotčeny dodatečné podmínky pro změnu Poddodavatele, jehož prostřednictvím Zhotovitel prokazoval kvalifikaci ve Veřejné zakázce, uvedené v části 14 ZOP.

11.3. Seznam členů realizačního týmu je Přílohou č. 8 této Smlouvy. Pravidla pro realizační tým se řídí částí 15 Přílohy č. 6 ZOP.

12. Kontaktní osoby

12.1. Kontaktními osobami za účelem plnění této Smlouvy jsou za Zhotovitele [DOPLNÍ ZHOTOVITEL: titul, jméno, příjmení, telefon a e-mail].

12.2. Kontaktními osobami za účelem plnění této Smlouvy jsou za Objednatele [DOPLNÍ OBJEDNATEL: titul, jméno, příjmení, služební telefon a služební e-mail].

12.3. Kontaktní osobou Objednatele pro oblast kybernetické bezpečnosti je [DOPLNÍ OBJEDNATEL: titul, jméno, příjmení, služební telefon a služební e-mail].

13. Smluvní pokuty

13.1. Cenou pro účely stanovení výše smluvních pokut dle části 17 ZOP, části 21 ZOP a části 20 OOP se rozumí Cena díla ve smyslu čl. 5.1 této Smlouvy, není-li výslovně stanoveno jinak.

14. Servicedesk

14.1. Zhotovitel bude poskytovat Servicedesk v režimu 4 ve smyslu čl. 10.3. ZOP.

15. Servisní model

15.1. Zhotovitel bude poskytovat servisní model v režimu C2 ve smyslu čl. 12.2. ZOP. Nezvolí-li Objednatel výslovně v rámci Požadavku jinou kategorii, jedná se o požadavek kategorie B.

16. Kybernetická bezpečnost

16.1. Zhotovitel je povinen dodržovat ustanovení týkající se kybernetické bezpečnosti ve smyslu článku 21. ZOP.

17. Ochrana osobních údajů

17.1. Pokud bude v rámci plnění této Smlouvy docházet ke zpracování osobních údajů, zavazuje se Zhotovitel dodržovat opatření dle článku 22. ZOP.

18. Ochrana důvěrných informací

18.1. Zhotovitel se zavazuje k ochraně důvěrných informací dle části 23 ZOP.

19. Střet zájmů, povinnosti Zhotovitele v souvislosti s konfliktem na Ukrajině

19.1. Zhotovitel prohlašuje, že není obchodní společností, ve které veřejný funkcionář uvedený v ust. § 2 odst. 1 písm. c) zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů (dále jen „***Zákon o střetu zájmů***") nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti, a že žádní poddodavatelé, jimiž prokazoval kvalifikaci v zadávacím řízení na zadání Veřejné zakázky, nejsou obchodní společností, ve které veřejný funkcionář uvedený v ust. § 2 odst. 1 písm. c) Zákona o střetu zájmů nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti.

19.2. Zhotovitel prohlašuje, že:

a. on, ani žádný z jeho poddodavatelů, nejsou osobami, na něž se vztahuje zákaz zadání veřejné zakázky ve smyslu § 48a zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů,

b. on, ani žádný z jeho poddodavatelů nebo jiných osob, jejichž způsobilost byla využita ve smyslu evropských směrnic o zadávání veřejných zakázek, nejsou osobami dle článku 5k nařízení Rady (EU) č. 833/2014 ze dne 31. července 2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, ve znění pozdějších předpisů, jimž se zakazuje zadat nebo dále plnit jakoukoli veřejnou zakázku nebo koncesní smlouvu spadající do oblasti působnosti směrnic o zadávání veřejných zakázek, jakož i čl. 10 odst. 1, 3, odst. 6 písm. a) až e), odst. 8, 9 a 10, článků 11, 12, 13 a 14 směrnice 2014/23/EU, článku 7 písm. a) až d), článku 8, čl. 10 písm. b) až f) a písm. h) až j) směrnice 2014/24/EU, článku 18, čl. 21 písm. b) až e) a písm. g) až i), článků 29 a 30 směrnice 2014/25/EU a čl. 13 písm. a) až d), f) až h) a j) směrnice 2009/81/ES a hlavy VII nařízení Evropského parlamentu a Rady (EU, Euratom) 2018/1046,

c. on, ani žádný z jeho poddodavatelů nebo jiných osob, jejichž způsobilost byla využita ve smyslu evropských směrnic o zadávání veřejných zakázek, nejsou osobami dle článku 2 nařízení Rady (EU) č. 269/2014 ze dne 17. března 2014, o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, ve znění pozdějších předpisů, a dalších prováděcích předpisů k tomuto nařízení Rady (EU) č. 269/2014 anebo osobami dle čl. 2 nařízení uvedených v odstavci 19.5 této Smlouvy (dále jen „***Sankční seznamy***").

19.3. Je-li Zhotovitelem sdružení více osob, platí podmínky dle odstavce 19.1 a 19.2 této Smlouvy také jednotlivě pro všechny osoby v rámci Zhotovitele sdružené, a to bez ohledu na právní formu tohoto sdružení.

19.4. Přestane-li Zhotovitel nebo některý z jeho poddodavatelů nebo jiných osob, jejichž způsobilost byla využita ve smyslu evropských směrnic o zadávání veřejných zakázek, splňovat podmínky dle tohoto článku Smlouvy, oznámí tuto skutečnost bez zbytečného odkladu, nejpozději však do 3 pracovních dnů ode dne, kdy přestal splňovat výše uvedené podmínky, Objednateli.

19.5. Zhotovitel se dále zavazuje postupovat při plnění této Smlouvy v souladu s nařízením Rady (ES) č. 765/2006 ze dne 18. května 2006 o omezujících opatřeních vzhledem k situaci v Bělorusku a k zapojení Běloruska do ruské agrese proti Ukrajině, ve znění pozdějších předpisů, ve znění pozdějších předpisů, nařízením Rady (EU) č. 208/2014 ze dne 5. března 2014 o omezujících opatřeních vůči některým osobám, subjektům a orgánům vzhledem k situaci na Ukrajině, ve znění pozdějších předpisů, a dalších prováděcích předpisů k těmto nařízením.

19.6. Zhotovitel se dále zavazuje, že finanční prostředky ani hospodářské zdroje, které obdrží

od Objednatele na základě této Smlouvy a jejích případných dodatků, nezpřístupní přímo ani nepřímo fyzickým nebo právnickým osobám, subjektům či orgánům s nimi spojeným uvedeným v Sankčních seznamech, nebo v jejich prospěch.

19.7. Ukáže-li se jakékoliv prohlášení Zhotovitele dle tohoto článku Smlouvy jako nepravdivé nebo poruší-li Zhotovitel svou oznamovací povinnost nebo některou z dalších povinností dle tohoto článku Smlouvy, je Objednatel oprávněn odstoupit od této Smlouvy. Zhotovitel je dále povinen zaplatit za každé jednotlivé porušení povinností dle předchozí věty smluvní pokutu ve výši 5 % procent z Ceny. Ustanovení § 2004 odst. 2 Občanského zákoníku se nepoužije.

20. Compliance

20.1. Smluvní strany stvrzují, že při uzavírání této Smlouvy jednaly a postupovaly čestně a transparentně a zavazují se tak jednat i při plnění této Smlouvy a veškerých činnostech s ní souvisejících. Každá ze Smluvních stran se zavazuje jednat v souladu se zásadami, hodnotami a cíli compliance programů a etických hodnot druhé Smluvní strany, pakliže těmito dokumenty dotčené Smluvní strany disponují, a jsou uveřejněny na webových stránkách Smluvních stran.

20.2. Správa železnic, státní organizace, má výše uvedené dokumenty k dispozici na webových stránkách: https://www.spravazeleznic.cz/o-nas/nezadouci-jednani-a-boj-s-korupci.

20.3. Zhotovitel má výše uvedené dokumenty k dispozici na webových stránkách: [doplní Zhotovitel x nemá-li Zhotovitel výše uvedené dokumenty, celý bod 20.3 odstraní].

21. Přímé platby poddodavatelům

21.1. Zhotovitel je povinen uhradit své závazky vůči poddodavatelům ve sjednané výši za sjednaných podmínek.

21.2. Objednatel si v souladu s § 106 ZZVZ vyhrazuje možnost úhrady splatných částek odpovídajícím plněním poskytnutých ze strany poddodavatele, a to na základě písemné žádosti poddodavatele, jestliže je Zhotovitel v prodlení s úhradou příslušné částky poddodavateli po dobu nejméně 30 dnů.

21.3. Poddodavatel může Objednatele požádat o úhradu splatné částky pouze za takové plnění, které již bylo poskytnuto.

21.4. Přímá platba poddodavateli bude Objednatelem provedena na základě oznámení vystaveného poddodavatelem Objednateli, které bude obsahovat informaci o výši částky, která má být přímo uhrazena poddodavateli (dále jen „**částka k úhradě**“) a podloženou kopii faktury vystavené poddodavatelem Zhotoviteli se všemi zákonem požadovanými náležitostmi. Nedílnou součástí faktury bude i kopie dokladu o existujícím závazku mezi Zhotovitelem a poddodavatelem, výše sjednané ceny (případně cen dílčích plnění) ve vazbě na plnění předmětu této Smlouvy a informace o tom, kdy byla částka, kterou měl Zhotovitel poddodavateli uhradit, splatná.

21.5. Částka k úhradě nesmí být vyšší než částka odpovídající skutečně poskytnutému plnění.

21.6. Objednatel informuje Zhotovitele bez zbytečného odkladu o skutečnosti, že obdržel oznámení poddodavatele k přímé úhradě poddodavateli. V případě, že Zhotovitel do 10 dnů ode dne obdržení této informace od Objednatele neprokáže, že tvrzení uváděná poddodavatelem v žádosti o přímou platbu jsou nesprávná, má se za to, že s provedením přímé úhrady poddodavateli souhlasí.

21.7. Splatnost částky k úhradě činí 60 dnů ode dne doručení žádosti poddodavatele k přímé úhradě. Objednatel je oprávněn před uplynutím lhůty splatnosti vrátit oznámení, které neobsahuje požadované náležitosti nebo obsahuje nesprávné údaje. Objednatel je rovněž oprávněn vrátit poddodavateli oznámení v případě, že Zhotovitel prokázal, že tvrzení poddodavatele uvedená v oznámení jsou nesprávná. Oprávněným vrácením oznámení přestává běžet lhůta splatnosti.

21.8. V případě, že částka k úhradě již byla uhrazena Zhotoviteli, Objednatel ji uhradí poddodavateli, a následně bude o částku k úhradě snížena celková odměna Zhotovitele, a to formou započtení proti pohledávce nebo pohledávkám Zhotovitele vzniklých na základě

plnění této Smlouvy. O zápočtu proti pohledávce Zhotovitele musí Objednatel Zhotovitele písemně informovat. Není-li již budoucí platba, kterou by Objednatel mohl započíst proti své pohledávce vůči Zhotoviteli, představuje částka k úhradě výši smluvní pokuty za nesplnění povinnosti dle čl. 21.1 této Smlouvy a Zhotovitel se zavazuje tuto smluvní pokutu uhradit nejpozději do 15 dnů ode dne doručení výzvy k zaplacení.

22. Další povinnosti Zhotovitele

22.1. Zhotovitel je povinen uchovat veškerou dokumentaci související s plněním této Smlouvy na veřejnou zakázku včetně účetních dokladů minimálně do 31. 12. 2035.

22.2. Zhotovitel je povinen minimálně do 31. 12. 2035 poskytovat požadované informace a dokumentaci související s plněním této Smlouvy zaměstnancům nebo zmocněncům pověřených orgánů (Centra, Ministerstvo pro místní rozvoj ČR, Ministerstvo financí ČR, Evropská komise, Evropský účetní dvůr, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout ji při provádění kontroly součinnost.

22.3. Zhotovitel je povinen při plnění předmětu plnění této Smlouvy dodržovat pracovněprávní předpisy, a to zejména, nikoliv však výlučně, předpisy upravující mzdy zaměstnanců, pracovní dobu, dobu odpočinku mezi směnami, placené přesčasy, bezpečnost práce apod. Zhotovitel je dále povinen zajistit férové pracovní podmínky a odpovídající úroveň bezpečnosti práce pro všechny osoby podílející se na plnění této Smlouvy. Zhotovitel se zavazuje výše uvedené zajistit i u svých poddodavatelů.

22.4. Plnění povinností dle čl. 22.3 této Smlouvy je Zhotovitel povinen prokázat kdykoli do 5 pracovních dnů od doručení písemné výzvy Objednatele, a to prostřednictvím všech potřebných dokladů dle aktuálních právních předpisů, resp. též s příslušnými výstupy ze mzdového a účetního systému Zhotovitele.

22.5. Zhotovitel je povinen udržovat v platnosti po celou dobu trvání této Smlouvy pojistnou smlouvu, jejímž předmětem bude pojištění odpovědnosti za újmu způsobenou Zhotovitelem Objednateli nebo jakékoliv třetí osobě při provádění Plnění dle této Smlouvy s limitem pojistného plnění minimálně 50 000 000,- Kč za jednu pojistnou událost, přičemž maximální spoluúčast Zhotovitele může činit deset procent (10 %) nebo 1 000 000,- Kč z pojistného plnění. Zhotovitel je povinen o takovém pojištění předložit Objednateli doklady a na jeho žádost prokazovat, že jej udržuje v platnosti. Ve vztahu k pojištění dle tohoto článku se Zhotovitel zavazuje zajistit, že v případě vzniku pojistné události bude pojistné plnění placeno přímo Objednateli, a to až v plné výši pojistné částky dle tohoto článku Smlouvy.

22.6. Zhotovitel je povinen za každý den, po který není pojištěn, zaplatit Objednateli smluvní pokutu ve výši 10 000,- Kč. V případě, že doba, po kterou nebyl Zhotovitel pojištěn, překročila po dobu trvání smlouvu více jak 30 kalendářních dnů, je Objednatel oprávněn odstoupit od Smlouvy.

23. Závěrečná ustanovení

23.1. Smluvní strany berou na vědomí, že tato Smlouva podléhá uveřejnění v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, ve znění pozdějších předpisů (dále jen „***ZRS***"), a současně souhlasí se zveřejněním údajů o identifikaci Smluvních stran, předmětu Smlouvy, jeho ceně či hodnotě a datu uzavření této Smlouvy.

23.2. Zaslání Smlouvy správci registru smluv k uveřejnění v registru smluv zajišťuje obvykle Objednatel. Nebude-li tato Smlouva zaslána k uveřejnění a/nebo uveřejněna prostřednictvím registru smluv, není žádná ze Smluvních stran oprávněna požadovat po druhé Smluvní straně náhradu škody ani jiné újmy, která by jí v této souvislosti vznikla nebo vzniknout mohla.

23.3. Smluvní strany výslovně prohlašují, že údaje a další skutečnosti uvedené v této Smlouvě, vyjma částí označených ve smyslu následujícího odstavce této Smlouvy, nepovažují za obchodní tajemství ve smyslu ustanovení § 504 Občanského zákoníku (dále jen „***obchodní tajemství***"), a že se nejedná ani o informace, které nemohou být v registru smluv

uveřejněny na základě ustanovení § 3 odst. 1 ZRS.

23.4. Jestliže Smluvní strana označí za své obchodní tajemství část obsahu Smlouvy, která v důsledku toho bude pro účely uveřejnění Smlouvy v registru smluv znečitelněna, nese tato Smluvní strana odpovědnost, pokud by Smlouva v důsledku takového označení byla uveřejněna způsobem odporujícím ZRS, a to bez ohledu na to, která ze stran Smlouvu v registru smluv uveřejnila. S částmi Smlouvy, které druhá Smluvní strana neoznačí za své obchodní tajemství před uzavřením této Smlouvy, nebude Objednatel jako s obchodním tajemstvím nakládat a ani odpovídat za případnou škodu či jinou újmu takovým postupem vzniklou. Označením obchodního tajemství ve smyslu předchozí věty se rozumí doručení písemného oznámení druhé Smluvní strany Objednateli obsahujícího přesnou identifikaci dotčených částí Smlouvy včetně odůvodnění, proč jsou za obchodní tajemství považovány. Druhá Smluvní strana je povinna výslovně uvést, že informace, které označila jako své obchodní tajemství, naplňují současně všechny definiční znaky obchodního tajemství, tak jak je vymezeno v ustanovení § 504 občanského zákoníku, a zavazuje se neprodleně písemně sdělit Objednateli skutečnost, že takto označené informace přestaly naplňovat znaky obchodního tajemství.

23.5. Osoby uzavírající tuto Smlouvu za Smluvní strany souhlasí s uveřejněním svých osobních údajů, které jsou uvedeny v této Smlouvě, spolu se Smlouvou v registru smluv. Tento souhlas je udělen na dobu neurčitou.

23.6. Ustanovení Přílohy č. 1 *Bližší specifikace předmětu plnění* a Přílohy č. 2 *Technická specifikace* mají přednost před zněním Přílohy č. 4 *Platforma SŽ* (včetně jejích příloh). Ustanovení Přílohy č. 1 *Bližší specifikace předmětu plnění*, Přílohy č. 2 *Technická specifikace* a Přílohy č. 4 *Platforma SŽ* (včetně jejích příloh) mají přednost před ustanoveními obchodních podmínek uvedených v odst. 23.7. tohoto článku.

23.7. Smlouva se řídí Obchodními podmínkami Objednatele a Zvláštními obchodními podmínkami Objednatele. Ustanovení Zvláštních obchodních podmínek mají přednost před ustanoveními Obchodních podmínek, pokud jsou ustanovení těchto dokumentů v rozporu, uplatní se ustanovení uvedené ve Zvláštních obchodních podmínkách.

23.8. Odchylná ujednání v této Smlouvě mají přednost před ustanoveními jejích příloh vč. Obchodních podmínek a Zvláštních obchodních podmínek.

23.9. Tuto Smlouvu lze měnit pouze písemnými dodatky.

23.10. Tato Smlouva nabývá platnosti okamžikem podpisu poslední ze Stran. Je-li Smlouva uveřejňována v registru smluv, nabývá účinnosti dnem uveřejnění v registru smluv, jinak je účinná od okamžiku uzavření.

23.11. Tato Smlouva je vyhotovena v *elektronické* podobě, přičemž obě Smluvní strany obdrží její elektronický originál opatřený elektronickými podpisy. V případě, že tato Smlouva z jakéhokoli důvodu nebude vyhotovena v elektronické podobě, bude sepsána ve třech vyhotoveních, přičemž jedno vyhotovení obdrží Zhotovitel a dvě vyhotovení Objednatel.

23.12. Nedílnou součástí této Smlouvy jsou její přílohy:

Příloha č. 1	Bližší specifikace předmětu plnění
Příloha č. 2	Technická specifikace
Příloha č. 3	Ceník
Příloha č. 4	Platforma SŽ (včetně jejích příloh)
Příloha č. 5	Poddodavatelé
Příloha č. 6	Zvláštní obchodní podmínky k ICT zakázkám
Příloha č. 7	Obchodní podmínky
Příloha č. 8	Seznam členů realizačního týmu
Příloha č. 9	Harmonogram plnění
Příloha č. 10	Informace k systémům SŽ

Za Objednatele:

……

Ing. Mojmír Nejezchleb
zástupce pověřený správní radou
řízením organizace

……

Ing. Tomáš Čoček, Ph.D.
náměstek generálního ředitele
pro ekonomiku

Za Zhotovitele:

……

[DOPLNÍ ZHOTOVITEL]

Klasifikace: Veřejný dokument

SPRÁVA ŽELEZNIC

Příloha č. 1 smlouvy – Bližší specifikace předmětu plnění

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČ: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

Obsah

1 Seznam zkratek

Níže uvedená tabulka obsahuje seznam zkratek a pojmů použitých v rámci této Bližší specifikace předmětu plnění.

Přehled zkratek a pojmů:

Zkratka	Popis
AD	*(Active Directory)* Rozšiřitelná a škálovatelná adresářová služba, která umožňuje efektivně uspořádat síťové prostředky. Kromě informací o objektech v počítačové síti (uživatelské účty, počítače, tiskárny) umožňuje používat stromovou strukturu objektů, nastavovat globálně systémové politiky, instalovat programy na počítače nebo aplikovat kritické aktualizace v celé organizační struktuře. Má úzkou vazbu na DNS.
BÚ	Bezpečné úložiště
Data Vault	Datový trezor - bezpečnostní a archivační technologie, která vytváří ochráněné, neměnné a oddělené úložiště pro dlouhodobé uchování dat.
DNS	*(Domain Name System)* je distribuovaný hierarchický jmenný systém používaný v síti Internet. Překládá názvy domén na číselné IP adresy a zpět, obsahuje informace o tom, které stroje poskytují příslušnou službu.
DR	*(Disaster Recovery)* je soubor technologií, postupů a plánů, jejichž cílem je obnovit IT systémy, data a provoz organizace po závažné události, která způsobí přerušení běžného fungování IT.
EOS	*(End of Sale)* Datum ukončení prodeje.
EOL	*(End of Life)* Datum konce životnosti produktu.
Failover	Failover představuje proces, kdy v případě výpadku primárního prvku dochází k přesměrování provozu na záložní prvek.
GDPR	*(General Data Protection Regulation)* znamená nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).
HA	*(High Availability)* je vysoká dostupnost služeb. Předpokladem řešení je použití dvou a více nezávislých zařízení s cílem zajistit funkčnost v případě výpadku.

HTTPS	*(Hypertext Transfer Protocol Secure)* je šifrovaný protokol pro zabezpečenou komunikaci na webu.
HW	Hardware – znamená veškeré hmotné součásti počítačových systémů a veškeré související vybavení hmotné povahy spolu se vším příslušenstvím, a včetně veškeré související dokumentace.
IDS	*(Intrusion Detection System)* Systém detekce průniku používaný v NGFW.
IdM	*(Identity Management)* - řízení digitálních identit uživatelů a jejich přístupových oprávnění v IT systémech organizace
IPFabric	Nástroj pro automatizovanou analýzu a vizualizaci síťové infrastruktury, využívaný pro audit, návrh a správu sítí.
IPS	*(Intrusion Prevention System)* Systém prevence průniku používaný v NGFW.
IROP	Integrovaný regionální operační program.
Malware	Software vytvořený k poškození nebo neoprávněnému přístupu.
MD	*Man-day* – znamená člověkoden. Nestanoví-li Smlouva jinak, odpovídá jeden MD 8 MH (člověkohodinám).
NGFW	*(Next-Generation Firewall)* Oproti běžným FW nabízí také doplňkové funkce jako AVC, AMP, IPS, IDS, DPI, DLP, TD, IdM a dešifrování a kontrolu TLS/SSL obsahu.
NÚKIB	*Národní úřad pro kybernetickou a informační bezpečnost*
PAM	*(Privileged Access Management)* je řízení privilegovaných účtů a oprávnění, které zajišťuje, že administrátorský přístup je používán pouze oprávněně, dočasně, kontrolovaně a auditovatelně
RPO	*Recovery Point Objective (RPO)* je parametr, který vyjadřuje maximální ztrátu dat uživatelů při havárii systému a následné obnově.
RTO	*Recovery Time Objective (RTO)* - je parametr, který vyjadřuje dobu nutnou k obnově chodu služby do akceptované úrovně provozu.
SIEM	*(Security Information and Event Management)* Řešení zabezpečení, které organizacím pomáhá detekovat hrozby, analyzovat je a reagovat na ně dříve, než způsobí škody v provozu firmy/organizace.
SNMP	*(Simple Network Management Protocol)* protokol pro vzdálené monitorování a správu síťových zařízení.

SW	*Software* – má význam dle čl. 1.64 ZOP (tj. veškeré programové vybavení a další Autorská díla, stejně jako další věci či jiné majetkové hodnoty, které s programovým vybavením souvisí a jsou určeny ke společnému užívání s tímto programovým vybavením, tj. zejména Databáze, GUI, zvukové nahrávky, videa, obrázky, fotografie apod., včetně veškeré související dokumentace a updatů a upgradů tohoto programového vybavení, avšak s výjimkou Hardwaru a Databází).
Syslog	Protokol pro sběr a přenos systémových a bezpečnostních logů ze zařízení do centrálního systému.
SŽT	Správa železniční telematiky
TLS	*(Transport Layer Security)* protokol pro šifrovanou komunikaci v počítačových sítích.
VoKB	Vyhláška č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, v platném znění.
VPN	*(Virtual Private Network)* Virtuální privátní síť – prostředek pro důvěryhodné propojení komponent informačního systému v rámci obecně nezabezpečené komunikační sítě. Při navazování spojení je obvykle vyžadována autentizace, komunikace je většinou šifrována.
ZoKB	Zákon č. 264/2025 Sb., o kybernetické bezpečnosti, v platném znění.
ZOP	*(Zvláštní obchodní podmínky pro Zakázky v oblasti ICT)* - specifická ujednání doplňující nebo měnící všeobecné obchodní podmínky, která se vztahují k určitým produktům, službám nebo situacím.

2 Úvod

Tento dokument je přílohou a nedílnou součástí smlouvy na realizaci veřejné zakázky s názvem „Realizace systému Zabezpečeného úložiště v prostředí Správy železnic" (dále jen „**veřejná zakázka**"), pro organizaci Správa železnic, státní organizace (dále jen „**SŽ**" nebo „**Zadavatel**"). Dokument popisuje technické a jiné požadavky na veřejnou zakázku.

3 Záměr SŽ v oblasti bezpečného úložiště

SŽ v roli poskytovatele regulované služby v režimu vyšších povinností dle ZoKB, je povinna zajistit systematický postup pro správu, ukládání a archivaci důležitých dat napříč vybranými informačními systémy a technologiemi, a to za účelem zajištění odpovídající úrovně kybernetické bezpečnosti.

3.1 Současný stav

Data jednotlivých informačních a komunikačních systémů jsou nyní ukládána lokálně, a to v různých regionech v ČR. To má za následek rozdílné podmínky zajištění jejich fyzické i kybernetické bezpečnosti v závislosti na možnostech konkrétní lokality. Každá z lokalit poskytuje jinou úroveň ochrany v kategoriích fyzického přístupu k systémům, ochrany dat před škodlivým kódem, přístupu k datům, environmentální ochrany, či proti neočekávanému přerušení dodávek energie. Veškeré zálohy dat jsou dále ukládány na páskové technologie, což přináší velkou provozní náročnost.

3.2 Cílový stav

Bezpečné datové úložiště bude navrženo tak, aby splnilo následující klíčové cíle:

- **On-premises:** Celé řešení bezpečného úložiště musí být provozováno v on-premises prostředí SŽ, tedy výhradně v rámci její vlastní infrastruktury. Žádná data nesmí opustit perimetr interní sítě, a to včetně ukládání nebo přenosu do veřejného cloudu či jiných externích služeb.
- **Bezpečné řízení přístupu:** Centralizovaná správa přístupů a autentizace k uloženým datům – přístupy budou jednotně řízeny a auditovány, aby byla zajištěna důsledná kontrola nad tím, kdo může s daty nakládat.
- **Ochrana a šifrování dat:** Zabezpečené ukládání dat s využitím silného šifrování a bezpečné správy klíčů. Bude využit Hardware Security Module (HSM) Zadavatele, pro ukládání a správu kryptografických klíčů, aby uložená data nebyla možná číst bez autorizace. Pro ukládání a správu kryptografických klíčů bude využit Hardware Security Module (HSM) Zadavatele, aby uložená data nebylo možné číst bez autorizace.

- **Odolnost vůči incidentům:** Infrastruktura úložiště bude navržena pro vysokou odolnost (disaster recovery). Bude zahrnovat redundantní napájení, monitorování provozních stavů a prostředí a další prvky fyzické i logické ochrany, aby byl zajištěn nepřetržitý provoz i při mimořádných událostech.
- **Izolace citlivých dat:** Bezpečné úložiště bude umožňovat vytvoření bezpečnostních zón podle důležitosti a citlivosti dat, která jsou v nich uložena. Takovéto rozdělení omezuje možnost neoprávněného přístupu k citlivým datům a chrání před pokusy o jejich kompromitaci.
- **Prevence šíření útoků:** V případě úspěšného proniknutí do jedné zóny s daty, zůstanou ostatní uložená data izolována a chráněna díky předem definovaným přístupovým a retenčním pravidlům. To znamená, že útočník nemůže snadno přejít k dalším uloženým datům a pokračovat v útoku. Zóning úložiště tímto způsobem výrazně omezuje dopad bezpečnostního incidentu a zkracuje čas potřebný k reakci na útok.
- **Zjednodušení zálohovací operativy:** Dílčí cíl projektu je snížení počtu zálohovacích páskových mechanik a jejich využití pouze pro vybrané systémy, které vyžadují dlouhodobou archivaci dat.
- **Soulad s legislativou a standardy:** Řešení bude v souladu s požadavky na ochranu kritické infrastruktury, kybernetickou bezpečnost a ochranu osobních údajů a bude splňovat požadavky ZoKB, VoKB a souvisejících předpisů v platném znění. Zároveň bude zajištěn soulad s požadavky NÚKIB a implementována odpovídající bezpečnostní opatření, zejména v oblasti správy identit, řízení přístupů, kryptografie, fyzické bezpečnosti a dostupnosti informací. Dále bude brán zřetel na doporučení mezinárodních standardů (např. ISO/IEC 27001, NIST CSF) a osvědčené postupy.

4 Předmět plnění veřejné zakázky

Předmětem plnění této veřejné zakázky je realizace zákonné povinnosti Zadavatele, a to posílením fyzické a kybernetické bezpečnosti a ochranou aktiv proti kybernetickým hrozbám prostřednictvím dodávky technologie pro centralizované bezpečné datové úložiště (dále také jen „**BÚ**“), implementace a konfigurace dodané technologie, odborné školení správy a údržby dodané technologie pro vybrané odborné pracovníky Zadavatele. Očekávaným výstupem, kromě dodávky hardwaru samotného bezpečného úložiště a souvisejících síťových a dalších komponent (viz. kapitola 5.3 tohoto dokumentu), je také vytvoření koncepce Bezpečného úložiště. Ta zahrnuje nejen analytickou část (viz. kapitola 5.1 tohoto dokumentu), ale i zpracování detailního návrhu projektového implementačního postupu konfiguračních prací pro vybrané systémy (viz. kapitola 5.2 tohoto dokumentu), u kterých je nutné data ukládat do BÚ. Tento návrh bude sloužit jako implementační vzor, který následně Zadavatel případně použije při implementaci na další systémy v budoucnu.

Implementační postup vytvořený v rámci plnění této veřejné zakázky bude realizován na systémech vybraných pro napojení do BÚ. Technická specifikace těchto systémů bude výstupem analytické části plnění této zakázky. Dokument „Implementační plán Bezpečného úložiště" potom představuje souhrnný dokument, jehož cílem je definovat harmonogram a metodiku zavádění technologie BÚ do jednotlivých systémů. Součástí Implementačního plánu je i podrobný implementační postup konfigurace datových úložišť a síťových prvků, který popisuje konkrétní technické kroky nutné k dosažení cílového stavu, včetně návrhu síťových pravidel, topologie a definování retenčních politik.

Projekt bezpečného úložiště musí zohledňovat požadavky na snadnou správu a efektivní řešení případných bezpečnostních incidentů a ochranu před útoky, a to nejen z vnějšího prostředí, ale také v případě interních hrozeb.

5 Požadavky na plnění

Plnění veřejné zakázky se skládá z níže uvedených částí:

- Datový management vybraných systémů:
  - Analýza současného stavu data managementu
  - Návrh na změnu data managementu
- Implementační plán Bezpečného úložiště vč. Exit strategie
- Dodávka a implementace Bezpečného úložiště do primární a sekundární lokality
- Konfigurace Bezpečného úložiště
- Napojením na vybrané systémy
- Post-implementační testování
- Školení, dokumentace
- Post-implementační a Technická podpora
- Konzultační služby na vyžádání

5.1 Datový management vybraných systémů

Cílem je zhodnotit stávající nakládání s daty vybraných 24 systémů, způsob jejich zálohování a životní cyklus. Pro potřeby tohoto zhodnocení poskytne Zadavatel Dodavateli níže uvedené podklady. Dodavatel na základě uvedených podkladů a případně dodatečně vyžádaných podkladů zpracuje finální výstup popisující současný stav a návrh budoucích postupů k realizaci ukládání dat do bezpečného úložiště.

5.1.1 Analýza současného stavu data managementu

Podklady dodané Zadavatelem budou sloužit jako primární vstup do analýzy. Je však třeba počítat s tím, že některé dokumenty budou vyžadovat doplnění informací dodavateli vybraných systémů Zadavatele v průběhu analýzy. Některé informace mohou být dostupné pouze v omezeném rozsahu.

V rámci zahájení analýzy Zadavatel předpokládá realizaci workshopu s Dodavatelem a s IT pracovníky Zadavatele pro vytěžení potřebných informací pro analýzu.

Po celou dobu trvání analýzy Zadavatel určí pracovníka SŽT odpovědného za koordinaci součinnosti, který bude zastávat roli hlavního kontaktního bodu pro Dodavatele.

Tento pracovník bude podle potřeby zajišťovat komunikaci s dalšími odbornými rolemi Zadavatele (např. správci infrastruktury, bezpečnostní specialisté apod.).

Oblast	**Činnost**

Podklady Zadavatele	• Podklady k vybraným systémům:
	  ○ Seznam vybraných 24 systémů pro projekt BÚ.
	  ○ Výstupy ze současných zálohovacích nástrojů.
	  ○ Základní schémata topologie sítě sloužící pro zálohování dat.
	  ○ Současný zálohovací plán vybraných 24 systémů.
	• Určení konkrétních lokalit pro umístění BÚ v regionu Praha a Plzeň.

Výstupy Dodavatele	• Zhodnocení koncepce stávajícího zálohovacího plánu vybraných 24 systémů a návrh opatření pro optimalizaci a standardizaci dle požadavků Zadavatele a ZoKB a VoKB. • Analytický výstup popisující přístup řešení dále uvedených oblastí v prostředí SŽ (definování postupu kroků v rámci BÚ, specifikace postupu vlastní konfigurace, stanovení pořadí migrace dat jednotlivých systémů, přístup k migraci, definice rizik a jejich mitigace). Součástí analytického výstupu je i architektura systému, struktura dat, databázová technologie, objem dat, časové přírůstky, retenční politiky, současné zálohovací scénáře, řízení přístupu k datům, logování.

Výstup této části „Analýza současného stavu data managementu" bude Dodavatelem použit jako vstupní podklad pro vytvoření „Návrhu na změnu data managementu" a bude součástí dokumentu „Koncepce Bezpečného úložiště".

5.1.2 Návrh na změnu data managementu

Předmětem této části je návrh architektury úložiště a celého projektu BÚ, včetně definice pravidel pro nakládání s daty vybraných systémů a transformace stávajícího data managementu z technicky orientovaného, fragmentovaného přístupu na řízený, bezpečný a auditovatelný model.

Výstupem bude dokument obsahující analytickou část z kapitoly *5.1.1*, včetně popisu nakládání s daty v datových úložištích, bezpečnostních a komunikačních pravidel, pravidel přístupu k datům, principů šifrování dat, plánů obnovy dat a technických detailů řešení dle níže uvedených požadavků. Dokument jako celek posune data management z čistě technického provozu na strategicky řízenou disciplínu podporující výkon agend, bezpečnost informací a regulatorní compliance.

Oblast	**Činnost**
Návrh změny data managementu	**Výstup Dodavatele** • Návrh opatření pro optimalizaci zálohovacích plánů pro 24 vybraných systémů. • Návrh řízení dat jako aktiva. • Návrh životního cyklu dat. • Návrh tieringu a retence dat. • Návrh přístupu Zero Trust a princip nejmenších oprávnění, definice rolí. • Návrh opatření pro bezpečnost a neměnnost dat. • Kontrola splnění regulatorních požadavků ZoKB (dle relevance). • Návrh automatizace práce s daty, automatizace obnovy.

Výstupem výše uvedených požadavků bude samostatný dokument s názvem „Koncepce Bezpečného úložiště".

5.2 Implementační plán Bezpečného úložiště

Na základě úvodní části *5.1.1 Analýza současného stavu data managementu* a *5.1.2 Návrh na změnu data managementu* dojde k přípravě implementačních kroků pro realizaci vlastního BÚ ve spolupráci s provozními složkami Zadavatele. Součástí plánu bude vytvoření testovacích scénářů pro ověření funkčnosti nastavených pravidel pro zálohování a obnovu vybraných testovacích dat. Verifikace bude provedena v rámci akceptace fáze Zadavatelem.

Oblast	**Činnost**

Implementační plán	**Výstup Dodavatele** • Upřesněný časový harmonogram implementace BÚ s definováním odpovědných osob a součinností Zadavatele. • Definice, popis a rozdělení úkolů a odpovědností mezi členy týmu Dodavatele a SŽ. • Plán nastavení datových úložišť. • Pořadí konfigurace jednotlivých úložišť. • Plán nastavení implementačních postupů. • Postup pro konfiguraci prvků BÚ a síťových zařízení (přepínače, směrovače, firewally). • Plán napojení dat vybraných 24 systémů do BÚ. • Plán validací přenesených dat proti zdroji. • Implementační plán musí navazovat a být v souladu s harmonogramem předloženým Zadavatelem. • Exit strategie dle kapitoly 6.3.
Základní specifikace architektury	**Výstup Dodavatele** • High-level schéma architektury BÚ (např. Archimate, MS Visio) • Schéma fyzického zapojení obou lokalit bezpečných úložišť. • Popis jednotlivých komponent. • Definice segmentačních pravidel (zóningu) dle jednotlivých druhů dat. • Návrh propojení mezi primární a sekundární lokalitou včetně definice bezpečnostních a šifrovacích protokolů.
Vytvoření plánu rozmístění technologií BÚ	**Výstup Dodavatele** • Vytvoření plánu zapojení datové a elektrické kabeláže. • Vytvoření plánu umístění jednotlivých prvků v datovém rozvaděči.
Nastavení síťového prostředí SŽ	**Výstup Zadavatele** • Návrh síťového propojení obou lokalit. • Definice oprávněných osob a přístupových účtů (role a oprávnění, technické a uživatelské účty). • Specifikace a nastavení směrování mezi síťovými segmenty.

	• Specifikace implementace bezpečnostních politik pro komunikaci s BÚ na základě podkladů od Dodavatele.
Příprava kontrolních a testovacích scénářů	**Výstup Dodavatele** Kontrolní a testovací scénáře musí pokrývat uvedené oblasti: • Fyzická kontrola a diagnostika, HW diagnostika výrobce. • Kontrola verzí firmware a aktualizace na doporučené (ne nejnovější!) verze. • Testy vysoké dostupnosti technologií úložišť (High Availability/Failover). • Příprava testovacích dat pro výkonnostní a bezpečnostní testy. • Výkonnostní testy (IOPS, propustnost, latence). • Funkční testy (testy připojení a protokolů, testy snapshotů a replikace). • Testy kvality síťových parametrů v rámci BÚ (IOPS, propustnost, latence). • Testy kvality síťových parametrů mezi primární a sekundární lokalitou (IOPS, propustnost, latence). • Testy monitoringu a provozního dohledu. • Bezpečnostní testy (šifrování, přístupy, auditování). • Stress testy bezpečnostních funkcí. • Nastavení pravidel pro detekci kybernetických hrozeb. • Nastavení postupů pro izolaci napadené části BÚ. • Optimalizace bezpečnostních nastavení. • Plán obnovy testovacích dat, analýza průběhu a výsledku obnovy (DR-disaster recovery).

Výstupem výše uvedených požadavků bude samostatný dokument s názvem „Implementační plán Bezpečného úložiště".

5.3 Technické vlastnosti Bezpečného úložiště

5.3.1 Specifikace technických parametrů Bezpečného úložiště

Všechny technické parametry vztahující se k hardwarovým požadavkům Bezpečného datového úložiště pro primární i sekundární lokalitu jsou uvedeny v samostatném dokumentu *Příloha č. 2 smlouvy – Technická specifikace*.

Obecné technické požadavky jsou blíže popsány v následujících kapitolách *5.3.2 Základní vlastnosti* a *5.3.3 Funkční požadavky*.

5.3.2 Základní vlastnosti Bezpečného úložiště

5.3.2.1 Požadovaný typ diskového úložiště

- Pro primární lokalitu Praha je požadováno úložiště typu Bloková storage (SAN), pro uchovávání dat s krátkou a střednědobou retencí s maximální dostupnou ochranou dat proti kybernetickým hrozbám. Součástí řešení budou i vhodné servery pro potřebný výpočetní výkon a orchestraci úložiště.
- Pro sekundární lokalitu Plzeň je požadováno úložiště typu Datový trezor (Data Vault) pro dlouhodobé uchovávání dat s maximální dostupnou ochranou dat proti kybernetickým hrozbám. Součástí řešení budou i vhodné servery pro potřebný výpočetní výkon a orchestraci úložiště.

5.3.2.2 Kapacita diskového úložiště

- V primární lokalitě je požadována výchozí fyzická, nekomprimovaná a nededuplikovaná kapacita (RAW) - minimálně **1 PB** (PetaBajt).
- V sekundární lokalitě je požadována výchozí fyzická, nekomprimovaná a nededuplikovaná kapacita (RAW) - minimálně **1 PB** (PetaBajt).
- Navržené řešení musí zajistit dostatečnou kapacitu a výkon pro data vybraných systémů. Disková pole kapacitně pokryjí současné potřeby, včetně rezervy pro budoucí růst objemu dat. Je požadováno řešení, které umožňuje kapacitní škálování minimálně na **osminásobek výchozí kapacity** bez nutnosti změny architektury a současně využívá techniky deduplikace a komprese dat za účelem maximalizace efektivně využitelné kapacity úložiště.

5.3.2.3 Očekávaný typ ukládaných dat

- Strukturovaná i nestrukturovaná data všech typů.
- Krátkodobé a střednědobé zálohy a konfigurace vybraných provozních systémů.
- Data určená k dlouhodobé archivaci.

5.3.2.4 Výkon a technologie disků

- Pro primární úložiště typu bloková storage, je požadováno víceúrovňové diskové úložiště – Hybrid Storage s NVMe/SSD a SAS/NL-SAS disky.
    - Požadovaný poměr mezi NVMe/SSD a SAS/NL-SAS disky je procentuálně 10:90
        - SSD minimálně 100 TB
        - SAS minimálně 900 TB
    - Profil zátěže NVMe/SSD disků: úroveň Enterprise, mix sequential/random-read/write operace.
    - Profil zátěže SAS/NL-SAS disků: úroveň Enterprise, sequential-read/write operace.

- Pro sekundární úložiště typu Datový trezor (Data Vault) je dostačující technologie disků SAS/NL-SAS.
    - Profil zátěže SAS/NL-SAS disků: úroveň Enterprise, sequential-read/write operace.
- Často přistupovaná data, nebo data určená ke zpracování (deduplikace, komprimace), budou uložena na vysokorychlostních discích typu NVMe/ SSD s podporou Hot Swap.
- Objemná archivní nebo méně využívaná data budou uložena na rotačních discích s vysokou kapacitou (typu SAS/NL-SAS) s podporou Hot Swap.
- Řešení bude podporovat automatizované přesouvání dat mezi tiery (hierarchické archivy) dle nastavených politik. Tento storage tiering zajistí optimální poměr výkonu a nákladů.
- Kromě kapacity je důležitá i propustnost a IOPS navržené technologie. Systém musí zvládat simultánní zápis záložních dat z více zdrojů a případně i čtení při obnově, bez úzkých hrdel.

5.3.2.5 Síťová infrastruktura

LAN/SAN

Součástí dodávky bude i potřebná síťová infrastruktura o dostatečné propustnosti dle navržené technologie úložiště, aby nevznikala úzká hrdla v rámci zápisu, čtení a redistribuce a replikace dat. Síťové řešení bude provozováno v režimu vysoké dostupnosti (HA) s využitím Ethernetové technologie 10/25GbE, 40/100GbE. K propojení obou lokalit bude využita stávající DWDM technologie o rychlosti až 100 Gb/s. Bližší technická specifikace prvků, viz samostatná Příloha č. 2 smlouvy – Technická specifikace.

Firewall

Součástí dodávky musí být zabezpečení síťové komunikace v rámci prostředí bezpečného úložiště, včetně ochrany vnějšího perimetru pomocí Next-generation firewallů. Tato ochrana musí splňovat vysokou dostupnost a dále musí mít schopnost inspekce datového toku a kontroly obsahu procházejících dat vůči definovaným signaturám (IPS a DLP systém). Bližší technická specifikace viz Příloha č. 2 smlouvy - Technická specifikace.

5.3.3 Funkční požadavky

5.3.3.1 Vysoká dostupnost a geografická redundance

Pro maximální odolnost proti výpadkům, musí být obě úložiště navržena s architekturou pro vysokou dostupnost s geografickou redundancí.

- **Geo-redundance (dvě lokality):** Data budou uložena a zrcadlena mezi 2 fyzicky oddělenými datacentry provozovanými SŽ.
    - Primární datové úložiště bude umístěno v datovém centru CDP Praha.
    - Sekundární datové úložiště bude umístěno v datovém centru Plzeň.

Technologie vzájemného propojení obou lokalit bude dle navržené technologie úložiště a technologických možností datového propojení, (propustnost, šířka přenosového pásma, latence, jitter), vždy ale s dohledem na integritu dat. Bude se jednat o georedundanci s asynchronní replikací z primární do sekundární lokality.

- **Redundantní architektura úložiště a failover:** Oba typy úložiště musí být navrženy plně redundantně (více uzlů nebo multi-controller systém), aby i lokální porucha některého zařízení neznamenala nedostupnost služby. Při poruše některého z prvků (server, kontrolér diskového pole, síťový prvek) musí jeho funkci převzít redundantní prvek.

5.3.3.2 Škálovatelnost a tiering úložiště

- **Modularita systému:** Úložiště musí být navrženo jako modulární systém v horizontálním i vertikálním směru, který umožňuje přidávat diskové moduly, uzly nebo výkonové komponenty postupně podle potřeby růstu kapacity a výkonu a umožňovat tak v čase nárůst kapacity minimálně na osminásobek kapacity výchozí (viz kapitola 5.3.2.2). Systém by neměl trpět bottlenecky, které by se zhoršovaly s rostoucí zátěží.
- **Storage tiering a životní cyklus dat:** Data budou uložena podle frekvence použití a důležitosti do odpovídajících úložných vrstev (tiers). Systém musí umožňovat automatizovanou správu životního cyklu dat – tzn. definovat politiky, kdy se data přesouvají mezi vrstvami. Správné nastavení tieringu zajistí, že často využívaná data mají vysoký výkon, zatímco pro archivní účely je k dispozici velká kapacita. To vše transparentně pro uživatele a aplikace. Použitý systém by měl umět využít metadata (datum posledního přístupu, označení archivu apod.) k automatickému tieringu a vyhledávání dat.
- **Centrální správa úložišť:** Součástí dodávky musí být i potřebný software pro centrální správu úložišť (typu Storage Unified Manager), pro oba typy úložišť samostatně a nezávisle na druhém.

5.3.3.3 Bezpečnostní technologie

Bezpečnost uložených dat je absolutní prioritou, jelikož může jít i o data kritické infrastruktury, požadujeme tedy vícevrstvou ochranu.

Oba typy úložišť musí mít implementována opatření, jež zabrání kompromitaci záloh, využitím neměnných úložišť pro zálohy nebo jiných mechanismů, které znemožní dodatečnou úpravu či mazání záloh po jejich vytvoření po definovanou dobu. Úložiště musí podporovat funkce:

- **Immutable backup / WORM Lock:** zajištění nezměnitelnosti záloh v retenční době
- **Air-gap:** úložiště typu Datový trezor (Data Vault) musí navíc umožňovat fyzické nebo logické oddělení od provozní datové sítě
- **Automatická detekce kybernetických hrozeb:** pokud úložiště umožňuje využití integrovaných nástrojů pro proaktivní monitoring a automatickou detekci kybernetických hrozeb typu ransomware nebo

detekcí neobvyklého chování, musí být tato funkcionalita zapnuta, funkční a plně licencována

- **Ochrana proti škodlivému kódu:** Data musí být chráněna proti škodlivému kódu (Malware, ransomware…) po celou dobu manipulace, a i po uložení. Na vstupu do úložiště (při zápisu dat ze systémů) budou nasazeny bezpečnostní nástroje zadavatele na detekci známého malware (antivirové skeny záloh atd.), pokud to bude technicky možné. Cílem je, aby uložené zálohy již neobsahovaly například „spící ransomware". Řešení samostatně zajistí ochranu proti škodlivému kódu (virům) u již uložených dat. Pokud výrobce do řešení přímo integroval napojení na antivirové řešení, které hledá škodlivý kód v již uložených datech, je použita tato možnost. Jinak musí být dodána externí appliance/server, na kterém běží antivirové řešení, které si uložená data z centrální části pole (ne Vaultu) automaticky připojuje a kontroluje na přítomnost virů, případně funkční ekvivalent. Bude zajištěn read-back / re-scan - pravidelné měsíční nebo týdenní bezpečnostní kontroly záloh tímto interním/externím nástrojem. Vždy s výstupem do SIEM a řešení nesmí být založeno na cloudové kontrole, ale očekává se možnost stahování aktualizací z internetu. Tyto kontroly jsou součást technických a organizačních bezpečnostních opatření k řízení kybernetických rizik
- **Šifrování dat v klidu (at rest):** Veškerá data uložená v Bezpečném úložišti musí být šifrována pomocí šifrovacích algoritmů schválených ze strany NÚKIB s možností změny šifrovacího algoritmu v rámci konfigurace. Šifrování musí probíhat na úrovni diskových úložišť automaticky, transparentně pro aplikace. Tím se zajistí, že i v případě fyzického získání disků nebo neautorizovaného přístupu k úložišti útočník data nevyužije bez šifrovacích klíčů. Implementace musí být v souladu s požadavky a doporučeními NÚKIB (doporučení v oblasti kryptografické bezpečnosti), legislativy (ZoKB, nebo GDPR pro osobní údaje).
- **Správa šifrovacích klíčů (KMS/HSM):** Primární úložiště bude podporovat Hardware Security Module (HSM) pro generování, bezpečné ukládání a správu kryptografických klíčů. SŽ již HSM v nějaké formě používá – úložiště musí umožnit integraci s HSM (typicky prostřednictvím protokolu PKCS#11 nebo KMIP). Všechny klíče k šifrování dat úložiště budou spravovány tímto centrálním HSM modulem. Sekundární úložiště (Data Vault) musí mít vlastní dedikovaný HSM modul a vlastní TPM čip pro ukládání a správu šifrovacích klíčů. Kopie klíčů může být uložena i na externích úložištích (typu flash disc) pro případ kompromitace HSM.
- **Integrita a detekce změn:** Systém musí umět ověřovat integritu uložených dat (například skrze kontrolní součty, které detekují tichou korupci dat, tzv. bit rot, nebo neautorizovanou změnu).
- **Retence dat:** Systém musí podporovat různě definované retenční doby pro různé druhy dat, tak aby byla naplněna nejen provozní potřeba Zadavatele ale také legislativní požadavky na ochranu a archivaci.

- **Obnova dat:** Systém musí umožnovat, v případě kompromitace provozních dat, nejen manuální, ale i plně automatizovanou obnovu zálohovaných dat do bezpečného prostředí.
- **Cleanroom:** Zadavatel uvažuje o výstavbě cleanroomu a po dobu udržitelnosti tohoto projektu může dojít k jeho výstavbě. Výstavba Vaultu je prvním krokem před výstavbou cleanroomu, Zadavatel chce získat znalosti a kompetence pro případ vážného kybernetického incidentu. Dodavatel poskytne svoje know-how pro tento krok v rámci školení.
- **Testování dat:** Systém musí umožnit provádět automatizované zkoušky obnovy do izolovaného prostředí (cleanroom), aby SŽ měla jistotu, že zálohy jsou nekompromitované, validní a použitelné pro obnovu. Separátně, v rámci provozních procesů, bude zaveden plán periodických testů: například čtvrtletně provést obnovu vybraného kritického systému ze zálohy a také vyhodnotit, zda obnova odpovídá požadovanému RTO/RPO.

5.3.3.4 Řízení přístupu a správa identit

Pro efektivní a bezpečný přístup k datům musí systém umožňovat řízení přístupových oprávnění:

- **Centralizovaná autentizace a autorizace:** Primární úložiště se plně začlení do stávajícího systému pro správu identit Identity Management (IdM) a do stávajícího systému pro vzdálený přístup Privileged Access Management (PAM). Uživatelé (nebo služby) přistupující k datům úložiště budou ověřováni proti centrální databázi účtů (např. Active Directory/ADFS). Přístupová práva k datům pak budou udělována na základě rolí definovaných v IdM a řízena členstvím ve skupinách v AD (případně v několika na sobě nezávislých AD) – například administrátoři záloh, auditní role, běžní uživatelé konkrétní aplikace apod. Tím se zajistí jednotné přihlašování (Single Sign-On) a především efektivní a přehledná správa přístupových oprávnění.
- **Role-Based Access Control:** Systém musí podporovat RBAC – přiřazování oprávnění podle role. Např. administrátor úložiště může spravovat infrastrukturu, ale nedostane se k obsahu záloh konkrétní aplikace, pokud k tomu není důvod. Naopak správce dané aplikace může mít právo obnovit její data ze zálohy, ale nevidí jiné části úložiště. Tato granulární oprávnění lze spravovat přes IdM/PAM nebo lokálně v úložišti, ale preferujeme centralizaci. Privilegované účty (správci systému) by měly být spravovány právě přes PAM s minimem trvalých přístupů a případně vyžadovat víceúrovňové schválení pro nejcitlivější operace.
- **Důsledná autentizace:** Pro administrativní přístupy vyžadujeme vícefaktorovou autentizaci (MFA). Ať už přes integraci s existující MFA SŽ, nebo vlastnostmi PAM.
- **Audit a záznamy přístupů:** Systém musí logovat veškeré přístupy k datům i administrativní akce minimálně v rozsahu požadovaném VoKB. Každé přečtení či obnova záložního souboru, každá změna nastavení, přidání uživatele apod. Tyto logy budou dlouhodobě uchovávány pro

potřeby auditu a v souladu s legislativou (např. zákon o KB vyžaduje určitou dobu uchování záznamů o událostech). Mimo interního logování budou údaje předávány i do centrálního log managementu a SIEM. Systém musí podporovat běžné formáty log souborů (např. CLF, ELF, SysLog, JSON...).

- **Oddělení prostředí a tenantů:** Úložiště může sloužit více různým agendám (více systémům). Je žádoucí, aby bylo možné logicky oddělit data jednotlivých skupin systémů či útvarů (tzv. multitenancy). Například data provozních technologických systémů mohou být ve vyhrazeném oddílu, logicky odděleném od dat ekonomických systémů, pokud to správu zjednoduší a zvýší přehlednost přístupů. Oddělení by však nemělo bránit centrální správě – je to logická vrstva navíc pro případnou granularitu oprávnění.

5.3.3.5 Integrace, monitorování a dohled

Pro efektivní provoz úložiště, systém musí zapadat do ekosystému stávajících nástrojů pro správu a bezpečnostní dohled SŽ:

- **Kompatibilita s IT prostředím SŽ:** Navržené úložiště bude plně kompatibilní s existujícími systémy a technologiemi, které jej budou využívat. To zahrnuje podporu běžných standardních protokolů pro přístup k datům – např. CIFS/SMB v3, NFS, SFTP, FTPS pro souborové sdílení, příp. blokové protokoly (iSCSI, Fibre Channel) pro připojení databázových serverů. V případě, že řešení nějaký z protokolů nepodporuje, je možné v rámci před-implementační analýzy navrhnout napojení jiným protokolem v rámci pracnosti a dodávky Dodavatele. Úložiště by mělo umožnit snadnou integraci do virtualizační platformy (VMware vSphere) a do clusterových prostředí, pokud některé systémy používají sdílená datová úložiště.
- **Napojení na monitorovací systémy:** Infrastruktura bude připojena k centrálnímu monitorovacímu systému Zabbix, provozovaný SŽ tak, aby stav hardware (disky, zdroje, teploty), služby replikací a záloh byly neustále sledovány operátory. Výpadky, pokles výkonu nebo poruchy komponent budou automaticky hlášeny. Dále bude systém poskytovat telemetrii výkonu – využití kapacity, IO, síťové přenosy – pro účely kapacitního plánování. Budou podporovány běžné protokoly pro monitoring – SNMPv3, ICMP, HTTPS, IPMI, Storage Insights. Úložiště typu Data Vault bude monitorováno pouze jednosměrným kanálem typu SNMP trap.
- **SIEM a log management:** Všechny relevantní logy budou odesílány do centrálního Security Information and Event Management (SIEM) systému. Úložiště musí umět exportovat logy standardním způsobem (syslog, případně API integrace) a obsahovat dostatečné informace (uživatelská ID, IP adresy, kódy událostí). Odesílané logy musí být ve standardizovaném formátu JSON, CEF, LEEF atd. Pro úložiště typu Data Vault musí být logy aktivně odesílány z úložiště (push).
- **Provozní dohled a správa:** Dodané řešení musí zahrnovat nástroj pro správu konfigurace a diagnostiku, např. v podobě centrální management

konzole (Unified storage manager) pro veškerá úložiště, s možností skriptování rutinních úloh (Infrastructure as a Code).

- Integrace úložiště typu Data Vault na vnější prostředí musí být provedena skrze datovou diodu, která zajistí jednosměrnost komunikace na fyzikální úrovni.

5.3.4 Dodávka a implementace Bezpečného úložiště

Dodávka a implementace Bezpečného datového úložiště zahrnuje kompletní dodání, instalaci, konfiguraci a uvedení do provozu řešení v primární i sekundární lokalitě v souladu s technickou specifikací a funkčními požadavky Zadavatele. Součástí plnění je integrace do stávající infrastruktury SŽ, provedení nezbytných testů funkčnosti, dostupnosti a bezpečnosti, předání provozní dokumentace a zajištění součinnosti při akceptaci řešení.

Oblast	Činnost
Dodání technologií BÚ	**Výstup Dodavatele** • Dodávka technologií BÚ do dvou lokalit dle přílohy 2 smlouvy – Technická specifikace, Základních vlastností a Funkčních požadavků
Montáž technologií BÚ	**Výstup Dodavatele** • Montáž a zapojení prvků BÚ (úložiště, servery) • Montáž a zapojení síťových prvků (přepínače, firewally) • Kompletní kabelové propojení (napájecí, datové) • Kompletní vyvázání kabelových rezerv • Zapnutí všech HW komponent • Odvoz a ekologická likvidace obalových materiálů.

Výstupem výše uvedených požadavků budou dodací listy a montážní protokoly, a to samostatně pro primární a sekundární lokalitu.

5.4 Ověření funkčnosti řešení

Ověření funkčnosti řešení má za cíl komplexně prověřit správnost návrhu Bezpečného úložiště a všechny jeho provozní aspekty z pohledu fyzické instalace, funkčních vlastností, výkonových parametrů a rezerv, vysoké dostupnosti, kybernetické bezpečnosti, integrace do systémů Zadavatele a obnovy dat.

5.4.1 Konfigurace Bezpečného úložiště

Konfigurace dodaných HW komponent pro Bezpečné úložiště zahrnuje všechny kroky nutné pro oživení všech fyzických prvků, požadovaných serverů, diskových

polí, síťových prvků a záložních zdrojů. Konfigurace musí reflektovat požadavky na vysokou dostupnost, bezpečnost a škálovatelnost systému a musí být v souladu s akceptovaným dokumentem „Implementační plán Bezpečného úložiště", který je výstupem kapitoly 5.2 Příprava implementačního plánu pro realizaci Bezpečného úložiště. Změny a odchylky od schválené implementace musí být schváleny ze strany zadavatele a musí být zaneseny v rámci konfigurační dokumentace.

Veškerá vzdálená konfigurace všech komponent Bezpečného úložiště ze strany Dodavatele bude probíhat výhradně přes jmenný VPN přístup s multifaktorovou autentizací a výhradně přes nástroj PAM. SŽ pro PAM řešení používá nástroj CyberArk.

Oblast	Činnost
Síťová konfigurace	**Výstup Dodavatele** • Zprovoznění a napojení Out-of-band sítě dle požadavků Zadavatele. • Konfigurace portů • Konfigurace síťových protokolů • Konfigurace síťových prostupů • Konfigurace HA
Aplikační konfigurace	**Výstup Dodavatele** • Zprovoznění a napojení Out-of-band sítě dle požadavků Zadavatele. • Konfigurace aplikačních síťových protokolů

Výstupem výše uvedených požadavků bude samostatný dokument s názvem „Konfigurační dokumentace".

5.4.2 Napojení na vybrané systémy

Napojení vybraných systémů Zadavatele na BÚ zahrnuje veškeré kroky nutné k zajištění správného, bezpečného a funkčního přenosu dat mezi systémy a úložištěm. Cílem této části je zajistit, aby všech 24 vybraných systémů bylo připraveno pro ukládání, obnovu a kontrolu dat v souladu s definovanými technickými a bezpečnostními pravidly.

Toto navazuje na dokumenty „Koncepce Bezpečného úložiště" a „Implementační plán Bezpečného úložiště".

Oblast	Činnost
Technická příprava napojení	**Výstup Dodavatele**

	• Ověření technických parametrů jednotlivých systémů a jejich kompatibility s BÚ (protokoly, typy dat, požadavky na výkon, velikosti datových objemů). • Návrh konkrétního způsobu připojení pro každý systém (blokové, souborové, objektové rozhraní). • Upřesnění konfigurace síťové komunikace mezi systémem a úložištěm. • Návrh a specifikace potřebných firewallových pravidel, routingu a případného zónování.
Konfigurace a realizace napojení	**Výstup Dodavatele** • Implementace technických kroků pro připojení jednotlivých systémů k BÚ podle implementačního postupu. • Nastavení přístupových práv a autentizačních mechanismů dle definice v IdM/PAM. • Konfigurace retenčních politik a pravidel pro jednotlivé datové sady. • Zajištění funkčnosti přístupu systémů k úložišti a provedení základních funkčních testů (zápis, čtení, snapshoty, replikace).
Komunikace	**Vstup Zadavatele** • potřebné přístupy k systémům a infrastruktury, • konzultace s vlastníky a správci systémů, • schválení navržených komunikačních a bezpečnostních pravidel.

Výstupem výše uvedených požadavků bude samostatný dokument s názvem „Zpráva o napojení vybraných systémů na Bezpečné úložiště".

5.4.3 Post-implementační testování

Tyto testy ověřují, že je zařízení správně zapojené a fyzicky funkční a zda řešení dosahuje očekávaných výkonnostních parametrů (viz. kapitola 5.2 tohoto dokumentu - Kontrolní a testovací scénáře). Na základě testovacího scénáře, může Dodavatel vyžadovat spolupráci Zadavatele a naopak. Dodavatel poskytne plnou podporu při identifikaci a odstranění nálezů z testování a návrh nápravných opatření.

Oblast	**Činnost**
Testování funkčnosti řešení	**Výstup Zadavatele**

	• Testy kvality síťových parametrů mezi primární a sekundární lokalitou (IOPS, propustnost, latence) • Testy kvality datového přenosu v rámci BÚ a mezi BÚ (participace) • Výkonnostní testy BÚ (latence, IOPS, propustnost) • Testy obnovy dat, analýza průběhu a výsledku obnovy (disaster recovery) • Testy napojení a funkčnosti monitoringu a logování v systémech Zadavatele (Zabbix, Splunk) • Testy napojení a funkčnosti na bezpečnostní systémy Zadavatele (SIEM, XDR) • Spolupráci s Dodavatelem při identifikaci a nápravě nálezů z testování **Výstup Dodavatele** • Fyzická kontrola a diagnostika, HW diagnostika výrobce • Kontrola verzí firmware a aktualizace na doporučené (ne nejnovější!) verze • Testy vysoké dostupnosti (High Availability/Failover) • Výkonnostní testy BÚ (latence, IOPS, propustnosti) • Funkční testy (testy připojení a protokolů, testy snapshotů a replikace) • Testy kvality síťových parametrů v rámci BÚ (šířka přenosového pásma, propustnost, latence) • Testy kvality síťových parametrů mezi primární a sekundární lokalitou (propustnost, latence) • Test integrity dat • Test obnovy dat, analýza průběhu a výsledku obnovy (disaster recovery) • Poskytnutí testovacího prostředí (generátor provozu) pro testování NGFW pravidel definovaných během analýzy • Spolupráce se Zadavatelem při identifikaci a nápravě nálezů z testování
Bezpečnostní testování	**Výstup Zadavatele** • Validace síťové architektury • Vypracování analýzy bezpečnostních rizik • Test autentizace a identity • Test fyzické bezpečnosti • Test odolnosti proti kybernetickým hrozbám

	• Test detekování škodlivého kódu pomocí EICAR test file na již uložených zálohách • Test detekce kybernetického útoku (detekce ransomware), tento bude proveden ve spolupráci s dodavatelem • Test napojení a reakce bezpečnostních systému (SIEM) a propagace výstrah do SIEM, alertyTest obnovy šifrovacích klíčů (pokud úložiště využívá HSM technologii) ve spolupráci s dodavatelem • Penetrační testování třetí stranou • Spolupráci s Dodavatelem při identifikaci a nápravě nálezů z testování **Výstup Dodavatele** • Podklady pro test detekce ransomware včetně testovacího skriptu nebo programu, který takovou činnost simuluje • Nastavení pravidel pro detekci kybernetických hrozeb a ověření funkčnosti • Test odolnosti proti kybernetickým hrozbám (konzultace) • Test detekce kybernetického útoku (konzultace) • Test síťové izolace úložišť (konzultace) • Bezpečnostní testy (šifrování, přístupy, auditování) • Stress testy bezpečnostních funkcí • Testy izolace a segmentace • Nastavení postupů pro izolaci napadené části BÚ • Optimalizace bezpečnostních nastavení • Spolupráci se Zadavatelem při identifikaci a nápravě nálezů z testování
Optimalizace a dokumentace konfigurace	**Výstup Dodavatele** • Na základě zjištění z testování, Dodavatel vypracuje návrh finální optimalizace konfigurace řešení, kterou po validaci Zadavatelem následně realizuje. • Dokumentace skutečného provedení řešení

Výstupem výše uvedených požadavků bude Akceptační protokol post-implementačních testů.

6 Školení, dokumentace a exit strategie

6.1 Školení

Realizace projektu bude zahrnovat zaškolení administrátorů a dalších pracovníků SŽ, kteří budou úložiště spravovat. Vzhledem k zavedení nových technologií (např. HSM, podpůrné aplikace, nastavení IdM pro úložiště) je nutné, aby tým získal potřebné dovednosti. Odborné školení zajistí Dodavatel v českém jazyce pro vybrané specialisty, a to ještě před uvedením úložiště do produkčního provozu.

V oblasti odborného školení je požadováno následující plnění:

Typ školení	**Popis**
Odborné školení	Dodavatel zajistí pro vybrané zástupce Zadavatele odpovídající, výrobcem certifikované, školení dodávané technologie, včetně nástrojů centrální správy dodaných komponent, které odpovídá požadavkům na každodenní správu a údržbu zařízení, správu z pohledu kybernetické bezpečnosti a kybernetického monitoringu (například představení kybernetických funkcionalit, jejich napojení na dohledové nástroje typu SIEM a využití dodaných technologií pro forenzní šetření). Obecné požadavky na školení: • Školení bude realizováno v rozsahu minimálně **3 MD**. • Školení bude realizováno prezenční formou v lokalitě Praha. • Dodavatel poskytne Zadavateli kompletní školící materiály k dodávaným nástrojům. • Zadavatel bude moci pořídit z celého školení obrazový i zvukový záznam, který bude moci dále využívat pro potřeby školení vlastních pracovníků a externích partnerů. • Školení **nemusí** být zakončeno certifikační zkouškou.
Odborné školení SOC	Dodavatel zajistí odborné školení pro bezpečnostní specialisty ze SOC týmu, umožňující správu z pohledu kybernetické bezpečnosti a kybernetického monitoringu (např. představení kybernetických funkcionalit, jejich napojení na dohledové nástroje typu SIEM a využití dodaných technologií pro forenzní šetření), se zaměřením na:

- Pravidelné kontroly bezpečnosti záloh.
- Kompetence a postup pro bezpečnou obnovu dat.
- Obnovení dat z Datového trezoru do hypotetického cleanroomu, jehož výstavba je v budoucnosti plánována.
- Vytvoření návrhů krizových scénářů, včetně následných doporučení, např. odpojení Datového trezoru v případě kybernetického incidentu.
- Dále dle metodik NIST Special Publication 800-184, případně ISO 27001 Annex A.17 (A.17.1, A.17.2).

Obecné požadavky na školení:

- Školení bude realizováno v rozsahu minimálně **1 MD**.
- Školení bude zajištěno **osobou způsobilou dle ZoKB** pro roli **Architekta kybernetické bezpečnosti**.
- Školení bude realizováno prezenční formou v lokalitě Praha.
- Dodavatel poskytne Zadavateli kompletní školící materiály k dodávaným nástrojům.
- Zadavatel bude moci pořídit z celého školení obrazový i zvukový záznam, který bude moci dále využívat pro potřeby školení vlastních pracovníků a externích partnerů.
- Školení **nemusí** být zakončeno certifikační zkouškou.

Výstupem výše uvedených požadavků bude samostatný dokument s názvem "Zpráva o školení zaměstnanců Správy železnic" včetně prezenční listiny z obou výše uvedených školení.

6.2 Dokumentace

Dodavatel v rámci dodávky poskytne kompletní provozní dokumentaci. Dokumentace bude sloužit jako základ pro běžný provoz, školení personálu, interní audity a případné kontroly ze strany dozorových orgánů. Textová dokumentace musí být v elektronické podobě v běžném editovatelném formátu, např. MS Word, výkresy a plány v editovatelném formátu, např. MS Visio, Archimate, pro možnost pozdějších modifikací. Technická dokumentace výrobce zařízení, může být v elektronické podobě ve formátu PDF, nebo v podobě funkčního odkazu na Webové stránky výrobce jednotlivých komponent.

Typ dokumentace	**Popis**
Architektonická dokumentace	**Výstup Dodavatele** • dokumentace skutečného provedení

	• logická a fyzická architektura • síťová topologie • napojení na systémy Zadavatele • nákres rozmístění prvků v rackové skříni (rack layout)
Provozní dokumentace	**Výstup Dodavatele** • administrace serverů a úložišť • provozní monitoring • správa diskové kapacity • aktualizace a patchování • běžné provozní scénáře • postupy pro běžnou údržbu • postup obnovy systému (DRP)
Dokumentace zálohování a obnovy	**Výstup Dodavatele** • rozsah zálohovaných dat (co se zálohuje) • objem zálohovaných dat • specifikace umístění zálohovaných dat • klasifikace dat pro zálohovací scénáře • retenční doby • postupy testovací obnovy dat • postupy reálné provozní obnovy dat
Bezpečnostní dokumentace	**Výstup Dodavatele** • použité bezpečnostní technologie • princip ochrany dat • popis technologie šifrování dat • správa šifrovacích klíčů (HSM) • pravidla přístupu, MFA • role a oprávnění • proces přidělování/odebírání přístupů • popis logování a auditu
Technická dokumentace výrobce	**Výstup Dodavatele** • datové listy jednotlivých komponent (Datasheet) • odkaz na stránky technické podpory výrobce jednotlivých komponent

Výstupem výše uvedených požadavků bude samostatný dokument s názvem "Dokumentace skutečného provedení".

6.3 Exit strategie

V případě řádného nebo předčasného ukončení smlouvy požaduje Zadavatel součinnost Dodavatele pro zajištění kontinuity služeb.

Za tímto účelem zpracuje Dodavatel plán, který popisuje, jak a za jakých podmínek Zadavatel bezpečně a kontrolovaně ukončí smluvní vztah s Dodavatelem (dále a výše také jen „**Exit strategie**").

6.3.1 Vytvoření Exit strategie

Exit strategie bude zpracována Dodavatelem v rámci fáze F1.2 – Implementační plán Bezpečného úložiště. Požadavky na součinnost Dodavatele při ukončení smlouvy jsou vymezeny kap. 4.3.8 ZOP a v této Bližší specifikaci předmětu plnění a budou dále podrobně rozpracovány v samotné Exit strategii.

Obsah Exit strategie

Exit strategie bude nedílnou součástí Implementačního plánu a bude obsahovat zejména:

- harmonogram přechodu včetně milníků a odpovědností,
- varianty přechodu (převzetí jiným dodavatelem, migrace na nový systém apod.),
- způsob zajištění provozní kontinuity během přechodného období,
- postup předání dokumentace, dat, přístupů a licencí,
- podporu při testování, validaci a převzetí řešení novým správcem systému.

V rámci zachování kontinuity služeb Zadavatel požaduje základní součinnost Dodavatele při ukončení smlouvy definovanou v kap. 4.3.8 ZOP, která je dále rozšířená o následující výstupy a požadavky:

6.3.2 Předání znalostí a podkladů v případě ukončení smlouvy po dokončení Fáze F5

Dojde-li k ukončení smlouvy po dokončení Fáze F5, zavazuje se Dodavatel předat Zadavateli veškeré podklady, které případně ještě nebyly předány, viz kapitola 6.2 - Dokumentace a poskytnout maximální možnou spolupráci pro hladké předání know-how.

Dodavatel je při ukončení povinen dodat následující dokumenty a provést následující činnosti:

Oblast	Výstup
Dokumentace	Dodavatel provede a předá Zadavateli:

	• export všech konfigurací • aktuální dokumentaci skutečného provedení • bezpečnostní dokumentaci.
Konzultace	Dodavatel se zavazuje spolupracovat se zadavatelem po dobu dalších 3 měsíců a zodpovědět dotazy stavu ohledně díla, a to v rozsahu maximálně 10 MD.
Dokončení servisních požadavků	Dodavatel dořeší všechny servisní požadavky otevřené do dne vypovězení smlouvy.

6.3.3 Předání znalostí a podkladů v případě ukončení smlouvy před dokončením Fáze F5

Dojde-li k ukončení smlouvy před dokončením Fáze F5, zavazuje se dodavatel kromě níže uvedených výstupů předat ještě následující:

- Seznam kroků potřebných k dokončení konfigurace a dokončení díla.
- Seznam kroků potřebných pro uvedení prostředí do původního stavu.

Dodavatel je povinen dodat následující dokumenty a provést následující činnosti:

Oblast	Výstup
Dokumentace	Dodavatel provede a předá Zadavateli: • export všech konfigurací • aktuální dokumentaci skutečného provedení • bezpečnostní dokumentaci.
Přístupová oprávnění a uživatelské účty	Dodavatel předá Zadavateli: • Přístupové údaje k root uživatelům, pokud systémy nedisponují základním uživatelem s plnými oprávněními, dodavatel vytvoří pro zadavatele uživatelský účet/účty s plnými oprávněními, které mu předá. • Přístupové údaje hlavního administrátora do portálu podpory výrobce.

	• Seznam všech dodavatelem používaných účtů, ke kterým disponuje přístupovými údaji.
Konzultace	Dodavatel se zavazuje spolupracovat se zadavatelem po do dobu dalších 3 měsíců a zodpovědět dotazy ohledně stavu ohledně díla, a to v rozsahu maximálně 10 MD.
Licence a obnova	Dodavatel předá Zadavateli: • všechny licenční klíče. • Časový harmonogram nezbytných činností a obnovy licencí a certifikátů.
Dokončení servisních požadavků	Dodavatel dořeší všechny servisní požadavky otevřené do dne vypovězení smlouvy.

Odměna za činnosti uvedené v této kapitole 6.3 je již zahrnuta v ceně plnění a Dodavateli za ně nenáleží žádná zvláštní odměna.

7 Post-implementační a technická podpora

V oblasti post-implementační a technické podpory jsou definovány následující požadavky:

Oblast	Požadavky
Technická podpora výrobce	Zařízení nesmí mít k datu podání nabídky oznámené EOS (End Of Sale) dříve než za 2 roky a oznámené EOL (End Of Life) dříve než za 5 let od dodání. Dodavatel zajistí oficiální podporu výrobce po dobu 60 měsíců od ukončení fáze F2.1 pro primární lokalitu a po dobu 60 měsíců od ukončení fáze F2.2 pro sekundární lokalitu. Tato podpora zahrnuje minimálně: • Režim podpory minimálně 8x5 (8 hodin denně v rámci pracovních dní). • Podpora dostupná na webovém portálu výrobce, e-mailu a telefonu. • Přístup k novým verzím firmware či OS.

Post-implementační podpora Dodavatele	Dodavatel zajistí Post-implementační podporu v rozsahu: (1) Poskytování expertních služeb, které budou využívány zejména pro podporu činností SŽ v případě řešení nestandardních stavů a pro profylaxi, aby se předcházelo omezením jeho správné funkčnosti. (2) Konzultace při konfiguracích a změnách dodaných komponent a v rámci bezpečnostní strategie napojovaných systémů řešení definovaných výstupů této Veřejné zakázky. (3) Post-implementační podpora bude poskytována po dobu 60 měsíců od ukončení fáze F3.3. (4) Post-implementační podpora bude poskytována v souladu s ustanoveními ZOP podle servisního modelu C2. Nad rámec ZOP platí, že budou plánované změny či významné změny (aktualizace, patch atd.) ze strany Dodavatele poskytnuty (uvolněny) SŽ vždy v pracovních dnech, a to konkrétně v pondělí a ve středu. V případě, že plánovaná změna či významná změna a její poskytnutí vychází na státní svátek, vyzve Dodavatel SŽ k upřesnění poskytnutí (uvolnění). (5) Poskytování služeb ServiceDesk ze strany Dodavatele bude realizováno v souladu s ustanoveními ZOP v Režimu 4 (8×5, tj. v pracovních dnech v době od 7:00 do 15:00 na telefonním čísle určeném Dodavatelem). (6) Součinnost při auditech řešení, opravu a zapracování identifikovaných nedostatků.

8 Konzultační služby na vyžádání

V oblasti konzultačních služeb jsou definovány následující požadavky:

Oblast	Požadavky
Konfigurační konzultace a práce	Dodavatel poskytne konfigurační a konzultační práce prostřednictvím rolí **Architekt infrastruktury,** nebo **Síťový specialista,** nebo **Bezpečnostní specialista,** nebo **Datový analytik** (dle potřeby) v oblasti dodané technologie, který Zadavateli umožní konzultovat konfigurační parametry dodaného řešení.

Analytická konzultace	Dodavatel poskytne analytické konzultační práce prostřednictvím role **Datový analytik** v oblasti dodané technologie, který Zadavateli umožní konzultovat analytické parametry dodaného řešení.

Maximální počet k čerpání všech Konzultačních služeb na vyžádání je 150 MD. SŽ není povinna Konzultační služby na vyžádání čerpat.

9 Fáze dodávky a platební milníky

Plnění musí být dodáno v níže uvedených fázích. Každá z níže uvedených fází F1.1 až F5 je součástí jednoho z uvedených platebních milníků (A nebo B) a musí být Zadavatelem akceptována nejpozději v termínu uvedeném v Harmonogramu. Zadavatel akceptuje výstupy dané akceptační fáze, jestliže je Dodavatel provedl v šíři a kvalitě požadované v zadávací dokumentaci této veřejné zakázky. V opačném případě je Dodavatel povinen napravit nedostatky plnění.

Platební milník	Fáze	Popis	Způsob akceptace fáze	Kapitola obsahující požadavky
A	F1.1	Datový management vybraných systémů	Akceptační protokol: • Dokument – Koncepce Bezpečného úložiště	5.1
A	F1.2	Implementační plán Bezpečného úložiště	Akceptační protokol • Dokument – Implementační plán Bezpečného úložiště (vč. Exit strategie)	5.2
A	F2.1	Dodávka a implementace Bezpečného úložiště do primární lokality	Akceptační protokol: • Dodávka HW, SW a licencí, dle specifikace ZD • Dodací list • Montážní protokol	5.3 5.3.4
A	F2.2	Dodávka a implementace Bezpečného úložiště do sekundární lokality	Akceptační protokol: • Dodávka HW, SW a licencí dle specifikace ZD • Dodací list • Montážní protokol	5.3 5.3.4
B	F3.1 A	Konfigurace primární lokality	Akceptační protokol: • Dokument - Konfigurační dokumentace	5.4.1

Platební milník	Fáze	Popis	Způsob akceptace fáze	Kapitola obsahující požadavky
B	F3.1 B	Konfigurace sekundární lokality	Akceptační protokol: • Dokument - Konfigurační dokumentace	5.4.1
B	F3.2	Napojení na vybrané systémy	Akceptační protokol: • Dokument – Zpráva o napojení vybraných informačních systémů na Bezpečné úložiště	5.4.2
B	F3.3	Post-implementační testování	Akceptační protokol: • Dokument – Závěrečná zpráva z testování funkčních a bezpečnostních parametrů Bezpečného úložiště	5.4.3
B	F4	Školení	Akceptační protokol: • Dokument - Zpráva o školení zaměstnanců Správy železnic včetně prezenční listiny	6.1
B	F5	Dokumentace	Akceptační protokol: • Dokumentace skutečného provedení	6.2
Plnění bude hrazeno na základě potvrzených pravidelných měsíčních výkazů.	F6.1A	Technická podpora – primární lokalita	Fáze F6.1A bude vykazována na základě pravidelných měsíčních výkazů	7
Plnění bude hrazeno na základě potvrzených pravidelných měsíčních výkazů.	F6.1B	Technická podpora – sekundární lokalita	Fáze F6.1B bude vykazována na základě pravidelných měsíčních výkazů	7
Plnění bude hrazeno na základě potvrzených pravidelných měsíčních výkazů.	F6.2	Post-implementační podpora	Fáze F6.2 bude vykazována na základě pravidelných měsíčních výkazů	7

Platební milník	Fáze	Popis	Způsob akceptace fáze	Kapitola obsahující požadavky
Plnění bude hrazeno na základě skutečného čerpání ze strany Zadavatele.	F7	Konzultační služby na vyžádání	Akceptační protokol s ohledem na obsah požadovaných Konzultačních služeb	8

Klasifikace: Veřejný dokument

SPRÁVA ŽELEZNIC

Příloha č. 2 smlouvy – Technická specifikace

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČ: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

Obsah

1 Technické požadavky

1.1 Technické požadavky na Datové úložiště

1.1.1 Technická specifikace Položky A

V oblasti dodávky **jednoho (1)** zařízení pro datové úložiště (primární datové úložiště v lokalitě **Praha**) definuje Zadavatel následující požadavky:

[IDENTIFIKACE MODELU - DOPLNÍ DODAVATEL]

Požadavek	**Nabízené řešení** **(doplňte ANO/NE, případně uveďte technické parametry, pokud lze)**
Základní vlastnosti	
Typ zařízení: Hybridní datové úložiště typu SAN, s podporou SSD a SAS disků.	[DOPLNÍ DODAVATEL]
Třída diskového pole: Enterprise.	[DOPLNÍ DODAVATEL]
Fyzické provedení do standardní rackové skříně o šířce 19 palců, výšce 42U a hloubce 120 cm.	[DOPLNÍ DODAVATEL]
Rail kit pro montáž do racku pro všechny dílčí komponenty (pokud je k danému řešení v nabídce výrobce).	[DOPLNÍ DODAVATEL]
Zcela redundantní architektura bez SPOF.	[DOPLNÍ DODAVATEL]
Napájecí zdroje: AC 230 V, redundantní, hot-swap, s minimální účinností 90%.	[DOPLNÍ DODAVATEL]
Napájecí kabely 230V IEC C13/C14 nebo C19/C20 kompatibilní s napájecím zdrojem v délce minimálně 2 metry, v barvě černé a červené (v poměru 50:50), v potřebném množství dle navrhnutého řešení (Alternativně: Napájecí kabely 230V CEE7/7 kompatibilní s napájecím zdrojem v délce minimálně 2 metry, v barvě černé a červené (v poměru 50:50), v potřebném množství dle navrhnutého řešení).	[DOPLNÍ DODAVATEL]
Maximální celkový elektrický příkon řešení: **10 kW/rack.**	[DOPLNÍ DODAVATEL]
Velikost Rack Unit (U): Max. 2x42U (celé řešení při požadované kapacitě, včetně serverů a síťových prvků).	[DOPLNÍ DODAVATEL]
Typ podporovaných disků: **NVMe/SSD, SAS/NL-SAS HDD**.	[DOPLNÍ DODAVATEL]

Diskové pole musí obsahovat alespoň **4 řadiče** a musí být škálovatelné alespoň na 12 řadičů.	[DOPLNÍ DODAVATEL]
Konfigurace musí být tolerantní k výpadku dvou řadičů bez jakýchkoli dopadů na poskytované blokové služby. (Dodavatel během implementace pole prokáže odolnost proti selhání více řadičů).	[DOPLNÍ DODAVATEL]
Podpora připojení host serverů s aktuálními operačními systémy, včetně Windows Server 2022/2025, Solaris, HP-UX, VMware, IBM-AIX, Linux a Mainframe.	[DOPLNÍ DODAVATEL]
Podpora připojení host serverů v režimu clusterů viz seznam operačních systémů zmíněných výše.	[DOPLNÍ DODAVATEL]
Propojení všech řadičů prostřednictvím redundantního vysokorychlostního propojení s využitím technologie PCI-e Gen 3 (nesmí používat žádný ethernetový nebo optický přepínač). Dodavatel prokáže, že nabízená konfigurace nemá SPOF v propojení řadičů.	[DOPLNÍ DODAVATEL]
Podpora protokolů FC a iSCSI pro připojení externích diskových polí.	[DOPLNÍ DODAVATEL]
Technologie redukce dat (deduplikace a komprese) napříč všemi typy nabízených disků s minimálním dopadem na výkon.	[DOPLNÍ DODAVATEL]
Minimální konfigurace	
Celková minimální RAW kapacita diskového úložiště: **1 PB** (PetaBajt).	[DOPLNÍ DODAVATEL]
Z celkové velikosti minimálně **100 TB** čisté užitné kapacity (RAW) pomocí SSD disků.	[DOPLNÍ DODAVATEL]
Minimálně **16 FC portů 32 Gb/s** FC HBA, (min. 4 FC porty na řadič).	[DOPLNÍ DODAVATEL]
Konektivita Ethernet: iSCSI 10 Gb/s, minimálně 4 iSCSI portů (min. 2 porty na řadič).	[DOPLNÍ DODAVATEL]
Min. 512 GB cache paměti s možností rozšíření na 4 TB. Cache musí mít globální adresní prostor.	[DOPLNÍ DODAVATEL]
Škálovatelnost	
Škálovatelnost na více než 8 PB (PetaBajtů) RAW kapacity v rámci jednoho pole	[DOPLNÍ DODAVATEL]
Podpora konfigurace s kombinací jak NVMe, tak standardních SAS disků.	[DOPLNÍ DODAVATEL]
Podpora nejnovějších generací SAS a NL-SAS disků pomocí vhodných řadičů.	[DOPLNÍ DODAVATEL]

Podpora SAS disků s kapacitou alespoň 2,4 TB, NL-SAS disků s kapacitou alespoň 8 TB, SSD Flash disků a NVMe disků s kapacitou alespoň 12 TB.	[DOPLNÍ DODAVATEL]
Virtualizace externích polí	
Podpora virtualizace externích diskových polí od různých výrobců. Pomocí technologie externího diskového pole musí být možné vytvořit řešení o kapacitě až 200 PB. Technologie virtualizace externích diskových polí **musí podporovat minimálně výrobce Dell-EMC, Hitachi, HPE, IBM, Netapp**.	[DOPLNÍ DODAVATEL]
Funkcionalita virtualizace externího diskové pole musí být nedílnou součástí firmwaru diskového pole a nevyžaduje žádné další externí zařízení ani software.	[DOPLNÍ DODAVATEL]
Zabezpečení dat a šifrování	
Podpora minimálně Raid 1, Raid 0+1, Raid 5 a Raid 6.	[DOPLNÍ DODAVATEL]
Podpora šifrování (Data at Rest) silnými moderními algoritmy (minimálně AES 256b nebo lepší). Případná licence musí být součástí nabídky.	[DOPLNÍ DODAVATEL]
Schopnost vytvářet více než 64000 logických jednotek (LUN) a podporovat velikost jednoho svazku (LUN) až 256 TB.	[DOPLNÍ DODAVATEL]
Podpora alespoň 1024 ks snapshotů pro daný LUN. Podpora vytvoření snapshotu ze snapshotu (kaskádování). Diskové pole musí podporovat vytvoření alespoň milionu snapshotů.	[DOPLNÍ DODAVATEL]
Podpora schopnosti vytvářet nesmazatelné („immutable“) snapshoty s možností definice retenční doby.	[DOPLNÍ DODAVATEL]
Podpora synchronní replikace, asynchronní replikace, asynchronní replikace se žurnálem, replikace v 3DC (1na2), kaskádové replikace (1-1-1). Licence pro replikace na plnou kapacitu nabízeného diskového pole musí být součástí nabídky.	[DOPLNÍ DODAVATEL]
Active-active řešení podporující asynchronní replikaci založenou na žurnálu do třetí lokality.	[DOPLNÍ DODAVATEL]
Vytváření aplikačních konzistentních snapshotů pro různé kritické aplikace, jako jsou SAP HANA, Oracle DB, Exchange, SQL, VMware prostředí atd. Dodavatel musí dodat základní modul takového softwaru spolu s diskovým polem.	[DOPLNÍ DODAVATEL]
Automatická detekce, zaznamenávání a notifikace chyb.	[DOPLNÍ DODAVATEL]
Administrace	
Management software pro administraci z jednotného GUI (musí být součástí nabídky) i z CLI.	[DOPLNÍ DODAVATEL]

Software pro administraci musí být schopen spravovat více diskových polí z jedné konzole a je integrován s prostředím VMware v obrazovém formátu, který ukazuje alespoň CPU, paměť, IOPS, MB/s a latenci pro dané VM běžící v prostředí.	[DOPLNÍ DODAVATEL]
Možnost integrace s různými softwarovými nástroji pro automatizaci, monitorování a správu, jako jsou: • VMware vCloud suite. • Terraform • Redhat Ansible • Oracle Linux Virtualization Manager • Veeam cloud backup and recovery	[DOPLNÍ DODAVATEL]
Pro všechny činnosti související se správou diskového pole musí management software podporovat následující: • centralizovaný monitoring, konfiguraci a správu úložných komponent, • monitoring stavu, výkonu, utilizace a konfigurace, • shromažďování, ukládání a analýzu dat o výkonu diskového pole.	[DOPLNÍ DODAVATEL]
Tiering jak nad interní kapacitou, tak v rámci externích virtualizovaných diskových polí.	[DOPLNÍ DODAVATEL]
Opravy a výměny HW komponent musí být možné za běhu, bez dopadu na poskytované datové služby.	[DOPLNÍ DODAVATEL]
Upgrade firmware HW komponent diskového pole musí probíhat v režimu „Nondisruptive firmware upgrade", tzn. během aktualizace firmware nedochází k restartu žádného z kontrolérů a nedochází k přerušení služby.	[DOPLNÍ DODAVATEL]
Správa diskového pole musí podporovat RBAC (Role-Based Access Control).	[DOPLNÍ DODAVATEL]
Správa diskového pole musí být integrovatelná na externí IdM/PAM/SIEM řešení. Všechny relevantní logy budou odesílány do centrálního Security Information and Event Management (SIEM) systému. Úložiště musí umět exportovat logy standardním způsobem (syslog, případně API integrace) a obsahovat dostatečné informace (uživatelská ID, IP adresy, kódy událostí).	[DOPLNÍ DODAVATEL]
U všech disků (SSD, NVMe, SAS) a jiných datových nosičů je při poruše a/nebo reklamaci požadováno ponechání disku Objednateli, z důvodu prevence úniku dat.	[DOPLNÍ DODAVATEL]

1.1.2 Technická specifikace Položky B

V oblasti dodávky **jednoho (1)** zařízení pro datové úložiště (sekundární datové úložiště v lokalitě **Plzeň**) definuje Zadavatel následující požadavky:

[IDENTIFIKACE MODELU - DOPLNÍ DODAVATEL]

Požadavek	**Nabízené řešení** **(doplňte ANO/NE, případně uveďte technické parametry, pokud lze)**
Základní vlastnosti	
Typ zařízení: Hybridní datové úložiště typu SAN, s podporou SSD a SAS disků.	[DOPLNÍ DODAVATEL]
Třída diskového pole: Enterprise.	[DOPLNÍ DODAVATEL]
Fyzické provedení do standardní rackové skříně o šířce 19 palců, výšce 42U a hloubce 120 cm.	[DOPLNÍ DODAVATEL]
Rail kit pro montáž do racku pro všechny dílčí komponenty (pokud je k danému řešení v nabídce výrobce).	[DOPLNÍ DODAVATEL]
Zcela redundantní architektura bez SPOF.	[DOPLNÍ DODAVATEL]
Napájecí zdroje: AC 230 V, redundantní, hot-swap, s minimální účinností 90%.	[DOPLNÍ DODAVATEL]
Napájecí kabely 230V IEC C13/C14 nebo C19/C20 kompatibilní s napájecím zdrojem v délce minimálně 2 metry, v barvě černé a červené (v poměru 50:50), v potřebném množství dle navrhnutého řešení (Alternativně: Napájecí kabely 230V CEE7/7 kompatibilní s napájecím zdrojem v délce minimálně 2 metry, v barvě černé a červené (v poměru 50:50), v potřebném množství dle navrhnutého řešení).	[DOPLNÍ DODAVATEL]
Maximální celkový elektrický příkon řešení: **10 kW/rack.**	[DOPLNÍ DODAVATEL]
Velikost Rack Unit (U): Max. 2x42U (celé řešení při požadované kapacitě, včetně serverů a síťových prvků).	[DOPLNÍ DODAVATEL]
Typ podporovaných disků: **NVMe/SSD, SAS/NL-SAS HDD**	[DOPLNÍ DODAVATEL]
Diskové pole musí obsahovat alespoň **4 řadiče** a musí být škálovatelné alespoň na 12 řadičů.	[DOPLNÍ DODAVATEL]
Konfigurace musí být tolerantní k výpadku dvou řadičů bez jakýchkoli dopadů na poskytované blokové služby. (Dodavatel	[DOPLNÍ DODAVATEL]

během implementace pole prokáže odolnost proti selhání více řadičů).	
Podpora připojení host serverů s aktuálními operačními systémy, včetně Windows Server 2022/2025, Solaris, HP-UX, VMware, IBM-AIX, Linux a Mainframe.	[DOPLNÍ DODAVATEL]
Podpora připojení host serverů v režimu clusterů viz seznam operačních systémů zmíněných výše.	[DOPLNÍ DODAVATEL]
Propojení všech řadičů prostřednictvím redundantního vysokorychlostního propojení s využitím technologie PCI-e Gen 3 (nesmí používat žádný ethernetový nebo optický přepínač). Dodavatel prokáže, že nabízená konfigurace nemá SPOF v propojení řadičů.	[DOPLNÍ DODAVATEL]
Podpora protokolů FC a iSCSI pro připojení externích diskových polí.	[DOPLNÍ DODAVATEL]
Technologie redukce dat (deduplikace a komprese) napříč všemi typy nabízených disků s minimálním dopadem na výkon.	[DOPLNÍ DODAVATEL]
Minimální konfigurace	
Celková minimální RAW kapacita diskového úložiště: **1 PB** (PetaBajt).	[DOPLNÍ DODAVATEL]
Minimálně **16 FC portů 32 Gb/s** FC HBA, (min. 4 FC porty na řadič).	[DOPLNÍ DODAVATEL]
Konektivita Ethernet: iSCSI 10 Gb/s, minimálně 4 iSCSI portů (min. 2 porty na řadič).	[DOPLNÍ DODAVATEL]
Min. 512 GB cache paměti s možností rozšíření na 4 TB. Cache musí mít globální adresní prostor.	[DOPLNÍ DODAVATEL]
Škálovatelnost	
Škálovatelnost na více než 8 PB (PetaBajtů) RAW kapacity v rámci jednoho pole.	[DOPLNÍ DODAVATEL]
Podpora konfigurace s kombinací jak NVMe, tak standardních SAS disků.	[DOPLNÍ DODAVATEL]
Podpora nejnovější generace SAS a NL-SAS disků pomocí vhodných řadičů.	[DOPLNÍ DODAVATEL]

Podpora SAS disků s kapacitou alespoň 2,4 TB, NL-SAS disky s kapacitou alespoň 8 TB, SSD Flash disky a NVMe disky s kapacitou alespoň 12 TB.	[DOPLNÍ DODAVATEL]
Virtualizace externích polí	
Podpora virtualizace externích diskových polí od různých výrobců. Pomocí technologie externího diskového pole musí být možné vytvořit řešení o kapacitě až 200 PB. Technologie virtualizace externích diskových polí **musí podporovat minimálně výrobce Dell-EMC, Hitachi, HPE, IBM, Netapp**.	[DOPLNÍ DODAVATEL]
Funkcionalita virtualizace externího diskového pole musí být nedílnou součástí firmwaru diskového pole a nevyžaduje žádné další externí zařízení ani software.	[DOPLNÍ DODAVATEL]
Zabezpečení dat a šifrování	
Podpora minimálně Raid 1, Raid 0+1, Raid 5 a Raid 6.	[DOPLNÍ DODAVATEL]
Podpora šifrování (Data at Rest) silnými moderními algoritmy (minmáleně AES 256b nebo lepší). Případná licence musí být součástí dodávky.	[DOPLNÍ DODAVATEL]
Schopnost vytvářet více než 64000 logických jednotek (LUN) a podporovat velikost jednoho svazku (LUN) až 256 TB.	[DOPLNÍ DODAVATEL]
Podpora alespoň 1024 ks snapshotů pro daný LUN. Podpora vytvoření snapshotu ze snapshotu (kaskádování). Diskové pole musí podporovat vytvoření alespoň milionu snapshotů.	[DOPLNÍ DODAVATEL]
Podpora schopnosti vytvářet nesmazatelné („immutable“) snapshoty s možností definice retenční doby.	[DOPLNÍ DODAVATEL]
Podpora synchronní replikace, asynchronní replikace, asynchronní replikace se žurnálem, replikace v 3DC (1na2), kaskádové replikace (1-1-1). Pokud je replikace podmíněná licencí, Dodavatel je povinen tuto licenci zahrnout do dodávky řešení. Licence je součástí nabídkové ceny a nenáleží Dodavateli za ni zvláštní odměna.	[DOPLNÍ DODAVATEL]
Active-active řešení podporující asynchronní replikaci založenou na žurnálu do třetí lokality.	[DOPLNÍ DODAVATEL]
Vytváření aplikačních konzistentních snapshotů pro různé kritické aplikace, jako jsou SAP HANA, Oracle DB, Exchange, SQL, VMware prostředí atd. Dodavatel musí dodat základní modul takového softwaru spolu s diskovým polem.	[DOPLNÍ DODAVATEL]

Automatická detekce, zaznamenávání a notifikace chyb.	[DOPLNÍ DODAVATEL]
Administrace	
Management software pro administraci z jednotného GUI (musí být součástí nabídky) i z CLI.	[DOPLNÍ DODAVATEL]
Software pro administraci musí být schopen spravovat více diskových polí z jedné konzole a je integrován s prostředím VMware v obrazovém formátu, který ukazuje alespoň CPU, paměť, IOPS, MB/s a latenci pro dané VM běžící v prostředí.	[DOPLNÍ DODAVATEL]
Možnost integrace s různými softwarovými nástroji pro automatizaci, monitorování a správu, např: • VMware vCloud suite. • Terraform • Redhat Ansible • Oracle Linux Virtualization Manager • Veeam cloud backup and recovery	[DOPLNÍ DODAVATEL]
Pro všechny činnosti související se správou diskového pole musí management software podporovat následující: • centralizovaný monitoring, konfiguraci a správu úložných komponent, • monitoring stavu, výkonu, utilizace a konfigurace, shromažďování, ukládání a analýzu dat o výkonu diskového pole.	[DOPLNÍ DODAVATEL]
Tiering jak nad interní kapacitou, tak v rámci externích virtualizovaných diskových polí.	[DOPLNÍ DODAVATEL]
Opravy a výměny HW komponent musí být možné za běhu, bez dopadu na poskytované datové služby.	[DOPLNÍ DODAVATEL]
Upgrade firmware HW komponent diskového pole musí probíhat v režimu „Nondisruptive firmware upgrade", tzn. během aktualizace firmware nedochází k restartu žádného z kontrolérů a nedochází k přerušení služby.	[DOPLNÍ DODAVATEL]
Správa diskového pole musí podporovat RBAC (Role-Based Access Control).	[DOPLNÍ DODAVATEL]
Správa diskového pole musí být integrovatelná na externí IdM/PAM/SIEM řešení. Všechny relevantní logy budou odesílány do centrálního Security Information and Event Management (SIEM) systému. Úložiště musí umět exportovat logy standardním způsobem (syslog, případně API integrace) a	[DOPLNÍ DODAVATEL]

obsahovat dostatečné informace (uživatelská ID, IP adresy, kódy událostí).	
U všech disků (SSD, NVMe, SAS) a jiných datových nosičů je při poruše a/nebo reklamaci požadováno ponechání disku Objednateli, z důvodu prevence úniku dat.	[DOPLNÍ DODAVATEL]

1.2 Technické požadavky na servery

Součástí řešení Datových úložišť budou **2 (dvě)** serverové šasi a **8 (osm)** serverů, 4 do každého šasi, z důvodu škálovatelnosti a budoucího rozšíření jejich využití. Tato šasi a v nich obsažené servery budou určeny pro potřebnou správu každého úložiště a bezpečnostní kontrolu uložených dat.

1.2.1 Technická specifikace Položky C

Dvě (2) serverové šasi pro virtualizační farmu v konfiguraci:

[IDENTIFIKACE MODELU - DOPLNÍ DODAVATEL]

Požadavek	**Nabízené řešení** **(doplňte ANO/NE, případně uveďte technické parametry, pokud lze)**
Modulární technologie umožňující jednoduché škálování založené na otevřených průmyslových standardech typu x86.	[DOPLNÍ DODAVATEL]
Provedení do 19 racku o velikosti maximálně **10U** včetně veškeré potřebné konektivity, které pojme minimálně **12 serverů.**	[DOPLNÍ DODAVATEL]
Možnost osazení šasi minimálně 6 (šesti) síťovými moduly s 3+3 redundancí.	[DOPLNÍ DODAVATEL]
Podpora síťové konektivity Ethernet a FC.	[DOPLNÍ DODAVATEL]
Redundance napájení N+N s možností připojit alespoň dva nezávislé třífázové přívody napájení tak, aby výpadek jednoho z nich neznamenal omezení výkonu serveru.	[DOPLNÍ DODAVATEL]
Všechny zdroje musí poskytovat výrobcem dostupný maximální výkon pro maximální osazení šasi.	[DOPLNÍ DODAVATEL]
Napájecí kabely 230V IEC C13/C14 nebo C19/C20 kompatibilní s napájecím zdrojem v délce minimálně 2 metry, v barvě černé a červené (v procentuálním poměru počtu kabelů 50:50, pro odlišení zálohované a nezálohované napájecí větve), v potřebném množství dle navrhnutého řešení (Alternativně: Napájecí kabely 230V CEE7/7 kompatibilní s napájecím zdrojem v délce minimálně 2 metry, v barvě černé a červené (v procentuálním poměru počtu kabelů 50:50, pro odlišení	[DOPLNÍ DODAVATEL]

zálohované a nezálohované napájecí větve) v potřebném množství dle navrhnutého řešení).	
Zdroje musí podporovat řízení spotřeby CPU instalovaných v poptávaných serverech.	[DOPLNÍ DODAVATEL]
Šasi musí obsahovat HDMI/DisplayPort a USB port pro lokální připojení notebooku/monitoru.	[DOPLNÍ DODAVATEL]
Redundantní management moduly nezávislé na stavu serverů s dedikovanými 10GbE porty, každý management modul bude osazený 1x 10Gbit SFP+ SR modulem.	[DOPLNÍ DODAVATEL]
Management moduly musí umožňovat spojení více šasi do jednoho logického celku pro správu celého prostředí z jednoho místa.	[DOPLNÍ DODAVATEL]
LAN konektivita součástí šasi • Alespoň dva redundantní LAN prvky navzájem propojené min **2x 100Gbit** stack kabely s délkou 3m • Celková externí propustnost minimálně **6x QSFP28** z každého prvku • Každý prvek osazený min **2x 100Gbit QSFP+** Bidirectional modulem pro propojení do lokální LAN • Možnost mirroringu komunikace serverových portů pro diagnostiku sítě • Podpora 802.1Q (podpora VLAN), 802.1AB (LLDP), NIC teaming • Správa přes zabezpečené web rozhraní (HTTPS/SSL) a RESTful API	[DOPLNÍ DODAVATEL]
SAN konektivita součástí šasi • Alespoň dva redundantní SAN prvky s celkovou externí propustností minimálně **12x FC 32** z každého prvku • Každý prvek osazený min. **4x FC 32 SFP+** modulem typu short wave pro propojení s lokálními SAN přepínači/servery • Možnost vytváření společných agregačních skupin a pravidel pro SAN konektivitu serveru • Správa přes zabezpečené web rozhraní (HTTPS/SSL) a RESTful API	[DOPLNÍ DODAVATEL]
Management šasi musí umožňovat: • Jediné plně grafické rozhraní pro správu všech instalovaných komponent (servery, switche, zdroje, ventilátory) včetně možnosti přechodu do plně grafické konzole jednotlivých serverů • Řízení přístupových práv k centrální části SW a k management nástrojům pomocí Active Directory • Zapnutí, vypnutí a restart serveru na dálku • Namapování vzdálených medií CD, image souboru a adresářů • Management v HTML5 s podporou běžných www prohlížečů integrovaných v desktopovém OS pro správu serveru (IE, Firefox, Chrome) • Měření spotřeby celého šasi a instalovaných serverů	[DOPLNÍ DODAVATEL]

• Monitorování okamžité teploty a záznam hodnot s krátkou historií	

1.2.2 Technická specifikace Položky D

Osm (8) serverů, čtyři (4) do každého šasi z Položky C v konfiguraci:

[IDENTIFIKACE MODELU - DOPLNÍ DODAVATEL]

Požadavek	**Nabízené řešení** **(doplňte ANO/NE, případně uveďte technické parametry, pokud lze)**
Provedení serveru pro instalaci do blade šasi z Položky C.	[DOPLNÍ DODAVATEL]
2x CPU, každý minimálně **32 jader** se základní frekvencí minimálně 2,4 GHz a se spotřebou maximálně 300 W.	[DOPLNÍ DODAVATEL]
Architektura **Intel x86-64** z důvodu kompatibility současného ICT prostředí.	[DOPLNÍ DODAVATEL]
Operační paměť minimálně **512 GB DDR5** o přenosové rychlosti alespoň 6400 MT/s, s použitím modulů o maximální velikosti 64 GB s možností rozšíření na dvojnásobek pomocí stejných modulů.	[DOPLNÍ DODAVATEL]
Konvergovaný LAN adaptér s celkovou propustností min. 100Gb/s active-active, nebo 2x 50Gb/s active-passive (full duplex) s podporou RoCE V2 a NPAR.	[DOPLNÍ DODAVATEL]
SAN adaptér s minimálně 2x 32Gb/s FC.	[DOPLNÍ DODAVATEL]
2x NVMe M.2 SSD, každý o velikosti minimálně **960 GB** v konfiguraci RAID1 pro boot a běh OS nebo virtualizační platformy.	[DOPLNÍ DODAVATEL]
Možnost osadit až 8 přímo připojených EDSFF NVMe disků s podporou VMware vSAN.	[DOPLNÍ DODAVATEL]
Trusted Platform Module minimálně ve verzi 2.0.	[DOPLNÍ DODAVATEL]
U všech disků (SSD, NVMe, SAS) a jiných datových nosičů je při poruše a/nebo reklamaci požadováno ponechání disku Objednateli, z důvodu prevence úniku dat.	[DOPLNÍ DODAVATEL]

1.3 Technické požadavky na síťové prvky

1.3.1 Technická specifikace Položky E:

V oblasti dodávky **dvou (2)** switchů pro oddělenou síť pro management (OOB) definuje Zadavatel následující požadavky:

[IDENTIFIKACE MODELU - DOPLNÍ DODAVATEL]

Požadavek	Nabízené řešení (doplňte ANO/NE, případně uveďte technické parametry, pokud lze)
Provedení switche pro instalaci do rackové skříně o hloubce **100 cm.**	[DOPLNÍ DODAVATEL]
Velikost skříně switche o maximální výšce **1 RU** (45 mm).	[DOPLNÍ DODAVATEL]
48x 1G RJ45 port.	[DOPLNÍ DODAVATEL]
4x 1G SFP nebo **10G SFP** port s podporou rychlosti 1G (může být i formou vyměnitelného rozšiřujícího modulu).	[DOPLNÍ DODAVATEL]
Dedikovaný síťový port pro oddělený management.	[DOPLNÍ DODAVATEL]
2x hot-swap napájecí zdroj AC/230V s minimální účinností 80%.	[DOPLNÍ DODAVATEL]
Podpora stackování switchů: • spojení v jeden virtuální switch, • minimálně 6 switchů ve stacku, • možnost stacku na vzdálenost minimálně 100 m.	[DOPLNÍ DODAVATEL]
Podpora výrobce na 5 let.	[DOPLNÍ DODAVATEL]
Podpora protokolů IPv4 a IPv6.	[DOPLNÍ DODAVATEL]
Podpora funkce na vrstvě **L2** dle ISO/OSI modelu.	[DOPLNÍ DODAVATEL]
Minimální kapacita **32000 MAC adres.**	[DOPLNÍ DODAVATEL]
Podpora protokolů LACP a MVRP, VRRPv2 a VRRPv3.	[DOPLNÍ DODAVATEL]
Podpora technologií VRF, VLAN a Jumbo frame, IEEE 802.1v, IEEE 802.1s a IEEE 802.1w.	[DOPLNÍ DODAVATEL]
Podpora Energy Efficient Ethernet (IEEE 802.3az).	[DOPLNÍ DODAVATEL]
Minimální výkon zpracování packetů (forwarding rate) **35 Mpps.**	[DOPLNÍ DODAVATEL]
Potřebné licence na dobu 5 let zahrnující funkcionality: • Využití všech osazených síťových portů • VLAN • LACP • VRF	[DOPLNÍ DODAVATEL]
Vzdálená správa • Vzdálená správa s dedikovaným vlastním portem 1GbE. • Možnost vzdálené aktualizace firmware. • Podpora protokolu SNMP minimálně ve verzi 2c • Podpora protokolu Syslog a předávání logů na vzdálený systém	[DOPLNÍ DODAVATEL]
Síťové optické moduly pro každý optický port SFP, plně kompatibilní s dodávaným switchem, originální od výrobce	[DOPLNÍ DODAVATEL]

dodaných switchů v provedení „1/10Gbps nebo 10Gbps, Singlemode, LC, Long Range“.	

1.3.2 Technická specifikace položky F

V oblasti dodávky **čtyř (4)** datacentrových switchů pro připojení Datového úložiště definuje Zadavatel následující požadavky:

[IDENTIFIKACE MODELU - DOPLNÍ DODAVATEL]

Požadavek	**Nabízené řešení** **(doplňte ANO/NE, případně uveďte technické parametry, pokud lze)**
Provedení switche pro instalaci do rackové skříně o hloubce **100 cm.**	[DOPLNÍ DODAVATEL]
Velikost skříně switche o maximální výšce **1 RU** (45 mm).	[DOPLNÍ DODAVATEL]
Rail kit pro montáž do racku (pokud je k danému řešení v nabídce výrobce).	[DOPLNÍ DODAVATEL]
Minimálně **48x 25G SFP** port s podporou rychlostí 10G a 1G.	[DOPLNÍ DODAVATEL]
Minimálně **6x 100G SFP** port s podporou rychlosti 40G.	[DOPLNÍ DODAVATEL]
Dedikovaný síťový port pro oddělený management.	[DOPLNÍ DODAVATEL]
2x hot-swap napájecí zdroj AC/230V.	[DOPLNÍ DODAVATEL]
Směr proudu vzduchu ventilátorů: přes porty ven (BacktoFront)	[DOPLNÍ DODAVATEL]
Podpora výrobce na **5 let.**	[DOPLNÍ DODAVATEL]
Podpora protokolů IPv4 a IPv6.	[DOPLNÍ DODAVATEL]
Podpora funkce na vrstvách **L2** i **L3** dle ISO/OSI modelu.	[DOPLNÍ DODAVATEL]
Minimální kapacita **90000 MAC adres.**	[DOPLNÍ DODAVATEL]
Minimální kapacita **120000 ARP záznamů.**	[DOPLNÍ DODAVATEL]
Minimální kapacita **4000 aktivních VLAN** podle IEEE 802.1Q.	[DOPLNÍ DODAVATEL]
Podpora protokolů LACP a MVRP, VRRPv2 a VRRPv3.	[DOPLNÍ DODAVATEL]
Podpora technologií VRF, VLAN a Jumbo frame, IEEE 802.1v, IEEE 802.1s, IEEE 802.1w, IEEE 802.1AX, IEEE 802.1p.	[DOPLNÍ DODAVATEL]
Minimální výkon zpracování packetů (forwarding rate) **2000 Mpps.**	[DOPLNÍ DODAVATEL]
Podpora policy-based routing.	[DOPLNÍ DODAVATEL]

Dynamické směrování: RIP, RIPng, OSPFv2, OSPFv3, BGP, MP-BGP včetně BGP MD5 autentizace.	[DOPLNÍ DODAVATEL]
Podpora static a dynamic VXLAN s využitím BGP-EVPN.	[DOPLNÍ DODAVATEL]
Podpora TACACS+ a RADIUS.	[DOPLNÍ DODAVATEL]
Interní SSD úložiště pro sběr provozních dat s minimální kapacitou **60 GB**, včetně podpory standardního Linux Shellu (BASH) pro debugging a skriptování.	[DOPLNÍ DODAVATEL]
Analýza síťového provozu podle RFC 3176 pro oba směry (ingress a egress).	[DOPLNÍ DODAVATEL]
Vzdálená správa • Vzdálená správa s dedikovaným vlastním portem 1GbE. • Možnost vzdálené aktualizace firmware. • Podpora protokolu SNMP minimálně ve verzi 2c • Podpora protokolu Syslog a předávání logů na vzdálený systém	[DOPLNÍ DODAVATEL]
Materiál pro montáž dodaného Hardware do rackové skříně.	[DOPLNÍ DODAVATEL]

1.3.3 Technická specifikace Položky G

V oblasti dodávky čtyř **(4)** kusů zařízení NGFW definuje Zadavatel následující požadavky pro každé z nich:

[IDENTIFIKACE MODELU - DOPLNÍ DODAVATEL]

Požadavek	**Nabízené řešení** **(doplňte ANO/NE, případně uveďte technické parametry, pokud lze)**
Fyzické, rack mount provedení do rozvaděče o standardní šířce 19 palců.	[DOPLNÍ DODAVATEL]
Maximální velikost 2U.	[DOPLNÍ DODAVATEL]
Minimálně **16 portů 10/25G** s volitelným fyzickým rozhraním typu SFP+/SFP28.	[DOPLNÍ DODAVATEL]
Minimálně **4 porty 40/100G** s volitelným fyzickým rozhraním typu QSFP+/QSFP28.	[DOPLNÍ DODAVATEL]
Dedikovaný síťový port pro oddělený management.	[DOPLNÍ DODAVATEL]
Dedikovaný konzolový port – typ RJ45 nebo USB.	[DOPLNÍ DODAVATEL]
Lokální úložiště pro logy o minimální kapacitě 960 GB v režimu RAID1.	[DOPLNÍ DODAVATEL]
Podpora nasazení v HA Clusteru pomocí dedikovaných portů.	[DOPLNÍ DODAVATEL]

2x hot-swap napájecí zdroj AC/230V s účinností min. 80 Plus.	[DOPLNÍ DODAVATEL]
Interní redundantní ventilátory.	[DOPLNÍ DODAVATEL]
TPM (Trusted Platform Module) čip.	[DOPLNÍ DODAVATEL]
Celková minimální propustnost **130 Gbps.**	[DOPLNÍ DODAVATEL]
Počet souběžných TCP spojení minimálně **20 000 000.**	[DOPLNÍ DODAVATEL]
Minimální propustnost NGFW (IPS, Application control) min. **18 Gbps.**	[DOPLNÍ DODAVATEL]
Propustnost IPSEC VPN (AES256, SHA256) min. **50 Gbps.**	[DOPLNÍ DODAVATEL]
Propustnost SSL VPN minimálně **10 Gbps.**	[DOPLNÍ DODAVATEL]
Minimální propustnost SSL inspekce (IPS, HTTPS) **20 Gbps.**	[DOPLNÍ DODAVATEL]
Počet IPSec VPN tunelů Gateway-to-Gateway min. 18 000	[DOPLNÍ DODAVATEL]
Počet IPSec VPN tunelů Client-to-Gateway min. 60 000	[DOPLNÍ DODAVATEL]
Podpora virtuálních kontextů hardware appliance min. 10 kontextů – pokud jsou licencovány, musí být licence součástí nabídky.	[DOPLNÍ DODAVATEL]
Každý z virtuálních kontextů může pracovat buď v L2 režimu (transparentní režim inspekce) nebo L3 režimu (NAT/router režim s inspekcí).	[DOPLNÍ DODAVATEL]
Virtuální kontexty musí být možné propojit pomocí virtuálních propojů (bez nutnosti propojovat pomocí fyzických síťových rozhraní) bez omezení výkonu.	[DOPLNÍ DODAVATEL]
Podpora Active-Active i Active-Passive režimů.	[DOPLNÍ DODAVATEL]
Správa všech zařízení pracujících v režimu vysoké dostupnosti musí probíhat jednotně přes společné grafické konfigurační rozhraní.	[DOPLNÍ DODAVATEL]
Grafické konfigurační rozhraní pro správu celého clusteru, dostupné pomocí webového prohlížeče (HTTPS) bez omezení na počet administrátorů a bez nutnosti instalovat dodatečnou management platformu nebo aplikaci.	[DOPLNÍ DODAVATEL]
Podpora LACP (802.3ad).	[DOPLNÍ DODAVATEL]
VXLAN s BGP EVPN – podpora v HW (pokud je nutná licence, musí být součástí).	[DOPLNÍ DODAVATEL]

Podpora SSL offload.	[DOPLNÍ DODAVATEL]
Podpora TLS 1.3 i pro aplikační inspekce.	[DOPLNÍ DODAVATEL]
Podpora pravidel na základě identity uživatelů pro MS AD prostředí – nastavení bezpečnosti uživateli na základě členství v AD skupině na doménovém kontroléru.	[DOPLNÍ DODAVATEL]
Podpora VPN SSL - portálový režim i tunelovací režim.	[DOPLNÍ DODAVATEL]
Podpora Site-to-site IPsec VPN s podporou statického i dynamického routování.	[DOPLNÍ DODAVATEL]
Ověřování uživatelů proti LDAP, Radius, TACACS+.	[DOPLNÍ DODAVATEL]

Zařízení NGFW musí být dodány včetně veškerých potřebných licencí k provozu požadovaných služeb, viz. detailnější obecné požadavky uvedené v předchozí tabulce, s dobou platnosti a veškerými systémovými update po dobu **60 měsíců** od ukončení Fáze F2.1 pro primární lokalitu a od ukončení Fáze F2.2 pro sekundární lokalitu.

1.3.4 Technická specifikace Položky H

Požadujeme dodání kompatibilních optických modulů pro dodaná zařízení v následujících počtech:

Požadavek	**Nabízené řešení** **(doplňte ANO/NE, případně uveďte technické parametry, pokud lze)**
Minimálně 28x (nebo dle skutečné potřeby dle navrženého řešení) kabel **AOC 100Gbps**, v délce minimálně 5m, plně kompatibilní s dodávaným řešením a certifikovaný výrobcem řešení.	[DOPLNÍ DODAVATEL]
Minimálně 8x (nebo dle skutečné potřeby dle navrženého řešení) kabel **AOC 10/25Gbps**, v délce minimálně 5m, plně kompatibilní s dodávaným řešením a certifikovaný výrobcem řešení NGFW.	[DOPLNÍ DODAVATEL]
Minimálně 4x (nebo dle skutečné potřeby dle navrženého řešení) kabel **DAC 1/10Gbps**, v délce 5m, plně kompatibilní s dodávaným řešením a certifikovaný výrobcem řešení.	[DOPLNÍ DODAVATEL]

Minimálně 4x (nebo dle skutečné potřeby dle navrženého řešení) transceiver **SFP+ 1/10Gbps** multimode plně kompatibilní s dodávaným řešením a certifikované výrobcem řešení.	[DOPLNÍ DODAVATEL]
Minimálně 4x (nebo dle skutečné potřeby dle navrženého řešení) **SFP 1Gbps/RJ45** plně kompatibilní s dodávaným řešením a certifikovaný výrobcem.	[DOPLNÍ DODAVATEL]
Minimálně 16x (nebo dle skutečné potřeby dle navrženého řešení) transceiver **SFP 32Gbps FC** (Fibre channel).	[DOPLNÍ DODAVATEL]
Minimálně 10x (nebo dle skutečné potřeby dle navrženého řešení) kabel Eth RJ45, S/FTP, CAT6A v délce minimálně 5m.	[DOPLNÍ DODAVATEL]
Optické/metalické kabely v technických parametrech: • Multimode OM4 • Singlemode OS2 • Ethernet RJ45 S/FTP, CAT6A • Konektor: LC, kompatibilní s dodanými optickými moduly • Délka: 1/2/3/5/7/10m • Množství: dle skutečné potřeby dle navrženého řešení	[DOPLNÍ DODAVATEL]

2 Implementační požadavky

2.1 Implementace síťových přepínačů

V oblasti implementace síťových přepínačů jsou definovány následující činnosti, resp. požadavky:

Činnost	**Služba bude poskytnuta** **(doplňte ANO/NE, případně uveďte detailní popis služby)**
Dodávka zařízení: Zadavatel požaduje dodávku a montáž zařízení do obou lokalit organizace SŽ v Praze a Plzni, v souladu s navrženým plánem rozmístění prvků.	[DOPLNÍ DODAVATEL]
Základní konfigurace: • Ověření zařízení na absenci HW vad. • Registrace zařízení. • Instalace výrobcem doporučené verze operačního systému. • Konfigurace základních parametrů (management rozhraní, hostname, DNS, NTP, STP, administrátorské přístupy, napojení na centrální uživatelský systém (LDAP/RADIUS), odesílání událostí do externího zařízení).	[DOPLNÍ DODAVATEL]
Síťová konfigurace: • Linková agregace. • IP adresace a VLAN tagy • Nasazení v režimu Stack (pokud je vyžadováno)	[DOPLNÍ DODAVATEL]

2.2 Implementace Next Generation Firewall

V oblasti implementace NGFW jsou definovány následující činnosti, resp. požadavky:

Činnost	Služba bude poskytnuta (doplňte ANO/NE, případně uveďte detailní popis služby)
Dodávka zařízení: Zadavatel požaduje dodávku a montáž zařízení do obou lokalit organizace SŽ v Praze a Plzni, v souladu s navrženým plánem rozmístění prvků.	[DOPLNÍ DODAVATEL]
Základní konfigurace: • Ověření zařízení na absenci HW vad. • Registrace zařízení. • Instalace výrobcem doporučené verze operačního systému. • Konfigurace základních parametrů (management rozhraní, hostname, DNS, NTP, administrátorské přístupy, napojení na centrální uživatelský systém (LDAP/RADIUS), odesílání událostí do externího zařízení).	[DOPLNÍ DODAVATEL]
Konfigurace vysoké dostupnosti (HA) Nasazení v režimu Active – Passive.	[DOPLNÍ DODAVATEL]
Síťová konfigurace • Linková agregace. • IP adresace a VLAN tagy. • Směrování. • DHCP relay.	[DOPLNÍ DODAVATEL]
Vytvoření objektů a bezpečnostní politiky: • Specifikace nových pravidel pro nové NGFW. • Návrh jmenné konvence pravidel a objektů dle akceptované metodiky.	[DOPLNÍ DODAVATEL]
Dodavatel definuje vzorové bezpečnostní politiky dle vzoru Zadavatele: • IPS a/nebo IDS. • Application Control.	[DOPLNÍ DODAVATEL]
SSO Autentizace: Napojení na Active Directory řízení přístupů na základě identit.	[DOPLNÍ DODAVATEL]

2.2.1 Nástroj centrální správy NGFW - Položka I

Zadavatel požaduje plnou kompatibilitu dodávaných firewallů s jedním z nástrojů centrální správy a managementu, které již Zadavatel ve svém prostředí provozuje. Zadavatel ve svém prostředí provozuje centrální správu firewallových technologií pomocí nástrojů **FortiManager** a **Firewall Management Center**.

Pokud nebude možné zajistit plnou kompatibilitu dodávaných NGFW Dodavatelem se současným centrálním managementem, je Dodavatel povinen v rámci své dodávky dodat a naimplementovat v prostředí Zadavatele nový nástroj centrální správy NGFW včetně příslušných licencí s dobou platnosti a veškerými systémovými update po dobu minimálně 60 měsíců od zprovoznění nástroje centrální správy, který bude splňovat následující požadavky.

Požadavky na nástroj centrální správy NGFW

V oblasti dodávky nástroje pro centrální správu dodávaných NGFW definuje Zadavatel následující požadavky:

[IDENTIFIKACE NABÍZENÉHO NÁSTROJE - DOPLNÍ DODAVATEL]

Požadavek	**Nabízené řešení** **(doplňte ANO/NE, případně uveďte technické parametry, pokud lze)**
Typ nástroje: Nástroj může být realizován jako fyzický, nebo virtualizovaný, s podporou virtualizační platformy VMware, která je hlavní a jedinou virtualizační platformou provozovanou Zadavatelem.	[DOPLNÍ DODAVATEL]
Nástroj centrální správy musí umožnit správu minimálně 20 fyzických zařízení.	[DOPLNÍ DODAVATEL]
Nástroj centrální správy umožňuje příjem a uložení událostí v minimálním množství 10 GB událostí za den s možností licenčního rozšíření minimálně na 50 GB událostí za den.	[DOPLNÍ DODAVATEL]
Nástroj centrální správy umožňuje základní analýzu událostí za účelem včasné identifikace reálné či potenciální hrozby. Primárně bude pro vyhodnocování incidentů používán nástroj aktuálně využívaný v prostředí SŽ, log management a SIEM.	[DOPLNÍ DODAVATEL]

V oblasti implementace nástroje centrální správy jsou Zadavatelem definovány následující činnosti, resp. požadavky:

Činnost	Služba bude poskytnuta (doplňte ANO/NE, případně uveďte detailní popis služby)
Dodávka zařízení: Dodávka nástroje do lokality Praha. V případě virtualizovaného zařízení poskytnutí instalačních dat skrze internetovou konektivitu.	[DOPLNÍ DODAVATEL]
Základní konfigurace • Ověření zařízení na absenci HW vad (pouze u fyzického zařízení). • Registrace zařízení. • Instalace výrobcem doporučené verze operačního systému. • Konfigurace základních parametrů (management rozhraní, hostname, DNS, NTP, administrátorské přístupy, napojení na centrální uživatelský systém (LDAP/RADIUS), odesílání událostí do externího zařízení).	[DOPLNÍ DODAVATEL]
Integrace dodaných NGFW do centrální správy.	[DOPLNÍ DODAVATEL]
Poskytnutí plné podpory Dodavatele při konfiguraci dodaného nástroje až po úplné spuštění nástroje pro centrální správu NGFW.	[DOPLNÍ DODAVATEL]

3 Obecná ustanovení

Dodavatel se zavazuje dodat Hardware nový, nepoužitý a určený pro EU trh. V opačném případě se jedná o podstatné porušení Smlouvy.

Příloha č. 3 smlouvy - Ceník

Realizace systému Zabezpečného úložiště v prostředí Správy železnic

Tento soubor v listu "Nabídková cena" obsahuje formulář pro vyplnění nabídkové ceny.

Identifikace účastníka:

Postup pro vyplnění souboru

Nejprve účastník vyplní položku Identifikace účastníka na řádku 16 tohoto listu. Dále pokračuje s vyplňováním listu "Nabídková cena". Na listu "Nabídková cena" je popis konkrétních kroků pro jeho správné vyplnění.

Legenda zabarvených polí:

textové doplnění pole

Nabídková cena
Účastník vyplní jednotkovou cenu dle jednotlivých částí plnění pro předdefinovaný počet jednotek.

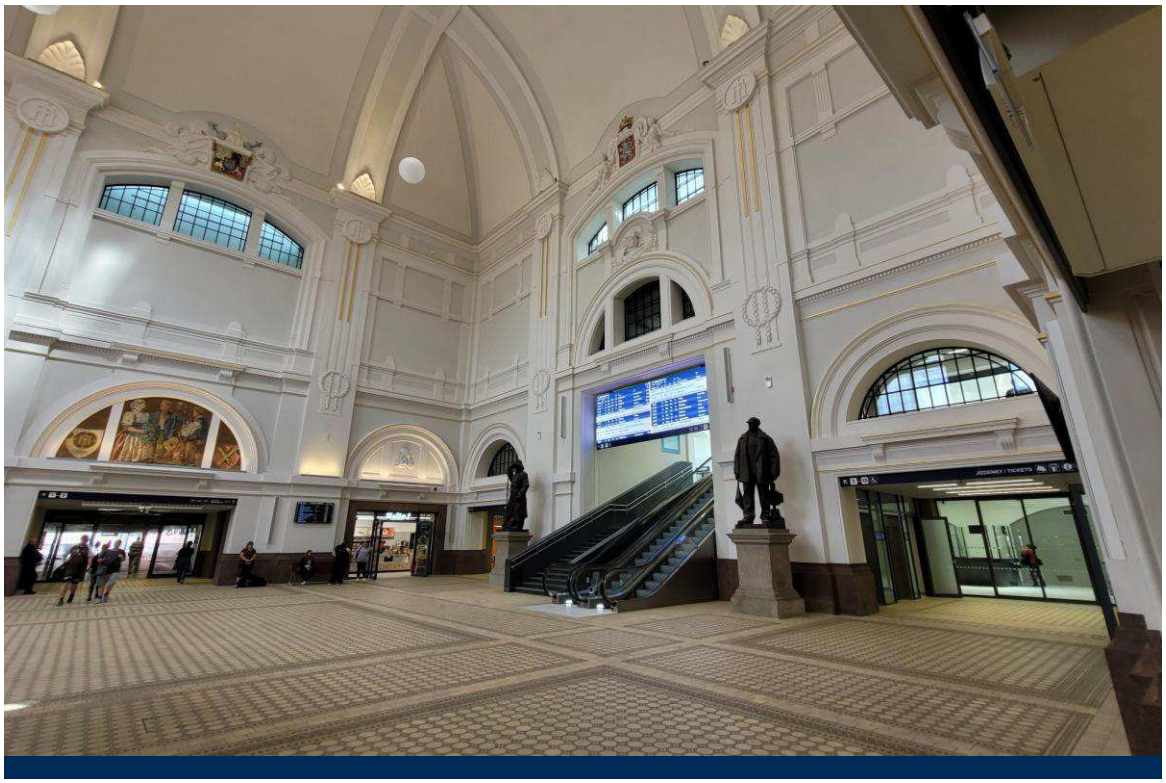
Nabídková cena

Účastník vyplní **ve sloupci E** ("Jednotková cena") jednotkovou cenu **v Kč bez DPH** za každou část plnění.

Ve sloupci I ("Omezení ceny za platební milník") je uvedena forma omezení ceny pro celkovou částku za vybrané části Plnění, jejíž cena je vypočítána ve sloupci H. Omezení je vztaženo k nabídkové ceně celkem (po odečtení ceny za fáze F6.1A, F6.1B, F6.2 a F7), a proto je nutné soulad s omezením revidovat až po doplnění jednotkové ceny za všechny položky.

Fáze	Část Plnění	Odkaz na kapitolu Bližší specifikace předmětu plnění	Jednotková cena (v Kč bez DPH)	Počet jednotek	jedn.	Nabídková cena (v Kč bez DPH)	Omezení ceny za platební milník	Vyjádření k zadaným hodnotám
F1.1	**Datový management vybraných systémů**	5.1		1	-	0,00 CZK	**Maximální souhrnná výše ceny za fáze F1.1 a F1.2 je omezena na 10 % z nabídkové ceny celkem po odečtení ceny za fáze F6.1A, F6.1B, F6.2 a F7**	
F1.2	**Implementační plán Bezpečného úložiště**	5.2		1	-	0,00 CZK		
F2.1	**Dodávka a implementace Bezpečného úložiště do primární lokality**	5.3 5.3.4		1	-	0,00 CZK	**Maximální souhrnná výše ceny za fáze F2.1 a F2.2 je omezena na 60 % z nabídkové ceny celkem po odečtení ceny za fáze F6.1A, F6.1B, F6.2 a F7**	
F2.2	**Dodávka a implementace Bezpečného úložiště do sekundární lokality**	5.3 5.3.4		1	-	0,00 CZK		
F3.1A	**Konfigurace primární lokality**	5.4.1		1	-	0,00 CZK		
F3.1B	**Konfigurace sekundární lokality**	5.4.1		1	-	0,00 CZK		
F3.2	**Napojení na vybrané systémy**	5.4.2		1	-	0,00 CZK		
F3.3	**Post-implementační testování**	5.4.3		1	-	0,00 CZK		
F4	**Školení**	6.1		1	-	0,00 CZK		
F5	**Dokumentace**	6.2		1	-	0,00 CZK		
F6.1A	**Technická podpora - primární lokalita**	7		60	měsíc	0,00 CZK		
F6.1B	**Technická podpora - sekundární lokalita**	7		60	měsíc	0,00 CZK		
F6.2	**Post-implementační podpora**	7		60	měsíc	0,00 CZK		
F7	**Konzultační služby na vyžádání**	8		150	MD	0,00 CZK		
	Nabídková cena celkem					**0,00 CZK**		

*MD = člověkoden



Platforma SŽ
Základní dokument

Červen 2025

Obsah

Seznam zkratek

AD	Rozšiřitelná a škálovatelná adresářová služba, která umožňuje efektivně uspořádat síťové prostředky. Kromě informací o objektech v počítačové síti (uživatelské účty, počítače, tiskárny) umožňuje používat stromovou strukturu objektů, nastavovat globálně systémové politiky, instalovat programy na počítače nebo aplikovat kritické aktualizace v celé organizační struktuře. Má úzkou vazbu na DNS (Active Directory)
API	Komplexně definované komunikační rozhraní aplikace *(Application Programming Inteface)*
CEF	Datový formát pro uložení logů *(Common Event Format)*
CIFS	Síťový komunikační protokol pro přenos souborů. Kompatibilní se SMB verze 1.0 *(Common Internet File System)*
CSV	Jednoduchý textový souborový formát (Comma-separated values)
DB	Databázový software/aplikace/entita/instance, která je zpravidla provozována na databázovém serveru *(Database Entity)*
DB	Soubor datových objektů v elektronické formě uložených společně podle jednoho schématu a zpřístupňovaných počítačem *(Database)*
DB	Komponenta DBMS umožňující operace s daty v databázi. Mnohé DBMS podporují více DB enginů s různými vlastnostmi a specifiky *(Database Engine, Storage Engine)*
DBMS	Systém řízení databáze *(Database Management System)*
DNS	Distribuovaný hierarchický jmenný systém používaný v síti Internet. Překládá názvy domén na číselné IP adresy a zpět, obsahuje informace o tom, které stroje poskytují příslušnou službu (Domain Name System)
HTTP	Standardizovaný protokol pro přenos webových stránek *(Hyper-text Transfer Protokol)*
HTTPS	Standardizovaný zabezpečený protokol pro přenos webových stránek *(Secured Hyper-text Transfer Protokol)*
HW	Hardware označuje veškeré fyzicky existující technické vybavení počítače
IaaS	Typ cloudové služby, který poskytuje zákazníkům základní IT infrastrukturu jako službu, včetně serverů, úložiště, sítě a virtuálních počítačů. Tyto služby se často poskytují prostřednictvím Internetu a umožňují zákazníkům snadno a rychle využívat IT infrastrukturu bez nutnosti jejího nákupu, instalace a správy. Mezi nejznámější poskytovatele IaaS patří Amazon Web Services, Microsoft Azure a Google Cloud Platform *(Infrastructure as a Service)*
ICMP	Síťový protokol, který slouží ke komunikaci mezi síťovými prvky (jako jsou routery) a k odesílání zpráv o stavu sítě. Tyto zprávy obsahují informace o stavu spojení, jako jsou například informace o chybách nebo omezeních v síti. ICMP se často používá k diagnostice a řešení problémů v síti, například k zjišťování, zda je určitý cíl dostupný nebo zda existuje cesta k němu *(Internet Control Message Protocol)*
ICT	Informační a komunikační technologie *(Information and Communication Technology)*
IPMI	Standardizovaný protokol pro vzdálený dohled a management fyzických zařízení
IT	Informační technologie *(Information Technology)*
JDBC	API v jazyce Java pro jednotné rozhraní k relačním databázím *(Java Database Connectivity)*
JSON	Datový formát primárně určený pro přenos dat. Jedná se o způsob zápisu dat nezávislý na počítačové platformě, která mohou být organizována v polích nebo agregována v objektech *(JavaScript Object Notation)*
LEEF	Datový formát pro uložení logů *(Log Event Extended Format)*
MFA	Více-faktorové ověření identity uživatele *(Multi-Factor Authentification)*
NFS	Síťový souborový protokol primárně pro připojení vzdálených souborových systémů *(Network File System)*
OS	Operační systém *(Operating System)*
PaaS	Typ cloudové služby, která poskytuje vývojářům a IT týmům platformu pro vývoj, nasazení a správu aplikací bez nutnosti starat se o správu hardwaru a infrastruktury. Poskytovatelé PaaS nabízejí vývojové nástroje, databáze, síťové služby a další nástroje jako služby, což umožňuje vývojářům se soustředit pouze na vývoj aplikace *(Platform as a Service)*

PAM	Řešení zabezpečení identit, které pomáhá chránit organizaci před kybernetickými hrozbami monitorováním, zjišťováním a prevencí neoprávněného privilegovaného přístupu k důležitým prostředkům *(Privileged Access Management)*
PoC	Tento pojem se pro předběžné vyzkoušení určitého návrhu (zpravidla na reálných datech či jejich výběru), aby došlo k vyzkoušení nebo předvedení použité logiky a proveditelnosti návrhu řešení. V podstatě se může jednat o testovací realizaci nějakého konkrétního návrhu zpravidla ve zjednodušených podmínkách. Cílem PoC je ukázat, že návrh je technicky proveditelný a že má potenciál být úspěšný *(Proof of Concept)*
REST/API	Webově založené klient-server API *(Representational State Transfer)*
RFC	Soubor standardů zejména pro oblast sítí, počítačů a Internetu. RFC jsou považovány spíše za doporučení než normy či standardy v tradičním smyslu jako jsou například normy ČSN nebo ISO, avšak v zájmu interoperability jsou dodržovány *(Request For Comments)*
S2S VPN	Šifrované VPN připojení zajišťující propojení dvou LAN *(Site-to-Site VPN, LAN-to-LAN VPN)*
SCCM	SCCM je softwarový nástroj společnosti Microsoft určený pro správu a nasazení koncových zařízení a softwarových aplikací v prostředí Windows. SCCM umožňuje centrální správu a monitorování koncových zařízení, aktualizace softwaru a operačních systémů, správu konfiguračních položek a politik, sledování bezpečnostních opatření a mnoho dalšího. SCCM může být použit v podnikovém prostředí pro správu tisíců koncových zařízení, od stolních a notebooků až po mobilní zařízení a servery *(System Center Configuration Manager)*
SFTP	Zabezpečený protokol pro přenos souborů. Pro zajištění šifrování využívá protokol SSH *(SSH File Transfer Protocol)*
SLA	Smluvní nastavení záruk, úrovně, dostupnosti a kvality služeb atd. *(Service-Level Agreement)*
SMB	Komunikační protokol pro přenos souborů. Lidově nazývaný Samba *(Server Message Block)*
SNMP	Jedná se o protokol pro správu sítí na úrovni aplikační vrstvy síťového OSI modelu, který umožňuje správcům sítě monitorovat a řídit chod síťových zařízení, jako jsou routery, switche a průmyslové kontroléry. Protokol umožňuje správcům sítě získat informace o stavu zařízení, jako jsou statistiky paketů, využití zdrojů a stav služeb, a měnit nastavení zařízení na dálku *(Simple Network Management Protocol)*
SW	Programové vybavení počítače či jiného obdobného zařízení. Speciálním druhem software je *firmware*, který je úzce spjatý s konkrétním hardwarem *(Software)*
SŽ	Správa železnic, státní organizace
SŽT	Správa železniční telematiky, organizační jednotka
UAS	Logická uživatelsko-aplikační síť SŽ, zahrnuje VRF v MPLS sítích a lokální VLAN, běžně se nazývá také „Intranet SŽ"
VoKB	Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů
VPN	Virtuální privátní síť – prostředek pro důvěryhodné propojení komponent informačního systému v rámci obecně nezabezpečené komunikační sítě. Při navazování spojení je obvykle vyžadována autentizace, komunikace je většinou šifrována *(Virtual Private Network)*
WEC	Technologie předávání logů v prostředí Microsoft Windows *(Windows Event Collector)*
WEF	Technologie předávání logů v prostředí Microsoft Windows *(Windows Event Forwarder)*
XDR	Koncepce bezpečnosti informačních technologií, která integruje různé nástroje a technologie pro detekci a reakci na hrozby v jednotném systému. Cílem XDR je zlepšit schopnost detekovat a reagovat na hrozby v celém IT prostředí, včetně cloudových a on-premise systémů. Funkce XDR zahrnují automatickou detekci hrozeb, škálovatelnou analýzu, pokročilou vizualizaci a integraci s jinými bezpečnostními technologiemi *(Extended Detection and Response)*
ZoKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů

Seznam vysvětlivek

Build	Označení konkrétní verze software, zpravidla operačního systému.
Disaster Recovery	Plán obnovy po havárii, součást kontinuity IT služeb.
Log Management	Systém centrálního sběru a ukládání logů
Platforma SŽ	Soubor dokumentů, rozdělený na veřejnou, interní a metodickou část, určený pro seznámení dodavatelů se standardy a technologiemi v ICT prostředí SŽ.
Syslog	Standardizovaný formát pro ukládání a předávání logů

1 Úvod

Cílem tohoto dokumentu je definovat Platformu SŽ, jakožto souhrn podporovaných infrastrukturních služeb, technologií, a architektonických principů, která určuje základní rámec pro návrh řešení ICT jako celku. Platforma SŽ podporuje naplnění strategických cílů IS/ICT Správy železnic, zejména v oblasti efektivního provozu a rozvoje ICT prostředí Správy železnic.

2 Platforma Správy železnic

Platforma Správy železnic definuje prostředí, které standardizuje a podporuje návrh, implementaci a provozování veškerého ICT řešení pro Správu železnic. Popisuje infrastrukturní a platformní služby, podporované technologie a upravuje pravidla jejich použití i rozšiřování. Primárním cílem Platformy SŽ je poskytnout potenciálním dodavatelům základní přehled o ICT prostředí SŽ a současně umožnit organizaci SŽ zajištění efektivního vytváření a provozování ICT řešení při dodržení vysoké kvality a bezpečnosti služeb.

Dokument včetně příloh je udržován a pravidelně aktualizován organizační jednotkou SŽT.

Platforma SŽ obsahuje:

- Základní popis ICT prostředí (v jednotlivých přílohách)
- Architektonické principy SŽ
- Přehled služeb Platformy SŽ
- Přehled technologií Platformy SŽ (v jednotlivých přílohách)

Při plánování a rozšiřování ICT řešení je nutné respektovat všechny části Platformy SŽ, které se daného řešení dotýkají. Jednotlivé přílohy se pak detailně zabývají vybranými oblastmi od serverové a síťové infrastruktury, přes softwarový vývoj až po integrace, komunikaci a zálohování.

3 Motivace Platformy SŽ

Platforma SŽ je motivovaná schválenou strategií IS/ICT SŽ, a to konkrétně cílem *zajištění dlouhodobého koncepčního rozvoje IS/ICT a jeho souladu se strategickými cíli SŽ, a to zavedením řízení celopodnikové IS/ICT architektury*[1].

Cílem Správy železnic je zajistit:

- Nastavení jasných a povinných požadavků na nová navrhovaná řešení.
- Uchazeči výběrových řízení na ICT řešení mohou být hodnoceni na základě jejich celkové ekonomické efektivity, a nikoliv pouze na základě nabídkové ceny. Podrobná pravidla stanoví Zadávací dokumentace,
- Externí dodávky ICT řešení budou koncepčně a technologicky zapadat do celopodnikového prostředí Správy železnic,
- Dodávané řešení bude možné bezpečně a ekonomicky efektivně provozovat v krátko-, středně-, i dlouhodobém časovém horizontu,
- Provozované technologie SŽ budou perspektivní, moderní a bezpečné,
- Technologická různorodost ICT prostředí SŽ bude:
    - na jednu stranu dostatečně široká, aby neúměrně neomezovala soutěž potenciálních dodavatelů, a

[1] Strategie IT a ICT Správy železnic (157463/2021-SŽ-GŘ-SŽT)

- na druhou stranu dostatečně ohraničená, aby umožnila efektivní správu systémů jak dodavateli, tak zaměstnanci Správy železnic.

Mezi hlavní přínosy Platformy SŽ patří:

- Nastavení společných (minimálních/maximálních) úrovní vyspělosti jednotlivých technologií napříč IS/ICT SŽ a postupné omezení velkých rozdílů v úrovních používaných technologií.
- Stanovení architektonických a technologických standardů pro tvůrce systémů a pro uchazeče o dodávku IS/ICT pro SŽ.
- Zajištění standardizace technických prostředků.
- Zajištění ochrany předchozích investic zamezením vzniku duplicit.
- Zajištění možnosti bezpečného převzetí systémů do provozu a zajištění provozu interními silami Správy železnic.

4 Architektonické principy

Při návrhu a realizaci ICT řešení je nutné respektovat a dodržet několik základních principů a pravidel stanovených v Platformě SŽ.

4.1 Bezpečnost a soulad s vnitropodnikovými předpisy

- Navrhované řešení a procesy jím podporované musí být v souladu s legislativními a regulatorními nároky a vnitropodnikovými předpisy Správy železnic.
- Řešení musí umožnit monitorování akcí uživatelů, zejména jejich práce s daty a dokumenty.
- Musí být zajištěna administrovatelnost a auditovatelnost integračních vazeb.
- Vývoj a test nesmí být realizován na produkčním prostředí.
- Topologie a architektura produkčního a testovacího prostředí musí být identická, odlišovat se může ve výkonu a použitých zdrojích.
- Před nasazením do produkčního prostředí je řešení prokazatelně otestováno.
- Nejsou realizovány integrace mezi produkčními a neprodukčními prostředími.
- Dohled a monitoring je zajištěn na všech vrstvách řešení (HW, OS, DB, aplikační server, aplikace, tenký a tlustý klient, koncový uživatel).
- Musí být zajištěno napojení na centrální dohledovou konzoli.
- Služby poskytované do prostředí Internetu musí projít penetračním testováním.
- Navrhované řešení musí využívat šifrovanou komunikaci a v případě ukládání jakýchkoli citlivých informací (hesla apod.) je ukládat v šifrované podobě. Šifrovací algoritmy musí respektovat doporučení NÚKIB v dokumentu *Minimální požadavky na kryptografické algoritmy* v aktuální verzi, která je uveřejněna na úřední desce NÚKIB.

Zdůvodnění: Bezpečnost umožňuje chránit hodnoty Správy železnic. Ve SŽ je nutné udržovat vysokou míru bezpečnosti, a to především v oblastech, které mohou mít dopady na lidské životy. Navrhovaná řešení také musí být nezbytně v souladu s VoKB.

4.2 Auditní záznamy

Celé řešení i jednotlivé prvky řešení (infrastrukturní prvky, aplikace, OS, webové servery, databáze a middlewary) musí umožňovat vytvářet auditní záznamy tedy logy (záznamy např. čas přihlášení uživatele, čas odhlášení, import, export souborů a podobně) a jejich přenos do centrálního uložiště log managment v SŽ.

Veškeré činnosti v systému musí být logovány a to včetně neúspěšných pokusů. Jde zejména o následující činnosti:

- přihlášení a odhlášení uživatelů a administrátorů
- neúspěšný pokus o přihlášení
- činnosti provedené administrátory

- činnosti vedoucí ke změně přístupových oprávnění
- neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů
- zahájení a ukončení činností technických aktiv (například spuštění zastavení služeb)
- automatická varovná nebo chybová hlášení technických aktiv
- pokusy o manipulaci s logy a změny nastavení nástroje pro logování
- použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení
- operace s citlivými daty
- veškeré události spojené se změnou bezpečnostních parametrů systému

Řešení musí být schopno předávat auditní záznamy v minimálně jednom z formátů:

- CEF
- Microsoft Windows Event Log
- LEEF
- Strukturované DB view
- JSON
- CSV

Pomocí aspoň jednoho z protokolů:

- Syslog RFC5424
- WEC
- JDBC
- REST/API
- NFS
- SFTP
- CIFS/SMB
- SNMPv3

A musí obsahovat minimálně následující informace:

- časové razítko
- druh provedené akce
- unikátní identifikátor uživatele nebo služby
- zdroj události (zdrojová IP adresa/hostname komponenty systému, na které k akci došlo)

Zdůvodnění: Auditní záznamy jsou klíčovou součástí bezpečnosti. Ve SŽ je nutné zajistit vysokou míru bezpečnosti, a to mimo jiné i auditovatelností veškerých událostí.

4.3 Provozovatelnost řešení

- Řešení je provozovatelné na službách a technologiích Správy železnic.
- Řešení musí umožňovat převzetí do provozního prostředí Správy železnic
- Řešení umožňuje škálování.

Zdůvodnění: Z důvodu snahy o udržitelnost provozu je stanoven udržitelný počet technologií, které jsou spolehlivé a mají perspektivu svého rozvoje. Aplikace provozovaná na takto definované skupině technologií tak může být v případě potřeby převzata do provozu a spravována týmem IT specialistů SŽ, jež disponuje patřičnými znalostmi, případně vlastní příslušné certifikace, aby mohli tyto technologie či systémy spravovat. Tím dochází nejen ke zvýšení produktivity, ale také k časové a finanční úspoře, především z pohledu lidských zdrojů.

4.4 Znovupoužitelnost řešení

- Řešení musí umožňovat logické oddělení dat pro současné využívání funkcionality různými subjekty (tzv. multitenant).
- V rámci Správy železnic se realizuje minimalizace počtu a rozsahu používaných technologií a aplikací.

- Snižováním počtu a rozsahu používaných technologií a aplikací snižujeme komplexitu správy technologického a aplikačního portfolia.
- Řešení je navrhované s opakováním ověřených jednoduchých návrhových vzorů a designových principů.
- Nasazování změn a nových řešení je seskupováno dle funkcionalit a cílových systémů do jednotlivých „release". Termíny releasů jsou stanoveny organizační jednotkou SŽT.
- Nasazované řešení nesmí ke svému provozu vyžadovat pravidelný nutný zásah administrátora (např. restarty, čištění logů, ...)

Zdůvodnění: V rámci Správy železnic usilujeme o minimalizaci počtu prostředí pro stejnou funkcionalitu. Znovupoužitelná řešení vedou k úspoře lidských, finančních, časových i materiálních zdrojů v životním cyklu celého řešení.

4.5 Nezávislost na dodavatelích

- Řešení je navrhované s ohledem na omezení či eliminaci rizika vendor-lock.
- U řešení převzatých do provozu je cíl převzetí schopnosti vytvořit build aplikace bez závislosti na dodavateli.
- Usilujeme o právo zásahu do zdrojových kódů a rozvoje řešení interními kapacitami Správy železnic nebo dalšími dodavateli. Výjimku mohou tvořit jen případy, kdy by takové požadavky byly ekonomicky výrazně nevýhodné nebo je důvod se domnívat, že tato práva budou nadbytečná.

Zdůvodnění: Nebýt závislí na malém počtu dodavatelů umožňuje SŽ být transparentní a flexibilní. Vyšší míra flexibility je také výhodná pro vyjednávaní s jednotlivými dodavateli o ekonomických a technických podmínkách.

4.6 Nákup a vývoj

- U nákupu standardizovaných komerčních produktů je požadována schopnost nastavení balíkového řešení interními kapacitami či nezávislými externími dodavateli.
- U standardizovaných agend je preferován nákup a úprava před zakázkovým vývojem zcela nového zákaznického řešení.
- Vzájemné integrace musí být realizované přes aplikační middleware. Integrační scénáře zajišťují, aby implementace nových funkcí v řídící aplikaci minimalizovala vyvolané změny na straně návazných aplikací. Detailněji se integracemi zabývá Příloha 5 – *Integrační standardy*.
- Preferujeme přírůstkovou integraci před přenosem kompletních informací.
- Preferujeme řešení v minimálně třívrstvé architektuře s oddělením databázové, aplikační a prezentační vrstvy.
- Minimalizujeme dodávku řešení s takovými úpravami, které by omezovaly nebo eliminovaly přechod na budoucí vyšší verze produktu.
- V transakčních systémech preferujeme pouze základní operativní reporting. Plný reporting je implementovaný v analytických nástrojích.
- Řešení je řádně dokumentované po stránce vývojové, provozní, administrátorské a uživatelské.
- Případné zdrojové kódy jsou verzovány a ověřeny, že z nich je možno vytvořit interními týmy Správy železnic plnohodnotný a funkční build aplikace. Zdrojové kódy a dokumentace jsou ukládány na standardizované úložiště Správy železnic.
- Návrh prostředí reflektuje trendy technologií a zároveň business potřeby.
- Rozšiřování a doplňování technologií a ICT prostředí je v souladu s normami, interními směrnicemi a Platformou SŽ.

Zdůvodnění: Regulace nákupu a případného do-vývoje integrací a aplikací slouží k co nejsrozumitelnějšímu a transparentnímu užívání daných technologií. Díky danému postupu v nákupu a vývoji je možné se efektivně vyrovnat s novinkami, které nově nakoupené produkty představují a efektivně je začlenit do ICT prostředí Správy železnic.

4.7 Business kontinuita

- Navržené řešení musí odpovídat kritičnosti aplikace a požadovaným parametrům SLA.
- Servisní model a parametry aplikace odpovídají bezpečnostní klasifikaci a byznysové kritičnosti aplikace.
- Dle servisního modelu jsou definované plány obnovy („disaster recovery" postupy).
- SLA je třeba nastavovat a měřit na celém řetězci navázaných technologií a služeb.

Zdůvodnění: Správa železnic jakožto správce kritické infrastruktury státu, musí být připraven na případné narušení provozu, a proto musí požadovat taková řešení, která umožní zajistit kontinuitu a obnovu klíčových procesů, činností a systémů organizace.

5 Služby Platformy SŽ

Platforma SŽ popisuje služby poskytované v rámci ICT prostředí Správy železnic, které je možné využívat v navrhovaných a dodávaných řešeních a současně nesmí být totožné služby součástí dodávky daného řešení mimo Platformu SŽ. Cílem je zajistit ve fázích přípravy poptávky, návrhu ICT řešení a realizace dodávky kompatibilitu se stávajícím ICT prostředím a v maximální míře využít již provozované komponenty a technologie. Tento seznam služeb a komponent je průběžně aktualizován tak, aby byl popis ICT prostředí v největší míře aktuální.

5.1 Infrastrukturní služby

Infrastrukturní službou je míněno poskytování IT infrastruktury na úrovni HW, virtualizace, operačních systémů a diskových úložišť. Jedná se o obdobu cloudových IaaS.

Detailní přehled o infrastrukturních službách je předmětem Přílohy 3 – *Virtuální prostředí, serverové farmy a servery*.

5.2 Platformní služby

Platformní služba poskytuje standardizované webové či aplikační servery, databázové platformy či portálová řešení, která integrují webové aplikace a služby do jednoho spolupracujícího celku. Podporuje standardizované komunikační rozhraní, protokoly a formáty dat. Jedná se o obdobu cloudových PaaS. Platformní služby jsou v současné době dostupné jen v UAS.

Detailní přehled o infrastrukturních službách je předmětem Příloh Platformy SŽ.

5.3 Podpůrné služby

Podpůrné služby zajišťují komplexní správu a provoz IT infrastruktury v prostředí Správy železnic. Jedná se například o monitorovací systémy, zálohování, patch management, mandatorní síťové služby nebo bezpečnostní systémy.

Podpůrné služby jsou povinné k využití dodavatelem, pokud není Správou železnic určeno jinak.

5.3.1 Bezpečnostní služby

Přehled dostupných služeb bezpečnostních aplikací

Služba	Popis
Antivirus	Antivirové řešení F-Secure, provozované jako virtuální appliance, zajišťuje ochranu koncových stanic a serverové infrastruktury před škodlivým obsahem, zejména malwarem, exploity, síťovými útoky a jinými bezpečnostními hrozbami. Každé datové centrum Správy železnic disponuje vlastní virtuální appliance F-Secure. Nasazením antivirového řešení F-Secure jako virtuální appliance, jsou minimalizovány konzumované výpočetní zdroje a dopad na výkon virtualizační infrastruktury.
PAM	Privileged Access Management je řešení které pomáhá kontrolovat, monitorovat, zabezpečit a auditovat privilegované identity před jejich zneužitím. Omezení: PAM je v současné době dostupný jen v UAS.
XDR	XDR monitoruje síťovou infrastrukturu pomocí sond a uživatelské chování pomocí agentů na serverech a uživatelských stanicích. Bezpečnostní řešení XDR detekuje

	pokročilé bezpečnostní hrozby v prostředí SŽ. Každý server či uživatelská stanice musí mít nainstalovaného agenta XDR. V případě potřeby je možné upravit nastavení agenta pro korektní běh dodávaného systému. Omezení: Služby XDR jsou v současné době dostupné jen v UAS.
Log management	Řešení log managementu provádí sběr auditních záznamů z ICT infrastruktury SŽ. Omezení: V současné době je log management provozován v režimu PoC a je dostupný pouze v UAS.
Active Directory and Domain Services	Adresářová služba společnosti Microsoft pro správu zařízení a identit a jejich autentizaci a autorizaci v podnikových sítích. Dodávaná řešení musí podporovat integraci na službu Active Directory Správy železnic. Správa železnic provozuje multi-forest prostředí, proto musí aplikace umožňovat využití více AD konektorů, za účelem ověření uživatelů. Omezení: Služby Active Directory jsou v současné době dostupné jen v UAS.

5.3.2 Služby monitoringu

Služba dohledu ICT infrastruktury je zajištěna pomocí nástroje Zabbix a dohledových agentů instalovaných na provozovaném prostředí nebo bez-agentově se vzdáleným dohledem, sledování standardními protokoly SNMP, IPMI, HTTP, HTTPS, ICMP apod.

Dodavatelé ve spolupráci s organizační jednotkou SŽT zajistí napojení dodávaných řešení na monitoring Zadavatele. Tím není dotčena případná povinnost dodavatele řešení monitorovat kvalitu a dostupnost dodávaného řešení. Preferovaným řešením je v takovém případě využití služeb monitoringu SŽ s nastavením potřebných notifikací a procesů.

5.3.3 Služby patch managementu

Popis služeb patch managementu, aktualizací a distribuce aplikací

Služba	Popis
Distribuce SW a aktualizace koncových stanic	Technologií System Center Configuration Manager (SCCM) je zajištěna distribuce softwarových balíčků a aktualizace koncových stanic. Patchování klientských stanic probíhá 1 x měsíčně a je plně v gesci Správy železnic.
Aktualizace serverových operačních systémů	Aktualizace serverových operačních systému Windows Server je řešena skriptovacím jazykem Powershell. Patchování serverových operačních systémů probíhá 1 x měsíčně a je zajištěno Správou železnic, pokud není s dodavatelem řešení dohodnuto jinak.
Aktualizace linuxových operačních systémů	Aktualizace linuxových operačních systémů je řešena vlastním repozitářem (např. Red Hat Satellite). Patchování linuxových operačních systémů probíhá dle potřeby a je zajištěno Správou železnic, pokud není s dodavatelem řešení dohodnuto jinak.

5.3.4 Služby zálohování

Detailní přehled o službách zálohování je předmětem Přílohy 7 – *Standardy zálohování a disaster recovery*.

5.3.5 Síťové služby

Přehled síťových služby

Služba	Popis
DNS	Domain Name System (DNS) je kritickou službou, která má zásadní vliv na bezpečnost, odezvu a dostupnost služeb SŽ. Je nezbytná pro správný chod podnikové sítě a služeb na bázi Active directory. Správa železnic provozuje interní i externí službu DNS.
Firewall	Zařízení typu firewall jsou je velmi důležitým bezpečnostním prvkem ve veškeré elektronické komunikaci v sítích SŽ, jenž pomocí pravidel filtruje síťový provoz a chrání ICT prostředky v síti Správy železnic.
Proxy	Proxy soustava zajišťuje přístup uživatelů a serverů k internetu. Naprostá většina komunikace uživatelů (zaměstnanců SŽ) do sítě Internet prochází přes ni, jiný přístup není povolen. Proxy servery fungují jako prostředník mezi klienty a cílovými servery, mimo perimetr sítě SŽ, překládá klientské požadavky a vůči cílovému serveru vystupuje sám jako klient.
Reverzní proxy	Všechna připojení z internetu směřující na některý ze serverů jsou směrována přes reverzní proxy server, který buďto požadavek zpracuje sám nebo ho předá dál serverům. Umožňuje SSL terminaci a kompresi.
VPN	Služba virtuální privátní sítě, umožňující dodavateli zabezpečený přístup konkrétních zaměstnanců ke konkrétním prostředkům v prostředí Správy železnic. Omezení: Jedná se o jmennou VPN s MFA pro konkrétního externistu.
VPN S2S	Služba virtuální privátní sítě Site-to-Site.

Omezení: S2S VPN jsou zřizovány jen ve výjimečných případech po schválení Odborem IT architektury.

6 Technologie Platformy SŽ

V rámci služeb poskytovaných Platformou SŽ je využívána celá řada ICT technologií.

Tyto technologické služby, softwarové i hardwarové prostředky nesmějí být přímo použity v návrhu řešení mimo využití těch, které již Platforma SŽ poskytuje.

Pro některé případy výběrových řízení pro aplikační software je přípustné použití tzv. zapouzdřených technologií, jež nejsou součástí Platformy SŽ, ale nabízené řešení vyžaduje jejich nasazení. Zapouzdřená technologie je zpravidla součástí jiné primární technologie jako tzv. podpůrný program. Takový program nevyžaduje samostatnou instalaci, jelikož je instalován jako součást dané komponenty.

Použití takových zapouzdřených technologií je možné jen v následujících případech:

1. Jejich použití nebude klást žádné dodatečné provozní, finanční ani implementační nároky po celou dobu životnosti primární technologie.
2. Nebudou vyžadovat žádné dodatečné licence nad rámec licencí hlavního dodávaného řešení.
3. Aktualizace zapouzdřených technologií bude probíhat pouze současně s aktualizací hlavního dodávaného řešení.
4. Jejich podpora bude poskytována současně a ve stejném rozsahu jako podpora hlavního dodávaného řešení.
5. Zapouzdřené technologie nebudou vyžadovat žádné speciální provozní podporu, ze strany Správy železnic.
6. Zapouzdřené technologie jsou v souladu se standardy kybernetické bezpečnosti (ZoKB, VoKB).

Při použití zapouzdřených technologií je nutné danou technologii identifikovat nejméně v následujícím rozsahu – Název, Verze, Výrobce, Licence, Termín a úroveň podpory.

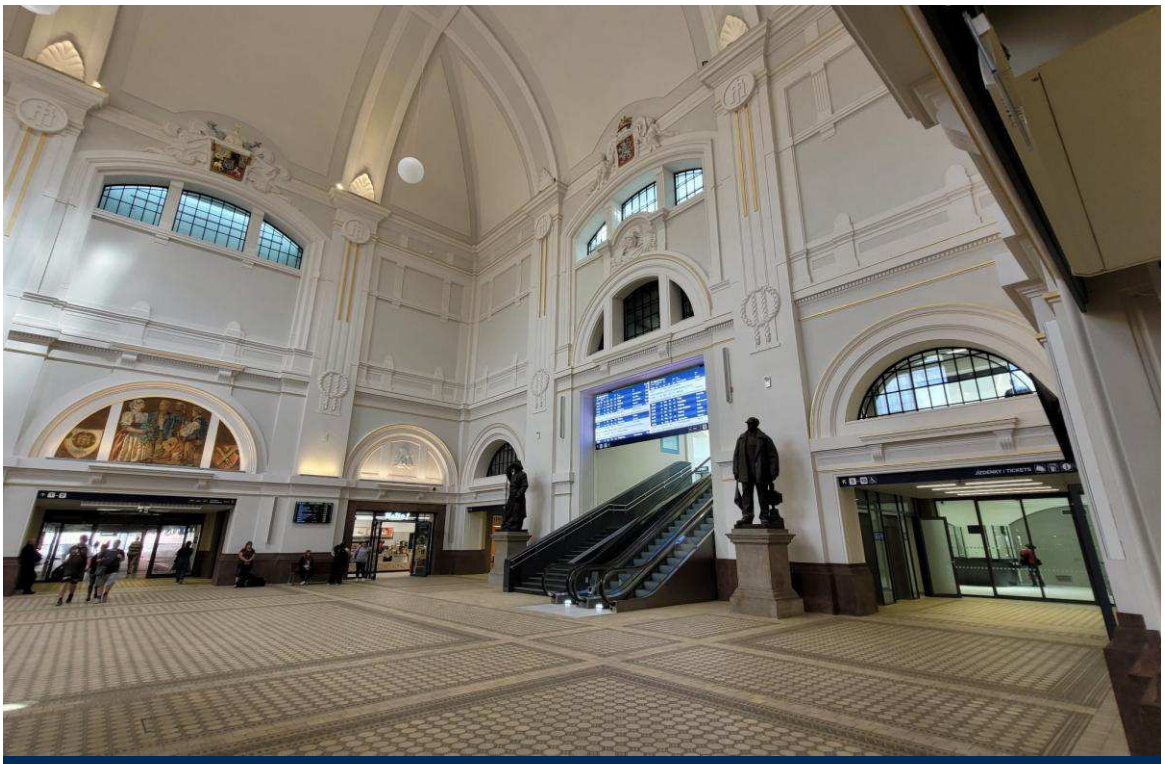
7 Přílohy Platformy SŽ

Jednotlivé oblasti jsou dále detailně zpracovány v těchto přílohách:

- Příloha 1 – Standardy softwarového vývoje
- Příloha 2 – Datová centra a serverovny
- Příloha 3 – Virtuální prostředí, serverové farmy a servery
- Příloha 4 – Konektivita a síťové prostředí
- Příloha 5 – Integrační standardy
- Příloha 6 – Komunikační standardy
- Příloha 7 – Standardy zálohování a disaster recovery
- Příloha 8 – Cloudové prostředí

Správa železnic, státní organizace
Správa železniční telematiky
Dlážděná 1003/7
110 00 Praha 1

Datum tisku
2025-07-30



Platforma SŽ Standardy vývoje software

Červen 2025

Obsah

Seznam zkratek

2FA	Dvou-faktorové ověření *(Two-Factor Authentification)*
3NF	Třetí normální forma návrhu tabulek databází řeší tranzitivní závislosti v rámci návrhu tabulek databází
DDL	*(Data Definition Language)*
EA	Podniková architektura *(Enterprise Architecture)*
GDPR	GDPR neboli Obecné nařízení o ochraně osobních údajů je zákon Evropské unie, který byl přijat v roce 2016 a začal platit v květnu 2018. GDPR upravuje ochranu osobních údajů občanů EU a stanovuje pravidla pro sběr, zpracování, uchovávání a předávání osobních údajů. Cílem GDPR je posílit ochranu osobních údajů a zvýšit kontrolu občanů nad jejich údaji. V ČR je implementován zákonem o zpracování osobních údajů č. 110/2019 Sb. *(General Data Protection Regulation)*
ICT	Informační a komunikační technologie *(Information and Communication Technology)*
IT	Informační technologie *(Information Technology)*
LDAP	*(Lightweight Directory Access Protocol)*
MFA	Více-faktorové ověření identity uživatele *(Multi-Factor Authentification)*
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
SAP	Modulární ERP systém od německé firmy SAP AG
SOA	Architektura orientovaná na služby – jedná se o softwarovou architekturu, která se zaměřuje na organizaci a strukturu aplikací a systémů jako soubor nezávislých a dobře definovaných služeb *(Service-Oriented Architecture)*
SQL	Standardní jazyk pro manipulaci s relačními databázemi. SQL umožňuje ukládat, manipulovat a vyhledávat data v relačních databázích. SQL je založeno na dotazech (queries) na data v databázích. Dotazy lze pak definovat a modifikovat strukturu databází, vytvářet a upravovat tabulky, indexy a další prvky, vkládat a aktualizovat data, mazat data a další operace. SQL je nezávislý na platformě, což znamená, že může být použit na různých operačních systémech a s různými databázovými systémy, avšak každá databázová platforma může mít různé změny v syntaxi *(Structured Query Language)*
SSO	*(Single Sign-On)*
SW	Programové vybavení počítače či jiného obdobného zařízení. Speciálním druhem software je *firmware*, který je úzce spjatý s konkrétním hardwarem *(Software)*
SŽ	Správa železnic, státní organizace
SŽT	Správa železniční telematiky, organizační jednotka SŽ
UI	*(User Interface)*
UNICODE	Univerzální kódování znaků s možností reprezentace všech národních znakových sad
UX	*(User Experience)*
VoKB	Vyhláška o kybernetické bezpečnosti č. 82/2018 Sb.
ZoKB	Zákon o kybernetické bezpečnosti č. 181/2014 Sb.
ZZOU	Zákon o zpracování osobních údajů č. 110/2019 Sb.

Seznam vysvětlivek

E-R model	*(Entity-Relationship model)*
Platforma SŽ	Soubor dokumentů, rozdělený na veřejnou, interní a metodickou část, určený pro seznámení dodavatelů se standardy a technologiemi v ICT prostředí SŽ.

1 Úvod

Cílem tohoto dokumentu je definovat Platformu SŽ, jakožto souhrn podporovaných infrastrukturních služeb, technologií, a architektonických principů, která definuje základní rámec pro návrh řešení ICT. Platforma SŽ naplňuje strategické cíle IS/ICT SŽ, zejména v oblasti efektivního provozu a rozvoje ICT prostředí Správy železnic.

2 Standardy vývoje informačních systémů Správy železnic

Při vývoji software ve Správě železnic je požadováno, aby byly plně respektovány obvyklé metodiky a „best-practice" pro návrh a vývoj software pomocí vícevrstvé architektury. Konkrétní užití jednotlivých vzorů se řídí vhodností, plánovanou zátěží a požadavky na dostupnost vyvíjeného software.

Aplikace či informační systém musí vždy podporovat škálování výkonu, redundanci a více-jádrové serverové systémy bez ohledu na zvolenou architekturu řešení.

2.1 Prostředí

Vývoj software, jeho testování i produkční nasazení musí probíhat v oddělených vzájemně se neovlivňujících prostředích.

2.1.1 Vývojové prostředí

Vývoj ve vývojovém prostředí (DEV) probíhá zpravidla u dodavatele. V prostředí Správy železnic probíhá vývoj v odůvodněných případech. Vývoj software současně využívá zcela oddělené instance databází a plně anonymizovaná data.

2.1.2 Testovací prostředí

Testování probíhá v testovacím prostředí (TEST) v prostředí Správy železnic. Mimo prostředí Správy železnic probíhá testování jen v odůvodněných případech. Při testování se používají zcela oddělené instance databází a plně anonymizovaná data. Testovací prostředí musí co nejvěrněji simulovat produkční prostředí, včetně konfigurace a objemu dat, aby případné chyby a nedostatky byly zachyceny ještě před nasazením změn do ostrého provozu.

2.1.3 Produkční prostředí

Po úspěšně akceptovaném testování je možné software přenést do ostrého produkčního prostředí (PROD) v prostředí Správy železnic. V případě software poskytovaného jako SaaS lze využít i cloudové prostředí Správy železnic nebo v odůvodněných případech i prostředí dodavatele.

2.2 Dvouvrstvá architektura

Dvouvrstvou architekturu při vývoji software lze využít v případě, kdy se jedná o menší, samostatný software, který nebude integrován na další informační systémy, nebo datové zdroje Správy železnic. Užití takovéhoto software je plánováno pro menší desítky uživatelů, bez požadavku na vysokou dostupnost a možnosti škálování výkonu a rozložení zátěže prostřednictvím clusterování. U tohoto typu software nejsou definovány požadavky na vysokou odolnost proti chybám, rychlou reakci systému, nebo správu dat pro velké sítě.

Využití dvouvrstvé architektury musí být předem diskutováno s Oddělením IT architektury, které v odůvodněných případech vydá příslušnou výjimku.

2.2.1 Datová vrstva

Realizace datové vrstvy je požadována prostřednictví preferované relační databáze (dle služeb Platformy SŽ) a respektováním metodiky 3NF. Je požadován jednoznačný datový model s minimální redundancí dat a datové struktury budou modelovány a popsány jazykovými konstrukcemi DDL, které jsou kompatibilní s určeným databázovým systémem.

Celá struktura dat bude popsána formálně prostředky E-R modelování. K datovému modelu je požadováno dodat korespondující SQL DDL skripty, který budou plně odpovídat dodané databázi. Je požadováno, aby správnost, úplnost a optimalizace datového modelu byla řešena již v rámci návrhu řešení.

V rámci dvouvrstvé architektury je umožněno, aby logika byla rozprostřena částečně v databázi a částečně v aplikační, resp. prezentační vrstvě.

2.2.2 Aplikační vrstva

Aplikační vrstva a prezentační vrstva je ve dvouvrstvé architektuře realizována jako jedna, společná a nedělitelná vrstva. Je požadováno, aby tato vrstva byla realizována v souladu s principy objektově orientovaného programování a komunikace mezi vrstvami byla realizována standardními zabezpečenými a šifrovanými protokoly. Je požadováno, aby uživatelské identity nebyly z aplikační vrstvy prezentovány do datové vrstvy, přičemž tyto vrstvy musí mezi sebou komunikovat technickým účtem, k tomu účelu v databázi vytvořeném.

Je požadováno, aby aplikační vrstva podporovala Multitasking, tedy umožňovala provádění několika procesů současně a systém byl již v rámci návrhu a vývoje optimalizován plánovaný výkon.

V rámci vývoje musí být ošetřena všechna bezpečnostní rizika popsaná v kapitole 2.5.

2.3 Třívrstvá a vícevrstvá architektura

Třívrstvá a vícevrstvá architektura je požadována při vývoji software ve všech případech, mimo výjimek uvedených v kapitole 2.1 nebo pokud není v zadávací dokumentaci VZ specifikováno jinak. Specifikace řešení vyžadující třívrstvou architekturu tak může disponovat následujícími vlastnostmi:

- Má být integrován na jiný software Správy železnic, nebo software třetích stran, a to z důvodu jednotného přístupu k datům a procesům vyvíjeného software
- Je plánováno využití pro větší počty uživatelů
- Je požadována vysoká dostupnost (HA)
- Je požadován Clustering pro rozložení zátěže a škálování výkonu
- Je požadována vysoká odolnost proti chybám, rychlá reakce systému, nebo správa dat pro velké sítě

2.3.1 Datová vrstva

Realizace datové vrstvy je primárně požadována prostřednictvím relační databáze nabízené Platformou SŽ, avšak pokud dodavatel navrhne jiné řešení (např. objektovou databázi či NoSQL), je povinen toto řešení zahrnout do své ceny implementace a provozu IS. Tento přístup zohledňuje různé typy úloh, kde využití relační databáze nemusí být vždy optimální.

Datový model musí být jednoznačný, s minimální redundancí dat, a datové struktury budou modelovány a popsány jazykovými konstrukcemi DDL, kompatibilními s určeným databázovým systémem. Formální popis celé struktury dat bude realizován prostředky E-R modelování, přičemž je možné povolit také objektový model, například formou diagramu tříd. K datovému modelu je nutné dodat odpovídající SQL DDL skripty, které plně reflektují implementovanou databázi. Důraz je kladen na to, aby správnost, úplnost a optimalizace datového modelu byly zajištěny již ve fázi návrhu řešení.

V rámci třívrstvé nebo vícevrstvé architektury není přípustné, aby logika byla rozdělena mezi databázi a aplikační vrstvu. Veškerá aplikační logika musí být umístěna výhradně v aplikační vrstvě.

2.3.2 Aplikační vrstva

Je požadováno, aby tato vrstva byla realizována v souladu s principy objektově orientovaného programování a komunikace mezi vrstvami byla realizována standardními zabezpečenými a šifrovanými protokoly. Je požadováno, aby uživatelské identity nebyly z aplikační vrstvy prezentovány do datové vrstvy, přičemž tyto dvě vrstvy musí mezi sebou komunikovat technickým účtem, k tomu účelu v databázi vytvořeném.

Je požadováno, aby aplikační vrstva podporovala Multitasking, tedy umožňovala provádění několika procesů současně a v již rámci návrhu a vývoje optimalizovat plánovaný výkon.

V rámci vývoje musí být ošetřena všechna bezpečnostní rizika popsaná v kapitole 2.5.

2.3.3 Prezentační vrstva

Pro interakci s uživatelem je požadováno, aby prezentační vrstva byla realizována desktopovým klientem (tlustým), nebo webovým klientem (tenkým), a to v závislosti na vhodnosti použití a požadavcích na software kladených. Komunikace mezi prezentační a aplikační vrstvou musí být realizována standardními zabezpečenými a šifrovanými protokoly.

V rámci prezentační vrstvy a desktopového klienta je možné přenesením části aplikační logiky na klienta, tedy využití prostředků klientské stanice ke zvýšení výkonu systému, ale pouze za předpokladu, že tento systému bude zabezpečovat konzistenci aplikační logiky, napříč všemi desktopovými klienty.

Bez aktualizačních mechanismů, které zajistí stejné verze software, na všech klientských stanicích v reálném čase není tato možnost povolena.

2.3.4 Integrační vrstva

V případě, kdy vyvíjený software má být integrován na jiný software Správy železnic, nebo software třetích stran, je požadováno, aby tato integrační vrstva byla realizována jako samostatná vrstva, umožňující škálování výkonu a rozložení zátěže.

Realizace integrací mezi aplikačními komponentami musí splňovat principy SOA. Veškerá komunikace tedy musí probíhat prostřednictvím definovaných služeb rozhraní, a není tedy povolena výměna dat prostřednictvím přímých vazeb, jako je sdílení paměti, souborů, nebo databází. Pokud je k dispozici, komunikace probíhá prostřednictvím k tomu určené sběrnice (ESB) nebo integrační platformy.

V případě, že má být vyvíjená komponenta integrována se **spisovou službou SŽ**, musí splňovat požadavky na integraci prostřednictvím Národního standardu pro elektronické systémy spisové služby[1] a integrace musí být rozhraními definovanými v tomto standardu také realizována.

V případě, že má být vyvíjená aplikace integrována s programovým prostředím komponent **systému SAP**, musí být realizována prostřednictvím určené integrační platformy (SAP Cloud Platform, příp. produktu, který jej nahradí). Detailní parametry požadavku na integraci budou definovány v příslušných případech.

Bez ohledu na zvolenou architekturu je zásadní klást důraz na kvalitní návrh a plánování celého řešení před zahájením implementace. Pečlivě promyšlený architektonický návrh výrazně snižuje riziko pozdějších problémů a nákladných úprav. Všechny požadované funkcionality by

[1] NSESSS, https://www.mvcr.cz/clanek/narodni-standard-pro-elektronicke-systemy-spisove-sluzby.aspx

proto měly být detailně navrženy a prověřeny již před implementací, čímž se předejde nutnosti dodatečně přepisovat nevhodně navržené části řešení. Zároveň je vhodné navrhovat systém modulárně s jasně definovanými komponentami a rozhraními. Oddělení jednotlivých funkčních celků zvyšuje soudržnost kódu a usnadňuje testování i budoucí údržbu.

Již v rámci architektonického návrhu je nutné zohlednit také bezpečnostní požadavky (např. způsob autentizace uživatelů, řízení oprávnění) a celkovou spolehlivost systému. Do návrhu je vhodné začlenit mechanismy pro ošetření chyb a podrobné logování, stejně jako podporu monitorování aplikace, aby bylo možné provozní problémy rychle detekovat a diagnostikovat. Před finálním schválením architektury by měl návrh projít revizí. Konečná podoba architektury musí být srozumitelná všem zainteresovaným stranám, což usnadní spolupráci při implementaci i následné řešení incidentů.

2.4 Požadavky na prezentační vrstvu

2.4.1 Uživatelské rozhraní

Pomocí uživatelského rozhraní může uživatel komunikovat se zařízením, počítačem a programy. Při navrhování vysoce kvalitního uživatelského rozhraní je požadováno zohlednit nejen vzhled rozhraní, ale také jeho logickou strukturu, aby s ním uživatel mohl snadno a rychle komunikovat a dosáhnout požadovaného výsledku bez zbytečného úsilí. Cílem je vytvořit rozhraní, které poskytuje jednoduchou, srozumitelnou a pohodlnou interakci uživatele s informačním systémem.

Pro návrh UI informačních systémů SŽ platí následující zásady:

- standardní ovládací prvky
- uživatelské rozhraní jednoduché a přehledné
- konzistentní prostředí
- účelné rozvržení obrazovek
- aplikace musí podporovat světlý i tmavý režim dle nastavení operačního systému a současně nastavení režimu nezávisle na nastavení operačního systému
- barvy a písma dle grafického manuálu
- hierarchie daná typograficky
- informování uživatele, co systém právě dělá
- odpovídající tvar a velikost ovládacích prvků
- kódování znaků UNICODE
- datumové položky dle českého standardu „DD.MM.RRRR“
- jednotný vizuální styl (pro některé projekty dle korporátní identity)
- webové aplikace musí mít responzivní design přizpůsobený určeným zařízením koncových uživatelů

2.4.2 Uživatelská zkušenost

Uživatelská zkušenost je to, co uživatel pocítí a pamatuje si v důsledku použití aplikace, systému nebo webu. UX formuje uživatelské chování a musí plnit požadavky uživatelů na danou aplikaci či webovou stránku. UX musí být bráno v úvahu při vývoji uživatelského rozhraní, vytváření informační architektury a testování použitelnosti informačních systémů SŽ. Po určení cílového publika a charakteristiky uživatelů je požadováno vytvořit seznam UX požadavků na projekt.

UX informačních systémů SŽ musí splňovat následující vlastnosti:

- usnadnění/zefetivnění práce uživatele
- návodné ovládání
- ergonomie
- jednoduché, intuitivní
- pravidla přístupnosti, tam kde je požadováno
- zobrazování relevantních a požadovaných dat

- doba zpracování požadavku na serveru by neměla přesáhnout 0,5 sekundy, aby celková doba odezvy uživatelských prvků byla kratší než 0,8 sekundy. Pokud bude předpokládaná doba odezvy delší než 0,8 sekundy, ale kratší než 2 sekundy, zobrazí se uživateli čekací kurzor. V případě, že doba odezvy přesáhne 2 sekundy, bude uživateli zobrazen indikátor průběhu operace (progress bar) pro lepší informovanost o stavu zpracování
- použít lazy loading tak, aby uživatel měl co nejrychlejší odezvu
- jednotná terminologie v celém systému
- ne všechno na jedné obrazovce
- ne všechno v rozbalovacím menu (příliš mnoho položek)
- navigace, kde se uživatel v aplikaci nachází
- minimalizace použití dlouhých textů
- vhodné využití grafických a obrazových prvků
- nepoužívat drobný text
- pečlivé plánování dialogů (logické skupiny)
- ne překrývající se dialogy
- jednotné, stejné ovládací prvky v dialozích na stejných místech s popisky s jednotnou terminologií

2.5 Bezpečnost

Všechny vyvíjené aplikace musejí splňovat požadavky kladené platnou legislativou. Požadovaný je také soulad s NÚKIB (Bezpečný vývoj aplikací).

Z pohledu požadavků na vyvíjený software je nutné zajistit oblasti:

- Zálohování a obnova
- Bezpečnost komunikací
- Řízení přístupu
- Ochrana před škodlivým kódem
- Logování a monitoring
- Bezpečné předávání a výměna informací
- Akvizice, vývoj a údržba

2.5.1 Zabezpečení aplikací

Je požadováno, aby jednotlivé vrstvy splňovaly minimálně tyto požadavky:

- Ke komunikaci mezi jednotlivými vrstvami je používán systémový účet, který lze v případě ohrožení kybernetické bezpečnosti deaktivovat, nebo změnit.
- Systémový účet, který je využíván ke komunikaci mezi vrstvami není privilegovaným účtem.
- Všechny vrstvy jsou ošetřeny proti nejzávažnějším bezpečnostním rizikům jako jsou[2]:
  - Injection
  - Broken Authentication
  - Sensitive Data Exposure
  - XML External Entities (XXE)
  - Broken Access Control
  - Security Misconfiguration
  - Cross-Site Scripting (XSS)
  - Insecure Deserialization
  - Using Components with Known Vulnerabilities
  - Insufficient Logging&Monitoring
- Jednotlivé vrstvy uchovávají své konfigurační parametry v šifrované podobě.

K zajištění bezpečnosti již během samotného vývoje je požadováno zavést a důsledně dodržovat jednotné standardy psaní kódu. Jasně definovaný styl psaní kódu (názvosloví, formátování, ošetření výjimek, validace vstupů apod.) zajistí konzistentní kvalitu kódu napříč vývojovým týmem a pomáhá předcházet chybám včetně bezpečnostních zranitelností.

[2] Dle aktuálního seznamu nejzávažnějších bezpečnostních rizik definovaných OWASP (https://owasp.org/).

Dodržování těchto standardů je potřeba průběžně ověřovat pomocí automatizovaných nástrojů, které dokáží odhalit porušení konvencí nebo potenciálně rizikové konstrukce již v rané fázi vývoje.
Neméně důležitou součástí procesu vývoje je pravidelná revize kódu prováděná druhým vývojářem před sloučením změn do hlavní vývojové větve. Uplatnění principu „čtyř očí" pomáhá odhalit chyby a nedostatky ještě před nasazením do produkce a ověřit dodržování stanovených standardů i architektonických principů. Každý podstatný zásah do kódu proto musí projít nezávislou kontrolou, aby se do produkčního prostředí dostal pouze prověřený kód odpovídající požadované kvalitě.
Aplikace musí důsledně logovat všechny podstatné události v systému. Zejména veškeré administrátorské akce, změny konfigurací nebo zásadních oprávnění a přístupy k citlivým datům musí být zaznamenány v auditních záznamech s informací o tom, kdo a kdy danou operaci provedl.
Logy je doporučeno centralizovat pomocí nástroje typu SIEM, což umožní efektivní vyhledávání a detekci podezřelých aktivit a vytvoření ucelené auditní stopy pro potřeby bezpečnostních kontrol či vyšetřování incidentů. Je zároveň nezbytné zajistit integritu a důvěrnost těchto záznamů – přístup k nim smí mít pouze pověřené osoby a úložiště logů musí být chráněno proti neoprávněným zásahům.

2.5.2 Autentizace a autorizace

2.5.2.1 Autentizace

Autentizace je proces ověření proklamované identity subjektu. Je požadováno, aby aplikace umožňovala následující typy autentizace:

- SSO (Single Sign-On), autentizaci pomocí protokolu Kerberos, nebo OpenID proti Active Directory
- Autentizaci pomocí protokolu LDAP, proti Active Directory
- Řešení 2FA či MFA

Zvláště u kritických systémů a všech privilegovaných účtů je požadováno použití silné MFA autentizace. Tento přístup výrazně snižuje riziko neoprávněného přístupu v případě prozrazení hesla.

Manuální přihlášení a autentizaci pomocí vyvíjeného software (uživatelská jména a hesla jsou uložena v databázi v šifrované podobě) je možné jen na základě schválené výjimky Odborem IT architektury SŽT.

2.5.2.2 Autorizace

Je požadováno, aby vyvíjený software obsahoval vlastní autorizační modul, který bude minimálně umožňovat:

- Vytváření uživatelských účtů
- Vytváření rolí
- Přidělování jednotlivých uživatelských účtů k rolím
- Přidělování konkrétních oprávnění na role

Kromě uvedené funkčnosti je nutné v rámci správy přístupů důsledně uplatňovat princip minimálních oprávnění. Každému uživateli se přidělují pouze taková práva, která nezbytně potřebuje k výkonu své role – nic víc. Správa privilegovaných účtů (administrátorů apod.) vyžaduje zvýšenou pozornost: každý administrátor musí používat svůj vlastní individuální účet s vyššími právy (nesmí se využívat sdílené ani výchozí „Administrator" účty) a počet těchto účtů je třeba omezit na nezbytné minimum. Je nutné pravidelně prověřovat používání privilegovaných účtů a okamžitě odebrat přístupy, které již nejsou nutné. Zároveň platí striktní oddělení odpovědností – žádná jednotlivá osoba by neměla mít plnou a nekontrolovanou správu kritického systému bez kontroly další osoby.

Pro zvýšení bezpečnosti privilegovaných přístupů jsou tyto řízeny nástroji PAM (Privileged Access Management). Tyto nástroje umožňují například dočasné udělení administrátorských oprávnění na nezbytně nutnou dobu (princip „just-in-time"), bezpečné uložení a

automatizovanou obměnu hesel privilegovaných účtů a detailní monitorování akcí prováděných administrátory.

V rámci naplnění povinností vyplývajících ze ZoKB a VoKB je požadováno, aby vyvíjený software umožňoval správu uživatelů a rolí pomocí externího nástroje na řízení identit. Integrace mezi vyvíjeným softwarem a Identity management bude realizována prostřednictvím integrační vrstvy vyvíjeného software.

2.5.3 Zpracování osobních údajů

Je požadováno kompletní splnění všech požadavků na zpracování osobních údajů dle zákona o zpracování osobních údajů č. 110/2019 Sb. (GDPR). Analýza a návrh opatření musí být řešen již v rámci návrhu řešení.

2.6 Dokumentace

Veškerá dokumentace musí být průběžně aktualizována při každé podstatné změně systému. Aktualizace příslušných dokumentů je nedílnou součástí dokončení každé vývojové etapy/milníku. Zastaralé nebo neúplné informace v dokumentaci mohou vést k nesprávným rozhodnutím a chybám při provozu či dalším vývoji systému.

Dokumentaci je zároveň nutné udržovat snadno dostupnou všem členům týmu i dalším zainteresovaným stranám (sdílený repozitář). Dobře strukturované a přehledné dokumentační výstupy usnadňují spolupráci v týmu a zaučování nových členů. Zároveň slouží jako spolehlivý zdroj informací při řešení incidentů a plánování změn, což přispívá k vyšší kvalitě a stabilitě dodávaného software.

Je požadováno, aby součástí dodávky vyvíjeného software byla dokumentace, a to minimálně v rozsahu:

2.6.1 Technická dokumentace jádra systému

Dokumentace jádra systému, jeho funkcí, služeb a rozhraní. Dokumentace bude obsahovat kompletní popis architektury jádra systému, výčet a podrobný popis všech jeho funkcí, přehled a popis služeb, které jádro poskytuje dalším komponentám systému, modulům a knihovnám.

2.6.2 E-R modely databáze

Kompletní dokumentace ve formě E-R schémat pro všechny implementované databáze včetně korespondujících DDL SQL skriptů.

2.6.3 Objektový model pro aplikace

Dokumentace obsahující objektové modely všech funkcí, jejich komponent, modulů, vztahů.

2.6.4 Procesní diagramy, schémata toků dat

Dokumentace obsahující procesní diagramy a mapu všech toků dat celého řešení.

2.6.5 Komunikační rozhraní

Dokumentace všech typů komunikačních rozhraní, všech jejich registrovaných služeb a všech funkcí, struktur dat a vlastností těchto služeb.

2.6.6 Drátové modely všech obrazovek uživatelského rozhraní aplikací

Dokumentace všech částí software musí obsahovat drátové modely všech obrazovek UI včetně popisu funkcí prvků každé obrazovky.

2.6.7 Popis konfigurace provozního prostředí

Dokumentace musí obsahovat soupis všech požadavků na nastavení hardwarových a softwarových komponent běhového prostředí jako jsou:

- mapování souborových systémů
- požadavky na operační paměť a počty jader
- konfigurační parametry jednotlivých podpůrných SW prostředků (např. specifika pro nastavení databáze, aplikačního serveru, webového serveru, apod.)

2.6.8 Uživatelská příručka

Příručka bude distribuována uživatelům. Musí obsahovat kompletní popis všech uživatelských funkcí pro práci se software. Příručka bude využívána jako základní materiál pro školení nových uživatelů. Příručka musí obsahovat kvalitně a jednoznačně zpracovaný popis kroků pro jednotlivé implementované funkce s vhodným doprovodným obrazovým materiálem ve formě výřezů obrazovek. Musí být napsána v českém jazyce a před finálním odevzdáním zpracovaná jazykovým korektorem.

2.6.9 Příručka administrátora

Příručka bude distribuována úzké skupině uživatelů, administrátorům systému. Musí obsahovat kompletní popis všech funkcí pro práci s administrací software. Příručka bude využívána jako materiál pro školení nových administrátorů. Příručka musí obsahovat kvalitně a jednoznačně zpracovaný popis kroků pro jednotlivé implementované funkce s vhodným doprovodným obrazovým materiálem ve formě výřezů obrazovek. Musí být napsána v českém jazyce a před finálním odevzdáním zpracovaná jazykovým korektorem.

2.6.10 Disaster Recovery postup (D/R Postup)

Dokumentace Disaster Recovery postupu bude obsahovat kompletní plán pro obnovu klíčových systémů a dat v případě mimořádné události nebo havárie. Tento plán bude zahrnovat podrobný popis zálohovacích strategií, metod obnovy, a kroků nutných pro minimalizaci výpadků a rychlou obnovu provozu. Dokumentace bude sloužit jako základní materiál pro školení týmů odpovědných za implementaci a správu obnovovacích procesů.

2.7 Modelování EA architektury

Každý Dodavatel je povinen řádně dokumentovat dodávané řešení v podobě modelu Enterprise Architektury. V rámci SŽ je využíván jako modelovací nástroj SPARX Enterprise Architect ve verzi 16 a notace Archimate 3.2.

Za účelem udržení kompatibility všech vytvářených modelů má SŽ vytvořený přehled povolených elementů pro jednotlivé vrstvy, včetně popisu jejich charakteristik a povinných atributů (závaznou metodiku tvorby a údržby EA modelů). Dodavatel může doplnit další elementy, jejich schválení však podléhá Odboru IT architektury SŽT.

Modelovaní bude realizováno na repozitory SŽ, kam bude Dodavateli vytvořen přístup za účelem možnosti sdílet vytvořené prvky a jejich definované vazby, tak aby byla zachována kompatibilita.

Hlavním schvalovatelem předkládaných modelů je Odbor IT architektury SŽT.

2.8 Předávání vývoje do provozu

Pokud nebude určeno jinak, veškeré výstupy (zdrojové kódy, konfigurační soubory, testovací data, dokumentace atp.) musejí být předávány prostřednictvím určeného repositáře. Bez předání kompletní dokumentace nelze danou aplikaci či informační systém považovat za bezchybný a akceptovatelný v rámci procesu akceptace.

Pro bezproblémové nasazování nových verzí do provozu se doporučuje využívat metodiky Continuous Integration/Continuous Deployment (CI/CD). Každá změna zdrojového kódu by

měla projít automatizovaným procesem sestavení a sadou testů v rámci CI pipeline, aby se zamezilo proniknutí chyb do produkční verze. Před ostrým nasazením nové verze je zároveň nutné nasadit ji nejprve do testovacího prostředí, které věrně kopíruje produkční podmínky, a ověřit v něm bezchybnou funkčnost systému.

Pro nasazování do produkčního prostředí je požadována co největší automatizace, aby se vyloučila rizika plynoucí z ručních zásahů a byl zajištěn opakovatelný proces. Pro každý release musí existovat předem připravený a otestovaný postup pro rychlé navrácení systému k předchozí funkční verzi v případě, že se po nasazení vyskytnou závažné problémy. Každé nasazení je zároveň nutné řádně logovat a verzovat, aby byl k dispozici přesný záznam o nasazené verzi a provedených změnách.

Po nasazení nové verze do produkce je nezbytné aktivně monitorovat její provoz. Centrální dohled nad logy aplikace a klíčovými metrikami umožní týmu včas odhalit případné problémy a rychle na ně reagovat. Doporučuje se nastavit notifikace (např. e-mailové alerty) pro případ selhání některé z funkcionalit, aby odpovědné osoby byly neprodleně informovány o vzniklých chybách. Doporučuje se využít verzovací systém k uchování kompletní historie všech změn i nasazení včetně identifikace autorů a popisů, což zajistí plnou sledovatelnost a usnadní následné audity.

Správa železnic, státní organizace
Správa železniční telematiky
Dlážděná 1003/7
110 00 Praha 1

Datum tisku
2025-07-30

Platforma SŽ Datová centra a serverovny

Červen 2025

Obsah

Seznam zkratek

ASHS	Stabilní hasicí zařízení, běžně se označuje i zkratkou SHZ a zpravidla bývá na bázi vodních sprinklerů nebo směsi inertních plynů, které jsou ekologicky neškodné
CDP	Centrální dispečerské pracoviště v kontextu organizační struktury SŽ (CDP Praha, CDP Přerov)
EPS	Technologie pro detekci a signalizaci požáru v budovách. Systém EPS zahrnuje detektory požáru, které jsou umístěny v různých částech budovy a slouží k detekci ohně nebo kouře. Detektory jsou připojeny k řídící jednotce, která sbírá a analyzuje data z detektorů a rozhoduje, zda má být spuštěna alarmová signalizace. Systémy EPS mohou být konfigurovány pro přenos informací o požáru na centrální monitorovací stanice nebo na místní hasičské sbory, aby byla zajištěna rychlá reakce a minimalizovány škody a ztráty na životech *(Elektronická požární signalizace)*
EZS	Technologie pro ochranu majetku, budov a objektů před neoprávněným vstupem a krádežemi. EZS zahrnuje detektory pohybu, otvírání dveří a oken, kamerové systémy, zabezpečovací panely a další zařízení pro monitorování a signalizaci neoprávněného vstupu nebo pokusů o krádež *(Elektronická zabezpečovací signalizace)*
ICT	Informační a komunikační technologie *(Information and Communication Technology)*
IT	Informační technologie *(Information Technology)*
OJ	Organizační jednotka SŽ
OŘ	Oblastní ředitelství SŽ
OT	Provozní technologie *(Operations Technology)*
SŽ	Správa železnic, státní organizace
TIER	Klasifikace datových center dle Uptime Institute. Datová centra se pak označují jako TIER 1 (nejnižší zabezpečení) až TIER 4 (nejvyšší zabezpečení)
UPS	Zdroj nepřerušovaného napájení je zařízení, které zajišťuje souvislou dodávku elektrické energie pro spotřebiče, které nesmějí být neočekávaně vypnuty *(Uninterruptible Power Supply)*

Seznam vysvětlivek

Platforma SŽ	Soubor dokumentů, rozdělený na veřejnou, interní a metodickou část, určený pro seznámení dodavatelů se standardy a technologiemi v ICT prostředí SŽ.

1 Úvod

Cílem této části Platformy SŽ je, dle kategorizace datových center a serveroven v prostředí Správy železnic, definovat technické požadavky na jejich výstavbu a s tím související popis používaných technologií v datových centrech, serverovnách a technologických místnostech. Současně dokument slouží jako popis fyzického ICT prostředí, kde jsou provozovány ICT technologie a provozovány informační systémy.

Z pohledu ICT infrastruktury jde o lokality, kde jsou umístěné zpravidla serverové technologie pro provoz aplikací a podpůrných systémů, technologie datových spojů, telefonie a další. Může zde být umístěna i technika externích dodavatelů či napojení na kritické podpůrné systémy externích subjektů (HZS ČR, PČR, ČEZ).

Datová centra jsou obecně definována jako samostatné budovy sloužící výhradně pro provoz ICT infrastruktury. Z pohledu provozu a dostupnosti jsou pak kategorizována hodnotami TIER. Kategorizace mimo jiné zohledňuje redundanci napájení, chlazení, konektivity, fyzické zabezpečení a technologické vybavení samotných prostor. Vše je následně přepočteno na nominální dostupnost v procentech za jeden rok (viz ukazatel TIER).

Serverovny jsou pak definovány obdobně jako datová centra, jen již není požadována vyhrazená samostatná budova, ale běžně bývají součástí administrativních či provozních a technologických budov. Většina menších serveroven, technologických a sdělovacích místností ve Správě železnic vznikla přebudováním stávajících místností v příslušné budově.

Tabulka 1. Rozdělení DC a serveroven dle velikosti a významu

Datacentrum / serverovna / rack	Počet rackových skříní	Kritické aplikace	Serverová infrastruktura	Redundance (napájení, chlazení, konektivita)
Datové centrum	10-200+	ANO	ANO	ANO
Významná serverovna	6-25	ANO	ANO	ANO
Menší serverovna	4-16	ČÁSTEČNĚ	ANO	ČÁSTEČNĚ
Lokální serverovna	1-8	NE	ČÁSTEČNĚ	NE
Technologické místnosti	1-5	NE	ČÁSTEČNĚ	NE
Sdělovací místnosti	1-6	NE	NE	NE
Samostatné rackové skříně v budovách	1-3	NE	NE	NE

Výstavba a projektování datových center a serveroven je standardizována v souboru norem **ČSN EN 50600** a fyzické zabezpečení datových center je dále interně ve Správě železnic specifikováno ve směrnici **SM07** a jejích přílohách.

2 Datová centra

Správa železnic disponuje dvěma datovými centry, kde jsou umisťovány technologie jak IT, tak OT. Tato datová centra jsou součástí technologických řídících center, odkud je dálkově řízen železniční provoz.

2.1 Datové centrum CDP Praha

Jedná se o primární datové centrum Správy železnic, které zajišťuje běh velkého počtu provozovaných informačních systémů a aplikací. V datovém centru jsou v samostatných sálech umístěny IT technologie i páteřní prvky celorepublikových sítí a rozsáhlé zařízení OT. Objekt je vně i uvnitř zabezpečen v souladu s běžnými standardy i interními směrnicemi.

Z technologického pohledu je zajištěno redundantní chlazení i napájení s kapacitou příkonu v průměru 3,5 kW pro jeden každý rack.

2.2 Datové centrum CDP Přerov

Jedná se o sekundární datové centrum Správy železnic, které zajišťuje záložní lokalitu pro běh provozovaných aplikací. V datovém centru jsou v hlavním sále umístěny veškeré serverové vybavení, technologické zařízení i síťové prvky.

Datové centrum v současné budově CDP Přerov je na své kapacitní hranici (jak fyzické, tak co se podpůrných technologií týká, jako jsou napájení nebo chlazení). V současné době probíhají práce na dostavbě a rozšíření CDP Přerov o druhou budovu, a to včetně nových datových sálů a nového řešení zálohovaného napájení.

3 Serverovny

Větších či menších serveroven Správa železnic provozuje desítky v mnoha lokalitách po celém území republiky.

3.1 Významné serverovny

Správa železnic provozuje řadu serveroven, které jsou z pohledu SŽ významné svým umístěním nebo účelem, nikoli však třeba velikostí nebo provozovanými technologiemi. Patří sem třeba serverovny v budově Generálního ředitelství SŽ, serverovny kde se realizuje připojení k vnějším sítím a tvoří tak perimetr sítě.

3.2 Serverovny dle geografických oblastí

Serverovny OŘ slouží primárně pro provoz ICT infrastruktury a aplikací určených pro jednotlivá OŘ.

3.3 Serverovny vybraných organizačních jednotek

Vybrané specializované OJ provozují serverovny dedikované pro své potřeby. Jedná se především o různé vysoce specializované aplikace informační systémy.

3.4 Technologické serverovny

Technologické serverovny slouží k provozu OT serverové infrastruktury a dalších technologických zařízení.

3.5 Technologické a sdělovací místnosti

Technologické a sdělovací místnosti jsou umístěny téměř v každé železniční stanici a v mnoha administrativních či přímo technologických budovách. Úroveň jejich technologického a provozního vybavení je na nižší úrovni a pramení výhradně ze základních potřeb provozovaných systémů. Tyto prostory nejsou primárně určeny k provozu serverových technologií.

4 Technologické vybavení

Technické a bezpečnostní vybavení je velmi důležitým parametrem daného prostoru. V datových centrech a serverovnách jsou tyto nároky nejvyšší, ale i v běžných administrativních budovách jsou některé prvky nutné. Následující kapitoly popisují jednotlivé klíčové technologické prvky:

- **Stavební provedení –** Specifické stavební provedení datových center a serveroven je předpokladem pro bezpečné a spolehlivé provozování ICT infrastruktury.
- **Napájení** – Specifickým prvkem pro datová centra a serverovny je redundantní zálohované napájení.
- **Chlazení** – Stejně tak je pro datová centra typické chlazení datových sálů.
- **Elektronická zabezpečovací signalizace (EZS)** – Tyto systémy fyzické bezpečnosti se týkají všech typů budov Správy železnic včetně administrativních budov.
- **Přístupové a docházkové systémy** – Přístupové a docházkové systémy se používají napříč prostředím Správy železnic.
- **Kamerový systém** – Kamerové systémy uvnitř i vně budou jsou součástí fyzického zabezpečení budov.
- **Elektronické požární signalizace (EPS)** – Požární signalizace je dnes standardem jak v datových centrech a serverovnách, tak ve všech moderních administrativních budovách.
- **Automatické hasicí systémy (ASHS)** – Pro datová centra je ASHS nutným standardem a v případě požáru dokáže minimalizovat škody.
- **Ochrana proti vodě** – V datových centrech by měla být instalována ochrana proti vodě pro případ havárie.
- **Monitoring prostředí** – Monitoring prostředí (teplota, vlhkost) je pro datová centra a serverovny nepostradatelný prvek zajišťující bezpečný a spolehlivý provoz.
- **Dohled prostor** – Dohled je základní součástí fyzické bezpečnosti budov.

Cílem je pak zajistit pro SŽ datová centra s dostatečnými technickými parametry odpovídajícími minimálně klasifikaci TIER II a současně s dostatečnou fyzickou kapacitou pro umístění ICT infrastruktury.

4.1 Stavební provedení

Datová centra, serverovny a datové sály musí být projektovány v souladu se souborem norem ČSN EN 50600. Nepsaným standardem je například dvojitá zvýšená podlaha nebo dostatečně dimenzovaný přístup umožňující přepravu rackové skříně na výšku na paletovém vozíku.

4.2 Napájení

Napájení datových center a serveroven je klíčovou součástí provozu těchto zařízení. V datových centrech se provozuje mnoho kritických aplikací a systémů a proto je důležité zajistit spolehlivé napájení s dostatečnou kapacitou a zálohováním.

Potřeba elektrické energie v serverové infrastruktuře se během poslední dekády díky virtualizacím a rostoucí potřebě výkonu posunula pro každou serverovou rackovou skříň na hodnotu v průměru minimálně 5 kW špičkového příkonu (2,5 kW provozního příkonu).

Pro zálohování napájení se u datových center a významných serveroven používají diesel-generátory, záložní zdroje napájení a napájení z více zdrojů elektrické energie (distribuční soustava, UNZ). Určujícím faktorem je vždy kritičnost instalovaných technologií a požadavek na dobu zálohy.

Významným požadavkem je pak využívání centrálních záložních zdrojů v rámci prostor, jejich dimenzování a postupné rozšiřování. Cílem o omezit vznik většího počtu menších „ostrovních" záložních zdrojů v jedné serverovně, nebo technologické či sdělovací místnosti.

4.3 Chlazení

Chlazení datových center je důležitým faktorem pro udržení vysoké dostupnosti a spolehlivosti serverů a dalších zařízení v datovém centru. Provoz datových center vyžaduje velké množství elektrické energie a výsledkem je produkce velkého množství tepla. Pokud se teplo neodvádí

dostatečně rychle, může dojít k přehřátí zařízení, přerušení provozu a v některých případech i porušení či ztrátě dat.

Pokud je to technicky možné, je nutné zajistit chlazení koncepcí zakrytované studené uličky, což musí respektovat i směr montáže aktivních prvků. V datových centrech a významných serverovnách je dále vyžadována redundance chladících jednotek.

4.4 Bezpečnost

V datových centrech i serverovnách je nutné zajistit plně funkční EZS, EPS, přístupový systém i kamerový systém, který obsáhne nejen vnější perimetr budovy, ale i jednotlivé sály a uličky mezi rackovými řadami.

Automatický hasicí systém jako rozšíření systému EPS je preferovaným řešením, jelikož v případě požáru dokáže výrazně snížit způsobené škody na ICT infrastruktuře.

Nedílnou součástí je také fyzická bezpečnost a fyzické zabezpečení datových center a budov, kde jsou umístěny významné serverovny.

4.5 Síťová infrastruktura

Datová centra a serverovny musí být síťově odděleny od zbytku sítě pomocí firewallu. Pro místní síťové připojení je nutné používat výhradně síťové prvky detailně definované v Příloze 4 – *Konektivita a síťové prostředí*.

4.6 Ostatní vybavení

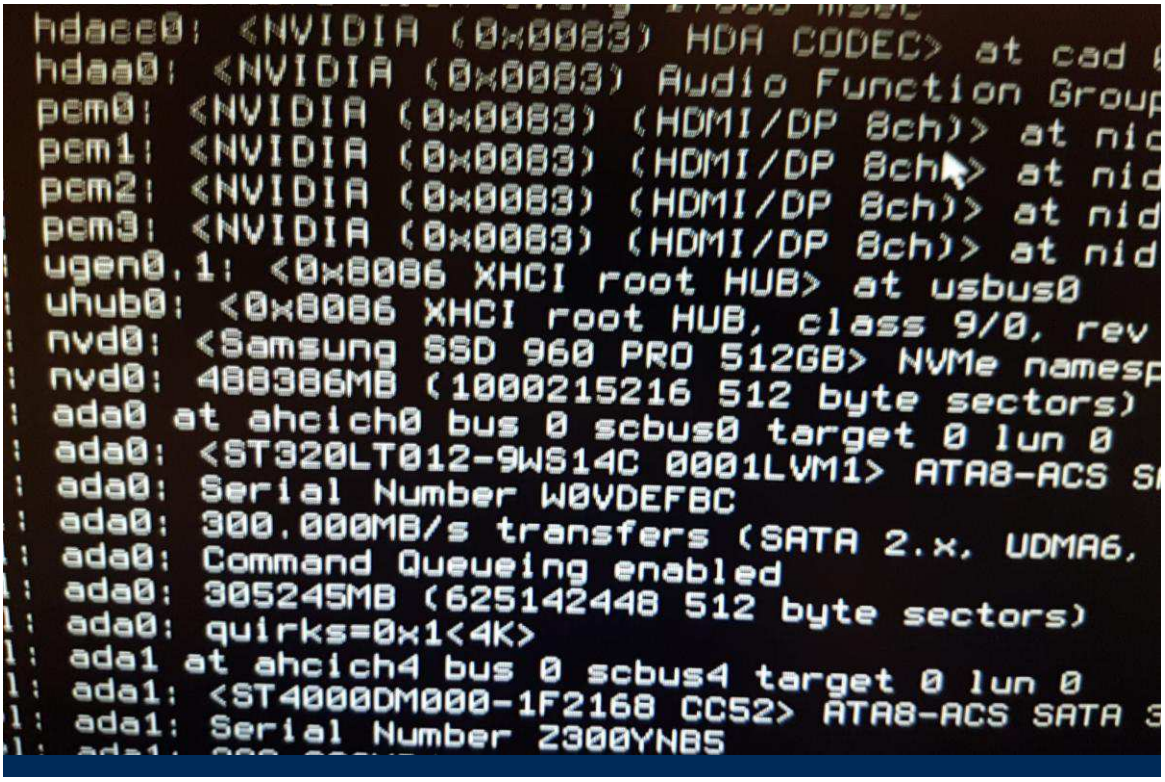
Monitorování prostředí v datových centrech je velmi důležité, protože kritické IT systémy jsou citlivé na změny teploty, vlhkosti a kvality vzduchu. Při narušení těchto parametrů může dojít ke vzniku problémů, jako jsou selhání systémů a ztráta dat. Proto se v datových centrech používají speciální senzory a zařízení pro monitorování a řízení prostředí.

Nová i rekonstruovaná datová centra a serverovny musí monitorovat minimálně tyto parametry:

- Teplota
- Vlhkost
- Stav napájení (zálohovaného i nezálohovaného)

Správa železnic, státní organizace
Správa železniční telematiky
Dlážděná 1003/7
110 00 Praha 1

Datum tisku
2025-07-30



Platforma SŽ
Virtuální prostředí, serverové farmy, servery

Červen 2025

Obsah

Seznam zkratek

ACI	Technologie aplikačně orientované infrastruktury firmy Cisco *(Cisco ACI)*
CPU	Hlavní procesor zařízení či počítače, který je zodpovědný za plynulé spouštění software *(Central Processing Unit)*
DB	Databázová aplikace *(Database Engine)*
DR	Plán obnovy po havárii, součást kontinuity IT služeb *(Disaster Recovery)*
FC	Vysokorychlostní datové rozhraní primárně používané pro datová úložiště *(Fibre Channel)*
HCI	Jde o formu softwarově definované serverové infrastruktury. V principu se jedná o virtualizační platformu, která redundantně sdílí v rámci clusteru vše – výpočetní výkon, paměť i datové úložiště *(Hyperconverged Infrastructure)*
HTTP	Standardizovaný protokol pro přenos webových stránek *(Hyper-text Transfer Protokol)*
HW	Hardware označuje veškeré fyzicky existující technické vybavení počítače
ICT	Informační a komunikační technologie *(Information and Communication Technology)*
iSCSI	Protokol, který umožňuje připojení k diskovým zdrojům přes počítačovou síť. To umožňuje serverům, aby mohly vzdáleně používat disky jako by byly připojeny přímo k nim, což umožňuje centralizaci a vzdálený přístup k datům. iSCSI je často používán v malých a středních podnicích jako alternativa k SAN *(Internet Small Computer System Interface)*
IT	Informační technologie *(Information Technology)*
LTO	Otevřený formát magnetické pásky určené pro záznam velkých objemů dat *(Linear Tape Open)*
NAS	Zařízení pro ukládání a správu dat, které je připojeno k počítačové síti a umožňuje přístup k datům přes souborové protokoly jako SMB, NFS, FTP a HTTP. NAS může být malé zařízení pro jeden či několik disků určené pro domácnosti nebo může jít profesionální zařízení určené pro montáž do racku *(Network Attached Storage)*
OS	Operační systém
SAN	Oddělená datová síť pro připojení datových úložišť. Zpravidla používá protokol FC nebo iSCSI *(Storage Area Network)*
SAP	Modulární ERP systém od německé firmy SAP AG
SOHO	Obecné označení pro zařízení pro domácí a kancelářské použití *(Small Office / Home Office)*
SW	Software je sada všech počítačových programů používaných v počítači, které provádějí nějakou činnost
SŽ	Správa železnic, státní organizace
SŽT	Správa železničních informačních technologií
VDI	Technologie, která umožňuje uživatelům pracovat na virtuálním desktopu odděleném od jejich fyzického zařízení. Tyto virtuální desktopy jsou hostovány na centrálním serveru a uživatelé se k nim připojují pomocí klientských zařízení, jako jsou stolní počítače, notebooky nebo mobilní zařízení *(Virtual Desktop Infrastructure)*
VM	Virtuální počítač *(Virtual Machine)*

Seznam vysvětlivek

Platforma SŽ	Soubor dokumentů, rozdělený na veřejnou, interní a metodickou část, určený pro seznámení dodavatelů se standardy a technologiemi v ICT prostředí SŽ.

1 Úvod

Cílem této části Platformy SŽ je popis podporovaných infrastrukturních služeb, technologií, a architektonických principů v oblasti virtualizačního prostředí, fyzických serverů a virtuálních serverů všech typů v ICT prostředí Správy železnic. Tato příloha definuje jak poskytované infrastrukturní služby v rámci veřejných zakázek a návrhů dodávaných řešení, tak i samotné budování a rozšiřování virtualizačního prostředí Správy železnic.

Cílem je zajistit ve fázích přípravy poptávky, návrhu ICT řešení a realizace dodávky kompatibilitu se stávajícím ICT prostředím Správy železnic a v maximální míře využít již provozované komponenty a technologie.

2 Virtualizační prostředí

Správa železnic postupně transformuje starší serverovou infrastrukturu na moderní virtuální řešení avšak s ohledem na rozsáhlost ICT prostředí SŽ je tento proces stále aktuální. Velmi efektivní je stále také virtualizace koncových počítačů (VDI) ve spojení s centralizovaným řízením dopravy.

2.1 Virtualizace serverů

Správa železnic ve svém ICT prostředí provozu větší množství serverových farem poskytujících virtuální prostředí pro běh virtuálních serverů.

Starší a konzervativnější technologií jsou virtualizace na software MS HyperV (nepreferované řešení určené výhradně pro singlenody) a na software VMware vSphere (vícenodové farmy s dedikovanou storage připojenou zpravidla přes Fibre Channel).

Novější technologií je pak HCI s využitím software VMware vSphere a VMware vSAN.

2.2 Virtualizace koncových počítačů

Virtualizace typu VDI je provozována na řešení VMware Horizon a slouží především pro dispečerské stanice dálkového řízení.

S ohledem na specifické určení není tato technologie součástí infrastrukturních služeb nabízených Platformou SŽ.

2.3 Kontejnerizace

V ICT prostředí Správy železnic probíhá testování a development virtualizačního řešení pro platformy Docker a Kubernetes. V současné chvíli není možné toto nabídnout jako infrastrukturní službu v rámci Platformy SŽ.

3 Serverové farmy

Správa železnic provozuje větší množství serverových farem různých velikostí od 3 nodů až po 16 serverových nodů na různých technologiích (klasická virtualizace, virtualizace v OS, HCI, VDI). Z důvodu vzájemné kompatibility jsou využívány výhradně CPU x86_64 verze 3 od firmy Intel.

3.1 Konvergovaná infrastruktura

V rámci konvergované infrastruktury provozuje SŽ tyto druhy farem:

- Jedno-nodové virtualizace na řešení Microsoft Hyper-V – jedná se o nepreferované řešení výhradně jen pro virtualizaci OS Windows Server.
- Jedno-nodové virtualizace na řešení VMware – jedná se obecně o nepreferované řešení, výhradně určené jen pro vzdálené lokality s minimálními nároky na virtualizaci.
- Klasická virtualizace s dedikovanou storage – preferované řešení pro menší clustery
- Virtualizace VDI – výhradní řešení pro virtualizaci koncových počítačů

3.2 Hyper-konvergovaná infrastruktura

V minulých letech Správa železnic úspěšně adoptovala technologii HCI a v současné době na ní provozuje více než 10 serverových farem ve velikostech od 4 nodů až po 16 nodů.

Všechny tyto nové HCI clustery umožňují v budoucnosti zapojení do topologie Cisco ACI jako Remote Leaf.

Rozšiřování těchto farem musí respektovat tato pravidla a současně je z důvodu kompatibility nutné dodržet vždy shodné parametry serverových nodů a technologií.

4 Fyzické servery

Nové samostatné fyzické servery již není možné do ICT prostředí Správy železnic umisťovat. Pokud je to technicky možné musí být nahrazeny virtualizovaným řešením. Výjimkou jsou návrhy řešení a dodávky hotových fyzických appliance, pokud jejich výrobce nedodává virtualizovanou verzi.

U fyzických serverů nedokáže Správa železnic zajistit stejné a plnohodnotné podpůrné služby jako u virtualizovaných serverů (monitoring, patch management, zálohování, …).

Výjimky posuzuje Odbor IT architektury SŽT v procesu tvorby a/nebo akceptace technické specifikace veřejné zakázky.

5 Datová úložiště

V ICT prostředí Správy železnic je provozováno více druhů datových úložišť.

5.1 Datová úložiště farem

Pro farmy klasické konvergované infrastruktury jsou provozovány datová úložiště:

- Umisťují se do rackových skříní.
- Slouží výhradně pro připojení daného serverového clusteru.
- Využívají výhradně disky typu SSD nebo NVMe v redundanci minimálně RAID6 nebo obdobném ekvivalentu. Preferovaná je modernější technologie NVMe.
- Velikost i výkon musí odpovídat potřebám konkrétní farmy.
- Preferované připojení je pomocí Fibre Channel, případně i iSCSI nebo přímé připojení SAS.

5.2 Datová úložiště pro zálohy a archivaci

Pro ukládání záloh a archivaci jsou určena datová úložiště:

- Umisťují se do rackových skříní.
- Slouží výhradně pro ukládání záloh.
- Využívají výhradně disky typu NL-SAS nebo SAS v redundanci minimálně RAID5 nebo vyšším. Disky nesmí používat technologii SMR.
- Velikost i výkon musí odpovídat potřebám zálohování farem.

- Preferované připojení je pomocí Fibre Channel, případně i iSCSI nebo přímé připojení SAS.

5.3 Datová úložiště pro off-line zálohy

Pro archivaci a offline ukládání záloh jsou určeny páskové knihovny:

- Umisťují se do rackových skříní v DR lokalitách a připojují se na backup server.
- Slouží výhradně pro ukládání offline záloh na LTO pásky.
- Využívají pásky typu LTO 9.
- Počet mechanik i počet pásek v knihovně musí odpovídat potřebám offline zálohování.
- Preferované připojení je pomocí Fibre Channel nebo přímé připojení SAS.
- Musí být zajištěn proces pravidelné a bezpečné manipulace s páskami a jejich ukládáním.

5.4 Kancelářská datová úložiště

Lokální zařízení typu NAS nejsou preferovaná a jejich zapojení do sítě Správy železnic podléhá schválení Odboru IT architektury SŽT.

Mála SOHO zařízení typu NAS umisťovaná mimo rackové skříně, typicky do kancelářských prostor, jsou nepřípustná a nesmí být připojována do ICT prostředí Správy železnic.

Větší disková úložiště typu NAS umisťovaná do rackových skříní lze na základě posouzení a výjimky Odboru IT architektury připojit do sítě SŽ. Redundance disků musí na úrovni RAID5 nebo vyšší.

6 Virtuální servery

Virtualizace v ICT prostředí Správy železnic poskytuje základní infrastrukturní služby jejichž seznam a popis prezentuje Platforma SŽ.

6.1 Služba virtuálních strojů

Infrastrukturní služba VM je provozována na vysoce dostupných virtualizačních technologiích VMware. Parametry služby jako sizing virtuálních strojů, výběr OS podporovaných Platformou SŽ, počet a konfigurace síťových karet jsou konfigurovány individuálně na základě požadavků projektu, resp. dodávaného řešení.

Správa železnic zajišťuje vysokou dostupnost služby virtuálních strojů na úrovni virtualizace i sítě, a to v rámci jednoho datového centra či serverovny. Pokud navrhované řešení vyžaduje také georedundanci nebo redundanci napříč datovými centry, musí být dodavatelem v rámci dodávky zajištěno řešení loadbalancingu.

Služby virtuálních serverů

Služba	Popis
Win.VMware.x86_64	Služby virtuálního serveru s operačním systémem Windows Server na virtualizaci VMware a architektuře x86_64
RHEL.VMware.x86_64	Služby virtuálního serveru s operačním systémem RHEL (RedHat Enterprise Linux) na virtualizaci VMware a architektuře x86_64
Debian.VMware.x86_64	Služby virtuálního serveru s operačním systémem Debian Linux na virtualizaci VMware a architektuře x86_64 Omezení: Preferované řešení pro kontejnerizaci.
SLES.VMware.x86_64	Služby virtuálního serveru s operačním systémem SLES (SUSE Linux Enterprise Server) na virtualizaci VMware a architektuře x86_64 Omezení: **Využití pro výhradně pro SAP**

6.2 Služby diskových uložišť

Disková kapacita těchto infrastrukturních služeb je provozována v datových úložištích farem, ať už dedikovaných, nebo interních v rámci technologie VMware vSAN, kde je zajištěna dostatečná úroveň redundance.

V rámci virtualizačních clusterů jsou dostupné výhradně disky SSD a NVMe. Starší rotační disky (HDD) jsou dostupné jen jako součást úložišť pro zálohy a archivace. Případný tiering není součástí služby a je nutné ho řešit na úrovni SW navrhovaného řešení.

Služby diskových úložišť

Služba	Popis
Datový disk HDD	Služba diskových úložišť pro zálohy a archivaci. Nelze použít pro systémové disky a/nebo pro provoz aplikací.
Datový disk SSD	Služba diskových úložišť pro aplikace. Není vhodné využívat pro zálohy a archivaci z důvodu enormní ceny řešení.

7 Databázové servery

V prostředí Správy železnic je provozováno několik typů databázových serverů a v rámci Platformy SŽ jsou poskytovány tyto platformní služby:

Služby databázových prostředí

Služba	Popis
Oracle DB na Oracle Exadata	Databázová služba Oracle DB provozovaná na optimalizovaném hardware Oracle Exadata Database Machine – kombinovaná hardwarová a softwarová platforma.
MS SQL na Win.VMware.x86_64	Služba virtuálních databázových serverů MS SQL Server provozovaná na serverech s operačním systémem Windows Server a virtualizační platformě VMware.

8 Webové servery

V prostředí Správy železnic je provozováno několik typů webových serverů a v rámci Platformy SŽ jsou poskytovány tyto platformní služby:

Služby webových serverů

Služba	Popis
Microsoft IIS na Win.VMware.x86_64	Služba webového serveru postavená na technologií Microsoft Internet Information Services (IIS) provozovaná na serverech s operačním systémem Windows Server s virtualizací VMware.
Apache HTTP Server na Win.VMware.x86_64	Služba webového serveru postavená na open-source technologii Apache provozovaná na serverech s operačním systémem Windows Server s virtualizací VMware.
Apache HTTP Server na RHEL.VMware.x86_64	Služba webového serveru postavená na open-source technologii Apache provozovaná na serverech s operačním systémem RHEL s virtualizací VMware.

9 Aplikační servery

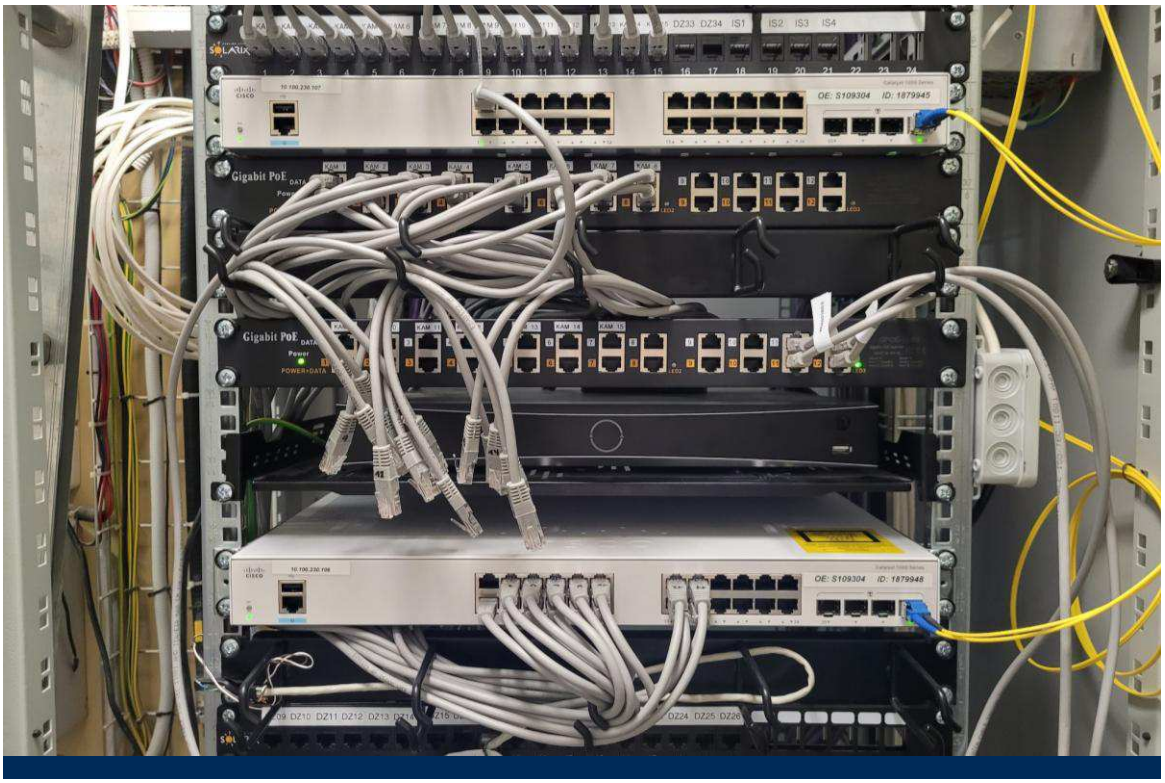
V prostředí Správy železnic je provozováno jedno portálové řešení, které je v rámci Platformy SŽ poskytováno jako platformní služba:

Služba zabezpečeného portálového řešení

Služba	Popis
Liferay na Win.VMware.x86_64	Liferay je přední open-source podnikové portálové řešení založené na jazyce Java, které umožňuje správu dat, aplikací, procesů a integrace současných i nových aplikací z jednoho centrálního uživatelského rozhraní.

Správa železnic, státní organizace
Správa železniční telematiky
Dlážděná 1003/7
110 00 Praha 1

Datum tisku
2025-07-30



Platforma SŽ Konektivita a síťové prostředí

Červen 2025

Obsah

Seznam zkratek

ACI	Aplikačně orientovaná infrastruktura
APN	Jméno brány mezi mobilní datovou sítí a jinou počítačovou sítí (může obsahovat MCC a MNC daného mobilního operátora) *(Access Point Name)*
CLI	Příkazový řádek *(Command Line Interface)*
DB	Databáze
DC	Datové centrum v kontextu lokalit *(Datacenter)*
DCS	Distribuovaný systém řízení technologií *(Distributed Control System)*
DDoS	Distribuované odmítnutí služby je technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a k pádu nebo nefunkčnosti a nedostupnosti systému pro ostatní uživatele, a to útokem mnoha koordinovaných útočníků *(Distributed Denial of Service)*
DMZ	Část síťové infrastruktury organizace, ve které jsou soustředěny služby poskytované někomu z okolí, případně celému Internetu. Tyto vnější (veřejné) služby jsou obvykle nejsnazším cílem internetového útoku; úspěšný útočník se ale dostane pouze do DMZ, nikoli přímo do vnitřní sítě organizace *(Demilitarized Zone)*
DoS	Odmítnutí služby je technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a k pádu nebo nefunkčnosti a nedostupnosti systému pro ostatní uživatele *(Denial of Service)*
DR	Plán obnovy po havárii, součást kontinuity IT služeb *(Disaster Recovery)*
DSL	Technologie pro vysokorychlostní připojení k internetu, která využívá telefonní linku. DSL umožňuje přenos dat přes kovový vedení telefonní sítě s využitím frekvenčního spektra, které není využíváno pro telefonní hovory *(Digital Subscriber Line)*
DWDM	Typ vlnového multiplexu, který je založený na multiplexování více optických signálů v jednom optickém vlákně na různých vlnových délkách nebo různých typech laserů *(Dense Wavelength Division Multiplex)*
GPRS	GPRS je mobilní datová služba první generace. Dnes je GPRS již zastaralou technologií a byla nahrazena modernějšími technologiemi, jako jsou například 4G a 5G *(General Packet Radio Service)*
HA	Vysoká dostupnost služeb. Předpokladem řešení je použití dvou a více nezávislých zařízení s cílem zajistit funkčnost v případě výpadku *(High Availability)*
HW	Hardware označuje veškeré fyzicky existující technické vybavení počítače
ICS	Průmyslové řídicí systémy *(Industrial Control System)*
ICT	Informační a komunikační technologie *(Information and Communication Technology)*
IKEv2	Protokol pro šifrování síťových spojení, který se používá k zabezpečení VPN a jakýchkoliv jiných síťových spojení. Tento protokol je specifikován jako standard Internet Engineering Task Force, nabízí vysokou úroveň bezpečnosti, dostupnosti a rychlosti. Dále pak podporuje automatické obnovování spojení, umožňuje rychle reagovat na změny síťového prostředí a také poskytuje podporu pro více typů šifrování a autentizace.
Industrial DMZ	Část síťové infrastruktury organizace, ve které jsou soustředěny služby poskytované někomu z okolí, případně do jiných sítí. Případným úspěšným útokem se ale útočník dostane pouze do Industrial DMZ, nikoli přímo do vnitřní sítě s vyšší bezpečnostní úrovní *(Industrial DeMilitarized Zone)*
IPsec	Jedná se o protokol, který se používá k šifrování a ochraně dat přenášených přes Internet. IPsec se často používá k ochraně VPN spojení, ale také může být použit k ochraně jakýchkoli dat přenášených přes internetové sítě. Šifrování zabraňuje neoprávněnému čtení dat, zatímco autentizace zajišťuje, že data pocházejí od autorizovaného zdroje. Tyto funkce pomáhají chránit síť před neoprávněným přístupem, únikem dat a jinými bezpečnostními hrozbami *(Internet Protocol Security)*
IT	Informační technologie *(Information Technology)*
LAN	Místní počítačová síť *(Local Area Network)*
LTE	Řešení mobilního bezdrátového vysokorychlostního přenosu dat čtvrté generace *(4G / Long Term Evolution)*
MFA	Více-faktorové ověření identity uživatele *(Multi-Factor Authentification)*

MGMT	Řízení, dohled, konfigurace, sběr dat a vzdálený pří tup k serverům a aktivním síťovým prvkům *(Management)*
MPLS	Multi-protokolové přepojování podle značek – metoda směrování síťového provozu používaná ve vysokorychlostních telekomunikačních sítích, která pro směrování nepoužívá relativně dlouhé a protokolově závislé síťové adresy, ale krátké značky pevné délky. Standard je definován v RFC 3031 *(Multiprotocol Label Switching)*
NGFW	Oproti běžným FW nabízí také doplňkové funkce jako AVC, AMP, IPS, IDS, DPI, DLP, TD, IdM a dešifrování a kontrolu TLS/SSL obsahu *(Next-Generation Firewall)*
OOB	Oddělená síť určená pro management serverů a aktivních síťových prvků. Z oprávněných provozních a technických důvodů lze požadavek na oddělení splnit užitím vyhrazených VLAN nebo VRF VPN *(Out-of-Band MGMT LAN)*
OŘ	Oblastní ředitelství SŽ
OS	Operační systém *(Operating System)*
OT	Provozní technologie *(Operations Technology)*
PAM	Řešení zabezpečení identit, které pomáhá chránit organizaci před kybernetickými hrozbami monitorováním, zjišťováním a prevencí neoprávněného privilegovaného přístupu k důležitým prostředkům *(Privileged Access Management)*
PLC	Programovatelný automat, typické koncové zařízení v OT *(Programmable Logic Controller)*
PoE	Technologie napájení zařízení přes standardní ethernetový kabel. PoE existuje v několika standardech, které se liší především přenášeným elektrickým výkonem *(Power over Ethernet)*
RJ45	Standardizovaný metalický konektor pro počítačové sítě *(Registered Jack 45)*
S2S VPN	Šifrované VPN připojení zajišťující propojení dvou LAN *(Site-to-Site VPN, LAN-to-LAN VPN)*
SAN	Oddělená datová síť pro připojení datových úložišť. Zpravidla používá protokol FC nebo iSCSI *(Storage Area Network)*
SCADA	Softwarové řešení zpravidla dispečerského dohledu a monitorování technologií *(Supervisory Control And Data Acquisition)*
SFP	Typ slotu a modulu pro datovou komunikaci zpravidla po optických vláknech. Podporuje rychlost maximálně 1 Gbps *(Small Form Factor Pluggable)*
SFP+	Typ slotu a modulu pro datovou komunikaci zpravidla po optických vláknech. Podporuje rychlost maximálně 10 Gbps *(Small Form Factor Pluggable Plus)*
SMS	Krátká textová zpráva
SW	Programové vybavení počítače či jiného obdobného zařízení. Speciálním druhem software je firmware, který je úzce spjatý s konkrétním hardwarem (Software)
SŽ	Správa železnic, státní organizace
SŽT	Správa železniční telematiky, organizační jednotka SŽ
TDS	Technologické datové sítě SŽ, jedná se o více VRF zpravidla vyhrazených pro OT, běžně se nazývají také „Techlan"
UAS	Logická uživatelsko-aplikační síť SŽ, zahrnuje VRF v MPLS sítích a lokální VLAN, běžně se nazývá také „Intranet SŽ"
VM	Virtuální počítač *(Virtual Machine)*
VPN	Virtuální privátní síť *(Virtual Private Network)*
VRF	Virtuální směrování a předávání technologie, která v počítačových sítích založených na protokolu IP umožňuje souběžnou existenci více instancí směrovací tabulky v rámci sítě stejného směrovače ve stejnou dobu *(Virtual Routing and Forwarding)*
WAF	WAF je druh firewallu, který se specializuje na zabezpečení webových aplikací a webových stránek. WAF slouží k ochraně webových aplikací před různými druhy útoků, jako jsou SQL injection, Cross-Site Scripting a další. WAF využívá různé techniky pro detekci a blokování nežádoucího provozu, včetně filtrace vstupů, detekce neobvyklých činností a analýzy protokolu HTTP. WAF může být nasazen jako samostatné zařízení, jako virtuální síťový prvek nebo jako součást firewallu sítě. WAF může být konfigurován pro konkrétní webové aplikace a stránky, aby poskytoval co nejlepší ochranu před útoky. Mezi funkce WAF patří například blokování útoků v reálném čase, sledování webových aplikací a identifikace bezpečnostních rizik, správa povolených a zakázaných přístupů a další. WAF může fungovat i jako load balancer pro webové servery *(Web Application Firewall)*

ZoKB	Zákon o kybernetické bezpečnosti č. 181/2014 Sb. a souvisejících zákonů v pozdějším znění

Seznam vysvětlivek

Active-Active	Distribuce zátěže na více nebo všechny síťové prvky.
Industrial DMZ	Část síťové infrastruktury organizace, ve které jsou soustředěny služby poskytované někomu z okolí, případně do jiných sítí. Případným úspěšným útokem se ale útočník dostane pouze do Industrial DMZ, nikoli přímo do vnitřní sítě s vyšší bezpečnostní úrovní
Jump server	Zabezpečené a monitorované zařízení, které spojuje dvě různé bezpečnostní zóny.
Platforma SŽ	Soubor dokumentů, rozdělený na veřejnou, interní a metodickou část, určený pro seznámení dodavatelů se standardy a technologiemi v ICT prostředí SŽ.
Purdue Model	Strukturální model pro zabezpečení průmyslových řídících systémů.
Site-to-Site	Propojení dvou a více vzdálených sítí.
Spine-Leaf	Dvouvrstvá síťová topologie switchů spine a leaf vyvinutá pro datová centra.
Standard IEEE 802.3af	Standard pro PoE napájení. Maximální přenášený výkon je 15,4 W.
Standard IEEE 802.3at	Standard pro PoE napájení, který se označuje jako PoE+. Maximální přenášený výkon je 30 W.
Standard IEEE 802.3bt	Standard pro PoE napájení, který se označuje jako PoE++. Maximální přenášený výkon je 60 W.

1 Úvod

Tento dokument je přílohou a nedílnou součástí Základního dokumentu Platformy SŽ a definuje základní principy a pravidla síťové komunikace v ICT prostředí Správy železnic. Současně popisuje síťové prostředí a poskytované služby ze strany Správy železnic.

2 Perimetr Správy železnic

2.1 Perimetr

Perimetrem se označuje část systémů, které jsou využity pro komunikace mimo interní sítě SŽ. Jde o významnou součást celé ICT infrastruktury. Hlavními aspekty pro perimetr sítě jsou dvě oblasti:

- **Bezpečnost** – kontrola komunikace a ochrana před proniknutím z oblastí mimo síť Správy železnic (Internet, sítě externích dodavatelů).
- **Výkonnost** – předpokladem perimetru je koncentrace komunikace v obou směrech, tedy, jak překlad provozu na vnitřní aplikace (web služby, mail systém, VPN), tak i komunikace ze sítě ven (Internet, aplikace a služby třetích stran).

Perimetr a vnější zabezpečení sítě v sobě spojuje více služeb dále využívaných v ICT infrastruktuře. Jde primárně o služby ochrany proti DDoS, oddělené DMZ a terminace VPN připojení.

2.2 Demilitarizovaná zóna

Demilitarizovaná zóna (DMZ) je bezpečnostní mechanismus, který se používá v síťové architektuře pro umístění systémů dostupných z Internetu, či dalších lokalit mimo bezpečnostní perimetr. DMZ se v prostředí SŽ nachází na hranici sítě mezi Internetem a vnitřní sítí organizace a obsahuje servery, WAF, VPN koncentrátory a další zařízení, která mají být přístupná ze sítě Internet.

Definici DMZ určují pravidla v NGFW, na základě těchto pravidel je striktně zakázána komunikace z vnitřní sítě přímo do Internetu bez použití DMZ a stejně tak i opačný směr.

2.2.1 Demilitarizovaná zóna pro OT

Princip industriální DMZ spočívá v použití firewallu mezi IT a OT sítí, neboli mezi uživatelskou a technologickou sítí a vytvoření bezpečného prostředí pro umístění aplikací a zařízení pro přenos dat mezi těmito sítěmi, např. jump servery, integrační koncentrátory, integrační servery a jiné. V síti SŽ je totiž striktně zakázán přímý přístup z uživatelské do technologické sítě a naopak.

2.3 Přístup přes VPN

Jde o službu pro realizaci šifrované komunikace z externího prostředí na aplikace či hardware ve vnitřních sítích a také pro jejich správu. VPN bývá provozována ve dvou základních režimech, a to jako Site to Site VPN (určeno pro připojení celých počítačových sítí nebo serverů) nebo jako uživatelská Client to Site VPN s MFA (multifaktorovou autentizací) pro přístup zaměstnanců a externistů k zařízením a službám v prostředí Správy železnic.

Pro externí Dodavatele je možné zřídit VPN přístup na konkrétní servery a systémy v UAS nebo v TDS.

2.3.1 Uživatelské VPN s MFA

Klientské VPN jsou řešené pomocí Cisco AnyConnect klientů s ověřením přes multifaktorovou autentizaci (MFA). MFA je vyžadováno pro další ověření uživatele pomocí jednorázového kódu doručeného prostřednictvím SMS na zaregistrované telefonní číslo.

Pro tyto VPN platí následující pravidla:

- Není povolený split-tunnel.
- Pro externisty není přes VPN povolen přístup k síti Internet.
- Pro řešení MFA je krom SMS používán i MS Authenticator nebo Cisco DUO.
- Ověřování uživatelů se provádí pomocí Cisco ISE.

Pro přístup na cílová zařízení je povinné využít bezpečnostní systém PAM. Přístup na cílové technologie mimo systém PAM je umožněn pouze na výjimku ze strany Odboru Kybernetické bezpečnosti SŽT, například pokud cílový systém není možné integrovat do systému PAM. Při zavádění systému je nutné poskytnout aktivní spolupráci Dodavatele se Správou železnic (poskytnout potřebné informace – použité protokoly pro vzdálený přístup, testovací účty, ověření funkčnosti) pro zprovoznění vzdáleného přístupu skrze bezpečnostní systém PAM.

2.3.2 Site to Site VPN

Pro připojení vzdálených lokalit či podpůrných systémů mimo síť SŽ se používají S2S VPN s protokolem IPsec IKEv2. Z důvodů vyžadovaných ZoKB musí být komunikace z těchto S2S VPN explicitně omezena jen na konkrétní vyjmenovaná zařízení (servery apod.) a je nutné u připojené protistrany zajistit průkaznou identifikaci uživatelů, kdo a kdy vyžil přístup skrze S2S VPN. Tyto záznamy musí poskytnout na požádání SŽ. Je nutné mít odůvodněný požadavek pro použití S2S VPN. Pokud je to provozně/technicky možné jsou preferované jmenné VPN vázané na konkrétní osobu.

2.4 Komunikační směry

Správa železnic má na základě běžných síťových standardů a praktik vydefinovány povolené a zakázané směry síťové komunikace, tak aby byla zajištěna nejvyšší úroveň zabezpečení sítí, informačních systémů i celého ICT prostředí.

Pravidla síťové komunikace na perimetru SŽ

Zdroj	Směr	Cíl	Stav
UAS	→	DMZ	filtrováno
UAS	←	**DMZ**	**zakázáno**
VPN	←	DMZ	filtrováno
APN	↔	DMZ	filtrováno
APN	↔	**UAS**	**zakázáno**
APN	↔	**TDS**	**zakázáno**
APN	↔	Industrial DMZ	filtrováno
UAS	←	VPN	filtrováno
TDS	↔	**DMZ**	**zakázáno**
TDS	↔	Industrial DMZ	filtrováno
UAS	↔	Industrial DMZ	filtrováno
UAS	↔	**TDS**	**zakázáno**
UAS	→	Internet	filtrováno
Internet	←	VPN (zaměstnanecká)	filtrováno
Internet	↔	**VPN (externisté)**	**zakázáno**
Internet	↔	**S2S VPN**	**zakázáno**
Internet	↔	DMZ	filtrováno
Internet	→	**UAS**	**zakázáno**
Internet	↔	**TDS**	**zakázáno**

Na základě těchto pravidel veškerá komunikace mezi vnitřními sítěmi a Internetem probíhá výhradně přes aplikace nebo zařízení umístěná v DMZ na perimetru Správy železnic. Přímá komunikace z uživatelsko-aplikační sítě do sítě Internet není povolena, existují však specifické výjimky. Tato omezení platí i pro zabezpečené sítě datových center a serveroven a tedy stejně tak, přímá komunikace ze serverů do sítě Internet (aktualizace, stažení instalačních balíčků) není povolena. Vždy je nutné využít nepřímé komunikace přes proxy server nebo obdobná zařízení. I zde existuje výjimka a pro specifické systémy lze tuto komunikaci povolit.

Pokud nějaké konkrétní zařízení nebo informační systém není schopen z objektivních technických důvodů tato omezení dodržet při zachování své funkce, je nutné před implementací takového řešení požádat o výjimku u Odboru IT architektury SŽT, kde bude výjimka posouzena a povolena nebo zakázána, případně bude zvoleno alternativní řešení.

3 Fyzické sítě Správy železnic

3.1 Uživatelsko-aplikační síť

Jedná se o rozsáhlou komunikační síť pro veškerý kancelářský i podpůrný provoz, jsou zde umístěny běžné uživatelské počítače, tiskárny, skenery, ale i serverovny a datacentra pro provoz farem a aplikací. Servery pro IT jsou provozovány výhradně v této síti.

V současné době je uživatelsko-aplikační síť (UAS) provozována ve staré MPLS síti, kdy páteřní uzly komunikační infrastruktury UAS jsou navzájem propojeny, zajišťují směrování síťových komunikací a na vybraných trasách i redundanci v případě ztráty průchodnosti tras.

3.2 Technologické datové sítě

Tyto sítě jsou v prostředí Správy železnic určeny primárně pro OT zařízení a převážně pro provozní drážní a jejich podpůrné systémy. Jsou striktně definované a vlastnostmi odpovídají nejvyšším zabezpečovacím standardům pro provoz kritické i nekritické infrastruktury.

Jednotlivé technologické sítě v TDS jsou rozdělené dle konkrétních technologií na úrovni separátních VRF. Od UAS jsou odděleny pomocí firewallů, přístup k OT zařízením je umožněn pouze přes jump servery či jiné systémy (koncentrátory) umístěné v IT/OT DMZ. Zařízení ani uživatelé v TDS nemají přímý přístup do sítě UAS ani Internet a to včetně aktualizací SW atp.

3.2.1 Segmentace sítě

V nedávné době proběhl v prostředí SŽ projekt „Rekonstrukce a segmentace technologických sítí", jejímž cílem byla migrace z původní sítě do nově segmentované MPLS sítě, včetně zřízení šesti segmentů propojených přechodovými firewally.

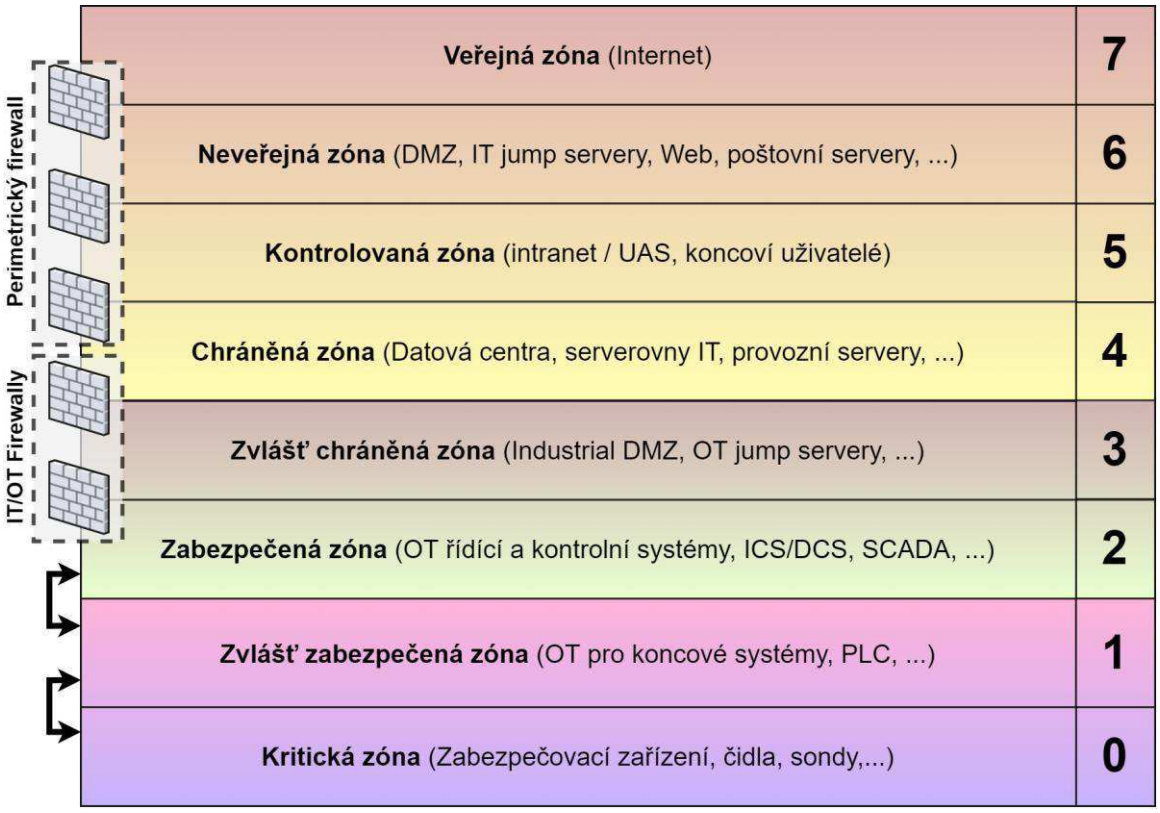
Segmentace UAS se v současné době aktivně připravuje, čili tato síť zatím není segmentována, rozdělena.

3.2.2 Ostrovní oddělené sítě

V prostředí SŽ se z důvodu kritické infrastruktury vyskytují rovněž oddělené (ostrovní) sítě, ty jsou fyzicky nebo virtuálně síťově odděleny od ostatních sítí pomocí firewallu tak, aby jejich provoz nemohl být narušen. Typickým příkladem můžou být sítě pro elektro dispečinky.

4 Logické síťové prostředí

V logickém síťovém prostředí je aplikován modifikovaný Purdue model pro ICS v podobě 8 vrstev. Potřebné oddělení mezi IT a OT prostředím pomocí industriální DMZ je prováděno IT/OT firewally. Jedná se o zásadní prvek zabezpečení OT provozu.



Obrázek 1: Purdue ICS model

4.1 Komunikace mezi sítěmi

Komunikace mezi sítěmi je řízena na základě výše zmíněného Purdue modelu, je řízena a kontrolována firewally v dané oblasti, firewally v perimetru nebo v datových centrech. Datová komunikace uživatelů je primárně navazována ze zóny s vyšší bezpečnostní úrovní do zóny s nižší bezpečnostní úrovní. Komunikace systémů s nižší bezpečnostní úrovní do zóny s vyšší bezpečnostní úrovní je ve výchozím stavu zakázána. Komunikace mezi jednotlivými OT sítěmi (VRF VPN) jsou řízeny pomocí FW, který je v rámci lokality nebo OŘ anebo centrální v rámci struktury WAN.

4.2 Georedundance

Díky možnostem rozsáhlé sítě Správy železnic se naplno využily výhody georedundance, čili distribuce na více fyzických lokalit, ať už z důvodu vysoké dostupnosti či rozdělení zátěže jednotlivých systémů. V rámci nového perimetru sítě je zajištěna sekundární konektivita do sítě Internet, v tuto chvíli se však nejedná o georedundantní řešení.

4.3 Řešení High Availability

Pro všechny klíčové prvky síťového prostředí je požadován provoz ve vysoké dostupnosti, tedy zajištění síťového provozu bez přerušení pomocí redundance.

- Clustering – redundance dvou a více prvků je možné provozovat v módech active-passive nebo active-active (Load Balancing), např. perimetr sítě je implementován v plném active-active režimu, segmentační firewally jsou v active-passive režimu, vždy záleží na konkrétní implementaci zařízení a nárocích na vysokou dostupnost.
- Síťové prvky i optické propoje páteřní MPLS sítě jsou redundantní a je realizováno připojení vždy z více směrů.

5 Sítě APN

Pro některé konkrétní, striktně definované aplikace jsou využívány mobilní služby přenosu dat protokolem LTE nebo GPRS. Každá taková aplikace je provozována v uzavřené síti (APN), zakončená na perimetru SŽ, s definovaným rozsahem IP adres a firewallovými pravidly. Pro přenos dat do sítě UAS se vždy používá DMZ, přímý přístup z APN do sítě Internet je zakázán. Vlastní APN slouží např. pro tablety strojvedoucích, sběr měřených hodnot z kolejových vozidel, IoT a další zařízení nekritické infrastruktury připojené mimo síť Správy železnic.

6 Síťová zařízení

Tato kapitola popisuje seznam komoditních ICT služeb a jednotlivých HW/SW komponent, které tvoří standard v rámci Správy železnic. Cílem je zajistit ve fázích přípravy poptávky, návrhu ICT řešení a realizace dodávky kompatibilitu se stávajícím ICT prostředím a v maximální míře využít již provozované komponenty a technologie. Seznam služeb a komponent je průběžně aktualizován.

6.1 Používané technologie

Níže je výčet a popis základních síťových technologií používaných v prostředí Správy železnic.

6.1.1 VLAN

Aktivní síťové prvky musí plně podporovat VLAN. Pro aktivní datovou komunikaci v sítích SŽ je zakázáno, pokud je to technicky možné, používat defaultní VLAN 1 a tato VLAN se nesmí používat jako nativní (PVID) VLAN na trunk portech. Nastavení trunk portů musí být statické. Automatické vyjednávání je povoleno, jen v krajním případě z technických důvodů na co nejkratší možnou dobu, kdy není jiná možnost.

6.1.2 VRF

Virtual Routing and Forwarding (VRF) je technologie používaná v sítích pro oddělení a izolaci síťového provozu na virtuální síťové segmenty. Každá VRF reprezentuje oddělenou síť, která má vlastní směrovací tabulky a rozhraní. Využívá se zejména v prostředí, kde se vyskytují různé typy síťového provozu, které se musí oddělit a izolovat, aby nedocházelo ke kolizím nebo únikům dat. VRF umožňuje vytvořit více logických sítí v jedné fyzické síti a zajistit tak bezpečné oddělení a izolaci síťového provozu.

Využití VRF VPN se obvykle pojí s technologií MPLS, která umožňuje efektivní směrování a přepínání datových toků mezi jednotlivými virtuálními sítěmi.

VRF Lite je technologie Virtual Routing and Forwarding (VRF) bez podpory MPLS. Oproti VRF VPN, která využívá MPLS pro směrování datových toků mezi různými virtuálními sítěmi, VRF Lite používá standardní směrování IP paketů v sítích založených na protokolu IP.

Správa železnic využívá VRF pro segmentaci MPLS sítí.

6.1.3 Technologie DWDM

U technologie DWDM jde o metodu vlnového multiplexování, díky tomu se optické vlákno využije pro více vlnových délek (více barev) pro oddělené datové přenosy.
V rámci celorepublikového řešení síťové infrastruktury Správy železnic jsou použity DWDM propoje mezi jednotlivými lokalitami jako nosná přenosová technologie pro MPLS sítě i pro přímé propoje datacenter, kde nejsou k dispozici přímá vlákna. DWDM síť obsahuje mnoho plnohodnotných přípojných bodů a více opakovačů pro zajištění spojů na velkou vzdálenost, zároveň poskytuje redundantní připojení jednotlivých DWDM bodů z více směrů.

Výčet používaných / preferovaných typů zařízení DWDM

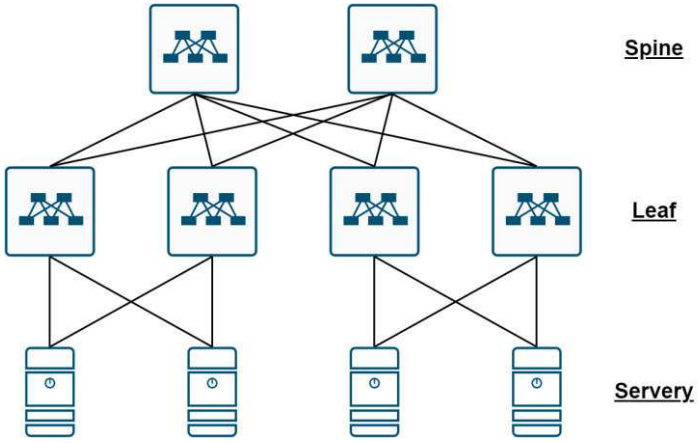
Typ zařízení	Popis	Konkrétní řady
DWDM	**Přípojný bod**	**NCS 1000** **NCS 2000**

6.1.4 Sítě MPLS

MPLS je technologie sítí, která umožňuje efektivní a spolehlivý přenos datových paketů vysokého objemu v rozsáhlých sítích. V prostředí Správy železnic jsou vybudovány dvě MPLS sítě. Stará MPLS síť pro uživatelsko-aplikační síť a některé technologické prvky a nová MPLS síť určená primárně pro technologické datové sítě. Záměrem SŽ je starou MPLS síť postupem času opustit.

6.1.5 Síťová spine-leaf topologie

Na rozdíl od klasické 3vrstvé topologie (Access-Distribution-Core) umožňuje Spine-Leaf díky dvouvrstvé topologii mimo jiné snížení latence mezi servery, snížení počtu fyzických switchů v datacentru, snížení počtu hopů při komunikaci mezi servery, zvyšuje propustnost a omezuje riziko vzniku úzkého hrdla.



Obrázek 2: Schéma Spine-Leaf topologie

Všechny nově instalované datacentrové switche v síťovém prostředí Správy železnic již plně podporují integraci do Spine-Leaf topologie, ať už přímým napojením, nebo jako Remote Leaf.

6.1.6 Technologie Cisco ACI

Cisco ACI (Application Centric Infrastructure) je softwarově definované síťové řešení, které zjednodušuje, automatizuje a zabezpečuje provoz sítě v datových centrech. V prostředí SŽ se používá výhradně v Network-Centric módu, který je síťově zaměřen na tradiční přístup k subnettingu a používání VLAN. Jedná se o poměrně nové řešení, v datových centrech se tato technologie postupně rozšiřuje, z toho důvodu všechny nově instalované switche v datových centrech již podporují integraci do Cisco ACI.

6.1.7 Sítě OOB

V datových centrech SŽ je vyžadováno, aby všechny servery a síťové prvky měly k dispozici dedikovaný síťový port pro dohled a konfiguraci těchto zařízení. Tyto porty se propojují do oddělené OOB (Out-of-band) sítě, která je síťově oddělena od hlavní datové sítě. Lokálně v datovém centru se jedná o fyzicky oddělenou síť, v rámci intranetu jsou odděleny virtuálně pomocí VLAN a VRF.

6.2 Firewally

Vzhledem k množství a různorodosti datových sítí jsou z pohledu kybernetické bezpečnosti firewally nejdůležitějšími síťovými prvky pro Správu železnic. Je kladen velký důraz na striktně oddělené provozy mezi uživatelskými a technologickými sítěmi, mezi uživatelskými sítěmi a datovými centry a samozřejmě mezi sítěmi SŽ a Internetem. Perimetrický firewall musí umožňovat testovací mód FW pravidel, který umožní odladit pravidla bez dopadu na probíhající provoz, dále musí podporovat HA zapojení a distribuovanou konfiguraci. Podle logického umístění firewallu je zvolen konkrétní model viz následující tabulka.

Výčet používaných / preferovaných typů firewallů

Typ routeru	Popis	Konkrétní řady
Perimetr	Hraniční firewall	Palo Alto vyšších řad
Pro segmentaci	Segmentační firewally pro IT sítě a IT/OT DMZ	Cisco Firepower 1xxx Cisco Firepower 31x0 Cisco Firepower 4xxx
Pro datová centra	Firewall pro aplikační farmy, clustery, single nody, NAS atd.	Cisco Firepower 31x0 Fortinet Fortigate 600F Fortinet Fortigate 1801F Fortinet Fortigate 2601F
Pro aplikace	Firewall na aplikační vrstvě OSI modelu (WAF)	F5 BIG-IP
Pro load balancing	Loadbalancer pro vyrovnání zátěže serverů	Kemp LoadMaster

6.3 Routery

Routery, nebo také směrovače, jsou zásadní aktivní síťové prvky pro segmentaci sítí. Podle způsobu použití jsou děleny na routery pro provoz v MPLS síti, routery v datových centrech a perimetru sítě, případně pro IT nebo OT sítě.

Jsou podporovány routery Cisco s požadovanými protokoly:

- **HSRP** – pro hraniční routery
- **VRF** – pro MPLS routery
- **VRF-Lite** – pro routery bez MPLS
- **BGP** – pro hraniční a MPLS routery
- **TACACS+**
- **RADIUS**

V následující tabulce jsou uváděny jednotlivé řady vždy pro konkrétní použití.

Výčet používaných / preferovaných typů routerů

Typ routeru	Popis	Konkrétní řady
MPLS	Routery typu P, PE a RR v MPLS síti	Cisco ASR Cisco NCS Cisco 8000
MPLS	Routery typu CE	Cisco C9400 Cisco C9300 Cisco C8000 Cisco ISR
IT	Routery pro datová centra a IT sítě	Cisco C9300 Cisco ISR
OT	Lokální routery pro OT sítě	Cisco IR

6.4 Switche

V prostředí SŽ jsou switche (přepínače) nejčastější síťová zařízení, proto existuje velké riziko možného nasazení nekompatibilních typů s následnou problematickou výměnou za kompatibilní. Obecně jsou preferované switche od renomovaného výrobce Cisco řady C9xxx a pro datacentra řada Nexus 9300, u nichž jsou do značné míry zaručené jednotné konfigurační prostředí (CLI), podpora VLAN bez omezení jejich počtu, kompatibilita používaných síťových protokolů, možnost stohování dedikovaným portem aj.

Jsou požadovány síťové a autorizační protokoly jako:

- **HSRP** – Hot Standby Router Protocol
- **PVST+** – Per-VLAN Spanning Tree Plus
- **TACACS+**
- **RADIUS**

Platí zákaz používání switchů bez managementu. V následujících podkapitolách jsou uváděny jednotlivé řady vždy pro konkrétní použití.

6.4.1 Switche pro datová centra

K již zmiňovaným požadavkům je u switchů pro datová centra vyžadováno redundantní napájení.

Výčet používaných / preferovaných typů

Typ switche	Popis	Konkrétní řady
Spine	Spine switch v topologii Spine-Leaf	Cisco Nexus 9332C Cisco Nexus 9364C
Leaf/ToR	Leaf switch v topologii Spine-Leaf nebo Top of Rack / Top of Row switch	Cisco Nexus 93180YC Cisco Nexus 93240YC Cisco Nexus 93360YC
Backend	Lokální propojení nodů farem (HCI)	Cisco Nexus 93180YC Cisco C9300X
Access	Jako access switch v malých serverovnách	Cisco C9300X Cisco C9300

6.4.2 Switche pro fibre channel

K již zmiňovaným požadavkům je u switchů pro datová centra vyžadováno redundantní napájení.

Výčet používaných / preferovaných typů

Typ switche	Popis	Konkrétní řady
Fibre Channel	Fibre Channel switche převážně pro připojení síťových úložišť typu SAN	Cisco MDS 9124T/V Cisco MDS 9132T/V Cisco MDS 9148T/V

6.4.3 Switche pro kamerové systémy

Pro kamerové systémy jsou požadovány switche s napájením PoE+ podle standardu 802.3at, případně PoE++ podle standardu 802.3bt.

Výčet používaných / preferovaných typů pro kamerové systémy

Typ switche	Popis	Konkrétní řady
Access	Běžný PoE switch pro připojení kamerových systémů	Cisco C9200, resp. C9200L Cisco C9300, resp. C9300L

6.4.4 Switche pro management zařízení

Pro OOB switche v datových centrech platí mimo jiné požadavek na redundantní napájení. V ostatních lokalitách, kde nejsou zajištěny dvě nezávislé napájecí větve, je tento požadavek bezpředmětný.

Výčet používaných / preferovaných typů pro management zařízení

Typ switche	Popis	Konkrétní řady
OOB	Běžný access switch s metalickými RJ45 porty pro připojení MGMT portů	Cisco C9200, resp. C9200L
OOB	Velká datacentra spine-leaf	Cisco Nexus 9348GC

6.4.5 Switche pro lokální sítě

Tyto switche pro lokální sítě musí být umístitelné v 19" racku přímo na jeho ližiny. Redundantní zdroj není vyžadován.

Výčet používaných / preferovaných typů pro lokální sítě

Typ switche	Popis	Konkrétní řady
Access	Běžný access switch pro připojení pracovních stanic, tiskáren atp.	Cisco C9200 všech variant Cisco C9300 všech variant
OT	Lokální switche pro OT sítě	Cisco IE2xxx
End of Support	Dosluhující řada, postupně se nahrazují	Cisco C2960 více variant Cisco C2950

6.5 Bezdrátová zařízení

Tato zařízení pro obsluhu bezdrátových sítí (WLAN) jsou používána v prostředí Správy železnic.

Výčet používaných / preferovaných typů pro zařízení pro bezdrátová sítě

Typ zařízení	Popis	Konkrétní řady
Controller	Controller pro bezdrátové sítě WLAN	Cisco Catalyst 9800
Access Point	Bezdrátové přípojné body (AP)	Cisco Catalyst 91xx

6.6 Huby

Ethernetový hub neboli síťový rozbočovač se v prostředí SŽ nenachází a jeho použití je zakázané.

6.7 Modemy a datová zařízení

V prostředí rozlehlé sítě SŽ se používají různé typy modemů, tedy zařízení pro převod mezi digitálním a analogovým rozhraním. Jde např. o GSM modemy s protokolem LTE nebo GPRS, DSL modemy, 2-pair / dial-up.

Výčet používaných / preferovaných modemů a datových zařízení

Výrobce	Technologie	Popis	Konkrétní řady/modely
Patton	DSL		1088, 3200, 3088
Albis / Siemens	DSL		BSTU4 / ULAF+
RAD	DSL		ASMi50
Patton	2-pair		3202

CONEL	GPRS	GPRS modem, již ukončená výroba	ER75i
Siemens	GPRS		M35i
Teltonika	4G/LTE	Průmyslové LTE routery s rozhraním RS232, RS485, Ethernet, M-bus	TRBxxx
Advantech	4G/LTE	Průmyslové LTE routery s rozhraním RS232, RS485, Ethernet	ICR-xxxx

6.8 Centralizovaná správa síťových prvků

V prostředí Správy železnic se pro centralizovanou správu síťových prvků používají nástroje Cisco Catalyst Center (dříve Cisco DNA Center) a Cisco Nexus Dashboard Fabric Controller (dříve Cisco Data Center Network Manager). Tyto nástroje slouží pro správu, maintainance, aktualizace, zajištění jednotné konfigurace pomocí šablon i dohled nad celou sítí.

Správa železnic, státní organizace
Správa železniční telematiky
Dlážděná 1003/7
110 00 Praha 1

Datum tisku
2025-07-30

Platforma SŽ Integrační standardy

Červen 2025

Obsah

Seznam zkratek

API	Komplexně definované komunikační rozhraní aplikace *(Application Programming Inteface)*
CSV	Jednoduchý textový souborový formát (Comma-separated values)
ESB	Softwarová architektura a technologie používaná v oblasti podnikové integrace a správy služeb *(Enterprise Service Bus)*
IoT	Internet věcí je souborné označení pro síť fyzických zařízení, která vzájemně, centrálně nebo i s vnějším světem komunikují a mají možnost předávat data. Každé z těchto zařízení je jasně identifikovatelné díky implementovanému výpočetnímu systému, ale přesto je schopno pracovat samostatně v existující infrastruktuře sítě *(Internet of Things)*
IT	Informační technologie *(Information Technology)*
ITIL	*(Information Technology Infrastructure Library)*
JSON	Datový formát primárně určený pro přenos dat *(JavaScript Object Notation)*
KII	Kritická informační infrastruktura
REST/API	Webově založené klient-server API *(Representational State Transfer)*
SAP	Modulární ERP systém od německé firmy SAP AG
SFTP	Zabezpečený protokol pro přenos souborů. Pro zajištění šifrování využívá protokol SSH *(SSH File Transfer Protocol)*
SMTP	Základní síťový protokol pro přenos elektronické pošty *(Simple Mail Transfer Protocol)*
SOA	Architektura orientovaná na služby – jedná se o softwarovou architekturu, která se zaměřuje na organizaci a strukturu aplikací a systémů jako soubor nezávislých a dobře definovaných služeb *(Service-Oriented Architecture)*
SŽ	Správa železnic, státní organizace
XML	Standardizovaný jazyk používaný pro serializaci dat *(Extensible Markup Language)*

Seznam vysvětlivek

Platforma SŽ	Soubor dokumentů, rozdělený na veřejnou, interní a metodickou část, určený pro seznámení dodavatelů se standardy a technologiemi v ICT prostředí SŽ.
Platforma WSO2	Open-source platforma pro správu služeb (ESB) a integraci aplikací (API Management) vyvinutá společností WSO2 Inc. WSO2 poskytuje komplexní sadu nástrojů a produktů, které pomáhají organizacím implementovat a spravovat architekturu orientovanou na služby (SOA) a rozhraní pro programování aplikací (API) v jejich IT infrastruktuře.

1 Úvod

Tento dokument slouží jako příloha k základního dokumentu Platformy SŽ, který je součástí veřejných zakázek a podrobněji rozvádí integrační standardy naší organizace. Cílem je poskytnout jasný a konzistentní rámec pro všechny integrační aktivity. Naše cíle dále zahrnují modernizaci a konsolidaci současných integračních mechanismů za účelem zvýšení efektivity a snížení nákladů na údržbu. Dokument specifikuje požadavky a standardy, které musí být dodrženy při implementaci integračních scénářů, s důrazem na bezpečnost a využití hybridních řešení kombinujících on-premise a cloudovou infrastrukturu s ohledem na celkovou IT strategii. Všechny aktivity musí cílit na ITIL rámec pro řízení IT služeb, neboť tímto rámcem se naše organizace rozhodla řídit IT služby.

2 Moderní architektonické rámce

V rámci moderního IT prostředí naše organizace využívá pro nová řešení různé architektonické rámce a principy k zajištění flexibility, škálovatelnosti a efektivního poskytování služeb. Tato kapitola se zaměřuje na popis klíčových architektonických principů a jejich implementaci v naší organizaci. Použití současně moderní architektury nám umožňují efektivně reagovat na měnící se potřeby a technologické požadavky.

2.1 Flexibilita

Naše architektura umožňuje snadné přizpůsobení se měnícím se potřebám businessu. Tím, že kombinujeme lokální a cloudové infrastruktury, jsme schopni efektivně reagovat na dynamické požadavky a přizpůsobit naše služby v reálném čase. Hybridní řešení nám umožňují optimalizaci výkonu a nákladů tím, že strategicky využíváme výhody obou typů prostředí. Tato flexibilita nám dává možnost optimalizovat zdroje podle aktuálních potřeb a strategických cílů, ale hlavně dodržování bezpečnostních kritérií.

2.2 Škálovatelnost

Díky využití mikroslužeb a škálovatelné cloudové infrastruktury můžeme dynamicky přizpůsobovat kapacitu našich systémů podle aktuální požadavků. To zajišťuje, že naše služby jsou vždy dostupné a výkonné, i při náhlých změnách v zatížení. Implementujeme mechanismy automatického škálování, které umožňují plynulý růst a adaptaci bez potřeby manuálního zásahu, což přispívá k vyšší efektivitě a spolehlivosti.

2.3 Bezpečnost

Naše integrační architektura zahrnuje robustní bezpečnostní opatření na všech úrovních. Zajišťujeme ochranu dat a služeb pomocí pokročilých metod autentizace a autorizace, šifrování dat a pravidelného monitorování bezpečnostních hrozeb. Primárně z pohledu Compliance a regulace dbáme na dodržování všech relevantních bezpečnostních standardů a právních předpisů, což zajišťuje důvěryhodnost a právní jistotu pro business partnery.

2.4 Efektivita

Využití automatizace v rámci integračních procesů nám umožňuje snížit provozní náklady a zvýšit produktivitu. Automatizované workflow a orchestrace služeb minimalizují potřebu manuálních zásahů a zvyšují přesnost a rychlost procesů. Tohoto stavu jsme dosáhli díky centrálnímu řízení integrací prostřednictvím platformy ESB, ta nám umožňuje efektivně monitorovat a spravovat všechny integrační toky, což přispívá k vyšší přehlednosti a lepší koordinaci mezi jednotlivými systémy.

3 Architektura integrací

V rámci naší organizace se zaměřujeme na implementaci moderní architektury integrací, která podporuje jak on-premise, tak cloudové prostředí. Tato hybridní přístup zajišťuje flexibilitu, škálovatelnost a bezpečnost, což jsou klíčové faktory pro úspěšné řízení IT služeb podle ITIL principů. Cílový stav architektury je ESB.

Naše integrační architektura je postavena hlavně na následujících architekturních principech:

3.1 Microservices Architecture

Naše organizace implementuje architekturu mikroslužeb, což znamená decentralizaci a rozdělení monolitických aplikací na menší, nezávislé služby. Tento přístup zajišťuje vysokou flexibilitu a usnadňuje správu jednotlivých služeb. Díky mikroservisům můžeme rychleji reagovat na změny a inovace, což nám umožňuje poskytovat kvalitnější služby našim zákazníkům v podobě businessu.

3.2 Event-Driven Architecture

Pro lepší škálovatelnost a reaktivitu využíváme architekturu řízenou událostmi. Tento přístup umožňuje systémům komunikovat prostřednictvím událostí, což zvyšuje jejich schopnost rychle reagovat na provozní incidenty. Díky tomu můžeme dosahovat vyšší efektivity a pružnosti v našich provozních procesech.

3.3 API-First Approach

Při návrhu a vývoji systémů se naše organizace řídí principem API-First. API jsou navrhována a vyvíjena jako primární prostředek komunikace mezi systémy. Tento přístup je v souladu s ITIL principy, které se zaměřují na poskytování hodnoty zákazníkům prostřednictvím dobře definovaných služeb. API-First nám umožňuje dosahovat vyšší konzistence a standardizace v naší IT infrastruktuře.

3.4 Hybridní architektura

Pro zajištění flexibility a škálovatelnosti kombinujeme on-premise a cloudová řešení. Tento hybridní přístup nám umožňuje využívat výhod obou prostředí, což zajišťuje kontinuitu služeb a splnění compliance požadavků. Díky hybridní architektuře můžeme optimalizovat naše IT zdroje a lépe podporovat business v naší organizaci. Toto je obzvláště důležité z důvodu kritické infrastruktury informací (KII), která vyžaduje vysokou míru bezpečnosti a spolehlivosti. Hybridní přístup nám umožňuje zajistit, že klíčové systémy a data jsou chráněny a zároveň flexibilně škálovatelné dle aktuálních potřeb.

4 Typy integrací

Pro celkové pochopení integrací je nutné zmínit úrovně integrací. Existuje totiž několik pohledů, které následně definují oblasti soustředění a úroveň detailu. Je potřeba podotknout, že při komplexním řešení integrací dochází k jejich vzájemnému prolínání. Zde jsou vyjmenovány ty hlavní z nich:

- **Datová integrace** – Tento typ integrace se zabývá shromažďováním dat z různých zdrojů a jejich následným poskytnutím uživatelům v jednotné a konzistentní struktuře a formátu. Datová integrace umožňuje kombinaci dat umístěných v různých zdrojích a poskytuje uživateli sjednocený pohled na tyto data.
- **Procesní integrace** – Procesní integrace má za cíl propojit aplikace z hlediska podnikových procesů. Jakmile skončí jedna činnost, je vykonána činnost druhá. Při dokončení prvního procesu se spustí proces další, a tím že různé procesy mohou být realizovány odlišnými subsystémy je důležité zajistit, že tyto procesy jsou správně a efektivně koordinovány.

- **Aplikační integrace** – U aplikační integrace jde v zásadě o realizaci výměny informací (různého charakteru) mezi různými aplikacemi. Výměna přitom může probíhat s využitím široké škály transportních technologií – např. přes webové služby, databáze, sdílený soubor, messaging apod.
- **Systémová integrace** – Systémová integrace je proces spojování různých softwarových komponent, subsystémů, v jeden fungující celek. Cílem je, aby tento celek pracoval co možná nejefektivněji, tedy z pohledu jednotlivých subsystémů, aby komunikace mezi nimi probíhala podle definovaného schématu.

Každý z těchto typů integrace má své výhody a nevýhody a je důležité na základě analýz vybrat ten vhodný typ integrace, který bude respektovat konkrétní potřeby a požadavky jednotlivých projektů.

5 Softwarová architektura Enterprise Service Bus

ESB je softwarová architektura pro distribuované výpočty. ESB implementuje komunikační systém mezi vzájemně interagujícími softwarovými aplikacemi v rámci SOA. ESB je centralizovaný, standardizovaný hub, který přijímá, transformuje a poskytuje data, aby různé aplikace a služby napříč organizací mohly snadno komunikovat. ESB je cílový stav architektury, která je preferovaná v naší organizaci. Vzhledem ke složitosti prostředí však je doplňován i jinými způsoby integrací na základě výše popsaných architektur integrací.

ESB poskytuje hlavně tyto funkce:

- **Transformace dat** – provádí transformování zpráv do formátů, které jsou pro příjemce zpracovatelné a srozumitelné
- **Směrování zpráv** – dokáže rozhodovat, kam má zprávu odeslat na základě atributů obsažených v obsahu daných zpráv
- **Mediace služeb** – může poskytnout jednotné rozhraní pro více služeb
- **Orchestrace** – koordinuje interakce mezi službami

ESB je navržen tak, aby zjednodušil vazby a pomohl se oprostit od „Spaghetti" architektury, která v organizaci zatím dominuje. ESB je sada nástrojů, která posílá zprávu přímo do konkrétní destinace mezi buď aplikací a/nebo komponentami. Ať už je to klient nebo proces, cokoli, co je připojeno k ESB, nekomunikuje přímo mezi sebou, protože komunikují prostřednictvím samotného ESB platformy.

6 Primární integrační scénáře

6.1 Integrační platforma

Naše organizace plánuje rozvinout integrační platformu WSO2 do podoby ESB, který bude sloužit jako hlavní integrační páteř. WSO2 bude poskytovat následující funkcionality:

- **Service Orchestration** – Koordinace a řízení komunikace mezi různými službami, což podporuje efektivní řízení provozu služeb a incidentů.
- **Data Transformation** – Převod a mapování datových formátů mezi různými systémy, což umožňuje jednotné zpracování dat v rámci celé infrastruktury.
- **Security Enforcement –** Implementace bezpečnostních politik a autentizace, což je klíčové pro řízení rizik a zajištění integrity služeb.

6.1.1.1 Preferované Protokoly pro Integraci s WSO2

- **REST/HTTPS** – Pro aplikační a datové integrace díky své jednoduchosti a široké podpoře, což umožňuje snadnou správu a podporu služeb.
- **SOAP** – Pro integrace, kde je vyžadována robustní bezpečnost a transakční podpora, což je v souladu s potřebami řízení kritických služeb.
- **MQTT** – Pro event-driven integrace a IoT komunikace, které podporují rychlou reakci na změny a incidenty.
- **AMQP** – Pro spolehlivý a škálovatelný messaging mezi aplikacemi, což zajišťuje stabilní a efektivní komunikaci.

6.2 SAP Business Technology Platform

SAP BTP hraje klíčovou roli v naší integrační strategii. Specifické požadavky na integraci SAP BTP zahrnují:

- **Integration Suite** – Použití SAP Integration Suite pro propojení SAP a non-SAP systémů, což podporuje jednotnou správu a provoz služeb.
- **Event Mesh** – Využití SAP Event Mesh pro událostmi řízenou architekturu, což umožňuje rychlé a efektivní řízení změn a incidentů.
- **Business Process Management** – Automatizace a optimalizace obchodních procesů pomocí SAP Workflow Management, což zajišťuje efektivní poskytování služeb.

6.2.1.1 Preferované Protokoly pro Integraci s SAP BTP

- **OData** – Pro přístup k datům a jejich manipulaci přes standardizované API, což podporuje transparentní správu dat.
- **RFC/BAPI** – Pro volání vzdálených funkcí v SAP systémech, což zajišťuje spolehlivou integraci služeb.
- **IDoc** – Pro elektronickou výměnu dat mezi SAP a non-SAP systémy, což umožňuje efektivní řízení datových toků.
- **SOAP** – Pro služby vyžadující vysokou úroveň bezpečnosti a transakční podporu, což zajišťuje integritu a důvěryhodnost služeb.

6.3 Microsoft nástroje a Azure

Integrace s Microsoft technologiemi, včetně Azure, zahrnuje tyto základní komponenty:

- **Azure Logic Apps** – Automatizace a orchestraci pracovních toků, což podporuje efektivní správu a provoz služeb.
- **Azure API Management** – Správa a bezpečné publikování API, což zajišťuje jednotný přístup a kontrolu nad službami.
- **Azure Service Bus** – Spolehlivá messagingová platforma pro integraci aplikací, což podporuje stabilní a efektivní komunikaci.
- **Azure Arc** – Pro správu a orchestrace zdrojů v hybridním prostředí, což umožňuje jednotnou správu a kontrolu napříč on-premise a cloudovými systémy.

6.3.1.1 Preferované Protokoly pro Integraci s Azure

- **REST/HTTPS** – Pro širokou škálu aplikačních a datových integrací, což podporuje snadnou správu a podporu služeb.
- **gRPC** – Pro vysoce výkonné, nízko-latentní komunikace mezi mikroservisami, což zajišťuje rychlou a efektivní komunikaci.
- **Event Grid** – Pro event-driven architekturu a notifikace, což umožňuje rychlou reakci na změny a incidenty.
- **Service Bus** – Pro messaging a integraci podnikových aplikací, což zajišťuje spolehlivou komunikaci a řízení služeb.

6.4 Integrace stávajících aplikací

Mnoho aplikací, je stále ještě integrováno point-to-point, ty budou postupně převedeny do centralizovaného integračního prostředí. Hlavní kroky zahrnují:

- **Inventarizace a Analýza** – Zmapování současných integrací a identifikace klíčových závislostí, což podporuje efektivní správu a plánování změn.
- **Standardizace API** – Vytvoření standardních API pro všechny aplikace, což zajišťuje jednotný přístup a kontrolu nad službami.
- **Refaktoring a Modernizace** – Přepsání nebo refaktoring stávajících integrací podle moderních standardů, což podporuje efektivní a bezpečné poskytování služeb.

Tabulka protokolů

Protokol	Použití	Výhody	Nevýhody	Důvod Preference/Nepreference
REST/HTTPS	Aplikační, datové	Jednoduchost, široká podpora, škálovatelnost	Omezená bezpečnost ve srovnání s jinými protokoly	Preferovaný pro svou jednoduchost a širokou podporu
SOAP	Kritické služby	Vysoká úroveň bezpečnosti, transakční podpora	Složitost, větší režie	Preferovaný pro kritické a transakční služby
MQTT	Event-driven, IoT	Nízká režie, efektivní pro nízko-šířková pásma	Omezená podpora pro složitější operace	Preferovaný pro IoT a event-driven architekturu
AMQP	Messaging	Spolehlivost, škálovatelnost	Komplexita implementace	Preferovaný pro spolehlivý a škálovatelný messaging
OData	Data, API	Standardizace, jednoduchý přístup k datům	Omezená funkčnost ve srovnání s plně funkčními API	Preferovaný pro transparentní správu dat
RFC/BAPI	SAP integrace	Efektivní volání SAP funkcí	Specifické pro SAP	Preferovaný pro spolehlivou integraci SAP
IDoc	EDI, SAP integrace	Robustní, vhodné pro velké objemy dat	Specifické pro SAP, složitost	Preferovaný pro EDI a integraci SAP
WebSocket	Real-time komunikace	Obousměrná komunikace, nízká latence	Omezená bezpečnost	Preferovaný pro real-time aplikace
gRPC	Mikroservisy	Vysoký výkon, nízká latence	Menší podpora ve srovnání s HTTP	Preferovaný pro výkonné komunikace mikroservis
FTP/SFTP	Přenos souborů	Jednoduchost, široká podpora	Zastaralost (FTP), bezpečnostní rizika (FTP)	Preferovaný (SFTP) pro bezpečný přenos souborů, FTP je nepreferovaný kvůli bezpečnostním rizikům
JMS	Messaging	Spolehlivost, asynchronní komunikace	Komplexita, omezená podpora	Preferovaný pro robustní messagingové potřeby
SMTP	Email	Široká podpora, standardní pro email	Zastaralost, omezená bezpečnost	Nepreferovaný pro datové a aplikační integrace kvůli zastaralosti
CORBA	Distribuované aplikace	Jazyková nezávislost, robustnost	Komplexita, zastaralost, velká režie	Nepreferovaný kvůli zastaralosti a komplexitě
RMI	Java aplikace	Efektivní pro Java, jednoduchost	Omezené na Java, bezpečnostní rizika	Nepreferovaný kvůli omezené použitelnosti mimo Java a bezpečnostním rizikům
Telnet	Vzdálená správa	Široká podpora	Velmi slabá bezpečnost (nešifrované)	Nepreferovaný kvůli vážným bezpečnostním rizikům

XMPP	Real-time komunikace	Široká podpora, rozšiřitelnost	Omezená škálovatelnost, bezpečnostní problémy	Nepreferovaný kvůli omezené škálovatelnosti a bezpečnostním problémům

Tabulka poskytuje přehled preferovaných a nepreferovaných protokolů pro integrační architekturu naší organizace, zdůvodňuje jejich použití a vyzdvihuje klíčové výhody a nevýhody. Protokoly jako REST/HTTP, SOAP, MQTT, AMQP a další jsou preferovány pro svou robustnost, flexibilitu a bezpečnost. Naopak protokoly jako FTP (nešifrované), SMTP, CORBA, RMI, Telnet a XMPP jsou nepreferované kvůli jejich zastaralosti, bezpečnostním rizikům nebo omezené funkčnosti.

7 Datové formáty

V rámci organizace je klíčové zajistit efektivní, bezpečnou a interoperabilní výměnu dat mezi různými informačními systémy a platformami. Výběr vhodných datových formátů hraje zásadní roli při dosahování těchto cílů. Datový formát určuje způsob, jakým jsou informace strukturovány a jakým způsobem mohou být přenášeny a zpracovávány mezi různými systémy. V této části se zaměříme na nejčastěji používané datové formáty, jejich typické použití, výhody, nevýhody a důvody, proč jsou preferovány nebo nepreferovány v naší organizaci, se zvláštním důrazem na bezpečnostní aspekty. Kromě toho uvádíme níže v tabulce i formáty, které jsou z bezpečnostních nebo jiných důvodů nevhodné a v podstatě zakázané.

Tabulka datových formátů

Formát	Použití	Výhody	Nevýhody	Důvod Preference/Nepreference
REST/HTTPS	Aplikační, datové	Jednoduchost, široká podpora, škálovatelnost	Omezená bezpečnost ve srovnání s jinými protokoly	Preferovaný pro svou jednoduchost a širokou podporu
JSON (JavaScript Object Notation)	Webové API, konfigurace, mobilní aplikace	Jednoduchost, čitelnost, podpora v moderních programovacích jazycích	Není vhodný pro složité datové struktury, bez schématu	Preferován pro svou jednoduchost a širokou podporu, bezpečnostní riziko lze mitigovat validací a šifrováním
XML (eXtensible Markup Language)	Webové služby, dokumenty, datová výměna mezi systémy	Flexibilita, podporuje složité datové struktury, možnost validace pomocí XSD	Verbóznost, vyšší nároky na výkon	Preferován pro komplexní strukturovaná data, bezpečnost lze zlepšit pomocí šifrování a podpisů
CSV (Comma-Separated Values)	Export/import dat, tabulkové aplikace	Jednoduchost, široká podpora v aplikacích	Omezená strukturovanost, citlivost na formátování	Preferován pro jednoduchou tabulkovou data, nepreferován pro složité struktury, bezpečnostní riziko při přenosu nešifrovaných dat
YAML (YAML Ain't Markup Language)	Konfigurace, data pro DevOps nástroje	Čitelnost, jednoduchost, podpora komplexních datových struktur	Méně robustní než XML, obtížnější validace	Preferován pro konfigurace a čitelnost, nepreferován pro kritická data kvůli chybějícímu schématu a validaci
EDIFACT (Electronic Data Interchange for Administration, Commerce and Transport)	EDI v obchodních a státních systémech	Standardizace, spolehlivost, široká akceptace v EDI	Složitost, náročná implementace	Preferován pro standardizované obchodní procesy, bezpečnostní riziko lze řešit šifrováním EDI zpráv
Plain Text (neformátovaný text)	Základní komunikace, logy	Jednoduchost, univerzální čitelnost	Žádná strukturovanost, vysoké riziko chyb	Zakázán pro přenos citlivých dat, protože postrádá jakoukoliv formu zabezpečení a struktury

HTML (HyperText Markup Language)	Webové stránky, obsah dokumentů	Flexibilita, široká podpora v prohlížečích	Neefektivní pro strukturovaná data, riziko XSS útoků	Zakázán pro datovou výměnu kvůli bezpečnostním rizikům a nevhodnosti pro strukturovaná data
Proprietární Formáty (např. specifické formáty určitého softwaru)	Specifické aplikace	Optimalizace pro konkrétní software	Omezená interoperabilita, závislost na konkrétním dodavateli	Zakázány kvůli uzamčení na jednoho dodavatele a nízké interoperabilitě, což zvyšuje riziko vendor lock-in

Tabulka níže poskytuje přehled jednotlivých datových formátů, jejich specifické použití, výhody a nevýhody, a důvody preference či nepreference v kontextu naší organizace.

8 Metody

Metody integrací se liší v závislosti na povaze dat, četnosti výměny, úrovni transformace dat a typu architektury integrace dat. Metody primárně využívané naší organizací lze rozdělit na tyto čtyři základní:

- **ETL - extract, transform, load** – je běžnou metodou pro dávkové/hromadné zpracování velkých objemů strukturovaných nebo částečně strukturovaných dat
- **ELT extract, load, transform** – je podobná ETL, ale transformace se provádí až po načtení do cílového místa určení
- **CDC - change data capture** – zachycuje a přenáší pouze změny ve zdrojových datech a je užitečná pro integraci v reálném čase nebo téměř v reálném čase
- **Virtualizace dat** – vytváří virtuální vrstvu, která integruje data z různých zdrojů, aniž by je fyzicky přesouvala nebo ukládala, tato metoda poskytuje jednotný pohled na data a je vhodná pro komplexní a heterogenní datová prostředí

9 Dokumentace integračních scénářů

V naší organizaci je dokumentace integračních scénářů klíčovým nástrojem pro zajištění přehlednosti a konzistence v rámci všech integračních aktivit. Pro tento účel používáme standardizovaný dokument s názvem Integrační specifikace, který obsahuje veškeré potřebné informace k pochopení, implementaci a konfiguraci konkrétního integračního scénáře. Tento dokument slouží jako detailní blueprint pro všechny zúčastněné strany.

9.1.1.1 Integrační specifikace zahrnuje primárně:

- Stručný popis integračního scénáře, jeho účel a přínosy.
- Název integračního scénáře přidělený dle katalogu Integračních scénářů a zavedené jmenné konvence, což zajišťuje konzistenci a snadnou identifikaci.
- Popis technologií, protokolů a datových formátů použitých v integraci.
- Detailní popis procesních a datových toků, které jsou součástí integračního scénáře.
- Specifikace bezpečnostních opatření, jako je šifrování, autentizace a autorizace.

Kromě textového popisu využíváme modelovací jazyky, jako je Archimate v poslední platné verzi, pro vizualizaci integračních scénářů. Tyto modely poskytují grafický přehled o architektuře, komponentách a vztazích mezi nimi, což usnadňuje pochopení komplexních integrací.

9.1.1.2 Další používané modelovací jazyky zahrnují:

- UML (Unified Modeling Language) - Pro vytváření diagramů tříd, sekvencí a aktivit, které detailně popisují jednotlivé části integračního scénáře.

- BPMN (Business Process Model and Notation) - Pro modelování procesů organizace a jejich interakcí v rámci integračních scénářů.

Integrace jsou v naší organizaci také popsány v katalogu Integračních scénářů, který obsahuje všechny aktuální a historické integrační scénáře s příslušnými metadaty. Tento katalog je pravidelně aktualizován a slouží jako centrální zdroj informací pro všechny týmy zapojené do integračních projektů.

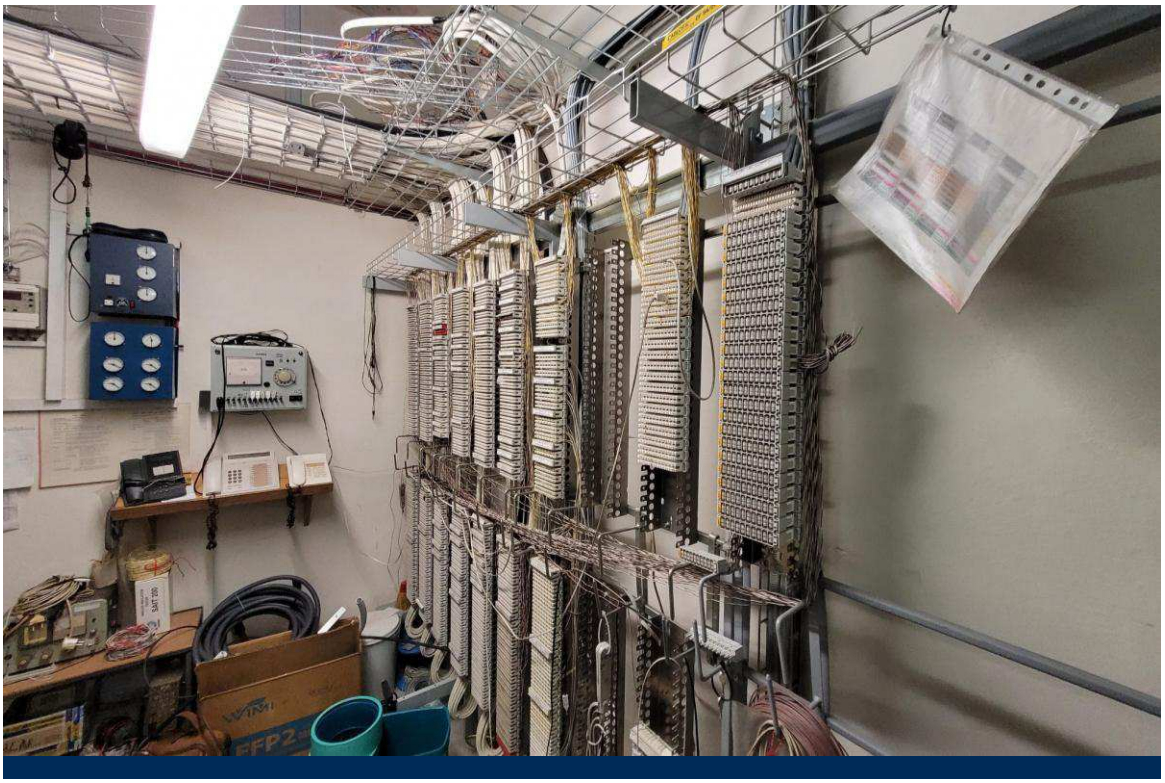
Dokumentace integračních scénářů je důkladně verifikována a validována, aby byla zajištěna její přesnost a úplnost. To zahrnuje revize od technických odborníků, bezpečnostních specialistů a dalších relevantních stakeholderů. Tento proces zajišťuje, že všechny integrační aktivity jsou prováděny konzistentně, efektivně a bezpečně.

10 Řízení integračních scénářů

Jakékoliv nové Integrační scénáře, či změny Integračních scénářů musí projít skrze Architecture Board nebo Change managment a být posouzeny v širším kontextu. Skrze jaký proces bude integrační scénář posuzován určí matice, která zahrnuje posouzení složitosti změny a její dopady. Integrační scénář následně bude nově zaevidován do katalogu Integračních scénářů nebo proběhne aktualizace u již existujícího.

Správa železnic, státní organizace
Správa železniční telematiky
Dlážděná 1003/7
110 00 Praha 1

Datum tisku
2025-07-30



Platforma SŽ Komunikační standardy

Červen 2025

Obsah

Seznam zkratek

API	Komplexně definované komunikační rozhraní aplikace *(Application Programming Inteface)*
APN	Virtuální vyhrazená část mobilní datové sítě. Nejedná se tak o mobilní připojení k Internetu, ale k lokální síti daného zákazníka mobilního operátora.
CPS	Centrální poštovní systém Správy železnic
ICT	Informační a komunikační technologie *(Information and Communication Technology)*
O27	Odbor komunikace GŘ SŽ
SAP	Modulární ERP systém od německé firmy SAP AG
SMS	Krátká textová zpráva *(Short Message Service)*
SMTP	Základní síťový protokol pro přenos elektronické pošty *(Simple Mail Transfer Protocol)*
SŽ	Správa železnic, státní organizace
SŽT	Správa železničních informačních technologií
UAS	Logická uživatelsko-aplikační síť SŽ, zahrnuje VRF v MPLS sítích a lokální VLAN, běžně se nazývá také „Intranet SŽ“
VPN	Virtuální privátní síť *(Virtual Private Network)*

Seznam vysvětlivek

Platforma SŽ	Soubor dokumentů, rozdělený na veřejnou, interní a metodickou část, určený pro seznámení dodavatelů se standardy a technologiemi v ICT prostředí SŽ.

1 Úvod

Cílem této přílohy Platformy SŽ je popsat podporovaných komunikačních služeb a technologií, které lze v rámci Platformy SŽ využít a současně definuje služby, zařízení a technologie, které není možné z důvodu duplicity v rámci navrhovaných řešení dodávat do ICT prostředí Správy železnic.

2 Komunikační služby

Platforma Správy železnic definuje základní komunikační služby, které lze v rámci aplikací a informačních systémů využívat primárně technické notifikace. Použití k jiným účelům (například pro marketingové účely nebo komunikaci s veřejností) je možná jen po předchozím schválení ze strany Správy železnic, a to minimálně ze strany SŽT a O27.

3 SMS brána

SMS je negarantovaná služba telekomunikačních operátorů. Garantován není čas doručení ani samotné doručení SMS zprávy vůbec. SMS brána je aplikace instalovaná v prostředí SŽ napojená přímo na telekomunikačního operátora. Nejedná se tedy o použití koncového zařízení přihlášeného do veřejné mobilní telefonní sítě.

SMS brána umožňuje obousměrnou komunikaci, to znamená odesílání SMS zpráv definovaným příjemcům a příjem odpovědí na odeslané zprávy. Stejně tak umožňuje evidenci (logování) doručenek zpráv. Komunikaci se SMS bránou zajišťuje jednoduché API rozhraní popsané v implementačním manuálu.

Službu SMS brány lze využít jen pro aplikace a informační systémy umístěné v ICT prostředí Správy železnic a to pouze v UAS.

4 Emailová komunikace

Pro navrhovaná řešení, pokud je součástí i emailová komunikace, poskytuje službu emailového serveru pro odchozí poštu. je pro aplikace odpůrné služby standardně poskytované k využití pro dodávaná ICT řešení.

4.1 Z uživatelsko-aplikační sítě

Z UAS je služba odesílání emailových zpráv zprostředkována takto:

- Nešifrovaně přes CPS a jeho Open-Relay SMTP servery umístěné ve vnitřní síti
- Šifrovaně přes služby MS Exchange

4.2 Z technologických datových sítí

Z technologických datových sítí není v současné době služba odesílání elektronické pošty podporováno.

4.3 Z externích sítí Správy železnic

Z externích sítí a připojení Správy železnic (VPN a APN) není služba odesílání emailových zpráv dostupná.

4.4 Mimo sítě Správy železnic

Odesílání emailové komunikace z vnějších sítí mimo perimetr Správy železnic (například SAP Cloud, MS Azure atp.) není v současné době možné.

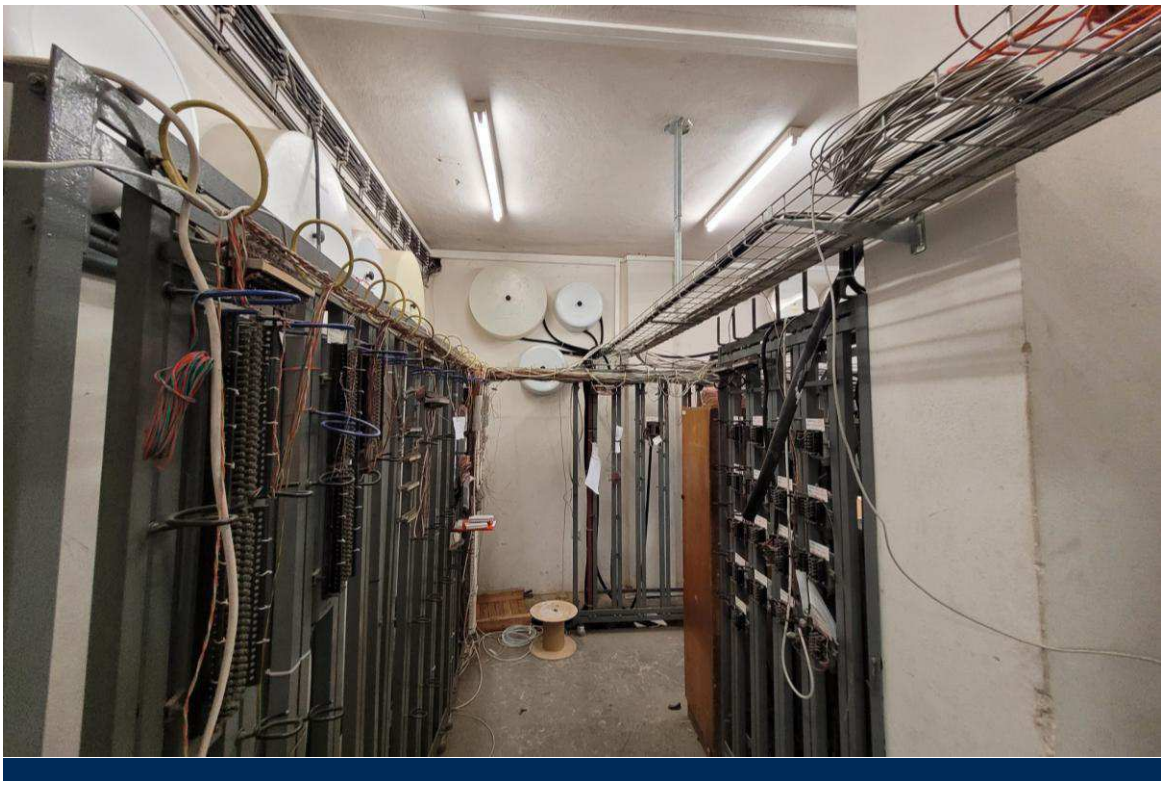
Pro tuto službu je nutné využít lokálních SMTP služeb s omezením, že z technických a bezpečnostních důvodů nelze takto odesílat emaily z domén Správy železnic.

5 Komunikační platforma dispečerských pracovišť

Komunikační platforma pro zajištění komunikace v rámci dispečerských pracovišť je Cisco Webex.

Správa železnic, státní organizace
Správa železniční telematiky
Dlážděná 1003/7
110 00 Praha 1

Datum tisku
2025-07-30



Platforma SŽ Standardy zálohování a disaster recovery

Červen 2025

Obsah

Seznam zkratek

DB	Databázová aplikace *(Database Engine)*
DR	Plán obnovy po havárii, součást kontinuity IT služeb *(Disaster Recovery)*
IBM	Americká technologická společnost *(International Business Machines)*
ICT	Informační a komunikační technologie *(Information and Communication Technology)*
LTO	Otevřený formát magnetické pásky určené pro záznam velkých objemů dat *(Linear Tape Open)*
MSSQL	Databázový server od firmy Microsoft *(Microsoft SQL Server)*
OS	Operační systém *(Operating System)*
SQL	Standardní jazyk pro manipulaci s relačními databázemi. SQL umožňuje ukládat, manipulovat a vyhledávat data v relačních databázích. SQL je založeno na dotazech (queries) na data v databázích. Dotazy lze pak definovat a modifikovat strukturu databází, vytvářet a upravovat tabulky, indexy a další prvky, vkládat a aktualizovat data, mazat data a další operace. SQL je nezávislý na platformě, což znamená, že může být použit na různých operačních systémech a s různými databázovými systémy, avšak každá databázová platforma může mít různé změny v syntaxi *(Structured Query Language)*
SŽ	Správa železnic, státní organizace
TSM	Nástroj pro zálohování, v současné době již nese název IBM Storage Protect *(Tivoli Storage Manager)*
UAS	Logická uživatelsko-aplikační síť SŽ, zahrnuje VRF v MPLS sítích a lokální VLAN, běžně se nazývá také „Intranet SŽ“

Seznam vysvětlivek

Platforma SŽ	Soubor dokumentů, rozdělený na veřejnou, interní a metodickou část, určený pro seznámení dodavatelů se standardy a technologiemi v ICT prostředí SŽ.

1 Úvod

Cílem této části Platformy SŽ je popis podporovaných služeb, technologií, a architektonických principů v oblasti zálohování a disaster recovery v ICT prostředí Správy železnic.

2 Služby zálohování

Služba zálohování ICT prostředí Správy železnic je zajištěna technologií IBM Storage Protect (dříve známý jako IBM Spectrum Protect nebo TSM). Jedná se o komplexní řešení pro fyzické fileservery, virtualizovaná prostředí a širokou škálu aplikací. IBM Storage Protect zálohuje data především s využitím technologie VMware Snapshot. Služba zálohování je dostupná v současné době jen v UAS.

Služba zálohování umožňuje 3 základní typy zálohování:

- Snapshot disku pro dosažení rychlé obnovy celého OS v Crash Consistent stavu včetně aplikační konfigurace. Zpravidla je takto zálohován pouze systémový oddíl virtualizovaného serveru. Záloha probíhá jednou denně a retence je nastavena na 30 posledních verzí.
- Záloha datových svazků připojených k jednotlivým serverům, pro dosažení maximální možné odolnosti proti náhodnému smazání či poškození apod. Záloha probíhá jednou denně, kdy se uchovává 90 posledních verzí souborů a poslední smazaná verze souboru je uchovávána 365 dní.
- Zálohy databází Oracle nebo MSSQL pomocí agentů. Záloha probíhá dvakrát denně. Přes den jsou zálohovány transakční logy databází, v noci pak vlastní databáze. Retence je nastavena na 60 posledních verzí.

Zálohy jsou řešeny lokálním backup serverem u každé virtualizační farmy, odkud jsou poté přenášeny do DR lokality a v rámci řešení offline záloh (pro další zvýšení odolnosti proti ztrátě dat) jsou zálohy dále ukládány na LTO pásky v páskové knihovně umístěné v DR lokalitě.

3 Řešení Disaster recovery

V rámci UAS byla jako DR lokalita určen objekt *Praha U2*, kam jsou pravidelně přenášeny zálohy ze všech lokálních backup serverů.

Všechny zálohy jsou pravidelně testovány a veškeré offline zálohy uložené na LTO páskách jsou pravidelně převáženy do zabezpečeného prostoru (do trezoru v jiné budově).

Správa železnic, státní organizace
Správa železniční telematiky
Dlážděná 1003/7
110 00 Praha 1

Datum tisku
2025-07-30

Platforma SŽ Cloudové prostředí

Červen 2025

Obsah

Seznam zkratek

AAD	Služba AD provozovaná v cloudovém prostředí MS Azure. Nový název služby je „MS EntraID" *(Azure Active Directory)*
AD	Rozšiřitelná a škálovatelná adresářová služba, která umožňuje efektivně uspořádat síťové prostředky. Kromě informací o objektech v počítačové síti (uživatelské účty, počítače, tiskárny) umožňuje používat stromovou strukturu objektů, nastavovat globálně systémové politiky, instalovat programy na počítače nebo aplikovat kritické aktualizace v celé organizační struktuře. Má úzkou vazbu na DNS *(Active Directory)*
AWS	Cloudové prostředí firmy Amazon *(Amazon Web Services)*
DNS	Distribuovaný hierarchický jmenný systém používaný v síti Internet. Překládá názvy domén na číselné IP adresy a zpět, obsahuje informace o tom, které stroje poskytují příslušnou službu *(Domain Name System)*
ERP	Informační systém pro řízení podniku, který integruje různé oblasti podnikání, jako je například finanční řízení, řízení zásob, výroby, prodeje, nákupu a personálního řízení. Cílem je poskytovat podnikovým uživatelům přehled o celkových aktivitách a umožňovat efektivní a koordinované řízení všech procesů v rámci podniku *(Enterprise Resource Planning)*
IaaS	Typ cloudové služby, který poskytuje zákazníkům základní IT infrastrukturu jako službu, včetně serverů, úložiště, sítě a virtuálních počítačů. Tyto služby se často poskytují prostřednictvím Internetu a umožňují zákazníkům snadno a rychle využívat IT infrastrukturu bez nutnosti jejího nákupu, instalace a správy. Mezi nejznámější poskytovatele IaaS patří Amazon Web Services, Microsoft Azure a Google Cloud Platform *(Infrastructure as a Service)*
ICT	Informační a komunikační technologie *(Information and Communication Technology)*
IP	Jeden ze základních komunikačních protokolů používaných v počítačových sítích *(Internet Protocol)*
IT	Informační technologie *(Information Technology)*
M365	Globální označení služeb společnosti Microsoft, umožňující licencování jejich produktů a provoz aplikací, a to ať už jako on-premise řešení, či v cloudovém prostředí *(Microsoft 365)*
MS	Microsoft Corporation, americký výrobce především SW a provozovatel cloudového prostředí MS Azure
PaaS	Typ cloudové služby, která poskytuje vývojářům a IT týmům platformu pro vývoj, nasazení a správu aplikací bez nutnosti starat se o správu hardwaru a infrastruktury. Poskytovatelé PaaS nabízejí vývojové nástroje, databáze, síťové služby a další nástroje jako služby, což umožňuje vývojářům se soustředit pouze na vývoj aplikace *(Platform as a Service)*
SaaS	Model poskytování software, kdy je software hostován v cloudovém prostředí a poskytován uživatelům přes Internet. Tyto služby jsou poskytovány vývojáři software jako služby a účtovány jsou za používání (pay-as-you-go). To umožňuje uživatelům využívat software bez nutnosti investovat do hardware a IT infrastruktury *(Software as a Service)*
SAP	Modulární ERP systém od německé firmy SAP AG
SSO	Metoda jednotného přihlášení *(Single Sign-On)*
SW	Software je sada všech počítačových programů používaných v počítači, které provádějí nějakou činnost
SŽ	Správa železnic, státní organizace
SŽT	Správa železničních informačních technologií

Seznam vysvětlivek

MS Azure	Cloudové prostředí firmy Microsoft.
MS EntraID	Služba AD provozovaná v cloudovém prostředí MS Azure.
Platforma SŽ	Soubor dokumentů, rozdělený na veřejnou, interní a metodickou část, určený pro seznámení dodavatelů s ICT prostředím SŽ a současně s používanými standardy a technologiemi.
Tenant	Dedikovaný virtuální prostor v cloudovém prostředí MS Azure

1 Úvod

Cílem této části Platformy SŽ je popis podporovaných cloudových služeb, technologií, a architektonických principů v rámci tenantu provozovaného Správou železnic v cloudovém prostředí.

Důvodem je zajistit ve fázích přípravy poptávky, návrhu ICT řešení a realizace dodávky kompatibilitu se stávajícím cloudovým prostředím Správy železnic a umožnit využití pro aplikace, které splňují podmínky pro umístění v cloudovém prostředí.

2 Cloudové prostředí

U aplikací a informačních systémů, kde je to z technických a bezpečnostních důvodů možné, adoptuje Správa železnic moderní technologie včetně cloudového prostředí. S ohledem na vysoké zastoupení kritické informační infrastruktury v portfoliu Správy železnic je tento proces řízen přísnou metodikou.

V současnosti využívá Správa železnic cloudová prostředí na platformách Microsoft Azure, Amazon AWS, SAP HANA Cloud a Oracle Cloud Infrastructure, která podporují různé typy cloudových služeb:

- IaaS – infrastruktura jako služba
- PaaS – platforma jako služba
- SaaS – software jako služba

V rámci Platformy SŽ pak nabízí výhradně SaaS na platformě MS Azure, jelikož ostatní cloudová prostředí jsou v případě SŽ úzce svázána s konkrétními informačními systémy.

2.1 Microsoft Entra ID

Správa železnic provozuje ve svém ICT prostředí službu Active Directory a spolu s příchodem cloudového prostředí ho rozšířila i tam, dříve pod názvem Azure Active Directory, dnes Microsoft Entra ID.

2.2 Služby M365

Správa železnic využívá velkou část portfolia SaaS služeb poskytovaných na platformě MS Azure pod názvem M365.

3 Cloudové služby

V rámci svého v současnosti používaného cloudového prostředí na platformě Microsoft Azure jsou Platformou SŽ poskytovány následující služby.

3.1 Služba ověření proti Microsoft Entra ID

Zejména u aplikací jejichž uživatelé se pohybují mimo interní sítě Správy železnic je k dispozici služba Microsoft Entra ID. Ověřování proti Microsoft Entra ID přináší vyšší bezpečnost a pohodlí uživatelů i pomocí jednotného přihlašování (SSO).

3.2 Integrace s M365

Pokud u informačního systému či aplikace předpokládá Dodavatel jakoukoli integraci s aplikacemi z rodiny M365, je nutné využít tenant Správy železnic.

Správa železnic, státní organizace
Správa železniční telematiky
Dlážděná 1003/7
110 00 Praha 1

Datum tisku
2025-07-30

SPRÁVA ŽELEZNIC

Příloha č. 5 Smlouvy

Poddodavatelé

Dodavatel provádí předmět plnění dle Smlouvy prostřednictvím následujících Poddodavatelů:

[OBCHODNÍ FIRMA PODDODAVATELE – NÁZEV, IČO, SÍDLO – DOPLNÍ DODAVATEL]	
Část Plnění dle Smlouvy prováděná prostřednictvím Poddodavatele ve finančním procentuálním vyjádření ve vztahu k Ceně.	[DOPLNÍ DODAVATEL] %
Stručný popis činností, které jsou prováděny Poddodavatelem.	[DOPLNÍ DODAVATEL]
Prostřednictvím Poddodavatele je prokazována kvalifikace	ANO/NE [DOPLNÍ DODAVATEL]

[Pokud Dodavatel provádí Plnění či jeho část prostřednictvím Poddodavatelů, uvede tabulku tolikrát, kolika Poddodavateli bude předmět plnění provádět. Dodavatel musí uvést všechny Poddodavatele, kteří se budou podílet na provádění Plnění dle Smlouvy.]

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384
Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČO: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

SPRÁVA ŽELEZNIC

Příloha č. 6 Smlouvy

Zvláštní obchodní podmínky pro Zakázky v oblasti ICT

OBSAH

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČ: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

1. VÝKLAD POJMŮ

1.1. **Akceptační kritéria** představují podmínku anebo vlastnost výstupu provádění Plnění dle Smlouvy, která musí být splněna, aby bylo Plnění dle Smlouvy provedeno, přičemž Akceptační kritéria jsou uvedena v Příloze Smlouvy, která obsahuje specifikaci Plnění (dále jen „**Specifikace Plnění**").

1.2. **Akceptační protokol** je protokol, který jsou zavázáni podepsat Objednatel i Dodavatel po provedení všech nezbytných činností v rámci Akceptačního řízení, potvrzující provedení výstupu provádění Plnění anebo výsledek Testů výstupů provádění Plnění. Protokol je připravený ze strany Dodavatele a následně upravený a vyplněný Objednatelem. Akceptační protokol obsahuje:

a. Specifikaci provedeného Plnění;

b. Akceptační kritéria;

c. informace o průběhu Testů, jsou-li prováděny;

d. další informace a dokumenty nezbytné pro provedení Akceptačního řízení provedeného Plnění.

1.3. **Akceptační řízení** je postupné provedení akceptačních procesů a podepsání Akceptačního/ch protokolu/ů pro Plnění dle Smlouvy.

1.4. **Aktualizace** je dílčí změna verze Softwaru, zpravidla odstraňující zranitelnosti či drobné nedostatky Softwaru většinou neprojevující se navenek uživatelům, v IT obvykle označovaná jako „patch" nebo „security update" (v rámci IT se také často označuje jako změna třetí číslice v čísle verze Softwaru, tedy např. 4.1.1. na 4.1.2.). Aktualizace představuje takovou změnu Softwaru, která není Modernizací ani Zásadní modernizací.

1.5. **Autorské dílo** znamená dílo ve smyslu § 2 Autorského zákona; zejména Software, Databáze a jakékoliv výstupy předávané Objednateli na základě Smlouvy, které splňují podmínky stanovené v § 2 Autorského zákona.

1.6. **Autorský zákon** znamená zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

1.7. **Cena** je celková cena za Plnění bez DPH dle Smlouvy. V případě:

a. Smlouvy na dobu neurčitou, jejímž předmětem jsou výhradně pravidelně se opakující či trvající služby či činnosti, se cenou Plnění bez DPH rozumí cena bez DPH za 12 měsíců poskytování takových služeb či činností.

b. Smlouvy na dobu neurčitou, součástí jejíhož předmětu jsou mj. pravidelně se opakující či trvající služby či činnosti, které je Dodavatel povinen poskytovat na dobu neurčitou, se cenou Plnění bez DPH rozumí souhrn cen bez DPH ostatních částí Předmětu Smlouvy a ceny bez DPH za 12 měsíců poskytování takových služeb či činností.

c. Smlouvy, která je rámcovou dohodou, se cenou za Plnění bez DPH této Smlouvy rozumí limit stanovený v této Smlouvě jako maximální souhrnná hodnota bez DPH všech dílčích smluv uzavřených na základě této Smlouvy.

d. Smlouvy, která je zčásti rámcovou dohodou, se cenou za Plnění bez DPH této Smlouvy rozumí souhrn cen bez DPH ostatních části Předmětu Smlouvy a limitu stanoveného v této Smlouvě jako maximální souhrnná hodnota bez DPH všech dílčích smluv uzavřených na základě této Smlouvy.

1.8. **Čas nahlášení Incidentu** představuje časový údaj, vyjadřující datum a čas, kdy byl Incident nahlášen Dodavateli způsobem stanoveným ve Smlouvě a ZOP, tj. vytvořením ticketu v Servicedesku, vytěžením e-mailu z e-mailového serveru Objednatele a jeho vložením do Servicedesku jako ticketu anebo ukončením telefonátu.

1.9. **Data** jsou záznamy jednání, skutečností nebo informací a soubory takových jednání, skutečností nebo informací, včetně provozních údajů a metadat, zejména v podobě textu, čísel, grafů, obrazů, zvuku a videa.

1.10. **Databáze** znamená databázi splňující požadavky na Autorská díla, databázi ve smyslu § 88 Autorského zákona a jakoukoliv jinou Autorským zákonem neupravenou databázi.

1.11. **Doba vyřešení** je pro každou kategorii Incidentů uvedena ve Smlouvě a ZOP a znamená rozdíl mezi časem nahlášení Incidentu a dodáním řešení. Do Doby vyřešení Incidentu se nezapočítává doba, po kterou nemůže Dodavatel řešit Incident z důvodu:

a. neobdržení podkladů a informací vyžádaných Dodavatelem, které jsou nezbytně nutné pro lokalizaci nebo replikaci Incidentu, od Objednatele;

b. řešení Incidentu u třetí osoby (vyjma Poddodavatele), jejíž součinnost je dle Smlouvy povinen zajistit Objednatel (např. poskytovatele služeb podpory IT prostředí Objednatele anebo systémů, na které je Software napojen);

c. neposkytnutí jiné nezbytně nutné součinnosti Objednatele vyžádané Dodavatelem v souladu s těmito ZOP či Smlouvou a souvisejícími přílohami.

1.12. **Doba zpracování či Reakční doba** je doba, ve které Dodavatel musí reagovat prostředkem odpovídajícím způsobu nahlášení Incidentu či Požadavku o přijetí takového nahlášení a o zahájení činností směřujících k vyřešení Incidentu či Požadavku.

1.13. **Dodavatel** označuje rovněž Poskytovatele, Zhotovitele či Prodávajícího v závislosti na typu uzavřené Smlouvy.

1.14. **Dodavatel strategicky významné služby** je Dodavatel, který se podílí na poskytování Strategicky významné služby.

1.15. **Dohledové centrum kybernetické bezpečnosti SŽ (SOC SŽ**) je specializovaný útvar SŽ, který ve režimu 24/7 zajišťuje činnosti související se zajištěním kybernetické bezpečnosti. Kontaktní údaje: soc@spravazeleznic.cz nebo +420 972 235 333.

1.16. **Dokumentace** znamená část specifikace Předmětu Smlouvy, která představuje jednotlivé dokumenty popisující Předmět Smlouvy a zacházení s ním, jako jsou uživatelská dokumentace, administrátorská dokumentace, bezpečnostní dokumentace, a také jakoukoliv jinou dokumentaci vytvářenou anebo poskytovanou Dodavatelem v rámci provádění Plnění. Dokumentace musí být vždy vyhotovena a předána Objednateli v elektronické podobě (pokud je vyhotovována v listinné podobě, pak Dodavatel předá Objednateli elektronickou kopii takové Dokumentace).

1.17. **Dostupnost** znamená stav Software či Hardware, v průběhu kterého je, anebo by v případě poskytování řádné a včasné součinnosti ze strany Objednatele za podmínek dle Smlouvy byl, možný řádný provoz Softwaru či Hardware v celém jeho rozsahu, přičemž Software se považuje za Dostupný, je-li přístupný a použitelný pro všechny uživatele Softwaru ve sjednaném rozsahu minimálně dle příslušného Servisního modelu dle ZOP.

1.18. **Důvěrné informace** znamenají informace, které jsou zpracovávány, ukládány nebo poskytovány v IT prostředí Objednatele, včetně Dat Objednatele, veškeré údaje a informace související s těmito informacemi, s technickým vybavením, komunikačními prostředky a programovým vybavením IT prostředí Objednatele a s objekty, ve kterých jsou tyto systémy umístěny, zaměstnanci nebo dodavateli podílejícími se na provozu, rozvoji, správě nebo bezpečnosti IT prostředí Objednatele. Mezi Důvěrné informace nepatří informace, které jsou veřejně přístupné.

1.19. **FOSS licence** znamená Free Open Source Software licence.

1.20. **GDPR** znamená nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

1.21. **GUI** znamená grafické uživatelské rozhraní.

1.22. **Hands-on** se rozumí školení vymezené v rámci Smlouvy či jejích příloh (je-li takové), zpravidla jde o školení, jehož součástí je komentované provedení části Plnění za účasti zástupců Objednatele

1.23. **Hardware** znamená veškeré hmotné součásti počítačových systémů a veškeré související vybavení hmotné povahy spolu se vším příslušenstvím, a včetně veškeré související dokumentace.

1.24. **Servicedesk** je Software provozovaný Dodavatelem nebo Objednatelem sloužící ke komunikaci Stran v průběhu provádění Plnění dle Smlouvy a zároveň bude sloužit jako kontaktní místo

Dodavatele pro nahlašování Incidentů a Požadavků, vznášení dotazů k Plnění, získávání odpovědí ve vztahu k Plnění a další zaznamenávání průběhu provádění Plnění dle Smlouvy.

1.25. **Informační či komunikační systém** znamená informační či komunikační systém kritické informační infrastruktury Objednatele nebo jiný informační či komunikační systém, který souvisí s poskytováním regulované služby Objednatelem.

1.26. **Incident** představuje neplánované přerušení fungování Předmětu Smlouvy, jakékoliv jeho části anebo Plnění dle Smlouvy, omezení kvality fungování Předmětu Smlouvy a souvisejícího Plnění, anebo jakoukoliv prokazatelnou nefunkčnost Předmětu Smlouvy a souvisejícího Plnění. Incident se projevuje zejména selháním oproti funkčnosti a funkcionalitě specifikované v Příloze Smlouvy *Specifikace Plnění*, anebo obvyklé pro Předmět Smlouvy. Vada je vždy Incidentem a jde tak o podmnožinu pojmu Incident. Za dobu trvání Incidentu se považuje doba od Času nahlášení Incidentu Ohlašovatelem do vyřešení Incidentu, které bude Ohlašovatelem nebo jeho nadřízeným uživatelem potvrzeno vhodným způsobem v Servicedesku, byl-li Incident vyřešen.

Kategorizace Incidentů dle důležitosti, zohledňující naléhavost a dopad Incidentu:

A) Vysoká – ohrožení kritických procesů a činností na straně Objednatele

B) Střední – Zásadní vliv na důležité procesy a činnosti Objednatele

C) Nízká – standardní řešení v efektivním režimu.

Mezi Incidenty dále patří také všechny Kybernetické bezpečnostní incidenty, které jsou podmnožinou pojmu Incident.

1.27. **Instalace** znamená provedení veškerých činností nezbytných ke zprovoznění Hardwaru nebo Softwaru vč. jeho Aktualizací, Modernizací či Zásadních modernizací poskytnutých v rámci Plnění dle Smlouvy v IT prostředí Objednatele, a to na platformě určené Objednatelem.

1.28. **ISDS** znamená informační systém datových schránek ve smyslu zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů.

1.29. **Interní předpisy** znamenají interní předpisy Objednatele, jejichž seznam včetně znění daných interních předpisů, jsou-li relevantní z hlediska Plnění, je uveden v Příloze Smlouvy *Seznam interních předpisů.*

1.30. **Insolvenční zákon** znamená zákon č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů.

1.31. **IT prostředí Objednatele** znamená veškerý Hardware a Software, který Objednatel oprávněně užívá. Jedná se zejména o servery, diskové pole a stanice, aplikace třetích osob, pasivní a aktivní datová infrastruktura (kabeláže, switche, VPN linky apod.). Podrobná specifikace IT prostředí Objednatele je uvedena v Příloze Smlouvy *Platforma Správy železnic* a v Příloze Smlouvy *Specifikace Plnění*.

1.32. **Kvalifikovaná osoba** je člen Realizačního týmu, kterým Dodavatel prokazoval splnění kvalifikačních předpokladů v rámci Veřejné zakázky.

1.33. **Kybernetický bezpečnostní incident** je narušení bezpečnosti informací v Kybernetickém prostoru SŽ.

1.34. **Kybernetická bezpečností událost** je událost podle ZoKB, která může vyústit v Kybernetický bezpečnostní incident.

1.35. **Kybernetický prostor SŽ** je soubor sítí elektronických komunikací a dalších technologií, ve kterém dochází ke zpracování informací a dat v elektronické podobě.

1.36. **MD** znamená manday/člověkoden. Nestanoví-li Smlouva jinak, odpovídá jeden MD 8 MH.

1.37. **MH** znamená manhour/člověkohodinu. Nestanoví-li Smlouva jinak, odpovídá jedna MH 60 minutám práce.

1.38. **Modernizace** je změna verze Softwaru, která zpravidla představuje výraznější zásah do dílčí funkcionality Softwaru, přepracováním jeho vybrané funkcionality či doplnění funkcionality nové, zvýšení kompatibility Softwaru s jinými prvky informačních a komunikačních technologií, či jinou optimalizaci funkce Softwaru nad rámec Aktualizace, zpravidla v IT označovaná jako „update" (v

rámci IT se také často označuje jako změna druhé číslice v čísle verze Softwaru, tedy např. 4.1. na 4.2.).

1.39. **NÚKIB** znamená Národní úřad pro kybernetickou a informační bezpečnost.

1.40. **Občanský zákoník** znamená zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

1.41. **Obchodní podmínky** znamenají obchodní podmínky Objednatele v posledním znění ke dni podání nabídky do Veřejné zakázky či aktualizace těchto Obchodních podmínek provedené v souladu se Smlouvou po dobu jejího trvání.

1.42. **Objednatel** je Správa železnic, státní organizace, IČO 70994234, se sídlem Praha 1 – Nové Město, Dlážděná 1003/7, PSČ 110 00, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze pod sp. Zn. A 48384.

1.43. **Ohlašovatel** znamená osobu určenou Objednatelem, zpravidla uživatele Předmětu Smlouvy.

1.44. **Opční právo** představuje vyhrazenou změnu závazku v souladu s ustanovením § 100 odst. 3 ZZVZ ze Smlouvy spočívající v pořízení dalšího obdobného Plnění od vybraného uchazeče v rámci zadávacího řízení Veřejné zakázky, tj. od Dodavatele dle Smlouvy.

1.45. **Osobní údaje** znamenají osobní údaje ve smyslu GDPR, včetně zvláštních kategorií osobních údajů ve smyslu článku 9 a rozsudků ve smyslu článku 10 GDPR.

1.46. **Pracovní den (PD)** znamená kterýkoliv den, kromě soboty a neděle a dnů, na něž připadá státní svátek nebo ostatní svátek podle platných a účinných právních předpisů České republiky.

1.47. **Paušální služby** jsou služby definované ve Smlouvě, jsou-li takové, zpravidla trvajícího či opakujícího se charakteru.

1.48. **Platforma Správy železnic/Platforma SŽ** je dokument, který definuje prostředí, které standardizuje a podporuje návrh, implementaci a provozování veškerého ICT řešení pro Správu železnic. Popisuje infrastrukturní a platformní služby, podporované technologie a upravuje pravidla jejich použití i rozšiřování. Primárním cílem Platformy SŽ je poskytnout potenciálním dodavatelům základní přehled o ICT prostředí SŽ a současně umožnit organizaci SŽ zajištění efektivního vytváření a provozování ICT řešení při dodržení vysoké kvality a bezpečnosti služeb.

1.49. **Plnění (též Předmět Smlouvy)** představuje plnění, které je Dodavatel povinen dle Smlouvy poskytovat. Plněním se rozumí jak činnost Dodavatele, tak její výsledek, je-li takový; tímto výsledkem je zejména HW, SW či jiný výstup plnění dle Smlouvy. Plnění je blíže specifikováno ve Smlouvě nebo v její příloze.

1.50. **Poddodavatel** znamená kteroukoli třetí osobu realizující poddodávky pro Dodavatele v souvislosti s Předmětem Smlouvy. Poddodavatelé mohou být výslovně uvedeni v Příloze Smlouvy *Poddodavatelé*.

1.51. **Požadavek** znamená žádost ze strany Objednatele o službu nebo její podporu předanou v souladu se Smlouvou Dodavateli, která nemá příčinu v chybovém stavu, tj. není Incidentem.

Kategorizace Požadavků dle důležitosti:

A) Vysoká – řešení je pro Objednatele kritické

B) Střední – řešení neovlivňuje využívání hlavních funkcí služby

C) Nízká – řešení výrazně neovlivňuje procesy Objednatele

1.52. **Produkční prostředí** znamená IT prostředí Objednatele v ostrém provozu běžně přípustnou uživatelům Software, vyjma Testovacího prostředí.

1.53. **Převzetí poskytování plnění** je předání znalostí Dodavateli a praktické seznámení se Dodavatele s podmínkami poskytování služeb. Pokud dochází k převzetí poskytování podpory, jsou podmínky pro Převzetí poskytování plnění uvedeny ve Smlouvě a v Příloze Smlouvy *Specifikace Plnění*.

1.54. **Příloha Smlouvy** je dokument, který tvoří nedílnou součást Smlouvy a obsahuje bližší specifikaci smluvních podmínek.

1.55. **Reakce** znamená kvalifikovanou a konkrétní odpověď na nahlášení Incidentu nebo na jiný požadavek, ve formě a způsobem dále definovanými v Příloze Smlouvy *Specifikace Plnění*.

1.56. **Reakční doba** je pro každou kategorii Incidentů uvedena v Příloze *Specifikace Plnění* a představuje dobu od Času nahlášení Incidentu do doručení Reakce Objednateli nebo Ohlašovateli.

1.57. **Realizační tým** znamená osoby uvedené v příloze Smlouvy *Realizační tým*, kterými Dodavatel prokazoval splnění kvalifikačních předpokladů v rámci Veřejné zakázky a další osoby (zaměstnanci Dodavatele či Poddodavatele), prostřednictvím nichž Dodavatel provádí Plnění dle Smlouvy.

1.58. **Recovery Point Objective (RPO)** je parametr, který vyjadřuje maximální ztrátu dat uživatelů při havárii systému a následné obnově.

1.59. **Recovery Time Objective (RTO)** je parametr, který vyjadřuje dobu nutnou k obnově chodu služby do akceptované úrovně provozu.

1.60. **Servisní model** je standardizovaný model provozu a podpory aplikace, systému nebo instance služby.

1.61. **SLA** znamená úroveň kvality Plnění představující dohodu o úrovni poskytovaných ICT služeb dle Smlouvy.

1.62. **Služby** jsou služby definované ve Smlouvě, jsou-li takové.

1.63. **Smluvní strany či Strany** jsou strany Smlouvy, tj. Objednatel a Dodavatel či jinak označené strany Smlouvy, jejíž součástí jsou tyto ZOP.

1.64. **Software** znamená veškeré programové vybavení a další Autorská díla, stejně jako další věci či jiné majetkové hodnoty, které s programovým vybavením souvisí a jsou určeny ke společnému užívání s tímto programovým vybavením, tj. zejména Databáze, GUI, zvukové nahrávky, videa, obrázky, fotografie apod., včetně veškeré související dokumentace a updatů a upgradů tohoto programového vybavení, avšak s výjimkou Hardwaru a Databází.

1.65. **Standardní Software** znamená Software, který je distribuován pod standardními licenčními podmínkami více třetím osobám. Mezi Standardní software patří:

a. Software renomovaných výrobců, jenž je na trhu běžně dostupný, tj. nabízený na území České republiky alespoň dvěma (2) na sobě nezávislými a vzájemně se neovládajícími subjekty, a který je v době uzavření Smlouvy prokazatelně užíván v produkčním prostředí nejméně u pěti (5) na sobě nezávislých a vzájemně nepropojených subjektů.

b. Software, u kterého je s ohledem na jeho (i) marginální význam, (ii) nekomplikovanou propojitelnost či (iii) oddělitelnost a nahraditelnost v IT prostředí bez nutnosti vynakládání větších prostředků (více než 50.000 Kč/rok) zajištěno, že další rozvoj Softwaru jinou osobou než tvůrcem/distributorem takového Softwaru je možné provádět bez toho, aby tím byla dotčena práva autorů takovéhoto Softwaru, neboť nebude nutné zasahovat do Zdrojových kódů takovéhoto Softwaru anebo proto, že případné nahrazení takovéhoto Softwaru nebude představovat výraznější komplikaci a náklad na straně Objednatele.

c. Software, jehož API („Application Programming Interface") pokrývá všechny moduly a funkcionality Softwaru, je dobře dokumentované, umožňuje zapouzdření Softwaru a jeho adaptaci v rámci měnících se podmínek IT prostředí Objednatele a Softwaru bez nutnosti zásahu do Zdrojových kódů Softwaru, a Dodavatel poskytne Objednateli právo užít toto rozhraní pro programování aplikací ve stejném rozsahu jako Software.

d. Software, o kterém to stanoví Smlouva.

1.66. **Strategicky významná služba (SVS)** je regulovaná služba, jejíž narušení by mohlo mít závažný dopad na bezpečnost České republiky nebo vnitřní pořádek a která je určena obecně závazným právním aktem – nařízením vlády ČR.

1.67. **Smlouva** uzavřená na základě zadávacího řízení Veřejné zakázky vztahující se k ICT, která se řídí těmito ZOP. Smlouvou se rovněž rozumí rámcová dohoda a dílčí smlouva uzavřená na základě takové rámcové dohody.

1.68. **Systém** znamená ucelený soubor technických, programových a datových prvků, včetně jejich konfigurace, rozhraní a vzájemných vazeb, který je provozován samostatně nebo jako součást IT infrastruktury a slouží k zajištění určité funkce, služby nebo procesu, zejména ke zpracování, ukládání, přenosu nebo poskytování informací.

1.69. **Testy** se rozumí provádění testovacího užívání Předmětu Smlouvy v Testovacím prostředí prostřednictvím simulace ostrého provozu v Produkčním prostředí a reálných situací a Testovacích scénářů.

1.70. **Testovací prostředí** znamená virtuální či fyzickou kopii Předmětu Smlouvy anebo IT prostředí Objednatele určenou Objednatelem k provádění Testů.

1.71. **Vada kategorie A** znamená kritickou vadu, která má zásadní dopad na základní funkce Plnění, má jakýkoli vliv na kvalitu a bezpečnost dat a výsledky jejich zpracování anebo způsobuje výpadky Plnění.

1.72. **Vada kategorie B** znamená vadu umožňující provoz základních funkcí Plnění, zároveň nemá vliv na kvalitu ani na bezpečnost dat a výsledky zpracování anebo hrozí, že by mohla způsobit výpadek Plnění.

1.73. **Vada kategorie C** znamená vadu, která není Vadou kategorie A anebo B (např. špatná grafická úprava aplikace, špatný pravopis u nápovědy apod.).

1.74. **Veřejná zakázka** je zakázka realizovaná na základě smlouvy mezi Objednatelem a Dodavatelem, jež byla uzavřena na základě zadávacího řízení dle ZZVZ nebo výběrového řízení dle vnitřních předpisů Objednatele.

1.75. **VoKB** znamená vyhlášku č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností.

1.76. **Výkaz** znamená dokument obsahující souhrnnou evidenci poskytnutého Plnění za období vymezené ve Smlouvě nebo v Příloze Smlouvy *Specifikace Plnění*. Výkaz je vystavován zpětně za vymezené období.

1.77. **Výpadek** znamená neplánované přerušení provozu Předmětu smlouvy či jakékoliv jeho podstatné části, při kterém je tento celek či příslušná část nedostupná pro uživatele (není dostupný). Za Výpadek se pro účely této Smlouvy nepovažuje Výpadek způsobený z důvodů způsobených třetími osobami, jejichž součinnost anebo bezvadné poskytování služeb je povinen zajistit Objednatel (poskytovatel služeb podpory IT prostředí Objednatele a informačních systémů, na které je Software napojen).

1.78. **Újma** znamená vždy újmu na jmění (škodu) ve smyslu § 2894 odst. 1 Občanského zákoníku a dále vždy i nemajetkovou újmu ve smyslu § 2894 odst. 2 Občanského zákoníku. Toto ustanovení je výslovným ujednáním o povinnosti stran odčinit nemajetkovou újmu v případech porušení povinností dle těchto ZOP a Smlouvy.

1.79. **Významný dodavatel** je ten, kdo SŽ poskytuje plnění, které je významné z hlediska zajištění kybernetické bezpečnosti regulované služby. Významní dodavatelé jsou evidováni v souladu s VoKB.

1.80. **Významná změna** znamená změnu Softwaru, Systému, Služby, IT prostředí Objednatele, nebo procesu, která může podstatným způsobem ovlivnit bezpečnost, dostupnost, integritu nebo funkčnost Předmětu plnění, plnění závazků vyplývajících ze Smlouvy nebo může mít významný dopad na plynulost či kontinuitu provozu Objednatele. Za Významnou změnu se považuje zejména změna, která zahrnuje podstatnou úpravu architektury, funkčnosti nebo způsobu provozu systému, zavádí novou technologii nebo zásadně mění technické řešení, může změnit úroveň rizik nebo vyžaduje provedení bezpečnostní analýzy či bezpečnostních testů, a dále změna, která může mít dopad na plnění povinností podle obecně závazných právních předpisů, zejména předpisů v oblasti kybernetické bezpečnosti. Významné změny podléhají předchozímu písemnému schválení Objednatele a musí být realizovány v souladu s procesy řízení změn Objednatele, včetně požadovaného bezpečnostního posouzení, testování nebo auditu, pokud tak stanoví Smlouva, Interní předpisy Objednatele nebo příslušná právní úprava.

1.81. **Zadávací dokumentace** je souborem dokumentů obsahujících zadávací podmínky, sdělované nebo zpřístupňované účastníkům zadávacího řízení na Veřejnou zakázku.

1.82. **Zásadní modernizace** je podstatná změna/rozšíření funkčnosti nebo změna koncepce Softwaru, přinášející podstatné změny pro chování Softwaru vůči uživatelům, zpravidla v IT označovaná jako „upgrade" (v rámci IT se také často označuje jako změna v čísle verze Software, tedy např. 4 na 5).

1.83. **Zdrojový kód** znamená zápis kódu počítačového programu (Softwaru) v programovacím jazyce, který je uložen v jednom nebo více editovatelných souborech, čitelný, opatřený komentáři vysvětlujícími jeho jednotlivé části alespoň ve standardu obvyklém pro open source projekty a procesy, ve spustitelném formátu odpovídajícím programovacímu jazyku a Produkčnímu prostředí, včetně ověřeného a podrobného postupu nezbytného pro sestavení plně funkčního strojového kódu, a v podobě, aby jej bylo možné zkompilovat do strojového kódu bez nutnosti provedení jiných úprav než kompilace v souladu s postupem k sestavení.

1.84. **ZoKB** znamená zákon č. 264/2025 Sb., o kybernetické bezpečnosti.

1.85. **ZOP** znamená tento dokument, tedy zvláštní obchodní podmínky, které definují další parametry a upřesňují konkrétní podmínky a specifické požadavky Objednatele.

1.86. **ZZVZ** znamená zákon č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů.

1.87. Není-li výslovně uvedeno jinak nebo nevyplývá-li něco jiného z povahy věci, mají pojmy, které nejsou definovány v těchto ZOP, význam uvedený v Obchodních podmínkách či Smlouvě a jejích přílohách.

1.88. Ustanovení ZOP mají přednost před ustanoveními Obchodních podmínek, pokud jsou ustanovení těchto dokumentů v rozporu, uplatní se ustanovení uvedené v ZOP. Ustanovení Smlouvy mají přednost před ustanoveními Obchodních podmínek i ZOP.

1.89. Pokud je uveden v ZOP čas, jedná se o čas SEČ.

1.90. Dodavatel je povinen se seznámit s Platformou Správy železnic, a to bez ohledu na to, zda plnění probíhá v IT prostředí Objednatele, a to minimálně v rozsahu, v kterém je pro Plnění relevantní.

2. DOBA A MÍSTO PLNĚNÍ

2.1. Provádění Plnění bude zahájeno ode dne nabytí účinnosti Smlouvy, není-li ve Smlouvě stanoveno jinak.

2.2. Plnění nebo dílčí části Plnění bude Dodavatel provádět v termínech sjednaných ve Smlouvě či definovaných v Příloze Smlouvy *Specifikace Plnění* nebo *Harmonogram.*

2.3. Místem provádění Plnění jsou místa umístění IT prostředí Objednatele (tj. Testovací prostředí a Produkční prostředí), není-li ve Smlouvě anebo Příloze Smlouvy *Specifikace Plnění* výslovně stanoveno jinak. Popis IT prostředí Objednatele obsahuje Příloha Smlouvy *Platforma Správy železnic*.

2.4. Služby budou poskytovány formou vzdáleného přístupu k IT prostředí Objednatele, není-li ve Smlouvě stanoveno jinak. Objednatel se zavazuje umožnit Dodavateli vzdálený přístup k IT prostředí Objednatele. Objednatel je oprávněn monitorovat a logovat přístupy Dodavatele do IT prostředí Objednatele, jakož i veškerou další aktivitu Dodavatele významnou z hlediska bezpečnosti Informačního či komunikačního systému za účelem posouzení souladu Plnění Smlouvy s pravidly uvedenými v těchto ZOP, zejm. pak v čl. 21. ZOP, a Dodavatel se zavazuje Objednateli za tímto účelem poskytnout veškerou nutnou součinnost. Vzdálený přístup k IT prostředí Objednatele může být Objednatelem okamžitě odepřen v případě Kybernetické bezpečnostní události ve smyslu § 2 ZoKB či porušení povinností stanovených v Interních předpisech.

2.5. Dodavatel bere na vědomí, že přístup k IT prostředí Objednatele:

a. je udělován fyzickým osobám Dodavatele, jakož i pro konkrétní zařízení, na základě výslovného požadavku Dodavatele a Objednatel je oprávněn dle svého uvážení přístup neudělit či kdykoli odebrat;

b. je poskytován na základě principů "*need to know*" a "*deny by default*"; a

c. je poskytován za podmínky dodržování veškerých bezpečnostních opatření a požadavků Objednatele.

3. PRÁVA A POVINNOSTI OBOU STRAN

3.1. Strany se zavazují postupovat v souladu s veškerými obecně závaznými právními předpisy a prohlašují, že Smlouva je v souladu s těmito právními předpisy. Pokud se v průběhu trvání Smlouvy některé její ustanovení dostane do rozporu s kogentním ustanovením obecně závazného právního předpisu, platí příslušné ustanovení právního předpisu s tím, že zbývající ustanovení Smlouvy zůstávají v platnosti.

3.2. Strany jsou v průběhu Plnění povinny postupovat v souladu s Interními předpisy Objednatele, pokud jsou jednoznačně specifikovány v Příloze Smlouvy *Seznam Interních předpisů.* Objednatel je oprávněn přiměřeným způsobem jednostranně měnit nebo doplňovat Interní předpisy uvedené v Příloze Smlouvy, pokud je to nezbytné pro zajištění souladu s právními předpisy, bezpečnostními požadavky nebo provozními standardy. Objednatel je povinen o každé takové změně informovat Dodavatele tak, aby měl Dodavatel reálnou možnost změny implementovat, není-li z povahy věci nutné jednat bezodkladně (např. při hrozbě Kybernetického bezpečnostního incidentu). Dodavatel je povinen změny implementovat v rozsahu, v jakém je to po něm lze spravedlivě požadovat, s ohledem na charakter plnění, technické možnosti a přiměřené náklady. Pokud Dodavatel prokazatelně doloží, že změna má podstatný dopad na cenu nebo termíny plnění, Strany sjednají odpovídající úpravu Smlouvy.

4. POVINNOSTI DODAVATELE

4.1. Dodavatel se zavazuje provádět pro Objednatele Plnění osobně, tj. prostřednictvím svých zaměstnanců, členů Realizačního týmu a prostřednictvím svých Poddodavatelů za podmínek stanovených ve Smlouvě a těchto ZOP. V případě, že je požadavek na složení Realizačního týmu uveden ve Smlouvě, je Dodavatel povinen provádět Plnění výhradně prostřednictvím členů Realizačního týmu, kterými prokázal splnění kvalifikace v průběhu zadávacího řízení na Veřejnou zakázku.

4.2. Dodavatel se během poskytování Plnění pro Objednatele zavazuje informovat Objednatele o Významné změně ovlivnění nebo ovládání Dodavatele podle ust. § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů (dále jen „ZOK"), nebo změně vlastnictví zásadních aktiv, využívaných Dodavatelem k Plnění Smlouvy, jakož i o změně oprávnění nakládat s těmito aktivy.

4.3. Dodavatel se zavazuje poskytovat v rámci Plnění veškerou součinnost nezbytnou k provádění Plnění, zejména:

4.3.1. poskytovat Plnění dle Smlouvy ve vysoké kvalitě s odbornou péčí odpovídající podmínkám sjednaným ve Smlouvě;

4.3.2. poskytovat Plnění dle Smlouvy alespoň v závazných parametrech kvality dle Smlouvy a SLA, a to zejména dodržování stanoveného Servisního modelu dle odst. 12.2. ZOP;

4.3.3. upozorňovat Objednatele včas na všechny hrozící vady svého Plnění či potenciální Výpadky či jiné výpadky Plnění, jakož i poskytovat Objednateli veškeré informace, které jsou pro Plnění potřebné;

4.3.4. zajistit v souladu s podmínkami Smlouvy poskytnutí Dokumentace, a to rovněž vždy při každé Aktualizaci nebo jiné změně Předmětu smlouvy, nestanoví-li Objednatel jinak;

4.3.5. počínat si při provedení Plnění tak, aby nedošlo k infikaci Softwaru, Standardního Softwaru nebo IT prostředí Objednatele virem či jiným škodlivým kódem (malware apod.) způsobujícím narušení zabezpečení Softwaru a Standardního Softwaru za účelem jeho poškození či jiného narušení běhu;

4.3.6. bez zbytečného odkladu na výzvu Objednatele předat Data, provozní údaje a informace ve formátu předem odsouhlaseném Objednatelem (zpravidla ve formátu daného prostředí, který umožňuje jejich nasazení „as is" do prostředí), které má k dispozici v souvislosti s Plněním Smlouvy, a poskytnout Objednateli za tímto účelem veškerou nezbytnou součinnost; tato Data musí být po dobu poskytování Plnění dle Smlouvy uložena u Dodavatele a mohou být Dodavatelem užívána v souladu se Smlouvou a příslušnými právními předpisy, avšak pouze v nezbytném rozsahu. Dodavatel se

zavazuje dodržovat přiměřená technická a organizační opatření k ochraně těchto Dat. Veškerá Data jsou vlastnictvím Objednatele, není-li ve Smlouvě výslovně stanoveno jinak. Toto ustanovení se uplatní obdobně i na jiná data poskytnutá Objednatelem Dodavateli;

4.3.7. plnit Interní předpisy Objednatele a jeho pokyny v oblasti likvidace Dat (ať už Dat na papírových médiích, Dat zpracovávaných elektronicky nebo prostřednictvím jakýchkoli dalších nosičů Dat) a případně dále na výzvu Objednatele bez zbytečného odkladu zlikvidovat Data v souladu s těmito pravidly a pokyny. Dodavatel musí především postupovat tak, aby nebylo možné odstraněná data zneužít. Za odpovídající způsob likvidace dat je považováno odstranění, přepsání či fyzická likvidace nosiče informace v souladu se standardem US DoD 5220.22-M;

4.3.8. poskytnout při ukončení smluvního vztahu přiměřenou součinnost při Převzetí poskytování Plnění novým Dodavatelem nebo Objednatelem, a to s odbornou péčí, zodpovědně a do doby úplného Převzetí poskytování Plnění. Součinnost zahrnuje zejména, pokud je součástí Plnění:

a. předání Dokumentace, konfiguračních informací, přístupových údajů a kryptografických klíčů;

b. migraci dat v bezpečném, odsouhlaseném formátu;

c. zajištění provozu služeb po přechodné období podle harmonogramu;

d. technická a bezpečnostní opatření k zajištění kontinuity a ochrany informací;

e. likvidaci dat a nosičů dle požadavků Objednatele po ukončení smlouvy

4.4. Dodavatel se během poskytování Plnění pro Objednatele zavazuje informovat Objednatele o žádosti cizozemského orgánu o zpřístupnění nebo předání dat zpracovávaných na území cizího státu, vyjma situace, kdy by takové informování bylo v rozporu s právním řádem, v jehož působnosti dochází ke zpracování dat nebo podle kterého byla žádost podána. V případě zpřístupnění nebo předání dat na základě žádosti cizozemského orgánu o zpřístupnění nebo předání dat zpracovávaných na území cizího státu se Dodavatel zavazuje tato data zpřístupnit nebo předat:

a. až po provedení přezkoumání zákonnosti žádosti,

b. až po vynaložení úsilí o zabránění zpřístupnění nebo předání dat v rámci možností daných právním řádem, v jehož působnosti dochází ke zpracování dat nebo podle kterého byla žádost podána,

c. pouze v nezbytném rozsahu.

5. POVINNOSTI OBJEDNATELE

5.1. Objednatel je povinen zajistit Testovací a Produkční prostředí pro činnost Dodavatele v rámci IT prostředí Objednatele, pokud je to nezbytné pro provádění Plnění. Zajištění prostředí zahrnuje zajištění vzdáleného přístupu personálu Dodavatele do IT prostředí Objednatele, v přiměřeném rozsahu odpovídajícího možnostem Objednatele a Zadávací dokumentaci a při respektování bezpečnostních pravidel Objednatele, zejména bezpečnostní dokumentace, která je součástí Interních předpisů. Objednatel je povinen zajistit fungování Dodavatelem vytvořeného Testovacího prostředí, na kterém bude Software Testován, a Produkčního prostředí, na kterém Software poběží v ostrém provozu, přičemž všechna prostředí budou umístěna na IT prostředí Objednatele, není-li ve Smlouvě stanoveno jinak.

6. LICENČNÍ UJEDNÁNÍ

6.1. Smlouva stanoví, která licenční ujednání dle tohoto článku se použijí ve vztahu k Plnění. Neobsahuje-li Smlouva takový odkaz, použije se ve vztahu k Plnění vedle společných ustanovení k licenčním ujednáním dle odst. 6.7 tohoto článku též odst. 6.3 tohoto článku a ve vztahu k částem Plnění, která obsahují Standardní Software, též odst. 6.5 tohoto článku. Je-li součástí Plnění Hardware, použijí se též pravidla dle odst. 6.6 tohoto článku.

6.2. Odměna za oprávnění dle tohoto článku je zahrnuta v ceně Plnění.

6.3. **Postoupení výkonu autorských majetkových práv k Software**

6.3.1. V případě, že je Software Autorské dílo vznikající v průběhu Plnění, Dodavatel neodvolatelně postupuje na Objednatele oprávnění k výkonu majetkových práv autorských k takovému Autorskému dílu).

6.3.2. Dodavatel prohlašuje, že Software byl vytvořen zaměstnanci či Poddodavateli jako zaměstnanecké dílo ve smyslu § 58 odst. 1 a 7 Autorského zákona, a že je oprávněn k postoupení výkonu majetkových práv v souladu s tímto odst. 6.3 ZOP a má k takovému postoupení náležité souhlasy, přičemž Dodavatel se zavazuje na požádání Objednatele neprodleně předložit nebo jinak vhodným způsobem zpřístupnit dokumenty prokazující rozsah oprávnění Dodavatele.

6.3.3. Objednatel je dále oprávněn postoupit oprávnění k výkonu majetkových práv na jakoukoli další třetí osobu dle volby Objednatele a udělovat licence a podlicence, s čímž Dodavatel výslovně souhlasí; pro zamezení pochybnostem je Dodavatel povinen podniknout veškeré kroky k získání náležitých oprávnění tak, aby mohl oprávnění k výkonu majetkového práva postoupit na Objednatele v souladu s tímto odst. 6.3 ZOP. S povinností převodu oprávnění k výkonu majetkových práv se pojí povinnost předání Zdrojového kódu dle čl. 7 ZOP.

6.3.4. Dodavatel dále prohlašuje, že má svolení autora/ů k zásahům do Software (včetně jeho Zdrojového a strojového kódu) ve smyslu § 58 odst. 4 Autorského zákona a tato svolení se vztahují na jakékoliv třetí osoby, jež budou vykonávat autorská majetková práva k tomuto Software.

6.3.5. Dodavatel dále prohlašuje, že vyloučil oprávnění autorů dle ustanovení § 58 odst. 3 Autorského zákona i vůči všem budoucím vykonavatelům autorských majetkových práv k Software.

6.3.6. Dodavatel dále převádí veškerá zvláštní práva pořizovatele k Databázím, jež tvoří součást Plnění. Nedojde-li z jakéhokoliv důvodu k převodu práva dle předchozí věty, uděluje Dodavatel Objednateli oprávnění k vytěžování a zužitkování celého obsahu takové Databáze nebo její kvalitativně nebo kvantitativně podstatné části a právo udělit jinému oprávnění k výkonu tohoto práva.

6.3.7. K ostatním majetkovým hodnotám, které spadají pod pojem Software a zároveň nespadají pod definici Autorského díla, uděluje Dodavatel Objednateli oprávnění v rozsahu dle odst. 6.3.8. ZOP. Ustanovení odst. 6.5 a 6.6 ZOP tímto nejsou dotčena.

6.3.8. Nevznikne-li Objednateli z jakéhokoliv důvodu ke kterékoliv části Softwaru oprávnění k výkonu autorských majetkových práv, uděluje Dodavatel Objednateli k dotčené části množstevně a územně neomezenou výhradní licenci ke všem známým způsobům užití, a to na dobu trvání autorských majetkových práv. Objednatel je oprávněn k dotčené části Softwaru udělovat licence, tyto dále postoupit a udělovat podlicence třetím osobám. Objednatel je dále oprávněn dotčené části upravovat a měnit (včetně Zdrojového a strojového kódu takové části Software), dokončovat, včetně práva takto upravené či dokončené části užívat, a dále tyto původní, upravené či dokončené části zveřejňovat, spojovat s jiným dílem či zařazovat do díla souborného, zpracovávat, překládat či jinak zasahovat, a to vše i prostřednictvím třetí osoby.

6.4. **Nevýhradní licence k Software**

6.4.1. Ve vztahu k Software Dodavatel tímto uděluje Objednateli okamžikem akceptace Plnění ve smyslu čl. 8 ZOP, nebo jinak vymezeným okamžikem akceptace Plnění Smlouvou a jejími přílohami nevýhradní oprávnění k výkonu práva užít Software v souladu s dalšími podmínkami odst. 6.4 ZOP (dále „***Licence***“). Ustanovení tohoto odstavce se nevztahují na oprávnění Objednatele k Software, který je Standardním Software; tato oprávnění jsou upravena samostatně v odst. 6.5 ZOP. V případě, že je Plnění rozděleno na části, použije se tento odstavec na každou část Plnění.

6.4.2. Licence se uděluje jako nevýhradní a opravňuje Objednatele k výkonu práva užít veškerá Autorská díla a k výkonu práva vytěžovat a zužitkovat Databáze, jež tvoří Plnění, a to:

a. k jakémukoliv účelu;

b. na dobu trvání majetkových práv autorských;

c. na jakémkoliv území;

d. jakýmkoliv způsobem; a

e. bez množstevního omezení.

6.4.3. Dodavatel okamžikem dle odst. 6.3. ZOP uděluje rovněž oprávnění takový Software upravovat a měnit (včetně Zdrojového a strojového kódu), dokončovat, včetně práva takto upravený, změněný či dokončený Software užívat v rozsahu Licence, a dále tyto původní, upravené, změněné či dokončené části spojovat s jiným dílem či zařazovat do díla souborného, zpracovávat, překládat či jinak do nich zasahovat, a to vše i prostřednictvím třetí osoby

6.4.4. Objednatel má v rámci Licence právo udělit k Softwaru podlicenci třetím osobám a právo postoupit Licenci zcela či z části na třetí osoby, s čímž Dodavatel výslovně souhlasí.

6.4.5. Licence zahrnuje povinnost Dodavatele předat Objednateli Zdrojový kód a Dokumentaci k Software dle článku 7 ZOP.

6.4.6. Licence se vztahuje ve stejné míře a rozsahu jako k Software taktéž na:

a. Dokumentaci specifikovanou ve Smlouvě nebo jejích přílohách;

b. jakoukoliv jinou Dokumentaci předávanou k Software nad rámec Dokumentace dle předchozího písmene;

c. loga či jiné předměty duševního vlastnictví, které souvisí s Plněním a jsou vhodné či nezbytné k užití spolu s Plněním;

d. jakákoliv jiná Autorská díla či jiné předměty duševního vlastnictví, které souvisí s Plněním.

6.5. **Licence ve vztahu ke Standardnímu Software**

6.5.1. V případech, kdy je součástí Plnění Standardní Software, Dodavatel uděluje Objednateli okamžikem akceptace Plnění ve smyslu čl. 8 ZOP, jehož součástí je Standardní Software, k veškerému takovému Standardnímu Software nevýhradní oprávnění k výkonu práva užít příslušný Standardní Software v souladu s dalšími podmínkami odst. 6.5 ZOP (dále „***Licence k Standardnímu Software***"). V případě, že je Plnění rozděleno na části, použije se tento odstavec na každou část Plnění, jehož součástí je Standardní Software či jeho část.

6.5.2. Licence k Standardnímu Software se uděluje jako nevýhradní a opravňuje Objednatele k výkonu práva užít veškerý Standardní Software, a to:

a. všemi způsoby odpovídajícími účelu, pro který je takový Standardní Software určen;

b. na dobu trvání majetkových práv autorských, nebo alespoň na dobu trvání Smlouvy;

c. na jakémkoliv území; a

d. bez množstevního omezení.

6.5.3. Dodavatel je v rámci Licence k Standardnímu Software povinen zajistit poskytnutí podpory (subscription/license maintenance) k veškerému Standardnímu Software, tj. zajistit poskytování nejnovějších verzí Standardního Software Objednateli a dalších služeb v souladu se standardními licenčními podmínkami Standardního Software, a to alespoň na dobu trvání Smlouvy.

6.5.4. Objednatel má v rámci Licence k Standardnímu Software oprávnění udělit ke Standardnímu Software podlicenci třetím osobám a právo postoupit Licenci k

Standardnímu Software zcela či z části na třetí osoby, s čímž Dodavatel výslovně souhlasí.

6.5.5. Licence k Standardnímu Software se vztahuje ve stejné míře jako k Standardnímu Software taktéž na:

a. Aktualizaci, Modernizaci a Zásadní modernizaci Standardního Software, který je součástí Plnění;

b. Dokumentaci k Standardnímu Software specifikovanou ve Smlouvě nebo jejích přílohách;

c. Dokumentaci nad rámec Dokumentace k Standardnímu Software dle předchozího písm.;

d. právo zužitkovat a vytěžovat Databáze obsažené ve Standardním Software, který je součástí Plnění;

e. loga či jiné předměty duševního vlastnictví, které se Standardním Software, jež je součástí Plnění, souvisí a jsou vhodné či nezbytné k užití spolu s takovým Standardním Software.

6.5.6. V parametrech, které nejsou upraveny Smlouvou, jejími přílohami anebo jinou částí Zadávací dokumentace, se Licence k Standardnímu Software řídí příslušnými licenčními podmínkami výrobce Standardního Software.

6.5.7. V případě, že Dodavatel využije při plnění předmětu Smlouvy Standardní Software, je Dodavatel za účelem vyloučení vzniku proprietárního uzamčení Objednatele (tzv. vendor lock-in) povinen použít výlučně takový Standardní Software, u kterého jsou splněny podmínky dle definice Standardního Software dle odst. 1.65. písm. a., b., c. nebo d. ZOP, v době využití Standardního Software, a u kterého lze zároveň důvodně předpokládat, že tento stav zůstane zachován minimálně po dobu trvání Smlouvy.

6.5.8. V případě, že Dodavatel v rámci plnění Smlouvy použije Standardní Software, který v průběhu trvání Smlouvy nebude anebo přestane splňovat podmínky stanovené v odst. 6.5.7 ZOP, je Dodavatel povinen, po dohodě s Objednatelem, a v případě, že tato dohoda nebude možná, pak dle volby Dodavatele:

a. na vlastní náklady dodat Objednateli Zdrojový kód předmětného Standardního Software a poskytnout Objednateli oprávnění užívat tento Standardní Software včetně Zdrojového kódu (včetně dalších způsobů nakládání) v rozsahu Licence dle odst. 6.4 ZOP; nebo

b. nahradit na vlastní náklady předmětný Standardní Software jiným Standardním Software, který bude mít alespoň srovnatelné funkcionality, kvalitu a technickou způsobilost jako nahrazovaný Standardní Software a zároveň splňovat podmínky stanovené v odst. 6.5.7 ZOP, a poskytnout k tomuto Standardnímu Software Objednateli Licenci k Standardnímu Software dle odst. 6.5 ZOP; nebo

c. nahradit na vlastní náklady předmětný Standardní Software vlastním Softwarem, tj. přeprogramovat část Díla představovanou předmětným Standardním Softwarem za využití vlastního Software vytvořeného na míru Objednateli, který bude mít alespoň srovnatelné funkcionality, kvalitu a technickou způsobilost jako nahrazovaný Standardní Software, a poskytnout k tomuto vlastnímu Softwaru Objednateli Licenci dle odst. 6.4 ZOP, a to včetně Zdrojového kódu.

6.5.9. Postupy dle odst. 6.5.8 písm. a) až c) ZOP podléhají samostatnému Akceptačnímu řízení. Vznikla-li Dodavateli povinnost dle odst. 6.5.8 ZOP, je Dodavatel povinen splnit povinnosti dle uvedeného odstavce i po ukončení Smlouvy. Ustanovení Smlouvy a ZOP relevantní pro splnění povinností dle předchozí věty se použijí i po ukončení Smlouvy.

6.5.10. Pokud v rámci Akceptačního řízení dle čl. 8 ZOP vyjde najevo, že Standardní Software nesplňuje podmínky odst. 6.5.7 ZOP, je Objednatel oprávněn Akceptační řízení přerušit, dokud Dodavatel nenapraví tento nedostatek předmětného Standardního Software jedním ze způsobů uvedených v odst. 6.5.8 ZOP. Objednatel není v takovém případě v prodlení.

6.5.11. Ustanovení odst. 6.3 a 6.6 ZOP se pro Standardní Software nepoužijí.

6.6. **Software vztahující se k Hardware**

6.6.1. V případech, kdy je k řádnému užívání dodaného Hardwaru potřebný určitý Software, je Dodavatel povinen poskytnout/zajistit Objednateli jako součást Plnění a za cenu zahrnutou v ceně Hardwaru, oprávnění užít tento Software v rozsahu, způsoby a za účelem obvyklým ve vztahu k Hardwaru, se kterým je spojen, nejméně však za podmínek dle Smlouvy a jejích příloh.

6.6.2. Ustanovení odst. 6.3 a 6.4 ZOP se pro Software vztahující se k Hardwaru nepoužijí.

6.7. **Společná ustanovení**

6.7.1. Nestanoví-li Smlouva a její přílohy či jiné části Zadávací dokumentace jinak, je Dodavatel při plnění Smlouvy oprávněn využít programy s otevřeným kódem či jejich části distribuovanými pod FOSS licencemi. Dodavatel však není oprávněn využít programy s otevřeným kódem či jejich části, které jsou distribuovány pod FOSS licencemi, jejichž podmínky by Objednateli ukládaly povinnost sdělovat nebo jinak šířit Software či jeho části, včetně Zdrojových kódů, třetím osobám, nebo umožnit jim změny, úpravy či jiné zásahy do Softwaru nebo jeho části.

6.7.2. Dodavatel je povinen zajistit Objednateli udělení oprávnění k veškerým programům s otevřeným kódem poskytnutým Objednateli v rozsahu takových FOSS licencí, které se na konkrétní program s otevřeným kódem, který je součástí Plnění, vztahují, přičemž konkrétní rozsah licence lze určit odkazem na soubor předávaný v rámci výstupu z Plnění anebo odkazem ve Zdrojovém kódu či jiným označením takové licence ve formátu vyžadovaném takovou veřejnou licencí, včetně odkazu na kompletní znění aktuálních licenčních podmínek příslušné FOSS licence; Dodavatel je dále povinen zajistit poskytnutí podpory k veškerým programům s otevřeným kódem, které jsou součástí Plnění, tj. povinnost Dodavatele zajistit poskytování nejnovějších verzí programů s otevřeným kódem a dalších služeb v souladu se standardními licenčními podmínkami programů s otevřeným kódem, a to alespoň na dobu trvání této Smlouvy. Ustanovení čl. 7 ZOP se pro programy s otevřeným kódem či jejich části, které jsou distribuovány pod FOSS licencemi, použije obdobně.

6.7.3. Dodavatel prohlašuje, že je oprávněn udělit Objednateli veškerá oprávnění v souladu s tímto článkem ZOP, má k takovému udělení veškeré potřebné souhlasy a jejich udělením Objednateli ani užíváním Plnění Objednatelem či uživateli Objednatele nebudou porušena práva duševního vlastnictví třetí osoby. Dodavatel odpovídá Objednateli za zajištění všech nezbytných oprávnění a souhlasů autora či autorů Software či Standardního Software k oprávněním udělovaným Objednateli dle tohoto článku ZOP. Dodavatel se zavazuje na výzvu Objednatele poskytnout Objednateli o zajištění oprávnění a veškerých souhlasů dle tohoto článku ZOP písemné prohlášení a tyto skutečnosti prokázat.

6.7.4. V případě, že by třetí osoba vznesla vůči Objednateli jakékoliv nároky z porušení práv duševního vlastnictví v souvislosti s užíváním Plnění Objednatelem, se Dodavatel zavazuje přijmout taková opatření, aby Objednatel byl Plnění oprávněn nerušeně užívat, a to zejména zajistit pro Objednatele udělení oprávnění v rozsahu dle tohoto článku ZOP bez dalších nákladů a požadavků na úplatu od Objednatele.

6.7.5. V případě, že jakákoliv třetí osoba uplatní nárok z důvodu porušení práv duševního vlastnictví ve vztahu k Plnění, je Dodavatel povinen nahradit Objednateli veškerou újmu takto způsobenou, jakož i účelné náklady vynaložené na obranu práv Objednatele. Dodavatel se v takovém případě dále zavazuje na svůj náklad poskytnout Objednateli veškerou možnou součinnost k ochraně jeho práv a oprávnění dle tohoto článku ZOP, zejména mu poskytnout všechny podklady, informace a vysvětlení k prokázání neoprávněnosti nároku třetí strany.

6.7.6. V případě nároku dle předchozího odst. 6.7.5 ZOP, nebo je-li důvodné předpokládat, že takový nárok bude uplatněn, zajistí Dodavatel Objednateli možnost dále příslušný výstup užívat bez nároku na úplatu nad rámec sjednaný ve Smlouvě.

6.7.7. Spolu se Standardním Software, je-li součástí Plnění, musí být Objednateli vždy předána kompletní Dokumentace, tj. zejména uživatelská, administrátorská, provozní dokumentace a dokumentace jeho API.

7. ZDROJOVÝ KÓD A DOKUMENTACE

7.1. Zdrojový kód bude předáván Objednateli na datovém nosiči společně s předáním výstupu z Plnění pro účely zahájení Akceptačního řízení, nebo za podmínek stanovených ve Smlouvě, zejména pokud bude smluvní vztah ukončen bez provedení Akceptačního řízení.

7.2. Na datovém nosiči dat musí být viditelně označen „Zdrojový kód" s označením části Modifikace a jeho verze a den předání Zdrojového kódu. O předání nosiče dat bude oběma Smluvními stranami sepsán a podepsán písemný předávací protokol.

7.3. Povinnost Dodavatele předávat Zdrojový kód se přiměřeně použije i pro jakékoliv opravy, změny, doplnění, upgrade nebo update Zdrojového kódu v rámci následného provádění Plnění anebo v rámci záručních oprav. Zdrojový kód musí obsahovat podrobný popis a komentář každého zásahu do Zdrojového kódu.

7.4. Objednatel nebude v průběhu provádění Plnění sám anebo prostřednictvím jiných osob zasahovat do Zdrojového kódu nasazeného anebo fungujícího v Produkčním prostředí či Testovacím prostředí.

7.5. Dodavatel je povinen předat Objednateli příslušnou Dokumentaci a Zdrojový kód ve standardní podobě (to nejméně v kvalitě obvyklé pro open source projekty), vždy obsahující následující:

a. Kompletní Zdrojové kódy celého díla.

b. Uživatelskou příručku obsahující konkrétní popis uživatelského prostředí, funkcí a postupů pro zaškolení zaměstnanců.

c. Administrátorskou příručku, popisující všechny parametry, které lze konfigurovat a popis dopadů změny konfigurace do systému.

d. Technickou dokumentaci systému, pakliže se jedná o vícevrstvou architekturu, popis každé vrstvy zvlášť:

i. Datová vrstva – popis datové vrstvy, čili tabulek v databázi včetně vazeb mezi tabulkami a včetně E-R schémat.

ii. Aplikační vrstva – popis jádra systému, jeho funkcí, služeb a rozhraní. Dokumentace musí obsahovat kompletní popis architektury jádra systému, výčet a podrobný popis všech jeho funkcí, přehled a popis služeb, které jádro poskytuje dalším komponentám systému, modulům a knihovnám.

iii. Prezentační vrstva – Dokumentace systému musí obsahovat drátové modely všech obrazovek uživatelského rozhraní včetně popisu funkcí prvků každé obrazovky.

e. Popis konfigurace provozního prostředí systému (serverová strana i klientská strana).

f. Dokumentace musí obsahovat soupis všech požadavků na nastavení hardwarových a softwarových komponent běhového prostředí jako jsou:

i. mapování souborových systémů;

ii. požadavky na operační paměť a procesory;

iii. konfigurační parametry jednotlivých podpůrných Softwarových prostředků (např. specifika pro nastavení databáze, aplikačního serveru, webového serveru apod.).

g. Objednatel požaduje, aby tato Dokumentace byla ve formátech XML DocBook (zdrojové) a PDF (export z XML zdroje pro snadnou distribuci uživatelům) nebo případně v jiném formátu, který Objednatel schválí po vzájemné dohodě s Dodavatelem. Všechny Dokumentace musí být verzované, opatřené seznamem

autorů, přehledem změn jednotlivých verzí a musí být obsahově úplné pro tu část systému, kterou popisují.

h. Řešení musí obsahovat návod na používání systému (uživatelský manuál) a popis systému – jeho vlastností, strukturu projektu, použité technologie (technická dokumentace). Součástí řešení je i Dokumentace a automaticky generovaná dokumentace (Javadoc). Součástí Dokumentace musí být zip archiv se zdrojovými soubory řešení a programátorskou dokumentací.

7.6. V případě jakýchkoli pochybností o správnosti předání Zdrojového kódu se bude uvedené posuzovat podle svého účelu, tedy zejména následné možnosti provádět samostatně či prostřednictvím třetích osob opravy, změny, doplnění, upgrady nebo updaty Zdrojového kódu. Za nesprávné předání se přitom považuje takové předání, které v důsledku vede ke znemožnění či podstatnému ztížení práce se Zdrojovým kódem ve výše uvedeném smyslu.

8. AKCEPTAČNÍ ŘÍZENÍ

8.1. Akceptační řízení Předmětu Smlouvy

8.1.1. Předání a převzetí Předmětu Smlouvy (tj. včetně Zdrojových kódů a Dokumentace) probíhá na základě Akceptačního řízení, tj. postupným provedením akceptačních procesů a podepsáním Akceptačního protokolu. Je-li Předmět Smlouvy rozdělen na části, použije se tento článek obdobně pro každou část, nestanoví-li Smlouva jinak. Jsou-li součástí Předmětu Smlouvy Služby nebo Paušální služby, použijí se, nestanoví-li Smlouva jinak, pro Služby ustanovení odst. 8.2 ZOP a pro Paušální služby ustanovení odst. 8.3 ZOP.

8.1.2. Akceptační řízení zahrnuje porovnání skutečných vlastností a funkcionalit s Akceptačními kritérii.

8.1.3. Nestanoví-li Smlouva či její přílohy Akceptační kritéria, rozumí se jimi:

a. vlastnosti a funkcionality uvedené ve specifikaci plnění určené Objednatelem, která je součástí Smlouvy, a dále vlastnosti a funkcionality uvedené ve specifikaci plnění Dodavatele či návrhu řešení (jsou-li takové), která je součástí Smlouvy, a

b. požadavky na Zdrojové kódy a Dokumentaci dle čl. 7 ZOP.

8.1.4. Dodavatel je povinen písemně informovat Objednatele minimálně se sedmi denním předstihem o termínu předání Předmětu Smlouvy či její části, nedohodnou-li se strany jinak.

8.1.5. Dodavatel předá Objednateli Předmět Smlouvy k realizaci Akceptačního řízení. Akceptační řízení může být zahájeno pouze v případě, že Předmět Smlouvy byl Dodavatelem skutečně předán Objednateli, a ten se s ním mohl seznámit. Objednatel na žádost Dodavatele bez zbytečného odkladu potvrdí převzetí Předmětu Smlouvy k Akceptačnímu řízení v Servicedesku, e-mailem, anebo jiným dohodnutým způsobem. Potvrzením převzetí Díla k Akceptačnímu řízení ve smyslu tohoto odstavce je zahájeno Akceptační řízení.

8.1.6. Předmět Smlouvy je způsobilý k akceptaci Objednatelem, pokud:

a. splňuje Akceptační kritéria a současně nevykazuje žádnou Vadu kategorie A, B a C či jiné zjevné vady (zejména vady, pro které není vhodné dělení Vad dle ZOP -> např. Některé vady Hardware jsou-li součástí plnění), pak Objednatel vyznačí na Akceptačním protokolu „**Akceptováno**"; nebo

b. splňuje Akceptační kritéria a současně nevykazuje žádnou Vadu kategorie A, B a současně nemá více než:

i. 30 Vad kategorie C nebo drobných vad, jež nebrání řádnému užívání Předmětu Smlouvy, je-li předmětem akceptace vytvoření Software či Dokumentace či vytvoření části Software či Dokumentace

ii. 10 Vad kategorie C nebo drobných vad, jež nebrání řádnému užívání Předmětu Smlouvy, nejde-li o případ uvedený v odst. 8.1.6 písm. b. i.

pak Objednatel vyznačí na Akceptačním protokolu „**Akceptováno s výhradou**".

8.1.7. V jiných případech než dle odst. 8.1.6 ZOP vyznačí Objednatel na Akceptačním protokolu „**Neakceptováno**".

8.1.8. Nedohodnou-li se Smluvní strany jinak, připraví Dodavatel návrh Akceptačního protokolu, který musí obsahovat minimálně:

a. označení Smluvních stran a odkaz na Smlouvu,

b. seznam Akceptačních kritérií společně s vedlejším sloupcem pro možnost vyznačení, zda Předmět Smlouvy splňuje příslušné Akceptační kritérium (např. ano/ne)

c. tabulku pro možnost vepsání zjištěných Vad včetně možnosti uvedení, o jakou Vadu se jedná (A/B/C),

d. tabulku pro možnost vepsání dalších zjištěných vad,

e. prostor pro závěrečné hodnocení (např. formou výběru z kolonek „**Akceptováno**", „**Akceptováno s výhradou**", „**Neakceptováno**") a

f. podpisové doložky pro oprávněné osoby za Smluvní strany.

8.1.9. Objednatel je povinen do 30 kalendářních dnů (v případě, že lhůta pro plnění akceptované části byla kratší než 60 kalendářních dnů, pak do 14 kalednářních dnů, nikdy však déle než činí polovina lhůty pro plnění) ode dne zahájení Akceptačního řízení posoudit Předmět Smlouvy postupem dle odst. 8.1.2 ZOP a v případě dle odst. 8.1.6 ZOP podepsat Akceptační protokol a vyznačit na něm „**Akceptováno**", nebo „**Akceptováno s výhradou**" včetně vyznačení Vad/y či vad/y. V opačném případě je Objednatel povinen ve výše uvedené lhůtě podepsat Akceptační protokol společně s vyznačením „**Neakceptováno**" včetně vyznačení nesplněných Akceptačních kritérií nebo vyznačení Vad/y a jejich/její kategorizace (A, B nebo C) nebo vyznačení dalších vad.

8.1.10. Okamžikem podpisu Akceptační protokolu společně s vyznačením „**Akceptováno**", nebo „**Akceptováno s výhradou**" je Předmět Smlouvy proveden.

8.1.11. Podpis Akceptačního protokolu s vyznačením „**Akceptováno s výhradou**" nezbavuje odpovědnosti Dodavatele odstranit vyznačené Vady či vady. Dodavatel je povinen takové Vady či vady odstranit ve lhůtě určené Objednatelem, jinak do třiceti (30) kalendářních dnů od podpisu Akceptačního protokolu s vyznačením „**Akceptováno s výhradou**". Neodstranění Dodavatel Vady či vady ve lhůtě dle tohoto odstavce, jedná se porušení této Smlouvy podstatným způsobem. Do doby odstranění vyznačených Vad či vad dle tohoto odstavce nezaplatí Objednatel Dodavateli část Ceny (či ceny příslušné části Plnění, je-li plněno po částech) odpovídající její padesáti (50) procentní výši. Objednatel není v takovém případě v prodlení se zaplacením části Ceny (či ceny příslušné části Plnění, je-li plněno po částech) dle předchozí věty. Pro účely ověření splnění povinností Dodavatele dle tohoto odstavce, je Dodavatel Objednateli povinen prokázat, že Plnění již nemá Vady či vady. Povinnost odstranit Vady či vady dle tohoto odstavce není splněna, neodstranil-li Dodavatel Vady či vady nebo objeví-li se v průběhu ověření:

a. nové Vady či vady, které vznikly v souvislosti s odstraňováním původních Vad či vad, nebo

b. Vady či vady, které v důsledku existence původních Vad či vad nebylo možné v Akceptačním řízení odhalit, nebo které bylo možno odhalit pouze s výraznými obtížemi.

8.1.12. V případě neakceptování Předmětu Smlouvy vyznačením na Akceptačním protokolu „**Neakceptováno**" se Dodavatel zavazuje odstranit nesplněná Akceptační kritéria a Vady uvedené v Akceptačním protokolu ve lhůtách výslovně stanovených v Akceptačním protokolu Objednatelem, a pokud nejsou takové, pak lhůtách přiměřených. Do odstranění nedostatků bránících akceptování není Předmět Smlouvy

proveden. Po odstranění nedostatků uvedených v Akceptačním protokolu Dodavatel opětovně předá Předmět Smlouvy Objednateli k dalšímu kolu Akceptačního řízení a Objednatel postupuje obdobně podle odst. 8.1.5 ZOP.

8.2. **Akceptační řízení ve vztahu ke Službám**

8.2.1. Řádné provedení Služeb bude Stranami písemně potvrzeno podpisem Akceptačního protokolu po ukončení Akceptačního řízení obdobně dle odst. 8.1 ZOP (s výjimkou odst. 8.1.3 ZOP). Pro účely akceptace Služeb se Předmětem Smlouvy rozumí příslušný výstup ze Služeb (např. rozvoj Software). Strany jsou oprávněny zkrátit lhůty Akceptačního řízení ve smyslu odst. 8.1 ZOP v dílčí smlouvě uzavřené na základě Smlouvy. Nestanoví-li dílčí smlouva Akceptační kritéria Služby, rozumí se jimi:

a. vlastnosti a funkcionality uvedené ve specifikaci plnění Objednatele, která je součástí dílčí smlouvy uzavřené na základě Smlouvy, a dále vlastnosti a funkcionality uvedené ve specifikaci plnění Dodavatele (je-li taková), která je součástí dílčí smlouvy, a

b. požadavky na Zdrojové kódy a Dokumentaci dle čl. 7 ZOP.

8.2.2. Jsou-li Služby plněny po částech, použijí se ustanovení pro Akceptační řízení ve vztahu ke Službám přiměřeně vždy na každou takovou dílčí část výstupu ze Služeb, nedohodnou-li se Strany výslovně jinak.

8.2.3. Akceptační řízení se neprovádí u Služeb, které z povahy věci nepodléhají Akceptačnímu řízení (např. konzultace apod.). Služby musí být v souladu s dílčí smlouvou a přílohou č. 1 této Smlouvy. Uvedeným postupem nejsou dotčena práva z vadného plnění ve vztahu k takovým Službám.

8.3. **Akceptační řízení ve vztahu k Paušálním službám**

8.3.1. Řádné provádění Paušálních služeb bude každý měsíc potvrzováno podpisem výkazu Paušálních služeb za bezprostředně předcházející měsíc. Podpisem výkazu Paušálních služeb Objednatelem jsou Paušální služby za příslušný měsíc akceptovány/provedeny. Objednatel není povinen podepsat výkaz Paušálních služeb, nebyly-li jednotlivé Paušální služby v příslušném měsíci řádně provedeny (jedná se např. o Paušální služby, u nichž konec lhůty pro splnění - např. doba pro vyřešení Incidentu – spadá do příslušného měsíce).

8.3.2. Návrh výkazu dle předchozího odstavce připraví Dodavatel. Výkaz musí obsahovat soupis provedených Paušálních služeb za bezprostředně předcházející měsíc a soupis dosud neukončených činností Paušálních služeb. Výkaz Paušálních služeb je Dodavatel povinen doručit nejpozději do deseti (10) kalendářních dnů po skončení měsíce, ve které byly služby poskytnuty.

8.4. **Akceptační řízení ve vztahu ke školení**

8.4.1. Dokladem o řádném provedení školení je prezenční listina podepsána účastníky školení, případně vydání certifikátu, mělo-li být školení zakončené vydáním certifikátu.

8.4.2. Vznikají-li pro školení školící materiály, akceptují se v akceptačním řízení odst. 8.1 ZOP se použije přiměřeně. V takovém případě je školení řádně provedené dnem, v němž je akceptován poslední požadovaný výstup.

8.4.3. V případě, že předmětem školení je hands-on školení, je školení řádně provedeno akceptací výstupu, který byl předmětem hands-on školení dle odst. 8.1 ZOP.

8.5. **Akceptace ve vztahu k Hardware**

8.5.1. Je-li předmětem Smlouvy či dílčí části, jež je určena k akceptaci pouze dodání Hardware, použije se pro akceptaci odstavec 8.5 ZOP.

8.5.2. Řádné dodání Hardware se předává a přebírá na základě předávacího protokolu podepsaného odpovědnými zástupci smluvních stran.

8.5.3. Nestanoví-li Smlouva či její přílohy jinak, Objednatel ověřuje v rámci akceptace Hardware:

a. parametry, vlastnosti a funkcionality uvedené ve specifikaci plnění Objednatele, která je součástí Smlouvy, a dále vlastnosti a funkcionality uvedené ve specifikaci plnění Dodavatele (je-li taková), která je součástí Smlouvy;

b. příslušenství a dokumentaci, jež mělo být dodáno spolu s Hardware.

9. ŠKOLENÍ

9.1. Vyplývá-li ze Smlouvy Dodavateli povinnost poskytnout školení, aniž jsou blíže určeny jeho podmínky, zavazuje se Dodavatel poskytnout školení osobám určeným Objednatelem pomocí metod výkladu (zejména popis jednotlivých prvků a funkcionalit Předmětu Smlouvy ve vztahu k jeho užívání), praktických ukázek obsluhy Předmětu Smlouvy a zodpovězení dotazů školených osob tak, aby tyto osoby byly na základě provedeného školení ve vztahu ke svým rolím nebo pracovnímu zařazení (dle sdělení Objednatele) schopné plně porozumět svým odpovědnostem při obsluze Předmětu Smlouvy, provádět obsluhu v souvislosti se svou rolí nebo pracovním zařazením samostatně, a přitom minimalizovat riziko chybné obsluhy nebo závad na Předmětu Smlouvy.

9.2. Dodavatel provede zaškolení příslušných osob určených Objednatelem v termínu dle Smlouvy, a pokud takový termín není, pak v termínu určeném Objednatelem po dohodě s Dodavatelem.

9.3. Dodavatel je dále povinen provést v přiměřeném rozsahu školení příslušných zaměstnanců Dodavatele a dalších osob podílejících se na poskytování Plnění dle Smlouvy za účelem splnění povinností dle čl. 21. ZOP. Tuto skutečnost je povinen na vyžádání Objednateli prokázat.

10. SERVICEDESK

10.1. Dodavatel se zavazuje:

10.1.1. nejpozději v den účinnosti Smlouvy založit a po celou dobu trvání Smlouvy udržovat v provozu Servicedesk (včetně úhrady případných licenčních poplatků za aplikaci Servicedesk) a udělit náležitá oprávnění k přístupu do Servicedesku, a to v počtu přístupů pro Ohlašovatele dle určení Objednatele. Servicedesk bude fungovat prostřednictvím webové adresy;

nebo

10.1.2. po celou dobu trvání Smlouvy užívat Servicedesk provozovaný Objednatelem.

10.2. Provozovatele Servicedesku stanoví Smlouva. Pokud Smlouva provozovatele Servicedesku nestanoví, má se za to, že provozovatelem Servicedesku je Dodavatel. V případě, že provozovatelem bude Objednatel, poskytne Dodavateli nezbytnou součinnost k řádnému užívání Servicedesku včetně případného poskytnutí licencí.

10.3. Dodavatel se zavazuje zajistit Servicedesk prostřednictvím přímého přístupu do Servicedesku na webové adrese určené Dodavatelem/Objednatelem dle provozních podmínek aplikace Servicedesk, případně prostřednictvím přímého datového propojení Servicedesků Objednatele a Dodavatele, a to v jednom z následujících režimů, který je vymezen ve Smlouvě:

a. Režim 1:

7x24, tj. dvacet čtyři (24) hodin sedm (7) dní v týdnu.

b. Režim 2:

7x12, tj. dvanáct (12) hodin sedm (7) dní v týdnu.

c. Režim 3:

5x12, tj. dvanáct (12) hodin pět (5) dní v týdnu

d. Režim 4:

5×8, tj. osm (8) hodin pět (5) dní v týdnu.

10.4. Nestanoví-li Smlouva jinak, počíná časový rozsah dle zvoleného režimu dle odst. 10.3 ZOP (s výjimkou režimu 1) shodně s časový rozsahem dle zvoleného Servisního modelu dle odst. 12.2 ZOP (např. pokud doba Servisního modelu začíná každý pracovní den v 7:00, provoz Servicedesku v rámci příslušného režimu začíná rovněž v 7:00).

10.5. Servicedesk zahrnuje mimo jiné příjem a evidenci Incidentů a Požadavků, oznámení o potřebě součinnosti Objednatele a dalších zpráv, potvrzování jejich přijetí, předávání jednotlivých úkolů odpovědným osobám, sledování stavu, průběhu a procesu prací a dalších zpráv, informování o stavu řešení, vytváření přehledů a statistik, a to přes přehledné webové rozhraní. Je-li Servicedesk provozován Dodavatelem musí být zabezpečen tak, aby odpovídal požadavkům vyplývajícím ze ZoKB a Interních předpisů. Výstupem z Servicedesku je záznam o veškerých úkonech Servicedesku ve formě přehledného logu, jež umožňuje vyhledávání a uchovávání záznamů tak, aby byly naplněny požadavky ZoKB a Interních předpisů na takové záznamy.

10.6. Servicedesk bude dostupný pouze pro Objednatele a Ohlašovatele.

10.7. Nestanoví-li Smlouva jinak, je Dodavatel povinen nezávisle na Servicedesku mít nejpozději k okamžiku nabytí účinnosti Smlouvy zřízenou elektronickou adresu a telefonní linku a tuto adresu a telefonní číslo linky sdělit Objednali, a to vše pro účely min. příjmu oznámení Incidentů a Požadavků, vznášení dotazů k Plnění, získávání odpovědí ve vztahu k Plnění a pro další komunikace dle Smlouvy. Doba provozu elektronické adresy a telefonní linky bude odpovídat zvolenému režimu Servicedesku dle odst. 10.3 ZOP.

11. NAHLÁŠENÍ INCIDENTU

11.1. Hlášení o Incidentu Dodavateli bude provedeno Ohlašovatelem bezodkladně po zjištění Incidentu, a to přímým zadáním Incidentu do Servicedesku (vytvoření ticketu v Servicedesku, tj. okamžikem, jímž se ticket zpřístupní Dodavateli), odesláním e-mailu nebo telefonátem na kontaktní číslo dle odst. 10.7 ZOP, přičemž Ohlašovatel je povinen uvést popis Incidentu, a to v následujícím rozsahu:

a. krátký a rámcově výstižný název Incidentu;

b. identifikace části Předmětu Plnění, které se Incident týká;

c. určení prostředí (Testovací prostředí, Produkční prostředí);

d. detailní popis Incidentu, průvodních jevů a všech významných souvisejících informací;

e. kategorii Incidentu (A, B, C);

f. identifikaci Ohlašovatele.

11.2. V případě, že některá z náležitosti dle odst. 11.1. ZOP chybí nebo je nedostatečná, může si Dodavatel vyžádat její doplnění od Ohlašovatele; tato skutečnost však nemá vliv na určení Času nahlášení Incidentu, ledaže bez tohoto doplnění hlášení Incidentu postrádá informaci natolik podstatnou, že bez ní objektivně nelze přistoupit k řešení Incidentu a Dodavatel o této skutečnosti Objednatele vyrozuměl, a to nejpozději v době určené na zpracování Incidentu dle určeného Servisního modelu dle čl. 12 ZOP, v takovém případě je Incident dle 11.3 ZOP nahlášen okamžikem doplnění požadované informace.

11.3. Je-li Incident nahlašován prostřednictvím Servicedesku, pak se za Čas nahlášení Incidentu považuje čas vytvoření ticketu v Servicedesku. Je-li Incident nahlašován písemně na e-mailovou adresu, pak se za Čas nahlášení Incidentu považuje čas odeslání e-mailu z e-mailového serveru Ohlašovatele, nebo v případě hlášení Incidentu telefonicky čas ukončení telefonického hovoru. Dodavatel je povinen prokazatelným způsobem bezodkladně potvrdit přijetí nahlášení Incidentu, a to vždy prostřednictvím Servicedesku. Nepotvrdí-li Dodavatel přijetí Incidentu, nemá to vliv na Čas nahlášení Incidentu.

11.4. Je-li je Incident nahlášen mimo časový rozsah Servisního modelu, avšak v rámci časového rozsahu Servicedesku dle zvoleného režimu dle odst. 10.3 ZOP, považuje se za Čas nahlášení Incidentu okamžik začátku nejbližšího následujícího časového rozsahu Servisního modelu.

11.5. Dodavatel se zavazuje po dobu poskytování Plnění evidovat všechny nahlášené Incidenty a způsob jejich řešení, včetně časových údajů o průběhu řešení jednotlivých Incidentů ve Výkazech.

11.6. Není-li v Servisní smlouvě, jejích přílohách jinak, ustanovení článku 11. ZOP se použijí přiměřeně i na nahlášení a evidování Požadavků.

11.7. Ustanovení článku 21 o Kybernetických bezpečnostních incidentech a Kybernetických bezpečnostních událostech se považují za speciální vůči tomuto článku 11 ZOP.

12. SERVISNÍ MODELY

12.1. Servisní model představuje standardizovaný model provozu a podpory aplikace, systému nebo instance služby.

12.2. Pokud je součástí Smlouvy zajištění provozu a podpory Softwaru nebo Hardwaru, je ve Smlouvě vymezen jeden z níže uvedených Servisních modelů:

Servisní model	Dostupnost	Doba provozu		Doba zpracování Incidentu	Doba vyřešení Incidentů kategorie A	Doba vyřešení Incidentů kategorie B	RTO	RPO	Doba zpracování Požadavku	Doba vyřešení Požadavku kategorie A	Doba vyřešení Požadavku kategorie B
A1 Kritický	99.5%	7x24	(0-24)	1 hod	2 hod	2 hod	4 hod	< 5 min	1 PD	1 PD	3 PD
A2 Kritický	99.5%	7x12	(6-18)	1 hod	2 hod	2 hod	4 hod	< 5 min	1 PD	1 PD	3 PD
A3 Kritický	99.5%	5x8	(7-15)	1 hod	2 hod	2 hod	4 hod	< 5 min	1 PD	1 PD	3 PD
A4 Kritický	99.5%	7x24	(0-24)	1 hod	4 hod	12 hod	4 hod	< 5 min	1 PD	2 PD	5 PD
A5 Kritický	99.5%	5x8	(7-15)	1 hod	4 hod	12 hod	4 hod	< 5 min	1 PD	2 PD	5 PD
B1 Závažný	98.0%	7x24	(0-24)	1 PD	2 PD	3 PD	48 hod	30 min	2 PD	3 PD	5 PD
B2 Závažný	98.0%	7x12	(6-18)	1 PD	2 PD	3 PD	48 hod	30 min	2 PD	3 PD	5 PD
B3 Závažný	98.0%	5x8	(7-15)	1 PD	2 PD	3 PD	48 hod	30 min	2 PD	3 PD	5 PD
C1 Normální	97.0%	5x12	(6-18)	1 PD	3 PD	6 PD	96 hod	24 hod	3 PD	7 PD	10 PD
C2 Normální	97.0%	5x8	(7-15)	1 PD	3 PD	6 PD	96 hod	24 hod	3 PD	7 PD	10 PD
D Minoritní	94.0%	5x8	(7-15)	2 PD	10 PD	14 PD	96 hod	24 hod	5 PD	10 PD	14 PD
E1 Customizovaný											
E2 Customizovaný											

12.3. Doba řešení Incidentu a Požadavku kategorie C je pro veškeré Servisní modely stanovena na 15 PD.

12.4. Do měření úrovně Dostupnosti (Software) nejsou započítávány:

a. dočasné vyřazení Softwaru z provozu na základě předchozí dohody Objednatele a Dodavatele (odstávka),

b. pravidelná vyřazení Softwaru z provozu Dodavatelem v časech sjednaných ve Smlouvě nebo její příloze (servisní okna),

c. smluvními stranami předem dohodnutý časový úsek za účelem instalace upgradu,

d. výpadky Softwaru způsobené Objednatelem přímo v důsledku jím provedených zásahů do Softwaru, které nebyly Dodavatelem předem schváleny,

e. skutečnosti ve vztahu k Hardware dle odst. 12.9 ZOP za podmínek, že je takový Hardware součástí Plnění a současně je nezbytný pro fungování Software.

12.5. Nedostupnost Softwaru dle odst. 12.4. ZOP se nepovažuje za nedosažení sjednaných parametrů Dostupnosti dle Smlouvy a nebude započítána do výpočtu dle odst. 12.6. a 12.7. ZOP.

12.6. Nestanoví-li Smlouva jinak, bude Dostupnost Software měřena na základě následujícího vzorce:

$$Dostupnost\ (\%) = \frac{Doba\ provozu - Doba\ výpadku}{Doba\ provozu} \times 100$$

12.7. Doba výpadku Softwaru je časový úsek z Doby provozu v hodinách, kdy je služba nedostupná, a počítá se podle následujícího vzorce:

$$Doba\ výpadku = \sum_{i}^{n} T_i$$

kde:

Σ je celková doba všech výpadků Softwaru za vyhodnocované období

T_i je doba jednotlivého výpadku Softwaru

n je počet všech výpadků

12.8. Doba Provozu Softwaru definovaná pro účely tohoto článku je celková doba provozu Softwaru v hodinách za vyhodnocované období, kterým je kalendářní měsíc.

12.9. Do měření úrovně Dostupnosti (Hardware) nejsou započítávány:

a. dočasná vyřazení Hardware z provozu na základě předchozí dohody Objednatele a Dodavatele (odstávka),

b. pravidelná vyřazení Hardware z provozu Dodavatelem v časech sjednaných ve Smlouvě nebo její příloze (servisní okna)

c. výpadky Hardware způsobené Objednatelem přímo v důsledku jím provedených zásahů do Hardware, které nebyly Dodavatelem předem schváleny

12.10. Ustanovení odst. 12.5. až 12.8 ZOP se použijí obdobně s tím, že odkaz v odst. 12.5 ZOP na odst. 12.4 ZOP se nahrazuje odkazem na odst. 12.9 ZOP a slovo Software se nahrazují slovem Hardware.

13. AKTUALIZACE PLNĚNÍ

13.1. Pokud bude Dodavatel v rámci provozu Plnění provádět jeho aktualizaci, bude postupovat podle:

13.1.1. hardeningových bezpečnostních politik, které jsou určeny standardem Center for Internet Security (CIS) level (group) 1, dostupné z https://www.cisecurity.org.

13.1.2. v souladu s Interními předpisy Objednatele a

13.1.3. v souladu s dokumentem v příloze – Platforma SŽ.

13.2. Dodavatel odpovídá za to, že systémy dodávané do Plnění budou obsahovat nejnovější, stabilní, bezpečné a řádně odzkoušené bezpečnostní aktualizace (patche).

13.3. Veškerý software musí splňovat požadavek na podporu od výrobce (podporovaný build).

13.4. Dodavatel je povinen za součinnosti oprávněných osob na straně Objednatele:

13.4.1. provádět analýzy topologie sítě či skenování aktivních částí Plnění;

13.4.2. realizovat bezpečnostní opatření pro odstranění nebo blokování síťových spojení, která neodpovídají požadavkům na ochranu integrity komunikační sítě a

13.4.3. zajistit řízení komunikace v rámci komunikační sítě a integritu dat při vzdáleném přístupu nebo při přístupu do komunikační sítě pomocí bezdrátových technologií.

14. ÚČAST PODDODAVATELŮ

14.1. Poddodavatele, jejichž prostřednictvím Dodavatel prokazoval kvalifikaci ve Veřejné zakázce, je Dodavatel povinen využívat při Plnění Smlouvy po celou dobu jejího trvání v rozsahu, v jakém jimi prokazoval kvalifikaci. Poddodavatele, jimiž Dodavatel prokazoval kvalifikaci ve Veřejné zakázce, lze vyměnit pouze s předchozím listinným souhlasem Objednatele, který může být dán výlučně za

předpokladu, že tyto osoby budou nahrazeny osobami splňujícími kvalifikaci požadovanou ve Veřejné zakázce ve stejném rozsahu jako nahrazované osoby.

14.2. Dodavatel se zavazuje, že při poskytování Plnění pro Objednatele budou všichni Poddodavatelé, které Dodavatel využívá k poskytnutí Plnění dle Smlouvy, dodržovat veškeré požadavky vyplývající ze Smlouvy a Příloh Smlouvy. Dodavatel odpovídá za to, že jeho Poddodavatelé budou k tomuto zavázáni a nebudou jednat v rozporu s ujednáními Smlouvy a jejími Přílohami, kterou mezi sebou uzavřeli Dodavatel a Objednatel.

14.3. Významný dodavatel je oprávněn využít k Plnění dle Smlouvy Poddodavatele neuvedené ve Smlouvě jen v případě, že to Smlouva výslovně připouští, a to za podmínek v ní uvedených. Nestanoví-li Smlouva jinak, podléhají jednotliví Poddodavatelé Významného dodavatele předchozímu písemnému schválení ze strany Objednatele. Dodavatel může ke schválení navrhnout nebo do Plnění Smlouvy zapojit pouze takové Poddodavatele, kteří nejsou v rozporu s požadavky Objednatele na Významného dodavatele.

14.4. Dodavatel nesmí zapojit k Plnění dle Smlouvy Poddodavatele, bylo-li by tím porušeno opatření obecné povahy vydané ze strany NÚKIB.

14.5. Dodavatel je povinen informovat Objednatele předem o zapojení Poddodavatelů a poskytnout mu veškeré potřebné údaje, zejm. identifikační údaje Poddodavatelů, aby Objednatel mohl splnit svoje povinnosti stanovené právními předpisy v souvislosti s prověřováním dodavatelského řetězce, zejm. povinnost zjišťovat a evidovat informace o dodavatelích bezpečnostně významných dodávek a informační povinnost vůči NÚKIB.

15. REALIZAČNÍ TÝM

15.1. Pokud je takový požadavek součástí Zadávací dokumentace, je Dodavatel povinen předat Objednateli seznam osob, které budou členy Realizačního týmu, který se bude podílet na Plnění dle Smlouvy. Členy Realizačního týmu lze měnit pouze s předchozím listinným souhlasem Objednatele, který může být dán výlučně za předpokladu, že tyto osoby budou nahrazeny osobami splňujícími kvalifikaci požadovanou ve Veřejné zakázce ve stejném rozsahu jako nahrazované osoby. V případě, že dochází ke změně člena realizačního týmu, který byl v zadávacím řízení hodnocen, je nezbytné, aby takového člena realizačního týmu nahradila osoba, jež by dosáhla v rámci hodnocení stejného či lepšího výsledku než osoba nahrazovaná. Při změně Realizačního týmu není nutné uzavírat listinný dodatek ke Smlouvě a Dodavatel je povinen vypracovat a předat Objednateli v listinné podobě aktualizované znění seznamu členů Realizačního týmu. Tento článek se týká pouze Veřejných zakázek, které požadují provádění Plnění prostřednictvím Realizačního týmu.

15.2. Dodavatel se zavazuje provádět Plnění prostřednictvím členů Realizačního týmu uvedených v Příloze Smlouvy *Realizační tým* tak, aby jednotliví členové Realizačního týmu, kteří jsou Kvalifikovanými osobami, prováděli činnosti na pozici dle jejich odbornosti (kvalifikace), které odpovídají tomu, pro jakou pozici prokazovali kvalifikaci v rámci Veřejné zakázky, a v rozsahu, který takové pozici běžně odpovídá.

15.3. Každá Kvalifikovaná osoba musí po celou dobu provádění Plnění splňovat kvalifikaci uvedenou v nabídce Dodavatele a zároveň minimální technické kvalifikační předpoklady kladené na pozici, kterou daná osoba zastává dle Zadávací dokumentace.

15.4. Nebude-li se Kvalifikovaná osoba řádně podílet na provádění Plnění v rozsahu stanoveném Smlouvou, např. v důsledku ukončení její spolupráce s Dodavatelem nebo její dlouhodobé absence (zejména dlouhodobá nemoc pravděpodobně překračující délku jednoho měsíce), je Dodavatel povinen neprodleně namísto Kvalifikované osoby zahájit provádění Plnění Náhradní Kvalifikovanou osobou a nejpozději do tří (3) Pracovních dnů ode dne, kdy taková situace nastala, informovat Objednatele o této skutečnosti.

15.5. Pokud Objednatel nesouhlasí s osobou Náhradní Kvalifikované osoby, je oprávněn žádat Dodavatele o její výměnu za jinou osobu se stejnou kvalifikací navrženou Dodavatelem, čemuž je Dodavatel povinen vyhovět.

16. KOMUNIKACE STRAN

16.1. Objednatel a Dodavatel si pro vzájemnou komunikaci ohledně Smlouvy zvolí kontaktní osoby, jejichž seznam uvedou ve Smlouvě.

16.2. Jsou-li naplněny podmínky 21.1 ZOP, vykonává kontaktní osoba na straně Dodavatele povinnosti kontaktní osoby pro kybernetickou bezpečnost vyplývající z článku 21. ZOP, nebo je pro plnění takových povinností Dodavatel povinen určit zvláštní kontaktní osobu ve Smlouvě (v takovém případě obě Strany zvolí kontaktní osobu pro kybernetickou bezpečnost, která má na starosti komunikaci týkající se článku 21. ZOP).

16.3. Strany si navzájem oznámí jakékoliv změny v kontaktních osobách, přičemž taková změna je účinná uplynutím sedmého (7.) dne po jejím doručení.

16.4. Není-li ve Smlouvě výslovně stanovena jiná forma pro doručování dokumentů anebo jiných právních jednání, lze takové dokumenty a jednání doručit v elektronické formě na e-mailovou adresu příslušné kontaktní osoby, prostřednictvím datové zprávy zaslané v rámci ISDS, anebo v listinné podobě.

17. NÁHRADA ŠKODY A SMLUVNÍ POKUTY

17.1. Poruší-li Dodavatel některé ze svých povinností stanovených ve Smlouvě či jejích přílohách, zejména pak pokud poruší SLA, resp. stanovený Servisní model dle odst. 12.2 ZOP, je Objednatel oprávněn požadovat zaplacení smluvní pokuty ve výši stanovené v odst. 17.11. ZOP, pokud nejsou ve Smlouvě výslovně zakotveny jiné sankce, které vylučují aplikaci odst. 17.11. ZOP.

17.2. Uplatněním smluvní pokuty není dotčeno právo druhé Smluvní strany na náhradu škody v plné výši.

17.3. Uplatněním nároku na zaplacení smluvní pokuty ani jejím uhrazením nezaniká povinnost Smluvní strany splnit utvrzenou povinnost.

17.4. Dopadají-li na jedno skutkově stejnorodé porušení povinnosti dvě a více ustanovení o smluvní pokutě, uplatní se pouze jedna smluvní pokuta, a to ta, která je v nejvyšší částce. Není vyloučen souběh smluvní pokuty za porušení smluvní povinnosti a smluvní pokuty za prodlení s odstraněním následku téže smluvní povinnosti, jelikož se nejedná o skutkově stejnorodé porušení smluvní povinnosti.

17.5. Smluvní pokuty se uplatňují bez DPH. Je-li základem pro výpočet smluvních pokut Cena či její část, je rozhodná Cena či její část bez DPH stanovená k okamžiku uzavření Smlouvy; k případným jejím následným úpravám po uzavření Smlouvy se nepřihlíží.

17.6. Smluvní pokuta je splatná do třiceti (30) dnů ode dne vystavení daňového dokladu – sankční faktury. Je-li povinná Smluvní strana v prodlení s uhrazením smluvní pokuty, musí uhradit druhé Smluvní straně zákonný úrok z prodlení z dlužné částky smluvní pokuty za každý započatý den prodlení.

17.7. Maximální celková výše všech uplatněných smluvních pokut v důsledku porušení Smlouvy je stanovena ve výši 30 % Ceny.

17.8. Dosažení maximální celkové výše veškerých uplatněných smluvních pokut podle předchozího odstavce představuje podstatné porušení Smlouvy, na základě, kterého je Objednatel oprávněn odstoupit od Smlouvy.

17.9. Objednatel je ze zákona povinen uplatnit a vymáhat veškeré smluvní pokuty, na které mu vznikl nárok, a to v plné výši bez možnosti její úpravy.

17.10. Jsou-li smluvní pokuty stanoveny formou procentního vyjádření vůči Ceně či její části za každý den (či kratší časový úsek) prodlení, platí, že maximální denní výše každé jednotlivé smluvní pokuty činí:

a. v případě Ceny do 10 mil. Kč maximálně 10.000 Kč,

b. v případě Ceny do 100 mil. Kč maximálně 50.000 Kč

c. v případě Ceny do 1 mld. Kč maximálně 100.000 Kč a

d. v případě Ceny nad 1 mld. Kč maximálně 200 000 Kč.

17.11. Objednateli vzniká vůči Dodavateli právo na zaplacení smluvní pokuty:

a. poruší-li Dodavatel svoji povinnost řádně a včas provést Plnění, nebo jeho část (je-li Plnění prováděno po částech) ve výši 0,2 % z Ceny, nebo ceny části Plnění za každý započatý den prodlení až do řádného splnění této povinnosti. Plnění se považuje pro účely této smluvní pokuty za řádně a včas provedené i v případě, že bylo akceptováno s výhradou;

b. poruší-li Dodavatel svoji povinnost dle odst. 8.1.11 ZOP ve výši 0,2 % z výše zadržené části Ceny dle dle odst. 8.1.11 ZOP za každý započatý den prodlení až do řádného odstranění poslední vytýkané vady ve smyslu odst. 8.1.11 ZOP ;

c. poruší-li Dodavatel povinnost udělit nebo zajistit Objednateli ze strany třetí osoby/třetích osob udělovaná oprávnění v rozsahu práv duševního vlastnictví ve výši 5 % z Ceny za každé jednotlivé porušení;

d. poruší-li Dodavatel povinnost řádně a včas předat Objednateli Zdrojový kód a veškerou související Dokumentaci, ve výši 0,05 % z Ceny za každý započatý den prodlení;

e. poruší-li Dodavatel některou z povinností týkající se účasti Poddodavatelů anebo Realizačního týmu, ve výši 10 % z Ceny za každé jednotlivé porušení povinnosti;

f. poruší-li Dodavatel svoji povinnost dodržet sjednanou Dobu vyřešení Incidentu, ve výši:

   i. 0,01 % z Ceny v případě každé započaté hodiny/den prodlení nad rámec sjednané Doby vyřešení v případě každého Incidentu kategorie A;

   ii. 0,01 % z Ceny v případě každé započaté hodiny/den prodlení nad rámec sjednané Doby vyřešení v případě každého Incidentu kategorie B;

   iii. 0,005 % z Ceny v případě každé započaté hodiny/den prodlení nad rámec sjednané Doby vyřešení v případě každého Incidentu kategorie C;

g. v případě prodlení nad rámec sjednané lhůty pro odstranění vad v Produkčním prostředí:

   i. Vada kategorie A ve výši 0,01 % z Ceny za každou započatou hodinu/den v případě každé Vady;

   ii. Vada kategorie B ve výši 0,01 % z Ceny za každou započatou hodinu/den v případě každé Vady;

   iii. Vada kategorie C ve výši 0,005 % z Ceny za každou započatou hodinu/den v případě každé Vady;

h. v případě prodlení nad rámec sjednané lhůty pro odstranění vad v Testovacím prostředí:

   i. Vada kategorie A ve výši 0,05 % z Ceny za každý započatý Pracovní den v případě každé Vady; a

   ii. Vada kategorie B ve výši 0,01 % z Ceny za každý započatý Pracovní den v případě každé Vady;

i. V případě, že Dodavatel nedodrží Dostupnost stanovenou Servisním modelem dle odst. 12.2. ZOP, ve výši dle tabulky uvedené níže v závislosti na míře nedodržení požadované Dostupnosti:

Výše poklesu Dostupnosti oproti stanovené Dostupnosti Servisním modelem je	Výše smluvní pokuty

Do 2 %	10 % z ceny poskytovaného Plnění odpovídající vyhodnocovanému období dle odst. 12.8 ZOP
Od 2 (včetně) do 5 %	15 % z ceny poskytovaného Plnění odpovídající vyhodnocovanému období dle odst. 12.8 ZOP
Od 5 (včetně) do 10 %	25 % z ceny poskytovaného Plnění odpovídající vyhodnocovanému období dle odst. 12.8 ZOP
Od 10 % (včetně) a více	50 % z ceny poskytovaného Plnění odpovídající vyhodnocovanému období dle odst. 12.8 ZOP

j. v případě prodlení Dodavatele reagovat na Požadavek Objednatele v době řešení Incidentu uvedeného v odst. 12.2. ZOP ve výši z 0,02 % z Ceny za každý jednotlivý případ;

k. ve výši a za podmínek dle článku 21. ZOP v oblasti kybernetické bezpečnosti;

l. ve výši a za podmínek dle článku 22. ZOP v oblasti ochrany osobních údajů;

m. ve výši a za podmínek dle článku 23. ZOP v oblasti ochrany Důvěrných informací; nebo

n. poruší-li Dodavatel svoji povinnost dle odst. 14.2. ZOP nebo 14.3. ZOP, ve výši 2 % z Ceny za každé jednotlivé porušení.

17.12. Pro smluvní pokuty stanovené v odst. 17.11. písm. 17.11.f. a 17.11.g. ZOP platí, že je-li lhůta pro splnění stanovena v hodinách, je smluvní pokuta počítána za každou započatou hodinu, je-li lhůta pro splnění stanovena ve dnech či Pracovních dnech, je smluvní pokuta počítána za každý započatý den.

17.13. Objednatel je oprávněn započíst nárok na zaplacení smluvní pokuty, i pokud ještě není splatný, proti jakémukoliv nároku Dodavatele na peněžité plnění vyplývajícímu ze Smlouvy.

17.14. Za každý den prodlení s úhradou Smluvní pokuty je Objednatel oprávněn požadovat po Dodavateli úhradu úroků z prodlení ve výši stanovené obecně závaznými právními předpisy.

18. ZÁRUKA ZA JAKOST A PRÁVA Z VADNÉHO PLNĚNÍ

18.1. Společná ustanovení

18.1.1. Dodavatel uděluje Objednateli záruku za jakost Plnění a všech jeho částí na dobu dvou (2) let ode dne akceptace výstupu Plnění.

18.1.2. Objednatel je oprávněn Vady, které se vyskytnou v průběhu záruční doby, nahlásit Dodavateli bez zbytečného odkladu od okamžiku, kdy je zjistil. Lhůta bez zbytečného odkladu činí vždy nejméně devadesát (90) dnů.

18.1.3. Dodavatel odpovídá za vady zjevné, skryté i právní, které měl výstup provádění Plnění v době akceptace Objednatelem, a dále za ty, které se na něm vyskytnou v záruční době, a zavazuje se, vedle dalších nároků Objednatele, je bezplatně odstranit.

18.1.4. Dodavatel neodpovídá za vady, pokud byly způsobeny zásahem do takových výstupů Plnění ze strany Objednatele nebo jím pověřené osoby, případně jiných dodavatelů Objednatele.

18.1.5. Objednatel je povinen oznámit vady Plnění Dodavateli prostřednictvím Servicedesku, nebude-li Stranami dohodnuto jinak.

18.1.6. Dodavatel neodpovídá za vady Plnění vzniklé:

a. provozováním Díla Objednatelem v rozporu s Dokumentací;

b. neoprávněným nebo neodborným zásahem či nesprávným užitím Díla Objednatelem;

c. vadami IT prostředí Objednatele.

18.2. Záruka vztahující se k Softwaru

18.2.1. Pokud výrobce Standardního Software poskytuje záruku za jakost, pak Dodavatel postupuje takovou záruku za jakost Objednateli. To nezbavuje Dodavatele povinnosti poskytnout Objednateli vlastní záruku za jakost ve smyslu tohoto článku.

18.2.2. V době trvání záruční doby je Dodavatel povinen odstraňovat vady ve lhůtách uvedených v tabulce níže. Lhůty stanovené v hodinách běží pouze v Pracovní dny osm (8) hodin denně v době od 9:00 do 17:00 hodin (režim 5x8). Lhůty stanovené v hodinách se mimo dobu uvedenou v předchozí větě staví a pokračují dále v běhu během další bezprostředně následující doby počítání. Strany pro zamezení pochybnostem prohlašují, že toto se netýká lhůt stanovených v Pracovních dnech ani počítání doby prodlení v rámci výpočtu smluvních pokut.

Produkční prostředí

Kategorie vady	Lhůta k odstranění počítaná od nahlášení vady Objednatelem
Vada kategorie A – kritická	do 4 hodin[1]
Vada kategorie B – střední	do 17:00 hod. třetího Pracovního dne od nahlášení vady[2]
Vada kategorie C – nízká	do 17:00 hod. pátého Pracovního dne od nahlášení vady[3]

Testovací prostředí

Kategorie vady	Lhůta k odstranění počítaná od nahlášení vady Objednatelem
Vada kategorie A – kritická	do 17:00 hod. druhého Pracovního dne od nahlášení vady[4]
Vada kategorie B – střední	do 17:00 hod. pátého Pracovního dne od nahlášení vady[5]
Vada kategorie C – nízká	do 17:00 hod. desátého Pracovního dne od nahlášení vady[6]

18.3. Záruka vztahující se k Hardwaru

18.3.1. Poskytuje-li výrobce anebo Dodavatel kterékoliv části Hardwaru na své výrobky anebo služby záruku za jakost delší, než je záruka za jakost dle tohoto článku, zavazuje se Dodavatel udělit Objednateli nebo na Objednatele postoupit danou záruku za jakost tak, aby Objednatel byl oprávněn po skončení záruky za jakost uplatnit nároky ze záruky za jakost bez nutnosti součinnosti ze strany Dodavatele.

18.3.2. Zjevné vady Hardware a dalších hmotných věcí je Objednatel povinen u Dodavatele reklamovat v rámci Akceptačního řízení. V případě, že Objednatel zjistí vady hmotných věcí po akceptaci, je povinen tyto vady bez zbytečného odkladu reklamovat u Dodavatele.

18.3.3. V případě, že odstranění reklamovaných vad bude trvat déle než dva (2) Pracovní dny, zavazuje se Dodavatel poskytnout Objednateli náhradní Hardware či jinou náhradní

[1] Lhůta je stanovena v hodinách.
[2] Lhůta je stanovena ve dnech.
[3] Lhůta je stanovena ve dnech.
[4] Lhůta je stanovena v hodinách.
[5] Lhůta je stanovena ve dnech.
[6] Lhůta je stanovena ve dnech.

hmotnou věc po dobu trvání odstranění reklamované vady, nedohodnou-li se Strany jinak.

19. UKONČENÍ SMLUVNÍHO VZTAHU

19.1. Obecně k odstoupení od Smlouvy:

a. Strany sjednávají, že vznikne-li Objednateli nárok na odstoupení od Smlouvy, může podle své volby odstoupit od Smlouvy v celém rozsahu či jen od některé části Plnění určené Objednatelem.

b. Strany se dohodly na vyloučení použití § 1978 odst. 2 Občanského zákoníku, který stanoví, že marné uplynutí dodatečné lhůty stanovené k plnění může mít za následek odstoupení od této Smlouvy bez dalšího.

c. Dodavatel nemá právo odstoupit od Smlouvy v případě nevhodných příkazů Objednatele či poskytnutí nevhodné věci Objednatelem dle § 2595 Občanského zákoníku.

19.2. Objednatel je oprávněn odstoupit od Smlouvy, v případě, že:

a. Dodavatel je v prodlení s plněním dle Smlouvy či jakékoliv části Plnění déle než 30 dnů a nezjedná nápravu ani do 15 dnů od doručení písemného oznámení Objednatele o takovém prodlení.

b. Dodavatel je v prodlení s Plněním dle Smlouvy déle než 60 dnů, a to i bez nutnosti zaslání předchozího upozornění.

c. Nastane některý ze zákonem stanovených případů a zejména v případech podstatného porušení povinností Dodavatele stanovených ve Smlouvě. Za podstatné porušení povinností Dodavatele se považuje zejména:

i. Dodavatel je opakovaně v prodlení s prováděním Plnění dle Smlouvy;

ii. prohlášení Dodavatele učiněné na základě Smlouvy se ukáže jako nepravdivé;

iii. Dodavatel bez upozornění a relevantního odůvodnění nepoužil k Plnění člena Realizačního týmu, ač k tomu byl povinen; nebo

iv. Dodavatel poruší některou z povinností uvedenou v čl. 21. ZOP opakovaně nebo závažným způsobem.

d. Dodavatel poruší kteroukoliv svoji povinnost dle Smlouvy jiným než podstatným způsobem a ve lhůtě 15 dnů od doručení písemného oznámení Objednatele toto své porušení nenapraví.

e. Dodavatel poruší svou povinnost dle odst. 14.2. ZOP nebo odst. 14.3. ZOP nebo Poddodavatel Dodavatele poruší některou z povinností vyplývající z požadavků dle odst. 14.2. ZOP.

f. Dodavatel podá insolvenční návrh jako dlužník ve smyslu § 98 Insolvenčního zákona nebo insolvenční soud nerozhodne o insolvenčním návrhu na Dodavatele do šesti (6) měsíců od zahájení insolvenčního řízení, nebo insolvenční soud vydá rozhodnutí o úpadku Dodavatele ve smyslu § 136 Insolvenčního zákona.

g. Je přijato rozhodnutí o povinném nebo dobrovolném zrušení Dodavatele (vyjma případů sloučení nebo splynutí).

h. Okolnost vylučující povinnost k náhradě Újmy kterékoli ze Stran trvá déle než 30 dnů;

i. dojde k Významné změně dle odst. 4.2. ZOP.

j. Dojde k Významné změně kontroly nad Dodavatelem nebo změny kontroly nad zásadními aktivy využívanými Dodavatelem k plnění Smlouvy, přičemž kontrolou se zde rozumí vliv, ovládání či řízení dle ust. § 71 a násl. ZOK, či ekvivalentní postavení.

k. Dojde k Významné změně ovlivnění nebo ovládání Dodavatele podle ust. § 71 a násl. ZOK nebo změně vlastnictví zásadních aktiv, využívaných Dodavatelem k plnění Smlouvy a změně oprávnění nakládat s těmito aktivy, či dojde ke změně ekvivalentní těmto změnám a tato změna bude Objednatelem vyhodnocena jako riziko bezpečnosti informací, které nelze odstranit jiným opatřením; toto ustanovení se uplatní i pro případ, že Dodavatel o takových změnách dopředu a včas neinformuje Objednatele.

19.3. Dodavatel je oprávněn odstoupit od Smlouvy pouze v případech jejího podstatného porušení, jestliže:

a. Objednatel nezaplatil jakoukoli dlužnou částku za Plnění dle Smlouvy řádně a včas a toto porušení nenapravil ani do 60 dnů ode dne obdržení písemné výzvy k nápravě; nebo

b. Objednatel poruší jinou povinnost dle Smlouvy podstatným způsobem a ve lhůtě 60 dnů ode dne obdržení písemné výzvy k nápravě toto své porušení nenapraví.

19.4. Dodavatel není oprávněn odstoupit od Smlouvy ve vztahu k části Plnění, za kterou mu již bylo Objednatelem zaplaceno.

19.4.1. Objednatel je oprávněn Smlouvu vypovědět bez výpovědní doby, nelze-li v jejím plnění pokračovat, aniž by bylo porušeno opatření obecné povahy vydané ze strany NÚKIB.

20. ZMĚNY SMLOUVY A ZMĚNOVÉ ŘÍZENÍ

20.1. Není-li ve Smlouvě nebo jejích Přílohách stanoveno jinak, může být Smlouva měněna nebo zrušena pouze v listinné podobě, a to v případě změn Smlouvy číslovanými dodatky, který musí být podepsány oběma Stranami a uzavřeny v souladu se ZZVZ.

20.2. Pokud je ve Smlouvě upraveno Opční právo, vyhrazuje si Objednatel v souladu s ustanovením § 100 odst. 3 ZZVZ vyhrazenou změnu závazku z této Smlouvy spočívající v pořízení dalšího obdobného Plnění od vybraného účastníka v rámci zadávacího řízení Veřejné zakázky, tj. od Dodavatele dle Smlouvy. Předmětem plnění Opčního práva je poskytnutí dalšího obdobného Plnění dle Smlouvy tak, jak bylo podrobně vymezeno včetně dalších zákonných náležitostí vyhrazené změny závazku dle § 100 odst. 3 ZZVZ v Zadávací dokumentaci předmětné Veřejné zakázky.

20.3. Objednatel je oprávněn do uplynutí tří (3) let od nabytí účinnosti Smlouvy kdykoliv uplatnit toto Opční právo, a to i opakovaně do vyčerpání limitů Opčního práva definovaných v Zadávací dokumentaci. Vyhrazená změna závazku ze Smlouvy bude Stranami projednána v rámci jednacího řízení bez uveřejnění dle § 66 ZZVZ, které bude zahájeno Objednatelem v souladu s tímto ustanovením, a jehož výsledkem bude uzavření listinného dodatku k této Smlouvě či uzavření nové smlouvy mezi Objednatelem nebo Dodavatelem.

21. KYBERNETICKÁ BEZPEČNOST

21.1. Tento článek se uplatní v případě, kdy je Smlouva uzavřena s Významným dodavatelem, pokud je Dodavatel Dodavatelem Strategicky významné služby, jakož i v dalších případech, kdy tak výslovně stanoví Smlouva.

21.2. Zda je Dodavatel Významným dodavatelem, stanoví Smlouva. Pokud se Dodavatel stane Významným dodavatelem v průběhu plnění Smlouvy, bude o této skutečnosti Objednatelem neprodleně informován a povinnosti dle čl. 21. se na něj uplatní v rozsahu v jakém to po něm lze spravedlivě požadovat.

21.3. Zda je Dodavatel Dodavatelem Strategicky významné služby, stanoví Smlouva. Pokud se Dodavatel stane Dodavatelem Strategicky významné služby v průběhu plnění Smlouvy, bude o této skutečnosti Objednatelem neprodleně informován a čl. 21. se na něj uplatní v rozsahu, v jakém to po něm lze spravedlivě požadovat.

21.4. Dodavatel se při plnění Smlouvy zavazuje postupovat v souladu se ZoKB, VoKB a souvisejícími právními předpisy, příp. vč. právních předpisů tyto předpisy provádějící, upravující či nahrazující, dodržovat zásady bezpečnosti informací, Interní předpisy Objednatele a z nich vyplývající povinnosti týkající se bezpečnostních opatření, provozní řády prostor Objednatele, rozhodnutí, protiopatření, opatření obecné povahy, či jiný správní akt NÚKIB či jiného správního orgánu anebo

závazné podmínky pro Objednatele stanovené orgánem veřejné moci ukládající Objednateli další povinnosti ve smyslu ZoKB a VoKB, včetně upozorňování a zajištění hlášení Kybernetických bezpečnostních incidentů Objednateli, jakož i další bezpečnostní politiky, metodiky a postupy, se kterými byl Objednatelem seznámen.

21.5. Dodavatel je povinen seznámit se s bezpečnostními požadavky Objednatele uvedenými ve Smlouvě, jejích přílohách, těchto ZOP, Interních předpisech Objednatele a seznámit s nimi osoby podílející se na plnění Smlouvy dle potřeby s ohledem na charakter jejich plnění s přihlédnutím k zajištění bezpečnosti informací. Pokud je to potřebné, je Dodavatel povinen provést školení bezpečnostních požadavků dle tohoto odstavce a dále je provádět v pravidelných intervalech, nejméně 1x ročně. Dodavatel je také povinen aktivně vynucovat dodržování takových bezpečnostních požadavků dotčenými osobami na straně Dodavatele. Za porušení těchto pravidel osobami uvedenými v tomto odstavci odpovídá Dodavatel tak, jako by je porušil sám.

21.6. Není-li ve Smlouvě ujednáno jinak, je Dodavatel povinen vytvořit, pravidelně aktualizovat a vynucovat vůči osobám podílejícím se, byť i nepřímo, na Předmětu Smlouvy:

21.6.1. politiku řízení přístupu, na základě které, není-li ve Smlouvě ujednáno jinak, je Dodavatel dále povinen průběžně monitorovat a zaznamenávat přístupy všech osob účastnících se na Plnění dle Smlouvy, a to v rozsahu, aby bylo možné jednoznačně určit uživatele, čas a provedenou činnost, jakož i vyhodnocovat oprávněnost těchto přístupů (logování přístupů) a tuto svou povinnost v politice řízení přístupu zohlednit a Dodavatel musí umožnit a poskytnout součinnost na jejich integraci do systému bezpečnostního monitoringu (SIEM), systému pro správu logů a centrální úložiště logů Objednatele;

21.6.2. politiku zvládání Kybernetických bezpečnostních událostí a Kybernetických bezpečnostních incidentů obsahující činnosti, role, odpovědnosti a pravomoci k rychlému a účinnému zvládání Kybernetických bezpečnostních událostí a Kybernetických bezpečnostních incidentů.

21.7. Nestanoví-li Smlouva jinak, Plnění musí využívat nástroj Objednatele pro centrální správu přístupových účtů, který zajišťuje přidělení oprávnění k výkonu činností jednotlivým rolím jednoznačně identifikovaných fyzických osob, které se podílejí na plnění Smlouvy, a to v nejmenším možném a nutném rozsahu tak, aby měly přístup k aktivům Objednatele pouze ty osoby, které takový přístup skutečně potřebují k výkonu činností týkajících se předmětu Plnění dle Smlouvy.

21.8. Dodavatel je povinen při nakládání s veškerými aktivy (dotčenými aktivy Dodavatele a Objednatele) postupovat tak, aby chránil jejich důvěrnost, dostupnost a integritu a zavést přiměřená opatření na jejich ochranu.

21.9. Dodavatel je povinen řídit rizika spojená s Plněním dle Smlouvy minimálně dle standardů požadovaných ZoKB pro regulované služby v režimu vyšších povinností a případně dle Interních předpisů, pokud obsahují závazná pravidla pro řízení rizik.

21.10. Dodavatel je povinen, na vyžádání, v pravidelných minimálně ročních intervalech předkládat Zprávu o přezkoumání stavu ISMS k relevantním aktivům související s Plněním.

21.11. Dodavatel je povinen zaslat některým z níže uvedených způsobů hlášení o událostech, které mají charakter Kybernetického bezpečnostního incidentu, včetně případů porušení zabezpečení Osobních údajů, vždy bez zbytečného odkladu, nejpozději však do tří (3) hodin po jejich zjištění, a sdělit Objednateli opatření, která již provedl ve vztahu k tomuto Kybernetickému bezpečnostnímu incidentu, případně zvolí jinou formu dohodnutou mezi Objednatelem a Dodavatelem určenou ke včasnému hlášení Kybernetického bezpečnostního incidentu a/nebo již učiněných opatření. Dodavatel je povinen veškeré Kybernetické bezpečnostní incidenty zaznamenávat a po nezbytně dlouhou dobu uchovávat. Dodavatel je povinen bez zbytečného odkladu poskytnout Objednateli veškerou nezbytnou součinnost k detekci, vyhodnocení či řešení Kybernetického bezpečnostního incidentu, a to včetně případné realizace nutných opatření dle pokynů Objednatele, a dále k tomu, aby Objednatel mohl ve lhůtě dle ZoKB předložit NÚKIB tzv. prvotní hlášení. Zapříčinil-li Dodavatel Kybernetický bezpečnostní incident nebo podílel-li se na jeho vzniku, provede analýzu příčin Kybernetického bezpečnostního incidentu a navrhne opatření za účelem zamezení jeho opakování v budoucnu. Dodavatel je povinen ohlásit každou událost,

která má charakter Kybernetického bezpečnostního incidentu, včetně případů porušení zabezpečení osobních údajů, jedním z následujících způsobů:

a. e-mailem nebo telefonicky Dohledovému centru kybernetické bezpečnosti SŽ (viz odst. 1.15 ZOP); nebo

b. ohlášením do Servicedesku Objednatele.

21.12. Dodavatel je povinen bez zbytečného odkladu informovat Objednatele o každém Kybernetickém bezpečnostním incidentu s významným dopadem, který může negativně ovlivnit poskytování služby nebo aktiva Objednatele, a poskytnout mu veškeré informace nezbytné k tomu, aby Objednatel mohl splnit povinnosti podle § 19 ZoKB. Dodavatel je dále povinen řídit se pokyny Objednatele týkajícími se rozsahu a obsahu poskytovaných informací, zejména v případech, kdy NÚKIB uloží Objednateli povinnost nebo zákaz informovat uživatele regulované služby.

21.13. Bude-li se jednat o Kybernetický bezpečnostní incident s významným dopadem ve smyslu § 16 odst. 3 ZoKB, zavazuje se dále Dodavatel poskytnout Objednateli veškerou potřebnou součinnost, aby Objednatel mohl předložit příslušným orgánům:

a. oznámení, v němž aktualizuje informace z prvotního hlášení, předloží prvotní posouzení Kybernetického bezpečnostního incidentu a uvede dopad a indikátory kompromitace, pokud jsou k dispozici, přičemž tuto součinnost Dodavatel poskytne bez zbytečného odkladu, nejpozději však do 48 hodin po zjištění Kybernetického bezpečnostního incidentu;

b. na výzvu NÚKIB nebo Národního CERT průběžnou zprávu o podstatných změnách stavu zvládání Kybernetického bezpečnostního incidentu, a

c. závěrečnou zprávu o vyřešení Kybernetického bezpečnostního incidentu, přičemž tuto součinnost Dodavatel poskytne bez zbytečného odkladu, nejpozději však do 25 dnů ode dne předložení oznámení podle písmene a); nebo aby, v případě, že i po uplynutí 30 dnů ode dne předložení oznámení podle písmene a) Kybernetický bezpečnostní incident stále trvá, mohl Objednatel předložit bez zbytečného odkladu průběžnou zprávu o aktuálním stavu zvládání Kybernetického bezpečnostního incidentu, a poté nejpozději do 30 dnů ode dne, kdy došlo k vyřešení Kybernetického bezpečnostního incidentu, závěrečnou zprávu o vyřešení Kybernetického bezpečnostního incidentu.

21.14. Dodavatel je povinen pravidelně alespoň jednou ročně Objednateli zprávu o počtu a druhu útoků a Kybernetických bezpečnostních incidentů, které zaznamenal ve spojení s Plněním a/nebo Předmětem Smlouvy.

21.15. Dodavatel se zavazuje poskytnout Objednateli veškerou součinnost nezbytnou k tomu, aby Objednatel řádně naplňoval právní povinnosti stanovené ZoKB, VoKB a dalšími souvisejícími právními předpisy a normami. Zejména se Dodavatel zavazuje poskytnout Objednateli součinnost směřující k zavedení a provádění bezpečnostních protiopatření podle ZoKB, VoKB a Kybernetických bezpečnostních incidentů.

21.16. Pokud Dodavatel při plnění Smlouvy zjistí či jako odborník mohl a měl zjistit rozpor ustanovení Interních předpisů se ZoKB, VoKB anebo rozhodnutím či jiným pokynem NÚKIB, je povinen takový rozpor Objednateli neprodleně ohlásit a poskytnout Objednateli součinnost k jeho odstranění.

21.17. Dodavatel je povinen udržovat a pravidelně aktualizovat vlastní plán kontinuity činností (BCP) a plán obnovy po havárii (DRP), které pokrývají služby, aktiva a procesy poskytované v souladu se Smlouvou. Na žádost Objednatele je Dodavatel povinen poskytnout k nahlédnutí relevantní části těchto plánů.

21.18. Dodavatel se zavazuje provádět pravidelné testování BCP/DRP nejméně jednou za dva roky, o provedeném testování vést záznamy a na žádost objednatele poskytnout souhrnnou zprávu o výsledcích testů, zjištěných nedostatcích a přijatých nápravných opatřeních.

21.19. V případě, že dojde k jakémukoliv rozporu mezi Dodavatelem a třetí osobou, která není jeho Poddodavatelem a je dodavatelem Softwaru nebo jiných technologií dotčených plněním povinností Dodavatele dle této Smlouvy, je Dodavatel povinen tuto skutečnost bez zbytečného odkladu oznámit Objednateli. Dodavatel je dále povinen poskytovat Objednateli nutnou součinnost pro

jednání s těmito třetími osobami a sám se těchto jednání účastnit, nebo na základě žádosti Objednatele jednat s těmito třetími osobami napřímo.

21.20. Objednatel má právo v souladu s ustanoveními § 2593 Občanského zákoníku prostřednictvím určených osob kdykoli kontrolovat plnění Smlouvy u Dodavatele a jeho případných Poddodavatelů, a to i prostřednictvím třetí osoby; předchozí věta se uplatní obdobně v případě kontroly některé ze Stran ze strany kontrolního orgánu ve smyslu zákona č. 255/2012 Sb., kontrolní řád, ve znění pozdějších předpisů.

21.21. Objednatel má právo prostřednictvím určených osob provádět v pravidelných intervalech (1x za dva roky, není-li ve Smlouvě ujednáno jinak), jakož i v případě důvodného podezření na závažné porušení povinností Dodavatele dle těchto ZOP, v případě Kybernetických bezpečnostních incidentů a/nebo v jiných případech vyžadovaných ZoKB a/nebo VoKB, audit kybernetické bezpečnosti, tj. dodržování bezpečnosti informací dle Interních předpisů, ZoKB a VoKB u Dodavatele a jeho případných Poddodavatelů, a to i prostřednictvím třetí osoby. V rámci auditu kybernetické bezpečnosti je Objednatel oprávněn zejména porovnávat zjištěné skutečnosti s bezpečnostní dokumentací Objednatele a nad rámec obvyklý u auditu kybernetické bezpečnosti dále provádět následující činnosti:

21.21.1. pravidelné konzultace, jimž bude předcházet minimálně týdenní ohlašovací povinnost (e-mail, telefonní kontakt). Tyto konzultace nebudou častější než jednou za tři měsíce;

21.21.2. nehlášený telefonát od Kontaktní osoby Objednatele s členem Realizačního týmu, který má přístup do Informačního či komunikačního systému, zahrnující konkrétní dotazy na zabezpečení a jiné aspekty informační bezpečnosti dotčeného Informačního či komunikačního systému.

21.21.3. Dodavatel je povinen umožnit Objednateli provedení kontroly a auditu kybernetické bezpečnosti a zajistit (i smluvně) právo na provedení této kontroly a auditu kybernetické bezpečnosti u svých případných Poddodavatelů, jakož i veškerou další součinnost nezbytnou pro provedení auditu. Kontrolu a audit kybernetické bezpečnosti může rovněž provést i třetí osoba pověřená Objednatelem. Průběh takového auditu je doložen např. auditní zprávou či jiným obdobným dokumentem. Případné náklady na straně Dodavatele na provedení auditu jsou součástí Ceny za Plnění dle Smlouvy. Dodavatel je oprávněn rozporovat výsledky auditu kybernetické bezpečnosti do 7 Pracovních dnů od oznámení výsledku auditu kybernetické bezpečnosti. Dodavatel může rozporovat a) existenci vytčeného porušení či hrozby; b) že porušení či hrozba byla Dodavatelem již odstraněna. V obou případech uvede skutečnosti a důkazy k podpoře svých tvrzení. Objednatel je v takovém případě povinen takové připomínky vypořádat. V případě, že Objednatel na svém zjištění setrvá, je Dodavatel povinen se tímto auditem řídit.

21.21.4. Pokud audit kybernetické bezpečnosti odhalí jakékoliv podstatné porušení či hrozbu takového porušení, je Dodavatel povinen napravit nedostatky vč. přijetí případných dalších bezpečnostních opatření a o tomto informovat Objednatele, pokud se jedná o Významného dodavatele, je povinen napravit nedostatky bezodkladně a informovat Objednatele nejpozději do 7 dnů.

21.22. Je-li součástí Plnění přenos Dat a informací, je Dodavatel povinen jej za součinnosti oprávněných osob na straně Objednatele zabezpečit odolnými kryptografickými algoritmy v souladu s aktuálními doporučeními a metodikami NÚKIB a požadavky příslušných právních předpisů, zejména VoKB. Dodavatel je povinen zejména:

21.22.1. používat pouze aktuálně odolné kryptografické algoritmy, klíče a certifikáty,

21.22.2. zajistit bezpečnou komunikaci všech forem datového přenosu souvisejícího s Plněním,

21.22.3. bezpečně nakládat s kryptografickými algoritmy, jejich implementacemi a parametry,

21.22.4. používat nástroje pro bezpečnou správu kryptografických klíčů a certifikátů,

21.22.5. zajistit možnost kontroly a auditu nakládání s kryptografickými klíči,

21.22.6. zajistit důvěrnost a integritu kryptografických klíčů a souvisejících procesů,

21.22.7. bezodkladně provést potřebné změny, pokud NÚKIB nebo jiný orgán upozorní na zranitelnost či nedostatečnou odolnost používaných kryptografických prostředků.

21.23. Je-li součástí Předmětu Plnění správa síťové infrastruktury a/nebo jejích prvků (aktivních či pasivních), je Dodavatel povinen za součinnosti oprávněných osob na straně Objednatele:

21.23.1. provádět analýzy topologie sítě či skenování aktivních částí Předmětu Plnění; a

21.23.2. realizovat bezpečnostní opatření pro odstranění nebo blokování síťových spojení, která neodpovídají požadavkům na ochranu integrity komunikační sítě.

21.24. Dodavatel je dále povinen:

21.24.1. provádět pravidelné zálohy dat, konfigurací a nastavení technických aktiv vztahujících se k Plnění dle Smlouvy, zabezpečit je vhodnými prostředky proti neoprávněným přístupům, ztrátě nebo narušení integrity, a to včetně šifrování záloh v souladu s požadavky VoKB. Dodavatel je povinen: provádět testování integrity, dostupnosti a obnovitelnosti záloh nejméně jedenkrát za měsíc, dokumentovat výsledky těchto testů a uchovávat je po dobu trvání Smlouvy, oddělit zálohovací prostředí od produkčního prostředí, zajistit bezpečnou správu konfigurací a nastavení technických aktiv;

21.24.2. zajistit, aby dodávaná aplikace, je-li součástí Plnění, poskytovala auditní záznamy (logy) o činnostech v ní provedených, v rozsahu stanoveném VoKB, které umožní jednoznačně určit uživatele, čas a provedenou činnost, a aby tyto záznamy byly uchovávány po dobu stanovenou právními předpisy a Interními předpisy Objednatele. Dodavatel je povinen umožnit jejich integraci do systému bezpečnostního monitoringu Objednatele, pokud to Objednatel vyžaduje.

21.25. Pokud Objednatel zjistí, že Dodavatel postupuje v rozporu s tímto článkem 21 ZOP, je Objednatel v takovém případě oprávněn dožadovat se toho, aby Dodavatel odstranil vady vzniklé vadným postupem Dodavatele, zdržel se provádění postupů, které jsou v rozporu s tímto článkem, nebo konal, jak je od něj vyžadováno tímto článkem, a dále Smlouvu plnil řádným způsobem. Strany se dohodnou na podmínkách a lhůtě k odstranění nedostatků plnění Smlouvy ve smyslu tohoto odstavce, přičemž nedohodnou-li se Strany na konkrétní lhůtě, pak je Dodavatel povinen odstranit nedostatky do třiceti (30) dnů. V případě, že Dodavatel postupuje v rozporu s tímto článkem 21 ZOP, jakož i v případech, kdy Dodavatel včas neodstraní nedostatky ve smyslu předchozí věty tohoto odstavce, je Objednatel oprávněn od Smlouvy odstoupit.

21.26. Kontaktní osoby Stran vzájemně komunikují v průběhu plnění Smlouvy za účelem dosažení standardů pro bezpečnost informací. V případě ohrožení anebo porušení bezpečnosti informací, zejména v případě výskytu Kybernetického bezpečnostního incidentu, jsou kontaktní osoby povinny vzájemně komunikovat, ihned po zjištění takových skutečností hlásit jejich výskyt druhé Straně a společně podnikat kroky k zajištění obnovení bezpečnosti informací.

21.27. Objednatel si vyhrazuje možnost provedení pravidelného penetračního testování nebo testování zranitelností v průběhu trvání Smlouvy.

21.27.1. Dodavatel je povinen neprodleně přijmout dodatečná, účinná nápravná opatření k odstranění kritických zranitelností, které byly zjištěny v průběhu penetračního testování aplikace (a to na úrovni hardwaru i softwaru).

21.27.2. Pro odstranění případných pochybností, penetračním testováním je myšleno jakékoliv zkoumání informačního/počítačového systému s cílem najít slabá místa (zranitelnosti) Plnění. S výsledky penetračního testování mohou být seznámeny výhradně pověřené osoby Dodavatele a Objednatele.

21.27.3. Při realizaci penetračního testování nebo testování zranitelností řešení, poskytne Dodavatel Objednateli veškerou potřebnou součinnost.

21.27.4. V případě, že výsledkem penetračního testování nebo testování zranitelností jsou kritická zjištění zranitelností, je Dodavatel povinen neprodleně přijmout dodatečná, účinná nápravná opatření k odstranění těchto zranitelností.

21.27.5. V případě, že opakované penetrační testování, i přes ujištění Dodavatele o přijetí nápravných opatření k odstranění zranitelností, bude obsahovat totožné zranitelnosti, bude se Dodavatel podílet na finančních nákladech testování.

21.28. Dodavateli nenáleží za plnění povinností souvisejících s bezpečností informací ve smyslu článku 21. ZOP jakákoliv další odměna, resp. taková odměna je součástí Ceny.

21.29. **Významný dodavatel**

21.29.1. Je-li Dodavatel identifikován jako Významný dodavatel, je dále nad rámec povinností uvedených v odst. 21.1 až 21.28 ZOP povinen:

a. průběžně detekovat známé zranitelnosti dotčených aktiv Objednatele a bezodkladně na ně upozorňovat Objednatele;

b. umožnit přístup k auditním údajům aplikace Objednateli, a to v takové podobě, která je v souladu zejména s CEF, CEE či LEEF / Windows event log formát/databázové VIEW tak, aby je bylo možné strojově zpracovávat pomocí nástroje SIEM Objednatele;

c. na vyžádání Objednatele předat veškerá Data, provozní údaje a informace v otevřeném nebo standardizovaném formátu dostupném bez nutnosti pořízení proprietárního softwaru (zejména ve formátech CSV, XML, JSON, PDF/A, XLSX nebo jiném standardizovaném formátu příslušného prostředí), který umožňuje jejich okamžité využití v prostředí Objednatele „as is". Dodavatel je povinen předat tato Data spolu s nezbytnými metadaty, popisy datových struktur, technickou dokumentací a informacemi o integračních rozhraních, aby byla Data plně čitelná, interpretovatelná a použitelná bez závislosti na Dodavateli. Dodavatel zajistí, aby tyto podmínky předání Dat splňovaly požadavky VoKB na specifikaci podmínek pro formát předání dat a informací po vyžádání povinnou osobou.

d. poskytnout potřebnou součinnost na integraci auditních záznamů do systému bezpečnostního monitoringu (SIEM), systému pro správu logů a do centrálního úložiště logů Objednatele;

e. zajistit, aby Plnění využívalo procesy pro ověřování identity uživatelů a administrátorů, které jsou založeny na autentizačním mechanismu využívajícím multifaktorovou autentizaci (MFA) s nejméně dvěma různými typy faktorů. Procesy pro využívání identity uživatelů musí být kompatibilní se systémem řízení identit Objednatele;

f. poskytnout potřebnou součinnost na integraci procesů pro ověřování identity do systému řízení identit Objednatele;

g. zajistit, aby zaměstnanci Dodavatele s administrátorskými oprávněním využívali k přístupu do Kybernetického prostoru SŽ, výhradně bezpečný přístup založený na řešení PAM (Privileged Access Management);

h. poskytnout Objednateli veškeré potřebné informace a součinnost v procesu řízení a změn a jeho dokumentace v souladu s § 11 VoKB dle potřeb Objednatele (zejm. při posouzení, zda je změna Významnou změnou, analýze souvisejících rizik, přijímání opatření za účelem snížení všech nepříznivých dopadů spojených se změnami, aktualizaci bezpečnostní a provozní dokumentace, souvisejícím testováním, zajištění možnosti navrácení do původního stavu a provedení dalších činností dle VoKB), a současně zajistit, aby veškeré navrhované změny byly posuzovány, řízeny a dokumentovány v souladu s požadavky VoKB, zejména pravidly systému řízení bezpečnosti informací, řízení rizik, prováděním bezpečnostních opatření, vedením evidence změn, záznamů o testování a ověřování, kontrolou účinnosti přijatých opatření a pravidelnou aktualizací související dokumentace;

i. bezodkladně odstranit všechny relevantní zranitelnosti, které se vztahují k aplikaci a které mají hodnocení zranitelností založené na systému CVSS (Common Vulnerability Scoring System) vyšší než 8.0, a to včetně 8.0, který je zobrazován pomocí standardu CVE (Common Vulnerabilities and Exposures);

j. zpracovat a pravidelně aktualizovat bezpečnostní a provozní dokumentaci v rozsahu stanoveném ve Smlouvě;

k. neprovést žádnou Významnou změnu bez předchozího písemného schválení Objednatele. Dodavatel je dále povinen informovat Objednatele o každé změně, která může mít dopad na kybernetickou bezpečnost, před jejím provedením, a poskytnout podklady pro posouzení dopadů a hodnocení rizik;

l. průběžně detekovat známé zranitelnosti dotčených aktiv Objednatele a bezodkladně na ně upozorňovat Objednatele;

m. vést v elektronické formě provozní deník obsahující veškeré podstatné okolnosti související s plněním povinností Dodavatele ZOP a/nebo Plněním, provozní události důležitých aktiv a zpřístupnit jej Objednateli prostřednictvím zabezpečeného vzdáleného přístupu, není-li ve Smlouvě ujednán jiný způsob;

n. na vyžádání předložit Objednateli provozní deník a výstup z monitoringu dostupnosti, důvěrnosti a integrity aktiv Objednatele, se kterými pracuje v rámci plnění Smlouvy;

o. dodržovat pravidla a standardy bezpečného vývoje, a to v souladu s požadavky ZoKB a VoKB, přičemž je nezbytné, aby veškeré činnosti spojené s návrhem, vývojem, úpravami a implementací aplikace probíhaly na základě principů „security by design" a „security by default". Významný dodavatel je povinen používat uznávané bezpečnostní standardy bezpečného vývoje (např. OWASP, secure coding guidelines (standardizované postupy pro bezpečné programování), bezpečný životní cyklus vývoje aplikací - SDLC), zavádět kontrolní mechanismy pro předcházení vzniku zranitelností, provádět bezpečnostní revize kódu a testování zaměřené na bezpečnost, zajistit průběžné sledování rizik spojených s použitými komponentami a knihovnami a odstranit zjištěné nedostatky před předáním Objednateli. Současně je povinen vést a udržovat dokumentaci potvrzující splnění požadavků bezpečného vývoje tak, aby Objednatel mohl prokázat naplnění povinností podle ZoKB a navazujících prováděcích předpisů;

p. vést v elektronické formě přehled vykonávaných činností (výkaz) obsahující veškeré podstatné okolnosti související s plněním povinností Dodavatele z oblasti plnění Kybernetických požadavků a provozem aplikace, provozní události důležitých aktiv a relevantní záznamy o plnění povinností Dodavatele, a tyto předávat v rámci měsíčního vyúčtování služeb.

21.29.2. Pokud je v rámci Plnění dodávána aplikace, musí Významný dodavatel využívat nástroj pro centrální správu přístupový účtů. A dále musí Aplikace dodávaná Významným dodavatelem:

a. přidělit každému uživateli a administrátorovi přistupujícímu k informačnímu systému Objednatele přístupová práva a oprávnění a jedinečný identifikátor;

b. zajistit přístup na základě přidělených rolí a oprávnění;

c. zajistit, že přístupová oprávnění jsou šifrována pomocí odolných kryptografických algoritmů v souladu s aktuálními doporučeními NÚKIB.

21.30. **Dodavatel strategicky významné služby**

21.30.1. Je-li Dodavatel Dodavatelem strategicky významné služby, je dále nad rámec povinností uvedených v odst. 21.1 až 21.28 ZOP povinen:

a. poskytovat Objednateli veškerou potřebnou součinnost za účelem splnění jeho povinností coby poskytovatele Strategicky významné služby;

b. postupovat při plnění Smlouvy tak, aby byla zajištěna dostupnost Strategicky významné služby v nezbytném rozsahu, ve stanoveném čase a kvalitě z území České republiky;

c. v případě potřeby poskytnout Objednateli potřebnou součinnost při shromažďování dat za účelem prověřování rizik spojených s Dodavatelem strategicky významné služby;

d. strpět povinnosti, které na Objednatele klade ZoKB, spojené s prověřováním bezpečnosti dodavatelského řetězce;

e. zajišťovat Strategicky významnou službu v nezbytném rozsahu mimo území České republiky, kterou musí pravidelně testovat. Zprávu o výsledcích takových testování předloží Dodavatel Strategicky významné služby Objednateli.

21.31. Objednatel je oprávněn požadovat na **Dodavateli** zaplacení smluvní pokuty:

a. za každý den prodlení při zavedení bezpečnostních opatření podle ZoKB, VoKB, těchto ZOP a Interních předpisů:

i. ve výši 0,05 % z Ceny po dobu prvních pěti (5) dnů prodlení;

ii. ve výši 0,1 % z Ceny po dobu od šestého (6.) dne prodlení do desátého (10.) dne prodlení; a

iii. ve výši 0,2 % z Ceny po dobu od jedenáctého (11.) dne prodlení;

b. za každý den Objednatelem zjištěného soustavného porušování bezpečnostních opatření podle ZoKB, VoKB, těchto ZOP a Interních předpisů:

i. ve výši 0,05 % z Ceny do šestého (6.) dne soustavného porušování; a

ii. ve výši 0,1 % z Ceny od šestého (6.) dne soustavného porušování;

c. ve výši 2 % z Ceny za každý případ porušení povinnosti hlášení událostí, které mají charakter Kybernetického bezpečnostního incidentu;

d. ve výši 2 % z Ceny za každý případ neumožnění nebo odepření provedení kontroly a auditu kybernetické bezpečnosti ve smyslu článku 21. ZOP;

e. ve výši 5 % z Ceny za každý případ porušení článku 21. ZOP, přičemž toto porušení vedlo ke Kybernetickému bezpečnostnímu incidentu;

f. ve výši 0,1 % z Ceny za každý započatý den trvání porušení povinností Významného dodavatele dle článku 21. ZOP, kdy dané porušení nebylo odstraněno a negativní následek porušení povinnosti stále trvá;

g. ve výši 1 % z Ceny za každý případ jiného porušení článku 21. ZOP neuvedeného výše.

22. OCHRANA OSOBNÍCH ÚDAJŮ

22.1. Budou-li údaje, ke kterým Dodavatel získá přístup v souvislosti s Plněním dle Smlouvy, mít povahu Osobních údajů, je Dodavatel povinen přijmout veškerá opatření k tomu, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k těmto Osobním údajům, jejich změně, zničení či ztrátě, neoprávněným přenosům či jinému zneužití, a zajistit nakládání s Osobními údaji v souladu s GDPR.

22.2. Pokud bude v rámci provádění Plnění docházet ke zpracování Osobních údajů, je rozsah zpracovávaných Osobních údajů uveden ve Smlouvě. Pokud dojde v rámci poskytování Plnění ke zpracování Osobních údajů, které Smlouva výslovně neuvádí, budou tato nová zpracování Osobních údajů prováděna za stejných podmínek.

22.3. Dodavatel bude zpracovávat Osobní údaje pro Objednatele výhradně za účelem poskytování služeb v rozsahu ujednaném podle Smlouvy. Dodavatel bude pro Objednatele zpracovávat Osobní údaje výhradně za uvedeným účelem, způsobem a na základě doložených pokynů a podmínek Objednatele a v souladu s nimi tak, jak vyplývají ze Smlouvy. Dodavatel neprodleně informuje Objednatele, pokud jsou podle jeho názoru určité pokyny Objednatele v rozporu s účinnými právními předpisy.

22.4. Dodavatel se zavazuje přijmout vhodná technická a organizační opatření podle GDPR, které se na něj jako na zpracovatele vztahují, a plnění těchto povinností na vyžádání doložit Objednateli.

22.5. Dodavatel může předávat Osobní údaje do třetí země nebo mezinárodní organizaci ve smyslu GDPR pouze na základě zvláštního pokynu Objednatele. Je-li takovéto předání založeno na povinnosti vyplývající z práva Unie nebo členského státu, které se na Objednatele vztahuje,

informuje Dodavatel Objednatele o tomto právním požadavku před předáním, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu.

22.6. Dodavatel je povinen zajistit, aby se osoby oprávněné zpracovávat osobní údaje zavázaly zachovávat mlčenlivost ve vztahu ke všem Osobním údajům, které zpracovává na základě Smlouvy, a rovněž tak o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů.

22.7. Dodavatel je povinen přijmout všechna opatření dle čl. 32 GDPR tak, aby byla zajištěna odpovídající bezpečnost Osobních údajů. Dodavatel může do zpracování zapojit Poddodavatele pouze na základě předchozího písemného souhlasu Objednatele. Dodavatel se zavazuje s těmito Poddodavateli uzavřít smlouvu v souladu s GDPR zajišťující dodržování práv a povinností stanovených Smlouvou a/nebo těmito ZOP, zvláště pak povinnosti mlčenlivosti a zajištění bezpečnosti Osobních údajů a poskytnutí dostatečných záruk pro zavedení stejných technických a organizačních opatření Poddodavatelem, jakož i v souladu s dalšími aplikovatelnými právními předpisy. Dodavatel je dále povinen zohlednit povahu zpracování, být Objednateli nápomocen prostřednictvím vhodných technických a organizačních opatření pro splnění povinnosti Objednatele reagovat na žádost o výkon práv subjektu údajů dle GDPR.

22.8. Dodavatel je povinen být Objednateli nápomocen při zajišťování souladu s povinnostmi podle článku 32 až 36 GDPR, a to při zohlednění povahy zpracování informací, jež má Dodavatel k dispozici. V případech, kdy povaha věci vyžaduje informování Objednatele ze strany Dodavatele, informuje Dodavatel Objednatele bez zbytečného odkladu.

22.9. Dodavatel je povinen umožnit Objednateli a jím pověřené osobě během běžné pracovní doby Dodavatele provést v sídle Dodavatele kontrolu dodržování povinností týkajících se zpracování Osobních údajů vyplývajících ze Smlouvy, a to i po ukončení stanovené doby zpracování, tj. po ukončení této Smlouvy, a to do 3 měsíců od jejího ukončení.

22.10. Po ukončení zpracování Osobních údajů podle Smlouvy je Dodavatel povinen poskytnout Objednateli všechna Zařízení obsahující Osobní údaje, pokud je to možné, a vymazat všechny zpracovávané Osobní údaje ze všech svých systémů nebo databází, včetně vymazání všech záložních kopií, s výjimkou, kdy uchovávání vyžadují právní předpisy, nebo k tomu dal písemný souhlas Objednatel.

22.11. V případě, že Dodavatel zpracuje osobní údaje nad rámec vymezený Smlouvou/doloženými pokyny Objednatele, považuje se ve vztahu k takovému zpracování za správce. Pokud tímto zpracováním nad rámec vymezený Smlouvou/doloženými pokyny Objednatele vznikne Objednateli škoda, je Dodavatel povinen škodu uhradit.

22.12. Pokud Dodavatel poruší povinnost chránit Osobní údaje v souladu s tímto článkem, vzniká Objednateli nárok na zaplacení smluvní pokuty ve výši částky sankce případně uložené z tohoto důvodu Objednateli ze strany Úřadu pro ochranu osobních údajů či jiným správním orgánem, který bude v budoucnu vykonávat působnost Úřadu pro ochranu osobních údajů. Objednatel je však za předpokladu, že mu k tomu Dodavatel poskytne nezbytnou součinnost, povinen uplatnit v příslušných řízeních veškeré přiměřené námitky, které mohl uplatnit ve svém zájmu, a v rámci řízení je povinen řádně hájit svá práva.

23. OCHRANA DŮVĚRNÝCH INFORMACÍ

23.1. Dodavatel se zavazuje zachovávat mlčenlivost o všech Důvěrných informacích, které získal nebo mu byly poskytnuty či zpřístupněny v souvislosti s plněním povinnosti dle Smlouvy, a uchovávat je v tajnosti.

23.2. Dodavatel se zavazuje použít Důvěrné informace pouze k plnění svých povinností vyplývajících ze Smlouvy. Dodavatel nesmí použít Důvěrné informace k jinému účelu.

23.3. Dodavatel nesmí bez předchozího písemného souhlasu Objednatele zpřístupnit Důvěrné informace žádné třetí osobě, a to v jakékoli formě. To neplatí u Důvěrných informací, ohledně kterých byla Dodavateli pravomocným rozhodnutím soudu, správního orgánu, či jiného příslušného státního orgánu v konkrétním případě uložena povinnost Důvěrnou informaci poskytnout nebo plyne-li taková povinnost Dodavateli z právního předpisu.

23.4. Dodavatel nesmí Důvěrné informace bez předchozího písemného souhlasu Objednatele rozmnožovat, kopírovat či jakýmkoliv jiným způsobem reprodukovat. Dodavatel dále nesmí Důvěrné informace bez předchozího písemného souhlasu Objednatele uchovávat v jakékoliv databázi, počítačovém programu, úložišti či na datovém nosiči, vyjma případů, kdy je takové uchovávání Důvěrných informací nezbytné pro účel vyplývající ze Smlouvy.

23.5. Dodavatel se zavazuje provést technická, organizační, právní a personální opatření, kterými zajistí dodržování povinnosti zachovat mlčenlivost o Důvěrných informacích a uchovat Důvěrné informace v tajnosti v rozsahu podle tohoto článku i ze strany svých zaměstnanců, Poddodavatelů, jakož i dalších osob, kterým budou Důvěrné informace poskytnuty či zpřístupněny.

23.6. Objednatel je oprávněn kdykoliv kontrolovat řádné plnění povinností Dodavatele uvedených v tomto článku, k čemuž se Dodavatel zavazuje bez zbytečného odkladu poskytnout Objednateli veškerou součinnost, zejména je Objednatel oprávněn kontrolovat řízení bezpečnosti Důvěrných informací Dodavatelem. V případě, že Objednatel vyzve Dodavatele na základě kontroly k nápravě, je Dodavatel povinen takové výzvě vyhovět v Objednatelem stanovené přiměřené lhůtě.

23.7. Dodavatel se během poskytování Plnění pro Objednatele zavazuje informovat Objednatele o fyzických osobách přicházejících do kontaktu s Důvěrnými informacemi Objednatele (jedná se například o osoby zastávající bezpečnostní role, penetrační testery a administrátory apod.).

23.8. Objednatel je oprávněn požadovat na Dodavateli zaplacení smluvní pokuty:

a. ve výši 500 000 Kč za každé jednotlivé jednání, které představuje porušení jakékoli z povinností Dodavatele dle tohoto článku, vyjma povinností stanovených v odst. 23.6. ZOP

b. ve výši 100 000 Kč za každé jednotlivé jednání, které představuje porušení jakékoli z povinností stanovených v odst. 23.6. ZOP.

SPRÁVA ŽELEZNIC

Příloha č. 7 Smlouvy

Obchodní podmínky ke Smlouvě o dílo

OBSAH OBCHODNÍCH PODMÍNEK

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČ: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

ČÁST 1 - ÚVODNÍ USTANOVENÍ

1. Pro účely těchto Obchodních podmínek mají následující slova význam u nich uvedený:
   - 1.1. **Občanský zákoník** – zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.
   - 1.2. **ZoDPH** – zákon č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.
   - 1.3. **ZoÚ** – zákon č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů.
   - 1.4. **SZ** – zákon č. 283/2021 Sb., stavební zákon, ve znění pozdějších předpisů.
   - 1.5. **ZZVZ** – zákon č. 134/2016 Sb., o zadávání veřejných zakázkách, ve znění pozdějších předpisů.
   - 1.6. **Objednatel** – Správa železnic, státní organizace, IČO 70994234, se sídlem Praha 1 – Nové Město, Dlážděná 1003/7, PSČ 110 00, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze pod sp. zn. A 48384.
   - 1.7. **Zhotovitel** – osoba uvedená ve Smlouvě o dílo jako Zhotovitel; též všechny osoby, které jsou ve Smlouvě o dílo uvedené na straně Zhotovitele, je-li na straně Zhotovitele více než jedna osoba.
   - 1.8. **Smluvní strany** – Objednatel a Zhotovitel.
   - 1.9. **Smluvní strana** – Objednatel nebo Zhotovitel dle smyslu ujednání.
   - 1.10. **Nabídka** – souhrn dokumentů, které Zhotovitel podal jako návrh do zadávacího řízení, na jehož základě byla uzavřena Smlouva o dílo.
   - 1.11. **Smlouva o dílo** – smlouva uzavřená mezi Smluvními stranami, která odkazuje na Obchodní podmínky.
   - 1.12. **Obchodní podmínky** – tento text obchodních podmínek.
   - 1.13. **Předmět díla** – věc, která má být zhotovena, nebo činnost s jiným výsledkem, specifikovaná ve Smlouvě o dílo.
   - 1.14. **Související plnění** – další plnění (práce, dodávky, služby, činnosti a výkony), která je Zhotovitel povinen dle Smlouvy o dílo poskytnout vedle samotného provedení Předmětu díla.
   - 1.15. **Rozhodnutí Objednatele** – veškerá rozhodnutí, sdělení, souhlasy, povolení či jiné výsledky úkonů orgánů státní správy, samosprávy či jiných subjektů, které pro účely Díla nebo v souvislosti s ním získal nebo do doby dokončení Díla získá Objednatel a jež Objednatel Zhotoviteli předal nebo s nimiž se Zhotovitel jinak seznámil.
   - 1.16. **Rozhodnutí Zhotovitele** – veškerá rozhodnutí, sdělení, souhlasy, povolení či jiné výsledky úkonů orgánů státní správy, samosprávy či jiných subjektů, které je Zhotovitel povinen dle Smlouvy o dílo získat. Jakékoliv Rozhodnutí Zhotovitele, které není v českém jazyku, musí být do českého jazyka přeloženo a překlad musí být úředně ověřen.
   - 1.17. **Veřejnoprávní podklady** – souhrn Rozhodnutí Objednatele a Rozhodnutí Zhotovitele.
   - 1.18. **Doklady** – veškeré listiny, které se vztahují k Předmětu díla nebo Souvisejícímu plnění a které jsou třeba k jejich převzetí a užívání; veškerá Rozhodnutí Zhotovitele; veškeré další listiny, vyjma Výzvy k úhradě, které je Zhotovitel dle Smlouvy o dílo povinen předat Objednateli. Všechny Doklady musejí být v českém jazyku, nebo v původním jazyku s překladem do českého jazyka, není-li uvedeno jinak.
   - 1.19. **Dílo** – souhrn veškerých plnění, která je Zhotovitel povinen provést za účelem splnění Smlouvy o dílo; zahrnuje zejm. provedení Předmětu díla, poskytnutí či provedení Souvisejícího plnění a dodání Dokladů.
   - 1.20. **Cena díla** – cena za Dílo sjednaná ve Smlouvě o dílo (částka bez DPH).
   - 1.21. **Výzva k úhradě** – daňový doklad, je-li Zhotovitel povinen dle ZoDHP uhradit v souvislosti s provedením Díla nebo jeho části DPH, nebo faktura, pokud Zhotovitel v souvislosti s provedením Díla nebo jeho části není dle ZoDPH povinen uhradit DPH.

1.22. **Vícepráce** – práce, dodávky nebo služby nad rámec Smlouvy o dílo, na jejichž provedení se Smluvní strany dohodnou po uzavření Smlouvy o dílo.
1.23. **Méněpráce** – práce, dodávky nebo služby v rámci Smlouvy o dílo, na jejichž vypuštění se Smluvní strany dohodnou po uzavření Smlouvy o dílo.
1.24. **Obalový materiál** – palety, dřevěné desky či jiné věci, které slouží pro potřeby přepravy nebo ochrany Předmětu díla. Dle kontextu Smlouvy o dílo se rozumí Obalovým materiálem též jednotlivý kus palety, dřevěné desky nebo jiné věci.
1.25. **Přejímací řízení** – proces, při kterém Zhotovitel předává a Objednatel kontroluje a přebírá Dílo, nebo je odmítá.
1.26. **Předávací protokol** – listina osvědčující předání a převzetí Díla nebo jeho části, jejíž minimální náležitosti jsou uvedeny v části Předání a převzetí Díla.
1.27. **Záruční doba** – doba, do jejíhož uplynutí je Objednatel oprávněn uplatňovat práva z vad plnění poskytnutého Zhotovitelem na základě Smlouvy o dílo; Záruční doba činí 24 měsíců.
1.28. **CTD** – Centrum techniky a diagnostiky, organizační jednotka Objednatele.

ČÁST 2 - NÁVRH NA UZAVŘENÍ SMLOUVY O DÍLO

2. Odpověď Smluvní strany na návrh na uzavření Smlouvy o dílo učiněný druhou Smluvní stranou, která vymezuje obsah návrhu jinými slovy nebo která obsahuje jakékoliv, byť nepodstatné, dodatky, odchylky, výhrady nebo omezení není přijetím návrhu.
3. I pozdní přijetí návrhu na uzavření Smlouvy o dílo má účinky včasného přijetí, pokud navrhující Smluvní strana bez zbytečného odkladu alespoň ústně vyrozumí druhou Smluvní stranu, že přijetí považuje za včasné, nebo pokud se začne chovat ve shodě s návrhem.
4. Plyne-li z písemnosti, která vyjadřuje přijetí návrhu na uzavření Smlouvy o dílo, že byla odeslána za takových okolností, že by došla navrhující Smluvní straně včas, kdyby její přeprava probíhala obvyklým způsobem, má pozdní přijetí účinky včasného přijetí, ledaže navrhující Smluvní strana bez odkladu vyrozumí alespoň ústně druhou Smluvní stranu, že považuje návrh za zaniklý.
5. Bez ohledu na jakékoliv okolnosti nelze přijmout návrh na uzavření Smlouvy o dílo tak, že se Smluvní strana, jíž je návrh určen, podle návrhu zachová.
6. **Odkáží-li Smluvní strany v návrhu na uzavření Smlouvy o dílo i v přijetí návrhu na obchodní podmínky, které si odporují, je Smlouva o dílo přesto uzavřena s obsahem určeným v tom rozsahu, v jakém obchodní podmínky nejsou v rozporu; to platí i v případě, že to obchodní podmínky vylučují. Vyloučí-li to některá ze Smluvních stran nejpozději bez zbytečného odkladu po výměně projevů vůle, Smlouva o dílo uzavřena není.**
7. Smlouva o dílo může být uzavřena pouze v písemné podobě.

ČÁST 3 - DÍLO

8. Zhotovitel se zavazuje provést na svůj náklad a nebezpečí pro Objednatele Dílo a Objednatel se zavazuje Dílo převzít a zaplatit Zhotoviteli Cenu díla a příslušnou DPH, bude-li Zhotovitel povinen dle ZoDHP uhradit v souvislosti s provedením Díla nebo jeho části DPH.
9. Zhotovitel je povinen provést Dílo v jakosti, provedení a způsobem uvedeným ve Smlouvě o dílo a zároveň
   9.1. v jakosti, provedení a způsobem, jenž odpovídá vlastnostem a způsobu, které Zhotovitel popsal nebo které Objednatel očekával s ohledem na povahu Díla, a to v rozsahu, ve kterém není v rozporu s jakostí, provedením a způsobem sjednaným ve Smlouvě o dílo,
   9.2. v jakosti, provedení a způsobem, jenž se hodí k účelu vyplývajícímu ze Smlouvy o dílo a není-li v ní vyjádřen pak k účelu, ke kterému se Dílo obvykle používá, a to v rozsahu, ve kterém není v rozporu s jakostí, provedením a způsobem sjednaným ve Smlouvě o dílo,

9.3. v souladu s Veřejnoprávními podklady,
9.4. v souladu s požadavky právních předpisů a příslušných ČSN.

10. Je-li jakost či provedení Předmětu díla zároveň určeno vzorkem nebo předlohou, musí Předmět díla odpovídat jakostí nebo provedením vzorku nebo předloze. Liší-li se jakost nebo provedení určené ve Smlouvě o dílo a vzorek nebo předloha, rozhoduje Smlouva o dílo. Určuje-li Smlouva o dílo a vzorek nebo předloha jakost nebo provedení rozdílně, nikoliv však rozporně, musí Předmět díla odpovídat Smlouvě o dílo i vzorku nebo předloze.
11. Opatřuje-li Zhotovitel věc za účelem jejího zpracování při provádění Díla, je povinen opatřit věc novou, nepoužitou a neopotřebovanou.
12. Je-li součástí Díla povinnost Zhotovitele zajistit jakékoliv Rozhodnutí Zhotovitele, je Zhotovitel povinen provést veškeré činnosti, kterých je k získání příslušného Rozhodnutí Zhotovitele třeba.

ČÁST 4 - CENA DÍLA

13. Cena díla zahrnuje veškeré náklady Zhotovitele spojené se splněním jeho povinností vyplývajících ze Smlouvy o dílo a Obchodních podmínek a zisk Zhotovitele.
14. Objednatel není povinen hradit v souvislosti se Smlouvou o dílo žádné jiné finanční částky, než Cenu díla a případně příslušnou DPH, není-li uvedeno jinak (tím není dotčeno právo Zhotovitele na případnou úhradu smluvní pokuty, úroků z prodlení, či jiných sankcí, a právo na náhradu škody způsobené Objednatelem).
15. Cena díla obsahuje předpokládaný vývoj cen vstupních nákladů a předpokládané zvýšení ceny v závislosti na čase plnění, a to až do dokončení Díla.
16. Je-li Zhotovitel povinen dle ZoDHP uhradit v souvislosti s provedením Díla nebo jeho části DPH, je Objednatel povinen Zhotoviteli takovou DPH uhradit vedle Ceny díla.
17. Cenu díla lze měnit pouze za podmínek uvedených v části Změna ceny Díla (viz ČÁST 5 - Obchodních podmínek).
18. Konečné finanční částky na fakturách/daňových dokladech nesmí být zaokrouhlovány na celé Kč. Objednatel nebude akceptovat zaokrouhlení a haléřové vyrovnání v případě uvedení na faktuře/daňovém dokladu nebude hradit.

ČÁST 5 - ZMĚNA CENY DÍLA

19. Změna ceny díla je možná pouze v případě
    19.1. víceprací nebo méněprací,
    19.2. zjistí-li Zhotovitel při kontrole projektové dokumentace předané mu Objednatelem vady nebo její nevhodnost či neúplnost, které mají vliv na náklady Zhotovitele,
    19.3. v jiných případech jen pokud se na tom Smluvní strany dohodnou.
20. V případě víceprací i méněprací Zhotovitel provede ocenění jejich soupisu jednotkovými cenami položkového rozpočtu, je-li ve Smlouvě o dílo zahrnut.
21. Pokud práce, dodávky nebo služby nebudou v položkovém rozpočtu obsaženy nebo položkový rozpočet není ve Smlouvě o dílo zahrnut, užije se pro jejich ocenění cena obvyklá.
22. V případě vad, nevhodnosti nebo neúplnosti projektové dokumentace, kterou předal Objednatel Zhotoviteli, je-li taková projektová dokumentace součástí Smlouvy o dílo, mají-li takové vady, nevhodnosti nebo neúplnosti vliv na náklady Zhotovitele, postupují smluvní strany obdobně jako při oceňování víceprací nebo méněprací.
23. Změnu Ceny díla lze provést jen uzavřením dodatku ke Smlouvě o dílo.

ČÁST 6 - PLATEBNÍ PODMÍNKY

24. Objednatel neposkytuje zálohy.
25. Zhotovitel vyúčtuje Objednateli Cenu díla a případnou DPH Výzvou k úhradě.

26. Cenu díla a případnou DPH je Objednatel povinen uhradit Zhotoviteli do 60 dnů ode dne převzetí Díla; má-li být dle Smlouvy o dílo proveden též zkušební provoz, pak do 60 dnů ode dne úspěšného ukončení zkušebního provozu, nastane-li den skončení zkušebního provozu později než převzetí Díla Objednatelem.
27. Cena díla a případná DPH je uhrazena dnem jejich odepsání z bankovního účtu Objednatele.
28. Je-li Výzva k úhradě fakturou, musí obsahovat náležitosti účetního dokladu dle §11 ZoÚ a náležitosti stanovené v §435 Občanského zákoníku.
29. Je-li Výzva k úhradě daňovým dokladem, musí obsahovat náležitosti daňového dokladu dle §28 ZoDPH a náležitosti stanovené v §435 Občanského zákoníku.
30. Výzva k úhradě musí vždy obsahovat číslo Smlouvy o dílo, včetně uvedení uzavřených dodatků, její přílohou musí být vždy jedno vyhotovení Protokolu o převzetí potvrzeného Objednatelem. Ve výzvě k úhradě musí být vždy uvedeny jako identifikace Objednatele nejméně následující údaje:
    Správa železnic, státní organizace
    Dlážděná 1003/7, 110 00 Praha 1 – Nové Město
    IČO: 709 94 234
    Obchodní rejstřík u Městského soudu v Praze, sp. zn. A 48384
31. Výzvu k úhradě je Zhotovitel povinen doručit Objednateli nejpozději 15 dnů před uplynutím doby uvedené v odstavci 26 Obchodních podmínek.
32. Výzvy k úhradě, vč. všech příloh, budou Objednateli zasílány následovně:
    32.1. v digitální podobě na e-mailovou adresu ePodatelnaCFU@spravazeleznic.cz, nebo
    32.2. v digitální podobě do datové schránky s identifikátorem Uccchjm, nebo
    32.3. v listinné podobě **ve dvou vyhotoveních** na adresu Správa železnic, státní organizace, Centrální finanční účtárna Čechy, Náměstí Jana Pernera 217, 530 02 Pardubice, nebo
    32.4. prostřednictvím kontaktního formuláře na webových stránkách Objednatele https://www.spravazeleznic.cz/kontakty/podatelna.

    Objednatel upřednostňuje příjem Výzev k úhradě v digitální podobě ve formátu PDF/A, ISO 19005, min. verze PDF/A-2b, na výše uvedené emailové adrese. **V případě, že je Výzva k úhradě zasílána na výše uvedenou e-mailovou adresu, považuje se za doručenou po obdržení notifikace doručení, která je automaticky odesílána odesílateli**.

33. Splatnost Výzvy k úhradě musí být stanovena tak, aby nenastala dříve, než uplyne doba stanovená v odstavci 26 Obchodních podmínek.
34. Stanoví-li Výzva k úhradě splatnost delší, než je jako minimální stanovena v předchozím odstavci, je Objednatel oprávněn uhradit Cenu díla a případnou DPH ve lhůtě splatnosti určené ve Výzvě k úhradě.
35. Stane-li se zhotovitel nespolehlivým plátcem nebo daňový doklad zhotovitele bude obsahovat číslo bankovního účtu, na který má být plněno, aniž by bylo uvedeno ve veřejném registru spolehlivých účtů, je objednatel oprávněn z finančního plnění uhradit daň z přidané hodnoty přímo místně a věcně příslušnému správci daně zhotovitele.
36. Je-li ve Smlouvě o dílo výslovně stanoveno, že Zhotovitel bude předávat Objednateli Dílo po částech, je Zhotovitel oprávněn vystavit Výzvu k úhradě předávané části Díla poté, co Objednatel převezme příslušnou část Díla. Ustanovení odstavců 26 - 35 Obchodních podmínek se užijí obdobně.
37. Ustanovení §2611, §2620–2622 a §2624 Občanského zákoníku se neužijí.

ČÁST 7 - MÍSTO PLNĚNÍ

38. Zhotovitel je povinen předat Objednateli Dílo v místě, jež vyplývá ze Smlouvy o dílo. Nelze-li takto místo předání Díla zjistit, vyzve Zhotovitel Objednatele, aby sdělil, ve kterém místě má Zhotovitel Objednateli Dílo předat. Nesdělí-li Objednatel místo plnění do 5 pracovních dnů ode dne doručení výzvy Zhotovitele, je Zhotovitel povinen Dílo předat Objednateli v sídle Objednatele.

ČÁST 8 - DOBA PLNĚNÍ

39. Zhotovitel je povinen zahájit provádění Díla bez zbytečného odkladu po uzavření Smlouvy o dílo.
40. Je-li součástí povinností Zhotovitele doprava Díla po jeho zhotovení do místa plnění dle Smlouvy o dílo, je Zhotovitel povinen dopravit Dílo do místa plnění v pracovní den v době od 8 do 15 hodin. Dodá-li Zhotovitel Dílo Objednateli v jiné než uvedené době, je Objednatel oprávněn odmítnout Dílo převzít a není zároveň v prodlení s převzetím Díla. Připadne-li konec sjednané doby plnění na sobotu, neděli nebo svátek, není Zhotovitel v prodlení, dodá-li Dílo nejblíže následující pracovní den v časovém rozmezí dle tohoto odstavce.
41. Není-li stanoveno jinak, je Zhotovitel povinen začít s plněním svých povinností vždy bez zbytečného odkladu.
42. Zjistí-li Zhotovitel jakékoliv skutečnosti, které by mohly mít vliv na dobu plnění, je Zhotovitel povinen bez zbytečného odkladu Objednatele o takových skutečnostech informovat.

ČÁST 9 - PROVÁDĚNÍ DÍLA

43. Zhotovitel provede Dílo s potřebnou péčí v ujednaném čase a obstará vše, co je k provedení Díla potřeba.
44. Při provádění Díla postupuje Zhotovitel samostatně, je však vázán příkazy Objednatele ohledně způsobu provádění Díla.
45. Zhotovitel se zavazuje brát v úvahu veškeré upozornění Objednatele, týkající se realizace Díla a upozorňující na možné porušování smluvních i právními předpisy stanovených povinností Zhotovitele.
46. Zhotovitel je povinen upozornit Objednatele bez zbytečného odkladu na nevhodnou povahu věcí převzatých od Objednatele nebo příkazů daných mu Objednatelem k provedení Díla, jestliže Zhotovitel mohl tuto nevhodnost zjistit při vynaložení odborné péče.
47. Překáží-li nevhodná věc nebo příkaz v řádném provádění Díla, Zhotovitel jej v nezbytném rozsahu přeruší až do výměny věci nebo změny příkazu; trvá-li Objednatel na provádění Díla s použitím předané věci nebo podle daného příkazu, má Zhotovitel právo požadovat, aby tak Objednatel učinil v písemné formě.
48. Doba stanovená pro dokončení Díla se prodlužuje o dobu vyvolanou přerušením dle předchozího odstavce.
49. Trvá-li Objednatel na provádění Díla s použitím předané věci nebo podle daného příkazu a zachová-li se Zhotovitel podle toho, nemá Objednatel práva z vady Díla vzniklé pro nevhodnost věci nebo příkazu.

Harmonogram

50. Je-li dle Smlouvy o dílo vyžadován Harmonogram provádění Díla, je Zhotovitel povinen jej předložit Objednateli bez zbytečného odkladu po uzavření Smlouvy o dílo, nejpozději však do 10 dnů ode dne uzavření Smlouvy o dílo.
51. Zhotovitel je povinen udržovat harmonogram v aktuálním stavu a v případě změny vždy předat Objednateli bezodkladně aktualizovaný harmonogram.

Kontrola provádění prací

52. Objednatel je oprávněn kontrolovat provádění Díla. Zjistí-li objednatel, že Zhotovitel provádí Dílo v rozporu s povinnostmi vyplývajícími ze Smlouvy o dílo, Obchodních podmínek, Veřejnoprávních podkladů, právních předpisů nebo příslušných ČSN, je Objednatel oprávněn dožadovat se toho, aby Zhotovitel odstranil vady vzniklé vadným prováděním a Dílo prováděl řádným způsobem. Jestliže tak Zhotovitel neučiní v přiměřené lhůtě, jedná se o podstatné porušení Smlouvy o dílo.
53. Zhotovitel je povinen písemně vyzvat Objednatele ke kontrole a prověření prací, které v dalším postupu budou zakryty nebo se stanou nepřístupnými. Zhotovitel je povinen vyzvat Objednatele nejméně 3 pracovní dny před termínem, v němž budou předmětné práce zakryty nebo znepřístupněny.

54. Před zakrytím nebo znepřístupněním prací je Zhotovitel povinen pořídit podrobnou fotodokumentaci prací a předat ji Objednateli v digitální podobě na CD nebo DVD nosiči bez zbytečného odkladu po pořízení fotodokumentace.
55. Pokud se Objednatel ke kontrole přes včasné písemné vyzvání nedostaví, je Zhotovitel oprávněn předmětné práce zakrýt. Bude-li se v tomto případě Objednatel dodatečně požadovat jejich odkrytí, je Zhotovitel povinen toto odkrytí provést na náklady Objednatele. Pokud se však zjistí, že práce nebyly řádně provedeny, nese veškeré náklady spojené s odkrytím prací, opravou chybného stavu a následným zakrytím Zhotovitel.
56. Obdobně bude-li Objednatel požadovat vykonání zvláštních zkoušek nebo ověření jakékoliv části Díla z důvodu podezření, že tato část Díla neodpovídá Smlouvě o dílo, Obchodním podmínkám, Veřejnoprávním podkladům, právním předpisům nebo příslušným ČSN, a bude-li zjištěno, že podezření bylo správné, nese náklady spojené s vykonáním zkoušek nebo ověřením Zhotovitel.
57. Zhotovitel je povinen umožnit výkon technického a autorského dozoru.

Kontrolní dny

58. Pro účely kontroly průběhu provádění Díla může Objednatel nebo jím pověřená osoba provést kontrolní dny v termínech nezbytných pro řádné provádění kontroly.
59. Kontrolních dnů se zúčastní zástupci Objednatele případně osob vykonávajících funkci technického dozoru a autorského dozoru.
60. Zástupci Zhotovitele jsou povinni se kontrolních dnů zúčastňovat. Zhotovitel má právo přizvat na kontrolní den své poddodavatele podílející se v souladu se Smlouvou o dílo a Obchodními podmínkami na provádění Díla.
61. Kontrolní dny vede Objednatel nebo jím pověřená osoba.
62. Obsahem kontrolního dne je zejména zpráva Zhotovitele o postupu prací, kontrola postupu prací, připomínky a podněty osob vykonávajících funkci technického a autorského dozoru a stanovení případných nápravných opatření a úkolů.
63. Objednatel nebo jím pověřená osoba pořizuje z kontrolního dne zápis, který předá všem zúčastněným.

Dodržování zákazu požívání alkoholických nápojů a užívání jiných návykových látek

64. Objednatel je oprávněn provádět u všech osob, které Zhotovitel používá při provádění díla, kontrolu, zda tyto osoby nejsou pod vlivem alkoholu nebo návykové látky.
65. Kontrola bude prováděna dle Směrnice SŽDC č. 120 Dodržování zákazu kouření, požívání alkoholických nápojů a užívání jiných návykových látek, č.j. 36503/2017-SŽDC-GŘ-O10 ze dne 3.11.2017, účinné od 7.11.2017 nebo dle jiného předpisu, který uvedenou směrnici případně nahradí.
66. Výše uvedená Směrnice je pro Zhotovitele a všechny osoby, které Zhotovitel používá při provádění Předmětu Díla závazná okamžikem platnosti a účinnosti Smlouvy o dílo. Zhotovitel a tím i všechny osoby, které Zhotovitel používá při provádění Předmětu Díla, se zavazují poskytnout Objednateli veškerou součinnost v souladu s výše uvedenou směrnicí.

Dodržování podmínek stanovisek příslušných orgánů a organizací

67. Zhotovitel se zavazuje dodržet při provádění Díla veškeré podmínky vyplývající z Veřejnoprávních podkladů.
68. Pokud nesplněním těchto podmínek vznikne Objednateli škoda, je Zhotovitel povinen nahradit škodu v plném rozsahu, ledaže prokáže, že škodě nemohl zabránit ani v případě vynaložení veškeré možné péče, kterou na něm lze spravedlivě požadovat.

Použité materiály a výrobky

69. Zhotovitel se zavazuje a odpovídá za to, že při realizaci Díla nepoužije žádný materiál, o kterém je v době jeho užití známo, že je škodlivý. Pokud tak Zhotovitel učiní, je povinen na vyzvání Objednatele provést nápravu, přičemž veškeré náklady s tím spojené nese Zhotovitel.
70. Zhotovitel se zavazuje, že k realizaci Díla nepoužije materiály, které nemají požadovanou certifikaci či předepsaný průvodní doklad, je-li to pro jejich použití nezbytné podle Smlouvy o dílo, Obchodních podmínek, Veřejnoprávních podkladů, právních předpisů nebo

příslušných ČSN. Certifikace a průvodní doklady Zhotovitele použitých materiálů jsou součástí Dokladů.

Částečné plnění

71. Nabízí-li Zhotovitel Objednateli částečné plnění Předmětu díla, aniž by částečné plnění bylo výslovně sjednáno ve Smlouvě o dílo, není Objednatel povinen částečné plnění přijmout. Přijme-li Objednatel částečné plnění, je Zhotovitel povinen nahradit Objednateli zvýšené náklady způsobené mu částečným plněním.

Ostatní ujednání

72. Vícepráce lze provést a méněpráce neprovést až poté, co budou vícepráce nebo méněpráce dohodnuty včetně změn Ceny díla dodatkem ke Smlouvě o dílo. Provede-li Zhotovitel vícepráce v rozporu s tímto odstavcem, ponese náklady na ně ze svého.
73. Dojde-li k jakémukoliv úrazu při provádění Díla nebo při činnostech souvisejících s prováděním Díla je Zhotovitel povinen zabezpečit vyšetření úrazu a sepsání příslušného záznamu. Objednatel je povinen poskytnout Zhotoviteli nezbytnou součinnost.
74. Žádný z podkladů, které Zhotovitel převzal od Objednatele v souvislosti s Dílem ani žádný Doklad není Zhotovitel oprávněn bez předchozího písemného svolení Objednatele užít k jiným účelům, než je provedení Díla, zejména je nesmí poskytnout třetím osobám.
75. Zhotovitel je povinen při provádění Díla postupovat v součinnosti s případnými jinými dodavateli Objednatele, a to dle pokynů udělených Objednatelem a nebudou-li pokyny uděleny, postupovat tak, aby umožnil ostatním dodavatelům v co největší míře plnit jejich závazky.
76. Objednatel se zavazuje poskytovat Zhotoviteli součinnost při provádění Díla v rozsahu a způsobem, ve kterém lze tuto součinnost po Objednateli spravedlivě požadovat. Bude-li Zhotovitelem požadována po Objednateli jakákoliv součinnost dle předchozí věty, je Zhotovitel povinen Objednatele k jejímu poskytnutí s dostatečným předstihem vyzvat a ve výzvě ji dostatečně specifikovat.
77. Zhotovitel na sebe přebírá nebezpečí změny okolností ve smyslu §1765 Občanského zákoníku.
78. Ustanovení §1912, §2595 Občanského zákoníku se neužijí.

ČÁST 10 - ZKUŠEBNÍ PROVOZ

79. Ustavení této části se užijí v případě, že ze Smlouvy o dílo nebo z povahy Předmětu díla vyplývá, že má být proveden zkušební provoz.
80. Zkušebním provozem se prověřuje, zda Předmět díla je za předpokládaných provozních a výrobních podmínek schopen dosahovat výkonů (parametrů) v kvalitě a množství stanovených Smlouvou o dílo, Obchodními podmínkami, Veřejnoprávními podklady, právními předpisy a příslušnými ČSN.
81. Zkušební provoz je Zhotovitel povinen provést před předáním Díla Objednateli, do doby úspěšného provedení zkušebního provozu není Dílo dokončeno.
82. Zkušební provoz musí trvat minimálně 48 hodin, nestanoví-li Veřejnoprávní podklady, právní předpisy nebo příslušné ČSN jinak.
83. Zhotovitel se zavazuje v průběhu zkušebního provozu neprodleně odstraňovat veškeré vady, které bude Předmět díla vykazovat.
84. Zkušební provoz bude úspěšně proveden, nebude-li Předmět díla k poslednímu dni doby stanovené pro zkušební provoz vykazovat vady bránící jeho užívání.
85. Bude-li k poslednímu dni doby zkušebního provozu Předmět díla vykazovat vady bránící užívání, prodlužuje se délka trvání zkušebního provozu o dobu dle dohody Smluvních stran, jinak o 24 hodin.
86. Úspěšné provedení zkušebního provozu je podmínkou převzetí díla Objednatelem.

ČÁST 11 - PŘEPRAVA DÍLA

87. Ustavení této části se užijí v případě, je-li Dílo po svém zhotovení za účelem předání Objednateli přepravováno.

88. Je-li dle Smlouvy o dílo nebo zvyklostí třeba Předmět díla zabalit, Zhotovitel Předmět díla zabalí dle Smlouvy o dílo; není-li ujednání o balení Předmětu díla ve Smlouvě o dílo, pak dle zvyklostí, a není-li jich, pak způsobem potřebným pro uchování Předmětu díla a jeho ochranu.
89. Jestliže Zhotovitel označí Obalový materiál nejpozději do doby převzetí Předmětu díla Objednatelem jako vratný, a to přímo na Obalovém materiálu, v Dokladech nebo jiným zřejmým způsobem, ze kterého bude zřejmé, který Obalový materiál je vratný, je Objednatel oprávněn předat Zhotoviteli při předávacím řízení (viz ČÁST 13 - Obchodních podmínek) stejné množství Obalového materiálu téhož druhu a srovnatelného nebo nižšího stupně opotřebení. V rozsahu předání Obalového materiálu Objednatelem Zhotoviteli dle předchozí věty zaniká právo Zhotovitele na vrácení Obalového materiálu.
90. V rozsahu, v němž Objednatel nevrátí vratný Obalový materiál Zhotoviteli dle předchozího odstavce, je Zhotovitel oprávněn Objednateli vyúčtovat zálohu na vratný Obalový materiál. Výše zálohy nesmí přesáhnout dvojnásobek pořizovací ceny Obalového materiálu.
91. Doposud nevrácený vratný Obalový materiál je Objednatel povinen na vlastní náklady dopravit do sídla Zhotovitele, a to nejpozději do jednoho roku od převzetí Předmětu díla Objednatelem. Objednatel je oprávněn nahradit nevrácený vratný Obalový materiál Obalovým materiálem stejného druhu a srovnatelného nebo nižšího stupně opotřebení. Bez zbytečného odkladu po převzetí vráceného Obalového materiálu nebo jeho náhrady Zhotovitelem, je Zhotovitel povinen vrátit Objednateli zaplacenou zálohu na vratný Obalový materiál. Nevrátí-li Objednatel dosud nevrácený vratný Obalový materiál nebo Obalový materiál stejného druhu a srovnatelného nebo nižšího stupně opotřebení ani do dvou let od převzetí Předmětu díla Objednatelem, stává se nevrácený vratný Obalový materiál vlastnictvím Objednatele a složená záloha se stává vlastnictvím Zhotovitele.
92. Pokud Zhotovitel Předmět díla Objednateli odesílá prostřednictvím dopravce, umožní Zhotovitel Objednateli uplatnit práva z přepravní smlouvy vůči dopravci, pokud o to Objednatel Zhotovitele požádá.
93. Pokud Zhotovitel Předmět díla Objednateli odesílá prostřednictvím dopravce, je Zhotovitel povinen zajistit dopravu u dopravce tak, aby Předmět díla byl dodán Objednateli v době uvedené v odstavci 40 Obchodních podmínek.
94. Je-li třeba provést vyložení Předmětu díla z dopravního prostředku, je vyložení povinen provést Zhotovitel na své náklady.
95. Je-li Objednatel v prodlení s převzetím Předmětu díla, uchová jej Zhotovitel, může-li s ním nakládat, pro Objednatele způsobem přiměřeným okolnostem. Převzal-li Objednatel Předmět díla, který zamýšlí odmítnout, uchová jej způsobem přiměřeným okolnostem. Smluvní strana, která uchovává Předmět díla pro druhou Smluvní stranu, má právo na náhradu účelně vynaložených nákladů spojených s uchováním Předmětu díla, nemůže jej však za účelem zajištění svého práva na úhradu nákladů zadržet.

ČÁST 12 - PODDODAVATELÉ

96. Zhotovitel je oprávněn pověřit provedením části Díla třetí osobu – poddodavatele. Zhotovitel odpovídá za činnost poddodavatele tak, jako by činnost prováděl sám.
97. Zhotovitel je oprávněn pověřit provedením části Díla poddodavatele pouze, pokud je poddodavatel uveden v příloze Smlouvy o dílo.
98. Zhotovitel se zavazuje, že poddodavatelé splní všechny povinnosti vyplývající Zhotoviteli ze Smlouvy o dílo, a to přiměřeně k povaze a rozsahu poddodávky.
99. Zhotovitel se zavazuje, že poddodavatelé, kterými prokazoval splnění kvalifikace v zadávacím řízení, se budou podílet na provedení příslušné věcně vymezené části Díla v rozsahu dle Nabídky Zhotovitele.
100. Zhotovitel je oprávněn změnit poddodavatele pouze s předchozím písemným souhlasem Objednatele. Objednatel vydá písemný souhlas se změnou do 10 dnů od doručení žádosti Zhotovitele. Objednatel souhlas se změnou nevydá, pokud

100.1. prostřednictvím původního poddodavatele Zhotovitel v zadávacím řízení prokazoval kvalifikaci a nový poddodavatel nebude mít stejnou či vyšší kvalifikaci jako původní nahrazovaný poddodavatel nebo
100.2. po Objednateli nelze spravedlivě požadovat, aby s takovou změnou souhlasil.

ČÁST 13 - PŘEDÁNÍ A PŘEVZETÍ DÍLA

101. Závazek Zhotovitele provést Dílo je splněn jeho dokončením a převzetím Díla Objednatelem, včetně převzetí veškerých Dokladů.
102. Součástí Dokladů je dle povahy a charakteru Díla též
102.1. dodavatelská výrobní a dílenská dokumentace,
102.2. atesty, záruční listy, prohlášení o shodě všech věcí, jež byly použity při provádění Díla,
102.3. zápisy a osvědčení o všech předepsaných zkouškách, měřeních,
102.4. dokumenty osvědčující průběh zkušebního provozu,
102.5. servisní plán, návod k obsluze a návod k použití částí Díla,
102.6. doklady o zabezpečení likvidace odpadů v souladu s právními předpisy,
102.7. fotodokumentace z průběhu provádění Díla, zejména fotodokumentace prací a konstrukcí, které byly dalším postupem prací zakryté nebo jinak znepřístupněné,
103. V případě, že Smlouva o dílo, Obchodní podmínky, Veřejnoprávní podklady, právní předpisy nebo příslušné ČSN předepisují provedení zkoušek, revizí, atestů a měření či zajištění prohlášení o shodě týkajících se Díla, je Zhotovitel povinen zajistit jejich úspěšné provedení před předáním Díla Objednateli.
104. Objednatel Dílo převezme za předpokladu, že provedení Díla odpovídá Smlouvě o dílo, Obchodním podmínkám, Veřejnoprávním podkladům, právním předpisům a příslušným ČSN, je dokončeno (plně funkční), a je prosté vad s výjimkou ojedinělých drobných vad, které samy o sobě ani ve spojení s jinými nebrání užívání Díla funkčně nebo esteticky, ani jeho užívání podstatným způsobem neomezují.
105. Splnění podmínek pro předání Díla bude ověřeno v rámci přejímacího řízení. Zhotovitel je povinen písemně vyzvat Objednatele k převzetí Díla (zahájení přejímacího řízení). Přejímací řízení bude Objednatelem zahájeno do 5 pracovních dnů po obdržení písemné výzvy Zhotovitele.
106. Objednatel je oprávněn přizvat k účasti v přejímacím řízení i jiné osoby, jejichž účast pokládá za nezbytnou.
107. O průběhu přejímacího řízení bude Zhotovitelem pořízen zápis s identifikací vad Díla, pokud budou v průběhu přejímacího řízení zjištěny. Zápis bude použit jako podklad pro zpracování Předávacího protokolu. Zpracování návrhu Předávacího protokolu zajistí Zhotovitel.
108. Předávací protokol obsahuje
108.1. výslovný souhlas Objednatele s převzetím Díla
108.2. datum převzetí Díla,
108.3. prohlášení Objednatele, zda přebírá Dílo bez výhrad, nebo s výhradami,
108.4. soupis zjištěných vad nebránících řádnému užívání Díla,
108.5. dohodnuté lhůty k odstranění zjištěných vad nebo jiná opatření (byla-li dohodnuta),
108.6. soupis Dokladů předaných Zhotovitelem Objednateli.
109. Objednatel převezme Dílo bez výhrad, je-li v předávacím řízení zjištěno, že Dílo je prosté vad.
110. Převezme-li Objednatel Dílo s výhradami, postupují Smluvní strany dále obdobně dle ustanovení odstavců 139 - 153 Obchodních podmínek, přičemž pro odstranění vad platí doba sjednaná v Předávacím protokolu, jinak doba 15 dní od oboustranného podpisu Předávacího protokolu a za reklamaci se považuje identifikace vad uvedená v Předávacím protokolu podepsaném Objednatelem.
111. V případě, že Objednatel Dílo nepřevezme, bude mezi Smluvními stranami sepsán záznam s uvedením důvodu nepřevzetí Díla a s uvedením stanovisek Smluvních stran. Zpracování záznamu zajistí Zhotovitel.

112. V případě nepřevzetí Díla Smluvní strany sjednají lhůtu pro odstranění zjištěných vad. Nebude-li vada odstraněna ve lhůtě sjednané, jinak do 15 dní, je Objednatel oprávněn zajistit odstranění vady jinou odborně způsobilou osobou na náklady Zhotovitele. Veškeré náklady vzniklé Objednateli v souvislosti s odstraněním vady způsobem dle předchozí věty je Zhotovitel povinen Objednateli uhradit. Zhotovitel je povinen ve stanovené lhůtě odstranit vady i v případě, kdy podle jeho názoru za vady neodpovídá. Náklady na odstranění v těchto sporných případech nese až do vyjasnění nebo do vyřešení rozporu Zhotovitel. Po odstranění vad vyzve Zhotovitel Objednatele k zahájení náhradního přejímacího řízení, které Objednatel zahájí bezodkladně, nejpozději do 2 pracovních dnů od obdržení výzvy Zhotovitele.
113. Podpisem Předávacího protokolu nebo záznamu o nepřevzetí Díla je přejímací řízení ukončeno.
114. Pro průběh náhradního přejímacího řízení se užijí ustanovení odstavců 104 - 113 Obchodních podmínek obdobně.
115. Připouští-li to povaha Předmětu díla, a není-li sjednán zkušební provoz, má Objednatel právo, aby byl Předmět díla před ním překontrolován nebo aby byly předvedeny jeho funkce.
116. Ustanovení §1921, §2112, §2605 odst. 2, §2606, §2609, §2618 a §2629 Občanského zákoníku se neužijí.

ČÁST 14 - VLASTNICKÉ PRÁVO A NEBEZPEČÍ ŠKODY

117. Vlastnické právo k Dílu náleží od počátku Objednateli.
118. Vlastnické právo k dodávkám materiálu a jiných hmotných movitých věcí nabývá Objednatel okamžikem jejich zapracování do Díla, učiněním součástí Díla nebo jakýmkoliv funkčním, estetickým či jiným spojením s Dílem.
119. Vlastnické právo k jakékoli dokumentaci vztahující se k Dílu, která není autorským dílem, nabývá Objednatel okamžikem jejího vyhotovení.
120. Je-li vlastníkem Díla nebo jeho části v souladu s §1083 a §1084 Občanského zákoníku vlastník pozemku, užijí se ustanovení odstavců 117 a 118 přiměřeně.
121. Nebezpečí škody na Díle nese Zhotovitel, na Objednatele přechází okamžikem oboustranného podpisu Předávacího protokolu. Pokud nebyly s Předmětem díla předány zároveň též všechny Doklady, nese Zhotovitel nebezpečí škody na dosud nepředaných Dokladech až do jejich převzetí Objednatelem.
122. Náklady nutné k odstranění škody na Díle vzniklé v době, kdy nebezpečí škody nese Zhotovitele, hradí Zhotovitel v plném rozsahu a tyto náklady nemají vliv na Cenu díla.
123. Škody na Díle vzniklé v době, kdy nebezpečí škody nese Zhotovitele, je povinen Zhotovitel odstranit v součinnosti s Objednatelem jako vlastníkem poškozené věci a dle jeho pokynů.
124. Ustanovení §2599 Občanského zákoníku se neužijí.

ČÁST 15 - VADY PLNĚNÍ A ZÁRUKA

125. Zhotovitel se zavazuje, že Dílo bude v okamžiku jeho převzetí Objednatelem vyhovovat všem požadavkům na dílo stanoveným Smlouvou o dílo, Obchodními podmínkami, Veřejnoprávními podklady, právními předpisy a příslušnými ČSN.
126. Zhotovitel se zavazuje, že Dílo bude vyhovovat též plnění nabídnutému Zhotovitelem v Nabídce.
127. Dílo musí být prosté všech faktických a právních vad. Plnění má právní vadu, pokud k němu uplatňuje právo třetí osoba.
128. Zhotovitel se zavazuje (poskytuje Objednateli záruku), že Dílo a veškeré jeho části si po celou dobu od okamžiku jeho převzetí Objednatelem, až do uplynutí Záruční doby zachová vlastnosti stanovené v odstavcích 125 - 127 Obchodních podmínek.
129. Záruční doba začíná běžet dnem převzetí Díla Objednatelem, nebo jeho poslední části, je-li Dílo dodáváno po částech, nebo ode dne úspěšného ukončení zkušebního provozu, je-li dle Smlouvy o dílo vyžadován a nastane-li okamžik úspěšného ukončení zkušebního provozu později než okamžik převzetí Díla, resp. jeho poslední části.

130. Dílo má vady (Zhotovitel plnil vadně), jestliže při převzetí Objednatelem nebo kdykoliv od převzetí Objednatelem do konce Záruční doby nebude mít vlastnosti stanovené v odstavcích 125 - 127 Obchodních podmínek.
131. Objednatel má práva z vadného plnění i v případě, jedná-li se o vadu, kterou musel s vynaložením obvyklé pozornosti poznat již při uzavření Smlouvy o dílo.
132. Objednatel nemá práva z vadného plnění, způsobila-li vadu po přechodu nebezpečí škody na věci na Objednatele vnější událost. To neplatí, způsobil-li vadu Zhotovitel nebo jakákoliv třetí osoba, jejímž prostřednictvím plnil své povinnosti vyplývající ze Smlouvy o dílo.
133. Zhotovitel neodpovídá za vady spočívající v opotřebení Předmětu díla, které je obvyklé u věcí stejného nebo obdobného druhu jako Předmět díla.
134. Zhotovitel odpovídá za vady spočívající v opotřebení Předmětu díla, ke kterému do konce Záruční doby vzhledem k požadavkům Smlouvy o dílo, Obchodních podmínek, Veřejnoprávních podkladů, právních předpisů a příslušných ČSN na jakost a provedení Předmětu díla nemělo dojít.
135. Zhotovitel nenese odpovědnost za vady způsobené Objednatelem nebo třetími osobami, ledaže Objednatel nebo takové osoby postupovaly v souladu s Doklady nebo pokyny, které obdrželi od Zhotovitele.

ČÁST 16 - UPLATNĚNÍ PRÁV Z VADNÉHO PLNĚNÍ

136. Odpovídá-li Zhotovitel za vady Díla, má Objednatel práva z vadného plnění.
137. Objednatel je oprávněn vady reklamovat u Zhotovitele jakýmkoliv způsobem, preferovaná je písemná forma. Zhotovitel je povinen přijetí reklamace bez zbytečného odkladu písemně potvrdit. V reklamaci Objednatel uvede popis vady nebo uvede, jak se vada projevuje.
138. Vada je uplatněna včas, je-li písemná forma reklamace odeslána Zhotoviteli nejpozději v poslední den Záruční doby. Připadne-li konec Záruční doby na sobotu, neděli nebo svátek, je vada včas uplatněna, je-li písemná forma reklamace odeslána Zhotoviteli nejblíže následující pracovní den.
139. Má-li Předmět díla vady, za které Zhotovitel odpovídá, má Objednatel právo
    139.1. na odstranění vady dodáním nového Předmětu díla nebo jeho části bez vady, pokud to není vzhledem k povaze vady zcela zřejmě nepřiměřené, nebo dodání chybějící části Předmětu díla,
    139.2. na odstranění vady opravou Předmětu díla nebo jeho části,
    139.3. na přiměřenou slevu z Ceny díla, nebo
    139.4. odstoupit od Smlouvy o dílo.
140. Objednatel je oprávněn požadovat odstranění vad dodáním nového Předmětu díla nebo jeho části bez vady, vyskytla-li se stejná vada po její opravě opětovně, nebo nemůže-li Objednatel řádně užívat Předmět díla nebo jeho část pro větší počet vad.
141. Objednatel je oprávněn nároky dle odstavce 139 kombinovat, je-li to vzhledem k okolnostem možné. Objednatel není oprávněn kombinovat nároky, které si navzájem odporují (např. dodání nové části Předmětu díla a zároveň slevy z Ceny díla na tutéž část Předmětu díla).
142. Objednatel sdělí Zhotoviteli volbu nároku z vady v reklamaci, nebo bez zbytečného odkladu po reklamaci. Provedenou volbu nemůže Objednatel změnit bez souhlasu Zhotovitele; to neplatí, žádal-li Objednatel opravu vady, která se ukáže jako neopravitelná.
143. Nesdělí-li Objednatel Zhotoviteli, jaké právo si zvolil ani bez zbytečného odkladu poté, co jej k tomu Zhotovitel vyzval, může Zhotovitel odstranit vady podle své volby opravou nebo dodáním nového Předmětu díla nebo jeho části; volba nesmí Objednateli způsobit nepřiměřené náklady.
144. Objednatel má nárok na náhradu nákladů účelně vynaložených v souvislosti s oznámením vad Zhotoviteli.

ČÁST 17 - PODMÍNKY ODSTRANĚNÍ VAD

145. Pokud Objednatel požaduje v reklamaci odstranění vady, je Zhotovitel povinen neprodleně po obdržení reklamace zahájit činnosti vedoucí k odstranění reklamované vady. Pokud Objednatel v reklamaci uvede, že se jedná o havárii, je Zhotovitel povinen zahájit odstraňování vady nejpozději do 48 hodin po obdržení reklamace.
146. Zhotovitel je povinen odstranit Objednatelem reklamovanou vadu nejpozději do 30 dnů ode dne oznámení vady Zhotoviteli. Jde-li o vadu označenou Objednatelem v reklamaci jako havarijní, je Zhotovitel povinen odstranit vadu nejpozději do 5 dnů.
147. Nezahájí-li Zhotovitel činnosti vedoucí k odstranění vady do 10 dnů od oznámení vady Zhotoviteli, nebo nebude-li vada odstraněna ve lhůtě dle předcházejícího odstavce, je Objednatel oprávněn
    147.1. zajistit odstranění vady jinou odborně způsobilou právnickou nebo fyzickou osobou na účet Zhotovitele,
    147.2. požadovat slevu z Ceny díla, nebo
    147.3. od Smlouvy o dílo odstoupit.
148. Veškeré náklady vzniklé Objednateli v souvislosti s odstranění vady způsobem dle předchozího odstavce je Zhotovitel povinen Objednateli uhradit.
149. Zhotovitel je povinen odstranit vadu bez ohledu na to, zda je uplatnění vady oprávněné či nikoli. Prokáže-li se však kdykoli později, že uplatnění vady Objednatelem nebylo oprávněné, tj. že Zhotovitel za vadu neodpovídal, je Objednatel povinen uhradit Zhotoviteli veškeré jím účelně vynaložené náklady v souvislosti s odstraněním vady.
150. Objednatel je povinen poskytnout Zhotoviteli součinnost nezbytnou k odstranění vady.
151. Do odstranění vady nemusí Objednatel platit dosud nezaplacenou část Ceny díla a případnou příslušnou DPH odhadem přiměřeně odpovídající jeho právu na slevu.
152. Při dodání nového Předmětu díla nebo jeho části vrátí Objednatel Zhotoviteli na náklady Zhotovitele Předmět díla nebo jeho část původně dodanou.
153. Týká-li se vada Dokladů nebo jiného plnění poskytnutého Zhotovitelem dle Smlouvy o dílo než Předmětu díla, užijí se ustanovení odstavců 136 – 152 obdobně.
154. Ustanovení §1917–1924, §2099–2101, §2103 – 2117, §2165 – 2172, §2618 a §2629 Občanského zákoníku se neužijí.

ČÁST 18 - POJIŠTĚNÍ

155. Ustanovení této části se užijí v případě, že ze Smlouvy o dílo vyplývá, že Zhotovitel je povinen být pojištěn pro případ odpovědnosti za škodu způsobenou při výkonu činnosti.
156. Zhotovitel je povinen mít ode dne zahájení provádění Díla, nejpozději však do 15 dnů od uzavření Smlouvy o dílo, až do uplynutí Záruční doby uzavřenou pojistnou smlouvu o pojištění odpovědnosti za škodu způsobenou Zhotovitelem při výkonu činnosti třetím osobám s limitem pojistného plnění pro 1 pojistnou událost ve výši odpovídající Ceně díla.
157. Zhotovitel je povinen předložit Objednateli uzavřenou pojistnou smlouvu dle této části nebo odpovídající pojistku nejpozději do 15 dnů ode dne uzavření Smlouvy o dílo a dále kdykoli v průběhu provádění Díla nebo trvání Záruční doby do 10 dnů ode dne, kdy k tomu byl Objednatelem vyzván. V případě změn v pojištění je Zhotovitel povinen bezodkladně tyto změny oznámit Objednateli a předložit dokumenty dokládající tyto změny.
158. Zhotovitel se zavazuje, že všichni poddodavatelé, kteří se budou podílet na provedení Díla, budou nejméně po dobu provádění poddodávky pojištěni pro případ škody způsobené poddodavatelem při výkonu činnosti třetím osobám s limitem pojistného plnění pro 1 pojistnou událost minimálně ve výši odpovídající ceně poddodávky.
159. Porušení jakékoli povinnosti Zhotovitele dle této části je podstatným porušením Smlouvy o dílo.
160. Náklady na pojištění nese Zhotovitel, jsou zahrnuty v Ceně díla.

ČÁST 19 - DUŠEVNÍ VLASTNICTVÍ

161. Zhotovitel je povinen při provádění Díla postupovat tak, aby při provádění Díla ani následným užíváním Díla Objednatelem nedošlo k porušení práv duševního vlastnictví. Bude-li v souvislosti s Dílem, jakkoliv dotčeno právo k duševnímu vlastnictví, je Zhotovitel povinen upravit veškeré právní vztahy s osobami, kterým taková práva náležejí nebo jež jsou oprávněny je vykonávat, tak, aby zamezil vznášení jakýchkoli oprávněných nároků těchto osob ve vztahu k Objednateli.
162. Zhotovitel tímto poskytuje Objednateli oprávnění k výkonu práva duševního vlastnictví (licenci nebo podlicenci) ke všem plněním poskytnutým Objednateli při provádění Díla, které jsou nebo budou předmětem duševního vlastnictví a ke kterým je oprávněn takové oprávnění poskytnout. Oprávnění Zhotovitel poskytuje
    162.1. bezúplatně,
    162.2. jako nevýhradní,
    162.3. z hlediska časového a územního v rozsahu neomezeném,
    162.4. z hlediska věcného rozsahu (způsobu užití) tak, že opravňuje Objednatele ke všem známým způsobům užití,
    162.5. bez množstevního omezení.
163. Objednatel není povinen oprávnění využít.
164. Objednatel je oprávněn oprávnění tvořící součást licence nebo podlicence poskytnout nebo též postoupit třetí osobě zcela nebo zčásti.
165. Zhotovitel se zavazuje, že na žádost Objednatele autor nebo autoři autorského díla, jež je součástí nebo příslušenstvím Díla, udělí Objednateli bez zbytečného odkladu bezúplatně právo
    165.1. upravit či jinak změnit označení autora,
    165.2. autorské dílo nebo jeho název upravit či jinak měnit,
    165.3. autorské dílo s jakýmkoliv jiným autorským dílem spojit či zařadit do díla souborného.
166. Žádný výsledek činnosti provedené na základě Smlouvy o dílo nebo v souvislosti s ní, který je předmětem duševního vlastnictví, není Zhotovitel oprávněn bez předchozího písemného svolení Objednatele užít k jiným účelům, než je provedení Díla, zejména je nesmí poskytnout třetím osobám.

ČÁST 20 - SANKCE

167. Uplatněním smluvní pokuty není dotčeno právo druhé Smluvní strany na náhradu škody v plné výši.
168. Uplatněním nároku na zaplacení smluvní pokuty ani jejím uhrazením nezaniká povinnost Smluvní strany splnit utvrzenou povinnost.
169. Dopadají-li na jedno skutkově stejnorodé porušení povinnosti dvě a více ustanovení o smluvní pokutě, uplatní se pouze jedna smluvní pokuta, a to ta, která je v nejvyšší částce. Není vyloučen souběh smluvní pokuty za porušení smluvní povinnosti a smluvní pokuty za prodlení s odstraněním následku téže smluvní povinnosti, jelikož se nejedná o skutkově stejnorodé porušení smluvní povinnosti.
170. Smluvní pokuty se uplatňují bez DPH. Je-li základem pro výpočet smluvních pokut Cena díla či její část, je rozhodná Cena díla či její část bez DPH stanovená k okamžiku uzavření Smlouvy o dílo; k případným jejím následným úpravám po uzavření Smlouvy o dílo se nepřihlíží.
171. Smluvní pokuta je splatná do třiceti (30) dnů ode dne vystavení daňového dokladu – sankční faktury. Je-li povinná Smluvní strana v prodlení s uhrazením smluvní pokuty, musí uhradit druhé Smluvní straně zákonný úrok z prodlení z dlužné částky smluvní pokuty za každý započatý den prodlení.
172. V případě porušení smluvní povinnosti týkající se neposkytnutí finanční záruky a pojistných smluv nebo jejich neudržování v platnosti nebo účasti poddodavatelů anebo realizačního týmu, které je možné jednáním Zhotovitele do patnácti (15) kalendářních dnů napravit, bude zhotovitel bezodkladně písemně vyzván ke zjednání nápravy v dodatečné lhůtě patnácti (15) kalendářních dnů ode dne doručení výzvy. V případě, že Zhotovitel zjedná

nápravu ve stanovené lhůtě, nárok Objednatele na smluvní pokutu nevznikne. V případě marného uplynutí této lhůty vzniká nárok na smluvní pokutu ode dne porušení smluvní povinnosti.

173. Maximální celková výše všech uplatněných smluvních pokut v důsledku porušení Smlouvy o dílo Zhotovitelem je stanovena ve výši 40 % Ceny díla. Limit dle předchozí věty činí maximálně 30 % Ceny díla do okamžiku podpisu protokolu o provedení/předání Díla tak, aby na dobu platnosti finanční záruky za odstranění vad připadalo minimálně 10 % Ceny díla.
174. Dosažení maximální celkové výše veškerých uplatněných smluvních pokut podle předchozího odstavce představuje podstatné porušení Smlouvy o dílo, na základě kterého je Objednatel oprávněn odstoupit od Smlouvy o dílo.
175. Objednatel je ze zákona povinen uplatnit a vymáhat veškeré smluvní pokuty, na které mu vznikl nárok, a to v plné výši bez možnosti její úpravy.
176. Poruší-li Zhotovitel povinnost provést Dílo, nebo jeho část (je-li Dílo prováděno po částech) ve sjednané době, je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 0,2 % z Ceny díla, nebo ceny části Díla za každý započatý den prodlení.
177. Poruší-li Zhotovitel povinnost odstranit vadu Díla, nebo jeho části (je-li Dílo prováděno po částech), ve sjednané době, je povinen uhradit Objednateli smluvní pokutu ve výši 0,1 % z Ceny díla, nebo ceny části Díla za každý započatý den prodlení až do odstranění vady. Jde-li o vadu, kterou Objednatel označil v reklamaci jako havárii, je Zhotovitel povinen uhradit smluvní pokutu ve dvojnásobné výši. Maximální denní výše smluvní pokuty dle tohoto odstavce činí, a to vždy ve vztahu k jednotlivé smluvní pokutě odpovídající Ceně Díla nebo ceně příslušné části Díla, v případě Ceny díla:
    177.1. do 10 mil. Kč částku 10 000 Kč,
    177.2. do 100 mil. Kč částku 50 000 Kč,
    177.3. do 1 mld. Kč částku 100 000 Kč a
    177.4. nad 1 mld. Kč částku 200 000 Kč.
178. V případě, že Zhotovitel pověřil prováděním Díla jiného poddodavatele než toho, který byl uveden v příloze Smlouvy o dílo, bez předchozího písemného souhlasu Objednatele postupem dle části 12 těchto Obchodních podmínek, je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 1 % z Ceny díla za každý takový případ.
179. V případě, že Zhotovitel provádí Dílo prostřednictvím jiného poddodavatele než toho, kterým byla prokazována kvalifikace, je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 10 % z Ceny díla za každý takový případ.
180. Poruší-li Zhotovitel povinnost provádět vyhrazené významné činnosti přímo Zhotovitelem, je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 10 % z Ceny díla za každý takový případ.
181. V případě, že Zhotovitel nesplní svoji povinnost stanovenou Smlouvou o dílo předložit pojistné smlouvy nebo povinnost udržovat po celou dobu provádění Díla v platnosti Objednatelem vyžadované pojistné smlouvy, je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 0,05 % z Ceny díla za každý započatý den neplnění této povinnosti, maximálně však ve výši 40.000, -Kč za každý započatý den prodlení.
182. V případě, že Zhotovitel nesplní svoji povinnost poskytnout Objednateli finanční záruku za odstranění vad Díla nebo udržovat tuto finanční záruku v platnosti v rozsahu vyžadovaném Smlouvou o dílo, je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 0,5 % z hodnoty finanční záruky za každý den neplnění této povinnosti, maximálně však ve výši 20.000 Kč za každý započatý den prodlení.
183. V případě, že Zhotovitel poruší plán BOZP, je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 1 % z Ceny díla, maximálně však ve výši 1 % z Ceny díla za každý takový případ
184. Poruší-li Zhotovitel povinnost nepostoupit žádnou svou pohledávku za Objednatelem vyplývající ze Smlouvy o dílo a/nebo poruší zákaz zřídit zástavní právo k pohledávce, byť by takové postoupení a/nebo zřízení zástavního práva bylo neplatné či neúčinné, je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 10 % z nominální hodnoty postoupené a/nebo zastavené pohledávky, včetně hodnoty případného příslušenství ke dni účinnosti postoupení vůči postupníkovi.

ČÁST 21 - OBECNÁ ODPOVĚDNOST ZHOTOVITELE

185. Zhotovitel je povinen po dobu plnění povinností ze Smlouvy o dílo chránit majetek Objednatele i třetích osob před jeho poškozením, znehodnocením, zničením a ztrátou a postupovat tak, aby neomezoval práva osob nad míru nezbytnou k provádění Díla.
186. Způsobí-li Zhotovitel v souvislosti s Dílem nebo porušením svých povinností vyplývajících ze Smlouvy o dílo, Obchodních podmínek, Veřejnoprávních podkladů, právních předpisů a příslušných ČSN jakoukoli újmu Objednateli nebo třetím osobám, je povinen nahradit Objednateli škodu a nemajetkovou újmu, včetně případných sankcí udělených Objednateli orgány státní správy, jejichž příčinou bylo porušení smluvních povinností Zhotovitele, a jde-li o újmu způsobenou třetím osobám, je povinen způsobenou újmu na vlastní náklady bezodkladně odčinit.
187. Újmou se pro účely Obchodních podmínek rozumí zejm. jakékoliv poškození, znehodnocení, či znečištění věcí nebo prostor nebo jejich jiná nežádoucí změna a jakékoliv neoprávněné omezení práv Objednatele nebo třetích osob.
188. Zhotovitel odpovídá za jakékoli porušení svých povinností stanovených Smlouvou o dílo, Obchodními podmínkami, Veřejnoprávními podklady, právními předpisy a příslušnými ČSN a je povinen uhradit veškeré pokuty udělené mu příslušnými orgány státní správy v souvislosti s prováděním Díla ze svého, ledaže mu byla pokuta udělena v souvislosti s respektováním příkazu Objednatele, proti kterému uplatnil písemnou výhradu a na jehož splnění Objednatel trval anebo v souvislosti s užitím Objednatelem opatřené věci, na jejíž nevhodnost Objednatele písemně upozornil a Objednatel na jejím užití trval.
189. Povinnosti k náhradě újmy způsobené porušením svých povinností ze Smlouvy o dílo, Obchodních podmínek, Veřejnoprávních podkladů, právních předpisů a příslušných ČSN se Zhotovitel vůči Objednateli zprostí, prokáže-li, že mu ve splnění povinnosti zabránila mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na jeho vůli. Překážka vzniklá z osobních poměrů Zhotovitele nebo vzniklá až v době, kdy byl Zhotovitel s plněním povinnosti v prodlení, ani překážka, kterou byl Zhotovitel povinen překonat, jej však povinnosti k náhradě nezprostí.

ČÁST 22 - ODSTOUPENÍ OD SMLOUVY O DÍLO

190. Poruší-li Smluvní strana Smlouvu o dílo podstatným způsobem, může druhá Smluvní strana písemnou formou od Smlouvy o dílo odstoupit.
191. Podstatné je takové porušení povinnosti, o němž Smluvní strana porušující Smlouvu o dílo již při uzavření Smlouvy o dílo věděla nebo musela vědět, že by druhá Smluvní strana Smlouvu o dílo neuzavřela, pokud by toto porušení předvídala, nebo je-li porušení povinnosti ve Smlouvě o dílo nebo v Obchodních podmínkách jako podstatné označeno; v ostatních případech se má za to, že porušení podstatné není.
192. Podstatným porušením Smlouvy o dílo je též prodlení Zhotovitele a Objednatele s plněním povinností vyplývajících Zhotoviteli a Objednateli ze Smlouvy o dílo o více než 30 dní.
193. Objednatel je oprávněn od Smlouvy o dílo odstoupit též
    193.1. z důvodů uvedených v části Předání a převzetí Díla (viz ČÁST 13 - Obchodních podmínek),
    193.2. nabylo-li právní moci rozhodnutí o nařízení exekuce vůči Zhotoviteli jako povinnému,
    193.3. ocitne-li se Zhotovitel ve stavu úpadku nebo hrozícího úpadku,
    193.4. jestliže Zhotovitel nebo jeho poddodavatel, nebo z jejich pokynu jakákoliv osoba, nabídne nebo poskytne jakékoliv osobě úplatek nebo jiný majetkový či jiný prospěch za účelem získání neoprávněného prospěchu nebo výhody v souvislosti s Dílem nebo jeho prováděním,
    193.5. uvedl-li Zhotovitel v Nabídce informace nebo doklady, které neodpovídají skutečnosti a měly nebo mohly mít vliv na výsledek řízení,
    193.6. stanoví-li tak Smlouvy o dílo.
194. Smluvní strana může od Smlouvy o dílo odstoupit, pokud z chování druhé Smluvní strany nepochybně vyplyne, že poruší Smlouvu o dílo podstatným způsobem, a nedá-li na výzvu oprávněné Smluvní strany přiměřenou jistotu.

195. Jakmile Smluvní strana oprávněná odstoupit od Smlouvy o dílo oznámí druhé Smluvní straně, že od Smlouvy o dílo odstupuje, nebo že na Smlouvě o dílo setrvává, nemůže volbu již sama změnit.
196. Zakládá-li prodlení Smluvní strany nepodstatné porušení její povinnosti ze Smlouvy o dílo, může druhá Smluvní strana od Smlouvy o dílo odstoupit poté, co prodlévající Smluvní strana svoji povinnost nesplní ani v dodatečné přiměřené lhůtě, kterou jí druhá Smluvní strana poskytla výslovně nebo mlčky.
197. Oznámí-li Smluvní strana Smluvní straně prodlévající, že jí určuje dodatečnou lhůtu k plnění a že jí lhůtu již neprodlouží, platí, že marným uplynutím této lhůty od Smlouvy o dílo odstoupila.
198. Poskytla-li Smluvní strana Smluvní straně prodlévající nepřiměřeně krátkou dodatečnou lhůtu k plnění a odstoupí-li od Smlouvy o dílo po jejím uplynutí, nastávají účinky odstoupení teprve po marném uplynutí doby, která měla být prodlévající Smluvní straně poskytnuta jako přiměřená. To platí i tehdy, odstoupila-li Smluvní strana od Smlouvy o dílo, aniž by prodlévající Smluvní straně dodatečnou lhůtu k plnění poskytla.
199. Plnil-li Zhotovitel zčásti, může Smluvní strana od Smlouvy o dílo odstoupit jen ohledně nesplněného zbytku plnění. Nemá-li však částečné plnění pro Objednatele význam, může Objednatel od Smlouvy o dílo odstoupit ohledně celého plnění. Odstoupil-li od nesplněného zbytku plnění Zhotovitel, je Objednatel oprávněn odstoupit od splněné části Smlouvy o dílo, nemá-li částečně plnění pro Objednatele význam.
200. Zavazuje-li Smlouva o dílo Zhotovitele k opakované činnosti nebo k postupnému dílčímu plnění, může Objednatel od Smlouvy o dílo odstoupit jen s účinky do budoucna. To neplatí, nemají-li již přijatá dílčí plnění sama o sobě pro Objednatele význam.
201. Smluvní strany se dohodly, že dojde-li k odstoupení od Smlouvy o dílo jen ohledně nesplněného zbytku plnění, užijí se na splněnou část plnění obdobně všechna ustanovení Smlouvy o dílo a Obchodních podmínek týkající se předání a převzetí Díla, přičemž přejímací řízení Smluvní strany zahájí nejpozději do 3 pracovních dnů ode dne odstoupení od Smlouvy o dílo, a dále všechna ustanovení Smlouvy o dílo a Obchodních podmínek o právech a povinnostech Smluvních stran, které jsou Smluvní stany povinny plnit v době ode dne převzetí Díla Objednatelem, tedy zejm. ustanovení o vadách Díla.
202. Ustanovení §1977, §2002–2003 Občanského zákoníku se neužijí.

ČÁST 23 - OSTATNÍ UJEDNÁNÍ

Částečné plnění

203. Ustanovení Smlouvy o dílo a Obchodních podmínek platí obdobně též pro části Díla, provádí-li Zhotovitel Dílo v souladu se Smlouvou o dílo po částech, není-li uvedeno jinak.

Postoupení, započtení

204. Zhotovitel není oprávněn postoupit žádnou svou pohledávku za Objednatelem vyplývající ze Smlouvy o dílo nebo vzniklou v souvislosti se Smlouvou o dílo.
205. K pohledávce za Objednatelem vyplývající se Smlouvy o dílo nebo vzniklé v souvislosti se Smlouvou o dílo nesmí být zřízeno zástavní právo.
206. Zhotovitel není oprávněn provést jednostranné započtení žádné své pohledávky za Objednatelem vyplývající ze Smlouvy o dílo nebo vzniklé v souvislosti se Smlouvou o dílo na jakoukoliv pohledávku Objednatele za Zhotovitelem.
207. Objednatel je oprávněn provést jednostranné započtení jakékoliv své splatné i nesplatné pohledávky za Zhotovitelem vyplývající ze Smlouvy o dílo nebo vzniklé v souvislosti se Smlouvou o dílo (zejm. smluvní pokutu) na jakoukoliv splatnou či nesplatnou pohledávku Zhotovitele za Objednatelem.

Mlčenlivost

208. Zhotovitel je povinen zachovávat mlčenlivost o všech skutečnostech a informacích, které jsou obsažené ve Smlouvě o dílo a dále o všech skutečnostech a informacích, které mu byly v souvislosti se Smlouvou o dílo nebo jejím plněním, jakkoliv zpřístupněny, předány či sděleny, nebo o nichž se jakkoliv dozvěděl, vyjma těch, které jsou v okamžiku, kdy se s nimi Zhotovitel seznámil, prokazatelně veřejně přístupné, nebo těch, které se bez zavinění Zhotovitele veřejně přístupnými stanou. Zhotovitel nesmí takové skutečnosti a

informace použít v rozporu s jejich účelem, nesmí je použít ve prospěch svůj nebo třetích osob a nesmí je použít ani v neprospěch Objednatele. Povinnosti dle tohoto odstavce je Zhotovitel povinen zachovávat i po zániku závazku ze Smlouvy o dílo, vyjma případů, kdy se takové skutečnosti a informace stanou prokazatelně veřejně přístupné bez zavinění Zhotovitele. Povinnosti dle tohoto odstavce se nevztahují na případy, kdy je Zhotovitel povinen zveřejnit takové skutečnosti nebo informace na základě povinnosti uložené mu právním předpisem nebo rozhodnutím orgánu veřejné moci.

Poskytování informací

209. Vzhledem k veřejnoprávnímu charakteru Objednatele Zhotovitel výslovně prohlašuje, že je s touto skutečností obeznámen a souhlasí se zveřejněním Smlouvy o dílo včetně Obchodních podmínek v rozsahu a za podmínek vyplývajících z příslušných právních předpisů.

Kontrola

210. Zhotovitel si je vědom, že je ve smyslu §2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů, povinen spolupůsobit při výkonu finanční kontroly a zavazuje se finanční kontrolu strpět.
211. Je-li Dílo z jakékoliv části financováno z prostředků Evropské unie, je Zhotovitel povinen
    211.1. strpět veškeré kontroly vyplývající z režimu financování Díla z prostředků Evropské unie,
    211.2. poskytnout při takových kontrolách veškerou nezbytnou součinnost,
    211.3. archivovat veškerou dokumentaci týkající se Smlouvy o dílo po dobu stanovenou pravidly, jimiž se řídí financování Díla z prostředků Evropské unie.

Jazyk

212. Ve všech záležitostech souvisejících se Smlouvou o dílo budou zástupci Smluvních stran komunikovat v českém jazyce. Všichni zástupci musí plynně český jazyk ovládat. Jestliže český jazyk plynně neovládají, jsou povinni na náklady své Smluvní strany zajistit, aby byl po celou dobu vzájemné osobní komunikace k dispozici kvalifikovaný tlumočník.

Forma, označení času

213. Písemnou formou (podobou) se rozumí listina podepsaná oprávněnou osobou Smluvní strany nebo email podepsaný zaručeným elektronickým podpisem oprávněné osoby Smluvní strany.
214. Je-li ve Smlouvě o dílo nebo Obchodních podmínkách uvedena lhůta nebo doba počítané podle dnů, měsíců nebo let, rozumí se tím vždy kalendářní den, měsíc nebo rok, není-li uvedeno jinak.

Reference

215. Zhotovitel je oprávněn uvádět Dílo a jméno Objednatele jako referenci na svou činnost pouze s předchozím písemným souhlasem Objednatele.

Salvatorní klauzule

216. Je-li nebo stane-li se některé oddělitelné ustanovení Smlouvy o dílo nebo Obchodních podmínek neplatné, neúčinné či nevymahatelné, nedotýká se tato skutečnost ostatních ustanovení. Smluvní strany se zavazují nahradit takové ustanovení jiným ustanovením, které svým obsahem a smyslem bude nejvíce odpovídat obsahu a smyslu ustanovení nahrazovaného.

SPRÁVA ŽELEZNIC

Příloha č. 8 Smlouvy

Seznam členů realizačního týmu

Účastník:

Obchodní firma/jméno	[DOPLNÍ ÚČASTNÍK]
Sídlo/místo podnikání	[DOPLNÍ ÚČASTNÍK]
IČO	[DOPLNÍ ÚČASTNÍK]
Zastoupen	[DOPLNÍ ÚČASTNÍK]

který podává nabídku na nadlimitní sektorovou veřejnou zakázku s názvem **„Realizace systému Zabezpečeného úložiště v prostředí Správy železnic“,** č.j. 60299/2026-SŽ-GŘ-O25, tímto níže předkládá seznam členů realizačního týmu, kteří se budou na plnění předmětu veřejné zakázky podílet:

Pozice člena realizačního týmu	Jméno a příjmení (titul)	Popis činnosti v rámci plnění Smlouvy
Architekt infrastruktury (Solution Architect)		Architekt infrastruktury je odpovědný za návrh a architektonické zpracování komplexních řešení ICT infrastruktury se zaměřením na oblast síťových technologií, serverových platforem a datových úložišť dodávaného technického řešení. V rámci výkonu této role zajišťuje návrh technické koncepce infrastruktury, včetně řešení vysoké dostupnosti, bezpečnosti, škálovatelnosti a kontinuity provozu. Odpovídá za zpracování architektonické a technické dokumentace, za návrh řešení pro prostředí s více lokalitami včetně geograficky oddělených datových center a za návrh mechanismů replikace dat, zálohování a disaster recovery.
Síťový specialista		Síťový specialista je odpovědný za praktickou realizaci a implementaci dodávaného řešení na základě architektonického návrhu zpracovaného Architektem infrastruktury. V rámci výkonu této role přebírá schválené technické řešení a zajišťuje jeho detailní rozpracování do úrovně implementační dokumentace, následnou konfiguraci, nasazení a uvedení do provozu. Odpovídá za instalaci, konfiguraci a optimalizaci aktivních síťových prvků, včetně OOB přepínačů, L3 směrovačů, bezpečnostních prvků FW a dalších komponent tvořících síťovou infrastrukturu. Jeho činností je realizace řešení pro prostředí Zadavatele s vysokými nároky na dostupnost, bezpečnost a výkon, včetně implementace redundance, segmentace sítě, vysoké dostupnosti a propojení geograficky oddělených lokalit. Zajišťuje implementaci mechanismů pro bezpečný přenos dat, monitoring síťového provozu, optimalizaci výkonu a řešení incidentů vzniklých v

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČO: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

		průběhu nasazení i převzetí do ostrého provozu. Odpovídá za provádění funkčních a zátěžových testů, spolupracuje při akceptačních řízeních a zajišťuje předání řešení do provozu včetně zpracování provozní a technické dokumentace.
Bezpečnostní specialista		Tato role bude vykonávat funkci architekta kybernetické bezpečnosti dle zákona č. 264/2025 Sb., o kybernetické bezpečnosti, v platném znění, resp. vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, v platném znění. Bezpečnostní specialista bude odpovědný za návrh, implementaci a dohled nad bezpečnostními opatřeními v oblasti dodávaného řešení s cílem zajistit důvěrnost, integritu a dostupnost informačních a komunikačních systémů na technické řešení provozovaném. V rámci své role vychází z architektonického návrhu infrastruktury a bezpečnostní koncepce organizace, které dále rozpracovává do konkrétních bezpečnostních mechanismů, technických konfigurací a provozních pravidel. Bezpečnostní specialista úzce spolupracuje s architektem infrastruktury i síťovým specialistou. Bezpečnostní specialista odpovídá za implementaci a konfiguraci bezpečnostních technologií, zejména v oblasti firewallů nové generace (NGFW), systémů pro detekci a prevenci průniků komunikace, systémů pro řízení přístupu, segmentaci sítí dle koncepce organizace, šifrování komunikace a napojení dohledových nástrojů. Podílí se na návrhu bezpečnostní architektury pro projekt bezpečného úložiště s vysokými nároky na dostupnost a odolnost, včetně řešení pro geograficky oddělené lokality a prostředí kritické infrastruktury Zadavatele.
Datový analytik pro data storage		Datový analytik pro data storage je role zaměřená na systematické zpracování, analýzu a interpretaci dat souvisejících s provozem bezpečného úložiště. Systém práce s daty je v kontextu bezpečnostních událostí a výkonnostních ukazatelů klíčových informačních systémů na daném úložišti. V rámci své role zajišťuje transformaci provozních, technických a bezpečnostních dat do strukturované podoby umožňující jejich další vyhodnocování, identifikaci trendů, rizik a optimalizačních či výkonových příležitostí. Datový analytik pro data storage odpovídá za návrh metodiky sběru dat, jejich konsolidaci z různých zdrojů relevantních pro organizaci. Provádí pokročilé analýzy zaměřené na výkonnost, dostupnost, kapacitní plánování, bezpečnostní události a efektivitu provozu úložiště. Výstupy svých analýz zpracovává do přehledných reportů, dashboardů a analytických podkladů a dokumentace.
Projektový manažer		Projektový manažer je odpovědný za komplexní řízení všech složek dodavatele v projektu Bezpečného úložiště, a to od návrhu řešení, přes jeho dodávku a implementaci až po akceptaci a předání do provozu Zadavatele. Odpovídá za plánování a koordinaci kapacit dodavatele, řízení úkolů a milníků projektu, věcnou kontrolu jednotlivých fází a včasnou identifikaci a řízení součinnosti potřebné pro řádné dokončení díla. Současně dohlíží na plnění smluvních podmínek, dodržování harmonogramu a požadovanou kvalitu plnění. V rámci své role zajišťuje vedení projektové dokumentace. Koordinuje činnost

		realizačního týmu dodavatele, zejména architekta, síťových a bezpečnostních specialistů a dalších odborných rolí, a zajišťuje efektivní komunikaci mezi všemi zapojenými stranami. Odpovídá za řízení rizik projektu, včasnou identifikaci problémů a návrh nápravných opatření předkládaných projektovému výboru a managementu SŽ, včetně pravidelného reportingu a organizace kontrolních dnů. Projektový manažer zároveň odpovídá za přípravu podkladů pro akceptační řízení, za soulad akceptačních protokolů se smlouvou a Zvláštními obchodními podmínkami pro Zakázky v oblasti ICT.

V …… dne ……

Příloha č. 9 smlouvy – Harmonogram plnění

HARMONOGRAM PLNĚNÍ

Fáze	Popis	Zahájení fáze	Ukončení od zahájení fáze
F1.1	Datový management vybraných systémů	Účinnost smlouvy	do 6 týdnů
F1.2	Implementační plán Bezpečného úložiště	Účinnost smlouvy	do 6 týdnů
F2.1	Dodávka a implementace Bezpečného úložiště do primární lokality	Účinnost smlouvy	do 8 týdnů
F2.2	Dodávka a implementace Bezpečného úložiště do sekundární lokality	Účinnost smlouvy	do 12 týdnů, ne dříve než F2.1
F3.1 A	Konfigurace primární lokality	Od ukončení F2.1	do 4 týdnů
F3.1 B	Konfigurace sekundární lokality	Od ukončení F2.2	do 4 týdnů
F3.2	Napojení na vybrané systémy	Od ukončení F3.1 A	do 4 týdnů
F3.3	Post-implementační testování	Od ukončení F3.2	do 3 týdnů
F4	Školení	Od ukončení F3.3	do 2 týdnů
F5	Dokumentace	Od ukončení F3.3	do 2 týdnů
F6.1A	Technická podpora – primární lokalita	Od ukončení F2.1	za 60 měsíců
F6.1B	Technická podpora – sekundární lokalita	Od ukončení F2.2	za 60 měsíců
F6.2	Post-implementační podpora	Od ukončení F3.3	za 60 měsíců
F7	Konzultační služby na vyžádání	kdykoli po dobu účinnosti smlouvy	dle objednávky

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČ: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

Klasifikace: Veřejný dokument

SPRÁVA ŽELEZNIC

Příloha č. 10 smlouvy - Informace k systémům SŽ

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384
Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČO: 709 94 234 DIČ: CZ 709 94 234
spravazeleznic.cz

Obsah

1 Seznam zkratek

Níže uvedená tabulka obsahuje seznam zkratek a pojmů použitých v rámci této přílohy.

Přehled zkratek a pojmů:

Zkratka	Popis
IS	Informační systém
KI	Kritická infrastruktura
TAF TSI	Technické specifikace interoperability, telematické aplikace v nákladní dopravě
ŽDC	Železniční dopravní cesta
GSM-R	Mezinárodní standard bezdrátové komunikace určený pro železniční aplikace
IROP	Integrovaný regionální operační program
SŽ	Správa železnic, státní organizace
TRS	Traťový rádiový systém
OT	Operational Technology - provozní technologie k přímému monitorování a řízení fyzických zařízení

2 Úvod

Tento dokument je přílohou č. 10 a nedílnou součástí smlouvy na veřejnou zakázku „Realizace systému Zabezpečeného úložiště v prostředí Správy železnic", pro organizaci Správa železnic, státní organizace (dále jen „*SŽ*"). Dokument popisuje nezbytné součásti prostředí organizace SŽ, které jsou relevantní k poskytnutí dodavatelům, kteří se budou ucházet o uvedenou veřejnou zakázku.

3 Anonymizovaný popis IS systémů SŽ

Dodavatel je povinen pro dále uvedené systémy zpřístupnit Bezpečné úložiště tak, aby v případě např. kybernetického útoku, poruchy nebo živelní události byla data v bezpečí a systémy bylo možné obnovit. Od dodavatele očekáváme, jednak dodávku samotného bezpečného úložiště a jeho integraci do sítě SŽ, aby vzniklo propojení mezi vyjmenovanými systémy a Bezpečným úložištěm.

Níže je uveden anonymizovaný a základní popis 24 informačních systémů (IS) kritické infrastruktury (KI), které byly zařazeny v rámci IROP pro aktivitu Bezpečné úložiště.

IS 1

Řídící technologie pro obsluhu napájení od distributora energie a uvnitř SŽ. Řízení dodávky elektrické energie.

IS zahrnuje následující informace:

- Informace o napájení trakčního vedení – stav prvků
- Informace o napájení zabezpečovacích zařízení
- Informace o odběru el. proudu dopravci
- Informace o stavu elektrických hnacích vozidel

IS 2

Komunikační systém zajišťující hlasovou komunikaci k řízení provozu (analogová / digitální a IP telefonie). Součástí systému je komunikační síť mezi "pevnými" telefony a přes brány do GSM-R a veřejných sítí. Systém mimo jiné zpracovává informace o stavu technologie (telefonie, IP telefonie, TRS, GSM-R).

IS 3

Komunikační počítačová síť vymezená pro provoz průmyslových a řídicích (OT) systémů. Informace, které jsou zpracovávány v tomto komunikačním systému mimo jiné jsou:

- Informace o stavu technologie sítí
- Informace o stavu klíčových aplikací/systémů
- Informace o provozu (zabezpečovací a signalizační systémy, provoz po trati apod.)

IS 4

Systém slouží k zajištění provozu. Konkrétně se jedná o dálkovou diagnostiku technologických systémů. Kromě diagnostiky také zajišťuje např. vytápění odstavených vagónů, ohřev výměn, atd. Informace, které tento IS zpracovává mimo jiné jsou:

- Informace o stavu prvků železniční infrastruktury
- Informace o stavu vozidel dopravců

IS 5

Systém slouží k dispečerskému řízení vlakové dopravy a jako podpora dispečerského plánování vlakové dopravy, včetně podpory vyhodnocení provozu vlaků. IS zahrnuje modul řízení vlakové dopravy a centrální dispečerský systém řízení dopravy.

IS zahrnuje následující informace:

- Informace o aktuální situaci na dopravní cestě
- Informace o aktuálním stavu dopravní cesty
- Informace o přidělené kapacitě pro vlak
- Informace o složení a připravenosti vlaku

Jeho druhou součástí je datový sklad SŽ. Sklad zpracovává data ze systému řídících železniční dopravní cestu.

IS 6

Vedení dopravní dokumentace na velkém množství jednotlivých PC, pořizování prvotních dat o jízdách vlaků, komunikace s dispečerskými systémy pro řízení vlakové dopravy a poskytování prvotních provozních dat pro datové sklady apod. IS zahrnuje informace o aktuálním stavu dopravní cesty.

IS 7

Systém slouží k automatickému vedení dopravní dokumentace na PC. Dále k řízení dopravních procesů na vymezeném úseku železniční sítě k pořizování prvotních dat o jízdách vlaků, komunikace s dispečerskými systémy pro řízení železniční dopravní cesty a poskytování prvotních provozních dat pro datové sklady apod.

IS zahrnuje následující informace:

- Informace o stavu prvků
- Nastavení prvků

IS 8

Informační systém fyzického řízení a provádění diagnostiky vozidel, systém sběru dat z indikátorů.

IS 9

Systém slouží k poskytování informací a podmínek pro provozování dráhy a drážní dopravy. Provozní informace, technické podmínky, předpisy, směrnice a veškerá relevantní legislativa. V rámci portálu existuje řada modulů.

IS zahrnuje následující informace:

- Informace dispečerského řízení
- Distribuce datově sdružených jízdních řádů
- Komunikace s dopravci

IS 10

Systém slouží k přidělování kapacity dráhy a tras vlaků v režimu ad-hoc. Webové rozhraní slouží dopravcům k vytvoření žádostí o přidělení kapacity a tras vlaků. Desktopová aplikace slouží provozovateli dráhy ke zpracování žádostí od dopravců, přidělení kapacity trati, konstrukci tras, tvorbě jízdního řádu a dalších opatření pro jízdu vlaků ad-hoc. Zahrnuje dva moduly (Webový klient IS a IS Desktop).

IS zahrnuje následující informace:

- Správa žádostí o přidělení kapacity ŽDC
- Konstrukce trasy požadovaného vlaku
- Generování a finalizace datových a tiskových výstupů (zaváděcí depeše, jízdní řád vlaku)
- Plánování jízdního řádu

IS 11

Informační systém zajišťující grafické zobrazení a řízení dopravní dokumentací či dopravního deníku. Zobrazení a kontrola aktuálního stavu jízdy vlaků. Mimo jiné umožňuje zobrazování výluk, příjezdů, odjezdů atd.

IS 12

Centrální databáze manažera infrastruktury složení vlaků pro poskytování informací dle příslušné legislativy RID a TAF TSI. IS 8 eviduje a ukládá došlé informace (pořízená data) o složení vlaku.

IS 13

Webová část systému IS 12, je nástroj pro dopravce k pořizování zpráv o složení vlaku, resp. správa vozového parku, případně rozboru vlaku a o připravenosti vlaku k odjezdu.

IS 14

Informační systém zajišťující agendu zpracování písemných rozkazů pro zpravení strojvedoucích vlaků s možností zasílat instrukce za svůj dispoziční úsek do stanic, kde vlak pravidelně zastavuje a tím např. umožnit průjezd vlaku ve vlastní stanici.

IS 15

Bezpečnostní systém pro správu, monitorování a zabezpečení přístupu k citlivým administrátorským účtům.

IS 16

Centrální evidence doručené a odeslané pošty, zpracování doručených a odeslaných datových zpráv. Je základním modulem komplexního řešení správy a řízení dokumentů a slouží ke komplexní evidenci dokumentů v souladu s legislativou a předepsaným národním standardem pro elektronické systémy spisové služby.

IS 17

Systém sloužící k příjmu, odeslání a zajištění přenosu elektronické komunikace prostřednictvím e-mailu.

IS 18

Personální portál zajišťující celou problematiku Human Resources (HR). Portál je postaven jako modulární, obsahuje následující moduly (funkční aplikace).

- Vzdělávání
- Spisová služba – umí sama o sobě klasifikovat
- Ekonomika
- Řízení provozu

IS 19

Zpracování dat z měřících prostředků železničního svršku (měřící vůz a měřící drezína). Systém poskytuje komplexní souhrn informací o reálném provozním stavu sítě tratí. Do systému jsou shromažďována data z mobilních diagnostických prostředků a data z ostatních dohledových činností na trati.

IS 20

Docházkový systém, který zpracovává data o docházce zaměstnanců a evidenci výkonů dle Sborníku prací. Pověřený zpracovatel docházky v úloze mj. zpracovává podklady pro výpočet mezd, plánuje směny nebo vytváří uzávěrku zaměstnancům.

IS 21

Bezpečnostní řešení dodavatele zaměřené na antivirovou kontrolu.

IS 22

Systém slouží ke sledování a managementu rychlostních omezení na železniční dopravní cestě a distribuci informací o těchto omezeních.

IS 23

Software pro zveřejňování veřejných zakázek a profilu. Používání je nařízeno legislativně.

IS 24

Modulární ERP systém. Je složen z následujících modulů:

- PM – Plant Maintenance: Modul údržby
- HR – Human Resources: Lidské zdroje
- FI – Financial Accounting: Finance a účetnictví
- CO – Controlling
- REM – Repetitive Manufacturing
- ASU – Power consumption

SPRÁVA ŽELEZNIC

Příloha č. 6 zadávací dokumentace – **Účastník předloží pouze v případě postupu dle čl. 23 zadávací dokumentace**

Čestné prohlášení

v souvislosti s ustanovením § 3 odst. 1 zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů (dále jen „*ZRS*")

Účastník:

Obchodní firma/jméno	[DOPLNÍ ÚČASTNÍK]
Sídlo/místo podnikání	[DOPLNÍ ÚČASTNÍK]
IČO	[DOPLNÍ ÚČASTNÍK]
Zastoupen	[DOPLNÍ ÚČASTNÍK]

který podává nabídku na nadlimitní sektorovou veřejnou zakázku s názvem **„Realizace systému Zabezpečeného úložiště v prostředí Správy železnic", č.j. 60299/2026-SŽ-GŘ-O25**, tímto čestně prohlašuje, že dále uvedené údaje a další skutečnosti uvedené či jinak řádné označené ve smlouvě na plnění předmětu veřejné zakázky, jež je součástí jeho nabídky (dále jen ***„smlouva"***), považuje účastník za obchodní tajemství ve smyslu ustanovení § 504 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen ***„obchodní tajemství"*** a ***„občanský zákoník"***), nebo se jedná o jiné informace, které nemohou být v registru smluv uveřejněny na základě ustanovení § 3 odst. 1 ZRS:

Obchodní tajemství či jiné informace dle § 3 odst. 1 ZRS	**Umístění ve smlouvě či jejích přílohách**
Zvolte položku.	Klikněte sem a zadejte text, např. „**Čl. 6 odst. 6.1 smlouvy.**"
	Klikněte sem a zadejte text.
	Klikněte sem a zadejte text.

Účastník tímto čestně prohlašuje, že údaje a skutečnosti uvedené ve smlouvě, která je nedílnou součástí nabídky, označené jako obchodní tajemství, naplňují současně všechny definiční znaky obchodního tajemství, tak jak je vymezeno v ustanovení § 504 občanského zákoníku, tj. obchodní tajemství tvoří konkurenčně významné, určitelné, ocenitelné a v příslušných obchodních kruzích běžně nedostupné skutečnosti, které souvisejí se závodem a jejichž vlastník zajišťuje ve svém zájmu odpovídajícím způsobem jejich utajení. Účastník dále čestně prohlašuje, že nese veškerou odpovědnost v případě, že část obsahu smlouvy, která se týká obchodního tajemství účastníka, a která v důsledku toho bude pro účely uveřejnění smlouvy v registru smluv znečitelněna, pokud by smlouva v důsledku takového označení byla uveřejněna způsobem odporujícím ZRS, a to bez ohledu na to, zda byla smlouva uveřejněna prostřednictvím registru smluv ze strany zadavatele nebo účastníka.

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČO: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

Účastník tímto čestně prohlašuje, že neprodleně písemně sdělí zadavateli skutečnost, že takto označené informace přestaly naplňovat znaky obchodního tajemství.

Účastník tímto čestně prohlašuje, že údaje a skutečnosti uvedené ve smlouvě, která je nedílnou součástí nabídky, jsou údaji nebo skutečnostmi (s výjimkou obchodního tajemství, uvedeného výše), které nemohou být v registru smluv uveřejněny na základě ustanovení § 3 odst. 1 ZRS. Účastník dále čestně prohlašuje, že nese veškerou odpovědnost v případě, že část obsahu smlouvy, která obsahuje informace označené účastníkem jako informace ve smyslu § 3 odst. 1 ZRS a která v důsledku toho bude pro účely uveřejnění smlouvy v registru smluv znečitelněna, pokud by smlouva v důsledku takového označení byla uveřejněna způsobem odporujícím ZRS, a to bez ohledu na to, zda byla smlouva uveřejněna prostřednictvím registru smluv ze strany zadavatele nebo účastníka.

V …… dne ……

Příloha č. 7 zadávací dokumentace

Čestné prohlášení účastníka o střetu zájmů

Účastník:

Obchodní firma/jméno	[DOPLNÍ ÚČASTNÍK]
Sídlo/místo podnikání	[DOPLNÍ ÚČASTNÍK]
IČO	[DOPLNÍ ÚČASTNÍK]
Zastoupen	[DOPLNÍ ÚČASTNÍK]

který podává nabídku v řízení na zadání nadlimitní sektorové veřejné zakázky s názvem **„Realizace systému Zabezpečeného úložiště v prostředí Správy železnic", č.j. 60299/2026-SŽ-GŘ-O25** (dále jen „***Veřejná zakázka***" a ***„Zadávací řízení"***), tímto čestně prohlašuje, že:

a. **není** obchodní společností, ve které veřejný funkcionář uvedený v ust. § 2 odst. 1 písm. c) zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů (dále jen ***„Zákon o střetu zájmů"***), nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti, a

b. žádní poddodavatelé, jimiž prokazuje kvalifikaci v Zadávacím řízení, **nejsou** obchodní společností, ve které veřejný funkcionář uvedený v ust. § 2 odst. 1 písm. c) Zákona o střetu zájmů nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti.

Účastník dále čestně prohlašuje, že dostane-li se Účastník nebo poddodavatel, jímž prokazoval kvalifikaci v Zadávacím řízení, do střetu zájmů dle § 4b Zákona o střetu zájmů, a to kdykoliv až do okamžiku ukončení Zadávacího řízení, oznámí tuto skutečnost bez zbytečného odkladu zadavateli Veřejné zakázky.

Účastník si je vědom všech právních důsledků, které pro něj mohou vyplývat z nepravdivosti zde uvedených údajů a skutečností.

V …… dne ……

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČO: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

SPRÁVA ŽELEZNIC

Příloha č. 8 Zadávací dokumentace

Čestné prohlášení účastníka

Účastník:

Obchodní firma/jméno	[DOPLNÍ ÚČASTNÍK]
Sídlo/místo podnikání	[DOPLNÍ ÚČASTNÍK]
IČO	[DOPLNÍ ÚČASTNÍK]
Zastoupen	[DOPLNÍ ÚČASTNÍK]

který podává nabídku v řízení na zadání nadlimitní sektorové veřejné zakázky s názvem „**Realizace systému Zabezpečeného úložiště v prostředí Správy železnic**", (dále jen „***Veřejná zakázka***" a „***Zadávací řízení***"), tímto čestně prohlašuje, že:

a) on sám jakožto dodavatel, ani jeho poddodavatelé, nejsou osobami, na něž se vztahuje zákaz zadání veřejné zakázky ve smyslu § 48a zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů,

b) on sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti v Zadávacím řízení, ani žádný z jeho poddodavatelů nebo jiných osob, jejichž způsobilost je využívána ve smyslu evropských směrnic o zadávání veřejných zakázek, **nejsou** osobami dle článku 5k nařízení Rady (EU) č. 833/2014 ze dne 31. července 2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, ve znění pozdějších předpisů,

c) on sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti v Zadávacím řízení, ani žádný z jeho poddodavatelů nebo jiných osob, jejichž způsobilost je využívána ve smyslu evropských směrnic o zadávání veřejných zakázek, **nejsou** osobami dle článku 2 nařízení Rady (EU) č. 269/2014 ze dne 17. března 2014, o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, ve znění pozdějších předpisů, a dalších prováděcích předpisů k tomuto nařízení Rady (EU) č. 269/2014 anebo osobami dle čl. 2 nařízení Rady (ES) č. 765/2006 ze dne 18. května 2006 o omezujících opatřeních vzhledem k situaci v Bělorusku a k zapojení Běloruska do ruské agrese proti Ukrajině, ve znění pozdějších předpisů anebo osobami dle čl. 2 nařízení Rady (EU) č. 208/2014 ze dne 5. března 2014 o omezujících opatřeních vůči některým osobám, subjektům a orgánům vzhledem k situaci na Ukrajině, ve znění pozdějších předpisů (**tzv. sankční seznamy**).

Účastník dále čestně prohlašuje, že přestane-li on sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti v Zadávacím řízení, nebo některý z jeho poddodavatelů nebo jiných osob, jejichž způsobilost je využívána ve smyslu evropských směrnic o zadávání veřejných zakázek, splňovat výše uvedené podmínky, k nimž se toto četné prohlášení vztahuje, a to kdykoliv až do okamžiku ukončení Zadávacího řízení, oznámí tuto skutečnost bez zbytečného

odkladu, nejpozději však **do 3 pracovních dnů** ode dne, kdy přestal splňovat výše uvedené podmínky, k nimž se toto četné prohlášení vztahuje, zadavateli Veřejné zakázky.

Účastník si je vědom všech právních důsledků, které pro něj mohou vyplývat z nepravdivosti zde uvedených údajů a skutečností.

V [DOPLNÍ ÚČASTNÍK] dne [DOPLNÍ ÚČASTNÍK]

Příloha č. 9 Zadávací dokumentace - Výstupy z PTK

pozn.: Některé údaje byly z důvodu zachování anonymity účastníků PTK z níže uvedených odpovědí odstraněny nebo anonymizovány.

Dotaz č.

SPRÁVA ŽELEZNIC

Účastník 1	Účastník 2

2	Je pro Vás přiložená technická specifikace předmětu plnění (Příloha č. 2 a č. 3) srozumitelná? Pokud ne, uveďte, proč a co je potřeba doplnit či upřesnit.	ANO	ČÁSTEČNĚ - Specifikace na požadované zabezpečené úložiště je dle našeho názoru velice obecná a nekonkrétní. Na základě uvedených požadavků nejsme schopni navrhnout konkrétní konfigurace řešení a uvést odhadovanou cenu. Pro to je potřeba další detailnější specifikace a vyjasnění relativně velkého množství nejasností. Nejasnosti, které je dle našeho názoru potřeba vyjasnit jsou následující: Bližší specifikace ukládaných dat a systémů, které budou na úložiště přistupovat. Požadované protokoly pro přístup na data. Funkcionalita řešení úložiště vzhledem k ukládaným datům – jak má probíhat jejich uložení a zpřístupnění. Zda je požadavek na úložiště, které pouze prezentuje kapacitu nějakým protokolem (CIFS, NFS, S3) a zajišťuje jeho uložení, replikaci, retenci atd. nebo zda je požadována ještě nějaká nadstavbová logika zajišťující další služby pro uložená data. Detailní kapacitní požadavky se specifikací požadavků na výkonnost a propustnost řešení pro jednotlivé typy dat Specifikace požadavků na replikaci a dostupnost dat v případě výpadku jedné z lokalit

3	Uveďte prosím všechny kapitoly z Technických specifikací a jejich části, které nejste schopni splnit, případně uveďte důvod. Např. „4.5 Testovací provoz a pilot“.	Účastnit se budeme pouze části – zabezpečené úložiště. V rámci toho jsme schopni splnit veškeré části.

4	Nabízíte dodávku řešení formou „na klíč" včetně kontejneru, IT hardware, software, služeb, zabezpečení a následné podpory? V případě částečného plnění, uveďte, kterou část/i jste schopný realizovat	ANO	ČÁSTEČNĚ Nenabízíme kontejner.
5	Je možné rozdělit dodávku na části (např. zvlášť hardware, zvlášť integrační služby)?	ANO	Ideální je v tomto případě dodávka celkového řešení – tedy HW včetně implementačních služeb a následné technické podpory.

6	Zajišťujete instalaci mobilního kontejnerového datového centra v lokalitě zákazníka?	ANO	NE
7	Poskytujete součinnost při testování řešení před spuštěním do produktivního provozu? Uveďte příklady Vámi poskytované součinnosti při implementaci dodávky.	ANO - Zajišťujeme služby inženýringu, projektovou dokumentaci, výkony týkající se stavební připravenosti, osazení mobilního datového centra na místo určení a osazení na předem připravenou infrastrukturu, kompletní testing and commisioning, zaškolení obsluhy, kompletní servisní podpora a služby dálkového monitoringu.	ANO - Ano v rámci služeb poskytovaných k dodávce úložiště jsme schopni poskytnout kompletní implementaci a integraci do prostředí včetně specifikace akceptačních testů a jejich ověření.

8	Je možné po dodavateli požadovat spolupráci na úpravě interní dokumentace zadavatele (např. směrnice, metodiky, politiky)? Uveďte konkrétní technologické (vybavení kontejneru) a SW (IdM, DLP, XDR) oblasti Vaší možné součinnosti.	ANO - Kompletní non-IT infrastruktura v oblastech bezpečného spolehlivého a efektivního provozu, řízení a dálkového monitoringu, Kompletní IT infrastruktura (včetně FW), HW vybavení (instalace, zprovoznění, zahoření), SW vybavení (instalace, nastavení), IdM, DLP, XDR, IDS/IPS, SIEM, NMS, Syslog, bezpečná architektura,	ANO - Jsme schopni spolupracovat na úpravě interní dokumentace související s dodávkou zabezpečeného úložiště. Typicky se jedná o provozní dokumentaci k dodanému řešení, zpracování bezpečnostní dokumentace a případně zpracování DR plánů pro službu zabezpečeného úložiště.

9	Jaká je nejkratší předpokládaná doba dodání díla od podpisu smlouvy? Uveďte dobu dodání včetně instalace a uvedení do provozu. V případě částečného plnění (kontejner/zabezpečené úložiště) uveďte dobu dodání za každou takovou část.	4 měsíce bez IT infrastruktury 6 měsíců včetně IT infrastruktury	Zabezpečené úložiště: Doba dodání záleží na konkrétním řešení HW komponent a rozsahu služeb. Obecně je možné počítat s dodáním HW komponent do 6 týdnů a následné implementaci řešení přibližně v rozsahu 2 měsíců. Pokud je součástí dodávky i migrace dat, pak je potřeba počítat s delším časovým úsekem podle objemu dat a způsobu migrace.

10	Jakou byste navrhoval architekturu zabezpečení komunikace vámi dodávaného bezpečného úložiště, aby byla v souladu s technickou specifikací (prosím uveďte popis nebo high level diagram)?	Předpokládáme, že z důvodu zaručení nízké latence pro geo-redundanci dat v požadované kvalitě jsou jednotlivá data centra součástí páteřní separované datové sítě. Stejně tak předpokládáme, že s ohledem na SLA jsou jednotlivá datová centra vždy připojena pomocí minimálně 2 separátních datových linek, kdy každá je zprostředkována jiným poskytovatelem. Každé datové centrum bude vybaveno hraničním firewallem a IPS, což bude zaručovat monitorování a vyhodnocování komunikace dovnitř a ven z datového centra. Samozřejmostí je, že veškeré komunikace je šifrována dle poslední platné legislativy. Interní síť je rozdělena do příslušných VLAN do jednotlivých kategorií. Komunikace mezi jednotlivými VLANami je řízena na bázi protokolů a omezena na pouhé nejnutnější minimum. Součástí VLAN jsou i nastražené decoy (honeypot), které budou sloužit pro detekci podezřelých aktivit v síti. Součástí je i síťová sonda	Zabezpečení komunikace závisí zejména na specifikaci systémů, které s úložištěm budou komunikovat a škálu komunikačních protokolů, které tyto systémy či uživatelé umožňují využít.

11	Máte zkušenosti s veřejnými zakázkami v oblasti kritické infrastruktury?	ANO	ANO

12	Splňuje řešení požadavky zákona o kybernetické bezpečnosti (ZoKB) 264/2025 Sb. a vyhlášky o kybernetické bezpečnosti (VoKB) 409/2025 Sb.? Jaké certifikace nebo audity to dokládají?	ANO ISO 27000 a příslušné podčásti. V případě auditu se musí zajistit pravidelné provádění penetračních testů.	ANO - V tom kontextu, že s pomocí navrhovaného řešení je možné zajistit splnění vybraných požadavků ZoKB a VoKB. Tato legislativa a priori nestanovuje explicitní požadavky na řešení nebo technologii. Ani nespecifikuje postupy a způsoby certifikace technologií. S využitím auditu je možné ověřit, že reálná implementace navrhovaných technologií splňuje požadavky ZoKB a VoKB, resp. přispívá ke splnění požadavků kladených touto legislativou na zadavatele.

13	Máte praktické zkušenosti s projektu pro klienta, na kterého se vztahuje ZoKB 181/2014 Sb. a VoKB? Pokud ano, stručně je popište.	ANO - V rámci XXX byl realizován návrh, implementace, zprovoznění a údržba infrastruktury v rámci IT a OT.	ANO - Máme zkušenosti s dodávkou infrastrukturních řešení pro klienty, na něž se vztahuje ZoKB a VoKB. Máme zkušenosti i s dodávkou řešení do oblasti kritické infrastruktury a významných informačních systémů. U vybraných projektů zpracovávání i bezpečnostní analýzu a bezpečnostní dokumentaci posuzující splnění požadavků VoKB při nasazení řešení, resp. dokumentující, jak implementace navrhovaného řešení zajišťuje splnění vybraných požadavků ZoKB a VoKB kladených legislativou na zadavatele

14	Dle jakých norem (ISO, EN, ČSN) je řešení navrhováno? Rozepište prosím dle jednotlivých kategorií (elektro, fyzická bezpečnost, požární bezpečnost a další)?	Elektro ▪ Zákon 183/2006 Sb. Stavební zákon ▪ Nařízení vlády 93/2012 Sb., kterým se stanoví podmínky ochrany zdraví při práci ▪ Nařízení vlády 258/2000 Sb. – Zákon o ochraně veřejného zdraví a o změně některých souvisejících zákonů ▪ Nařízení vlády 272/2011 Sb. – o ochraně zdraví před nepříznivými účinky hluku a vibrací. ▪ ČSN 33 2000-1 ed.2 Elektrické instalace nn – Část 1: Základní hlediska, stanovení základních charakteristik, definice ▪ ČSN 33 2000-4-41 ed.3 Ochrana před úrazem elektrickým proudem ▪ ČSN 33 2000-4-444 Ochrana před EMC (napěťovým a elektromagnetickým rušením) ▪ ČSN 33 2000-4-46 ed. Odpojování a spínání ▪ ČSN 33 2000-4-42 ed.2 Ochrana před účinky tepla ▪ ČSN 33 2000-4-43 ed.2 Ochrana proti nadproudům ▪ ČSN 33 2000-5-51 ed.3 Výběr a stavba elektrických zařízení – Všeobecné předpisy ▪ ČSN 33 2000-5-52 ed.2 Výběr soustav a stavba vedení	Není relevantní. Předmětem námi navrhovaného řešení není řešení samotného datového centra, k němuž se otázka vztahuje (elektro, fyzická bezpečnost, požární bezpečnost, …). Jednotlivé navrhované technologie splňují požadavky národní a EU legislativy v oblasti elektrické bezpečnosti a dalších relevantních norem

15	Jaká je orientační cena plnění za část „Mobilní kontejnerové datové centrum“? Prosíme o předložení cenového rozpadu.	22 500 000 Kč (bez DPH) bez IT Dodávka technologické části na klíč: 21 000 000 Kč Realizace služeb: 1 500 000 Kč	Tuto část nenabízíme.

16	Jaká je orientační cena plnění za část „Realizace systému zabezpečeného úložiště v prostředí Správy železnic“? Prosíme o předložení cenového rozpadu.	S ohledem na široká rámec zadání a nedostatek detailních informací se cena může pohybovat v rádu nižších desítek milionů korun	Pokud budou požadavky na systém zabezpečeného úložiště konkretizovány budeme schopni orientační cenovou nabídku zpracovat.

17	Byla by cena v případě dodání obou částí (kontejner + IT vybavení) pro zadavatele výhodnější? Uveďte předpokládanou cenu celkového plnění. Prosíme o předložení cenového rozpadu.	S ohledem na předchozí lze dovozovat, že realizací obou částí současně je možné předpokládat celkovou úsporu nákladů.	Kontejner nenabízíme.

18	Nabízíte možnost pořízení formou jednorázové investice (CapEx)?	ANO	ANO - Obecně jsme schopni k navrhovaným řešením nabídnou model financování OpEX i CapEX
19	Nabízíte možnost pořízení formou průběžných plateb (OpEx)?	ANO	ANO - Obecně jsme schopni k navrhovaným řešením nabídnou model financování OpEX i CapEX.

20	Je možné získat rámcový ceník nebo ukázkovou konfiguraci s cenou? Pokud ano, uveďte prosím odkaz k nahlédnutí či stažení.	NE - Rámcový ceník není k dispozici pro koncové zákazníky. Každá konfigurace je navrhovaná pro konkrétní technické a provozní podmínky zákazníka.	NE

21	Lze odhadnout provozní náklady řešení na 1 rok, 5 let a 10 let dopředu? Pokud ano, uveďte prosím částku.	Cca 600 000 Kč/1 rok 3 000 000 Kč /5 let 8 000 000 Kč/10 let	NE

22	Jaká je předpokládaná životnost jednotlivých technologií? kontejner + podpůrné technologie data storage, servery	20 let kontejner 15 let podpůrné technologie 5 let je standartní životní cyklus pro IT infrastrukturu	Datastorage a servery Jednotlivé HW komponenty mají životnost typicky do 7 let. Typicky je možné v iniciální dodávce zakoupit HW podporu na 5-7 let a případně po uplynutí této doby HW podporu prodloužit. PO cca 7 letech provozu již není možné standardní HW podporu prodlužovat a HW je již zastaralý a dochází k jeho obměně. U řešení s potřebou delšího životního cyklu je pak dlouhodobá životnost zajištěna na SW úrovni, která zajistí kontinuitu provozu datového úložiště i v případě výměny části HW komponent

23	Nabízíte model TCO výpočtu pro různé varianty konfigurace?	ANO	ANO

24	Dodávali jste v posledních 3 letech obdobné řešení jiným subjektům?	ANO	ANO

25	Uveďte prosím seznam vašich relevantních projektů v oblasti kontejnerového řešení a zabezpečeného úložiště včetně stručného popisu předmětu dodávky/služby.	Reference v oblasti mobilních datových center: • XXX - 2 ks • XXX – 1 ks • XXX – 1 ks • XXX – 1 ks • XXX – 4 ks • XXX • XXX – 1ks • XXX – 1ks • XXX – 1ks Reference v oblasti zabezpečeného uložiště: • XXX • XXX • 3 významné instalace v předních bankovních domech Uvádíme pouze reference z ČR, v případě zájmu můžeme předložit i zahraniční	Projekty zabezpečeného úložiště: XXX Objektová storage ECS (2023) -Dodávka, instalace, implementace a podpora objektové storage Objektová storage (2024) -Dodávka, instalace, implementace a podpora objektové storage Backup for IM infrastructure (2022) -Dodávka Data Domain včetně instalace a implementace XXX☐ Nové backup uložiště (objektová storage ECS) (2024) -Dodávka, instalace, implementace a podpora objektové storage v mobilním kontejnerovém datovém centru XXX Dodávka zálohovacích zařízení (2024)

26	Uveďte seznam vašich relevantních projektů v oblasti kritické infrastruktury (KII) včetně stručného popisu předmětu dodávky/služby.	XXX	Projekty zabezpečeného úložiště: XXX Objektová storage ECS (2023) -Dodávka, instalace, implementace a podpora objektové storage Objektová storage (2024) -Dodávka, instalace, implementace a podpora objektové storage Backup for IM infrastructure (2022) -Dodávka Data Domain včetně instalace a implementace XXX Dodávka zálohovacích zařízení (2024) -Dodávka zálohovacích zařízení (DataDomain, páskových knihoven, zálohovacího SW) včetně instalace a implementace. XXX Technická infrastruktura pro CMS 2.5

27	Máte zkušenosti s integrací HSM a IDM? Uveďte konkrétní příklady včetně stručného popisu předmětu dodávky/služby.	ANO	ČÁSTEČNĚ - Máme zkušenosti d integrací dodávaných úložišť na KMS systémy pro správu šifrovacích klíčů a IDM pro řešení identit.

28	Máte zkušenosti s integrací XDR od výrobce Fidelis?	ČÁSTEČNĚ	NE

29	Uveďte příklady vašich projektů, jejichž předmětem byla dodávka mobilního datového centra s minimální diskovou kapacitou 3 petabajtů, včetně provozní podpory (SLA).	Touto informací nedisponujeme, protože osazování námi dodávaných kontejnerových center si zajišťoval objednatel. Námi doposud realizované reference týkající se zabezpečeného uložiště a cloudových služeb byly umístěny do fixního datového centra.	XXX☐ Nové backup uložiště (objektová storage ECS) (2024) -Dodávka, instalace, implementace a podpora objektové storage v mobilním kontejnerovém datovém centru (3,4 PB) Typy podpory: Nabízíme technickou podporu na námi dodávaná řešení v režimu 5x9 i 7x24 s reakční dobou 2h (po dohodě i kratší). Technická podpora typicky řeší provozní incidenty vzniklé v rámci podporovaných komponent i mezi nimi. Komunikace probíhá prostřednictvím emailu, telefonu a webového portálu, kde je možné sledovat průběh řešení incidentu. Technickou podporu je pak možné rozšířit o další služby – Proaktivní podporu, Patch management, Předplacené konzultační a konfigurační služby.

30	Máte zkušenosti s migrací dat v rozsahu petabajtů? Jaké nástroje jste použili?	ANO	ANO - Máme zkušenosti jak z migrace primárních dat mezi produkčními datovými úložišti, tak z migrace záloh mezi různými zálohovacími SW. Konkrétní migrační postup a nástroj je zvolen na základě detailního posouzení zdrojové a cílové platformy pro uložení dat a specifik zákaznického prostředí.

31	Uveďte příklady vašich projektů s geografickou redundancí a disaster recovery včetně stručného popisu předmětu dodávky/služby.	3 významné instalace v předních bankovních domech	Geografickou redundancí: XXX VxRail stretched cluster (2022, 2023) -Vytvoření komplexní platformy „on-premise" pro provoz a rozvoj informačních systémů společnosti. Dodávka obsahovala VxRail cluster, networking, servery, datová uložiště a DPS. Součástí byla rovněž instalace, implementace a následná technická podpora řešení. XXX Obměna diskových polí (storage infrastruktury) v ústředí MZV a SZEU Brusel (2024) -Dodávka diskových polí do dvou lokalit (Praha a Brusel) včetně instalace, implementace a následné technické podpory Disaster recovery: XXX□ Nové backup uložiště (objektová storage ECS) (2024)

32	Poskytujete školení a dokumentaci v českém jazyce?	ANO	ANO - Pro řešení zabezpečeného úložiště jsme schopni nabídnout školení i zpracování dokumentace v českém jazyce.

33	Máte k dispozici náhled vzorového řešení? Například vzorový kontejner na ukázku nebo zprostředkovaná návštěva za účelem prohlídky kontejneru u zákazníka. Případně byla by možná návštěva Vašeho výrobního závodu?	ANO	NE

Účastník 3	Účastník 4	Účastník 5

ANO	Tento dotaz nebyl zodpovězen.	Technická specifikace IT části PTK neobsahuje parametry potřebné k definování typů a počtů jednotlivých částí řešení.

ANO	Tento dotaz nebyl zodpovězen.	Obecně jsme schopni splnit dodávku a implementaci IT prvků řešení, pokud je bude možno postavit na základě našeho portfolia.

ANO	Tento dotaz nebyl zodpovězen.	Jsme schopni dodat komplexní IT řešení na klíč i s podporou.
ANO	Tento dotaz nebyl zodpovězen.	Obecně ANO

ČÁSTEČNĚ - Instalace (myšleno kontejner včetně veškerého technického vybavení) se provádí ve výrobní hale Zhotovitele. V lokalitě zákazníka probíhají už pouze připojení na stávající infrastrukturu (napájení, konektivita, odpad, monitoring apod.), testování a zkušební provoz.	Tento dotaz nebyl zodpovězen.	NE
ANO	Tento dotaz nebyl zodpovězen.	Záleží na výsledném výběru technologií

ČÁSTEČNĚ	Tento dotaz nebyl zodpovězen.	Bez dalších informací není možno zodpovědět

Min. 6 - 8 měsíců. Podmínkou je získání stavebního povolení v místě instalace, pokud to daná lokalita a legislativa vyžaduje. Kontejner 6 měs. Úložiště 2 měs	Tento dotaz nebyl zodpovězen.	Záleží na vybraných technologiích

Tento dotaz nebyl zodpovězen.	Záleží na vybraném úložišti, účelu a způsobu jeho využití. Nemáme k odpovědi potřebné podklady.

ANO	Tento dotaz nebyl zodpovězen.	ANO

Toto by měl prokázat navrhovatel, projektant nebo zpracovatel zadání.

Tento dotaz nebyl zodpovězen.

Nelze zodpovědět, není známo řešení.

ANO	Tento dotaz nebyl zodpovězen.	ISZR, NAKIT

Toto by měl prokázat navrhovatel, projektant nebo zpracovatel zadání.

Tento dotaz nebyl zodpovězen.

Z pohledu IT infrastruktury bude záležet na vybrané technologii

15-20 mil. Kč bez DPH	Tento dotaz nebyl zodpovězen.	Nenabízíme

V tuto chvíli nedokážeme odhadnout cenu za tuto část

Tento dotaz nebyl zodpovězen.

Záleží na vybraném řešení. Nemáme k odpovědi potřebné podklady.

Předpokládáme, že ANO	Tento dotaz nebyl zodpovězen.	Záleží na vybraném řešení. Nemáme k odpovědi potřebné podklady.

ANO	Tento dotaz nebyl zodpovězen.	ANO
ČÁSTEČNĚ	Tento dotaz nebyl zodpovězen.	Záleží na vybraném řešení. Nemáme k odpovědi potřebné podklady.

NE	Tento dotaz nebyl zodpovězen.	Záleží na vybraném řešení. Nemáme k odpovědi potřebné podklady.

NE	Tento dotaz nebyl zodpovězen.	Záleží na vybraném řešení. Nemáme k odpovědi potřebné podklady.

kontejner + podpůrné technologie - min. 10 let data storage, servery – min. 5 let	Tento dotaz nebyl zodpovězen.	Záleží na vybraném řešení. Nemáme k odpovědi potřebné podklady.

ČÁSTEČNĚ	Tento dotaz nebyl zodpovězen.	Záleží na vybraném řešení. Nemáme k odpovědi potřebné podklady.

ČÁSTEČNĚ	Tento dotaz nebyl zodpovězen.	NE

Vzhledem k mlčenlivosti nelze v tuto chvíli poskytnout – státní organizace	Tento dotaz nebyl zodpovězen.	XXX

XXX	Tento dotaz nebyl zodpovězen.	XXX

ČÁSTEČNĚ	Tento dotaz nebyl zodpovězen.	ANO

NE	Tento dotaz nebyl zodpovězen.	NE

žádné	Tento dotaz nebyl zodpovězen.	Nedodávali jsme

NE	Tento dotaz nebyl zodpovězen.

XXX	Tento dotaz nebyl zodpovězen.	XXX

ANO	Tento dotaz nebyl zodpovězen.	ANO

NE	Tento dotaz nebyl zodpovězen.	NE

Název uchazeče

Účastník 6	Účastník 7	Účastník 8

ANO – z pohledu Mobilního kontejnerového Datového Centra ČÁSTEČNĚ – z pohledu Zabezpečeného úložiště. Mobilní kontejnerové DC: Řešení definované v dokumentaci předběžného návrhu nabídkového řízení je plně realizovatelné s využitím modulárního datového centra. Spolupráce ze strany klienta bude nezbytná zejména v následujících oblastech: • Zajištění přístupu na místo pro instalaci a následné činnosti související s provozem a případnou demontáží a přemístěním POD MDC na jiné místo klienta. • Přidělení vhodného prostoru na místě klienta pro umožnění stavební přípravy a instalace dle dokumentace předběžného návrhu nabídkového řízení. • Zajištění přípojek pro elektřinu, pitnou vodu a datovou konektivitu nezbytnou pro provoz modulárního datového centra. • Vedení jednání s příslušnými státními orgány, včetně získání potřebných stavebních povolení, provozních povolení atd.	Nezúčastnili se PTK.	Příloha č. 2 – ANO. V navrhovaném řešení si umíme představit několik úprav uvedených v poznámkách. Technická specifikace neobsahuje požadavky skladování v případě odstaveného modulu. Tato situace explicitně není v zadání uvedena, ale vyplývá ze souvislostí použití v krizových situacích.

Všechny kapitoly jsme schopni splnit. Nejsme však schopni splnit veškeré uvedené funkcionality nativně a to:

• DLP jako nativní část storage. Nabízíme možnost řešení na LAN vrsvě jinými produkty
• Nativní NAS souborový přístup

Navržené řešení je realizovatelné, doporučujeme zvážit různé technologie z důvodu optimalizace rozměrů a zvýšení transportovatelnosti.

ANO – společnost je schopna realizovat všechny požadované části. Na některé části bychom možná využili spolupráci s autorizovaným partnerem.	ANO
ANO	ANO

ANO, a zároveň samozřejmě umíme poskytnout i
součinnost před nasazením do provozu
Váš komentář k navrhovanému řešení.
Zařízení podléhají dvěma typům testování:
• FAT – Přejímací zkoušky ve výrobě, které se provádějí
ve výrobě před dodáním. To stejné se týká všech
produktů společnosti, tj. rovněž bezpečného
úložiště
• SAT – Přejímací zkoušky na místě, které se provádějí
u zákazníka před schválením

ANO - Jedná se například o:
xxx IT Module Dokumentaci
xxx Power Module Dokumentaci
xxx UPS System Dokumentaci
xxx Fire Suppression System Dokumentaci
Nasazení a provoz kontejneru
Nasazení a provoz hw/sw infrastruktury
Nasazení a provoz backup řešení
Nasazení a provoz
IDM+PAM+AD+SSO+MFA
Nasazení a provoz XDR řešení
Nasazení a provoz Monitorigu

ANO - Pro konkrétní umístění je nutné podchytit rizika:

Lokalita, umístění

Zabezpečení stanoviště

Zabezpečení servisního prostoru

Modulární řešení datového centra vyžaduje úpravu standardního XXX, což má vliv na časový harmonogram. Orientační harmonogram • 4–6 týdnů: Přípravná fáze (projektová dokumentace pro výrobu POD MDC a práce na místě) • 28–30 týdnů: Předpokládaná doba dodání IT a napájecích modulů po schválení finálního návrhu • 2 týdny: Doprava na místo a instalace (za předpokladu dokončení přípravy místa a povolení) • 1 týden: Uvedení do provozu, testování a předání Předpokládaná doba dodání zabezpečeného úložiště včetně instalace a uvedení do provozu je 6-8 týdnů	ANO

Modulární řešení datového centra vyžaduje úpravu
standardního XXX, což má vliv na časový harmonogram. Orientační harmonogram
• 4–6 týdnů: Přípravná fáze (projektová dokumentace
pro výrobu POD MDC a práce na místě)
• 28–30 týdnů: Předpokládaná doba dodání IT a
napájecích modulů po schválení finálního návrhu
• 2 týdny: Doprava na místo a instalace (za předpokladu
dokončení přípravy místa a povolení)
• 1 týden: Uvedení do provozu, testování a předání
Předpokládaná doba dodání zabezpečeného úložiště
včetně instalace a uvedení do provozu je 6-8 týdnů

Na základě aktuální situace je předpokládaná doba dodání díla 6 – 7 měsíců od podpisu smlouvy

Pro návrh přesné architektury bychom potřebovali
některé informace ještě dospecifikovat viz také Dotaz
č.2.
Velice bychom uvítali diskuzi přímo se zákazníkem,
abychom ještě více do detailů pochopili potřeby
zákazníka a navrhli tak co nejoptimálnější řešení.

ANO

ANO - Jsme dodavatelem technologických celků v oboru zabezpečovacích, sdělovacích, řídících a komunikačních technologií dopravní infrastruktury.

ANO

ANO - Společnost XXX, má praktické zkušenosti s projekty pro klienta, na kterého se vztahuje ZoKB 181/2014 Sb. a VoKB”

Řešení společnosti XXX je navrhováno dle norem ISO
9001:2015 a ISO 27001:2022
XXX splňují následující předpisy:
• EN50600
• Evropské předpisy
• Povinné certifikace pro Českou republiku týkající se
instalovaných systémů

Jedná se o celý soubor norem pokrývající jednotlivé části, jmenovitě nejdůležitější:

Non-it infrastruktura dle EN 50600

Konstrukce dle EN 1011, protikorozní ochrana dle ČSN EN 12944

Na základě poskytnutých vstupů je rozsah definován
velmi široce, proto je těžké určit cenu.
Náš odhad pro kompletní řešení XXX se pohybuje
mezi 2 miliony eur a 2,5 miliony eur, včetně hardwaru
POD, instalace, logistiky, uvedení do provozu,
dokumentace a školení

Část dodávka, instalace a zpuštění – 39 200 000 Kč bez DPH v rámci České republiky.

Část profylaktické kontroly a revize – 595 000 Kč bez DPH za 1 rok v rámci České republiky.

Náš odhad pro kompletní zajištění
Zabezpečeného
úložiště včetně HW (storage, servery),
služeb,
instalace, uvedení do provozu,
dokumentace, školení se
pohybuje okolo 4 milionů EUR

ANO
Konkrétní úsporu bychom byli schopni
vyčíslit po bližším
vyspecifikování technického řešení

ANO

ANO

ANO

NE

ČÁSTEČNĚ - Pro získání ukázkové konfigurace a ceny bychom určitě potřebovali dospecifikovat poptávané řešení

NE - Jedná se o specifický návrh odpovídající požadavkům Zadavatele.

ANO - Pro odhad provozních nákladů bychom ale potřebovali dospecifikovat poptávané řešení

ČÁSTEČNĚ - Jedná-li se o provozní náklady vztažené ke spotřebě energie, pak při výkonu IT zařízení 100kW, PUE 1.3 a ceně 4 Kč/kWh, jsou provozní náklady v hodnotě cca 4,5M Kč bez vlivu inflace a pohybu cen energie na trhu. Pro výpočet ostatních nákladů je potřeba znát bližší zadání, četnost transportů atd

Předpokládaná životnost kontejneru + podpůrných
technologií je 20 let pro hlavní plášť.
HW vybavení (data storage, servery) se nejčastěji
pořizuje na dobu 5ti let, nicméně jeho životnost je
samozřejmě delší. Z pohledu životního cyklu
doporučujeme obměnu HW nejpozději po 7mi letech,
doporučujeme však již zmíněných 5 let

ČÁSTEČNĚ - Životnost kontejneru je až 50 let při pravidelné údržbě a zejména obnově antikorozního nátěru. Celková délka životnosti je pak ovlivněna prostředím, ve kterém je kontejner umístěn z pohledu vlhkosti, větru, vody, sněhu.

Podpůrné technologie – životnost je zásadně ovlivněna provozními podmínkami, zejména teplotou, která může zásadně zkrátit životnost jednotlivých technologií. Při dodržení plánu údržby je typická životnost až 15 let.

ANO

ANO		ČÁSTEČNĚ - Sdělovací a zabezpečovací místnosti pro drážní infrastrukturu.

Technologické celky v oboru zabezpečovacích, sdělovacích, řídících a komunikačních technologií dopravní infrastruktury ve střední Evropě

Jednalo se o dodávky do veřejné, státní správy v rámci České Republiky. Poskytovat jména subjektů či projektů však nemáme dovoleno.

ANO - Některé integrace jsme zajišťovali přímo XXX
technickými lidmi, u některých projektů spolupracujeme
s našimi autorizovanými partnery

ČÁSTEČNĚ - Na integraci XDR od výrobce Fidelis bychom byli schopni spolupracovat s některým z našich autorizovaných partnerů, kteří XDR řešení od společnosti Fidelis prodávají a implementují

ANO - Z pohledu nástrojů využíváme
například: Vmware
Vmotion či Storage based migrace
prostřednictvím XXX
Peer Motion, VirtualDisc

ANO

ANO

ANO - Určitě je možné domluvit si návštěvu XXX v továrně v Nizozemsku nebo v Customer Innovation Centru v Ženevě	ČÁSTEČNĚ

Účastník 9	Účastník 10	Účastník 11

NE - Nejasnosti vyplývající z předaných podkladů PTK mají zásadní dopad na architekturu řešení i celkovou cenu. Pro úplnost odpovědi, uvádíme níže v jednotlivých odpovědích.	ČÁSTEČNĚ - Stavební připravenost lokality – Příloha č. 2, bod 1.5 je uvedeno, že dodavatel provede základové a výkopové práce. Bod 1.6 uvádí, že stavební připravenost není předmětem této veřejné zakázky a bude realizováno samostatně Zadavatelem. Které zadání platí? V orientační ceně je naceněno bez stavební připravenosti lokality. Optické předkonektorované trasy – Příloha č. 2, bod 1.33 uvádí předkonektorované trasy OM4, MM duplex SC/UPC a OS2, Simplex E2000/APC, přičemž dle bodu 1.33.1 má být rack vybaven patchpanelem s optickými porty duplex LC OM4. Co platí? Profylaxe chlazení – bod 1.37 – pro kritickou infrastrukturu a nepřetržitý provoz doporučujeme pravidelné prohlídky 2x ročně. Ventilace – pro delší pobyt obsluhy v uzavřeném prostoru chybí řízená ventilace. Pouhé větrání otevřenými dveřmi není vhodné z důvodu pronikání prachu a vlhkosti z vnějšího prostředí	V rámci technických specifikací Non-IT infrastruktury jsou u některých technologických komponent specifikovány požadavky tak, že směřují k velice úzce omezenému počtu výrobců, aniž by to reálně pro uživatele přinášelo nějaké benefity (technické, provozní či bezpečnostní). Výrazně se tak omezuje počet možných uchazečů a reálná hospodářská soutěž. Např. popis UPS Systém – požadována je DPA architektura – používají snad pouze 2 výrobci, z pohledu spolehlivosti systému a jeho elektrických vlastností nepřináší žádné benefity, je to pouze marketingový nástroj pro odlišení se a využití pro eliminaci konkurence. Architektura UPS DPA (Decentralized Parallel Architecture) je modulární design, ve kterém každý UPS modul má své vlastní napájecí a řídicí jednotky, integrovaný statický bypass. Tento typ architektury používá velice omezený počet výrobců, prakticky snad

Z PTK není jasné, zda se jedná o kontejner, který bude využívám pouze pro Compute a Storage (z popisu PTK nám to tak připadá) nebo se má jednat o kontejner jako plnohodnotné Datové mobilní centrum - prosíme o objasnění záměru. Za předpokladu, že má být plnohodnotné datové mobilní centrum a má sloužit i pro disaster recovery, bylo by vhodné mít i plnohodnotnou infrastrukturu v kontejneru, tedy názorně: o Routery o Firewally o DC Switche o SAN o WAF o XDR o Load-Balancery o Logování/SIEM o OoB Management, atpod Prosíme o objasnění, toto totiž může výrazně změnit celkové řešení a hlavně cenu . Za předpokladu, že se jedná o DR bez komponent výše, se můžete bránit pouze proti výpadku storage či compute v primární lokalitě (zbylé komponenty v primární lokalitě ale musí běžet a musí být z druhého DC dostupné) - toto řešení není úplně běžné a není z pohledu DR designu doporučované – žádáme o objasnění	Níže uvedené body neznamenají, že nejsme schopni splnit požadavky uvedené v Technické specifikaci. Uvádíme doporučení s ohledem na užití v kritické infrastruktuře státu. Chlazení – doporučujeme využití CW sálových jednotek v konfiguraci 2N namísto in-row jednotek. Pro splnění TIER III musí být in-row jednotky připojeny na 2 nezávislé okruhy. To představuje komplikované rozvody chladícího média s velkým počtem ventilů a složitým řízením. To představuje potenciální zdroj problémů pro regulaci a opakovanou transportovatelnost. Použitím sálových jednotek dojde k podstatnému zjednodušení rozvodů. Transportovatelnost - z důvodu dosažení co nejnižší výšky a omezení při transportu, navrhujeme dodávku ve 2 částech, modul a střešní platforma, kde budou umístěny chillery. Stabilní hasící zařízení – nedoporučujeme použití autonomního hasícího systému se zónovým hašením na	Obecné požadavky jsme schopni splnit Popis UPS – komentář viz. výše Kombinace parametrů na frontend diskového pole (protokoly SMB, NFS, FC, iSCSI současně – tj. požadavek na kombinaci blokového a file přístupu). Požadavek na rozšiřování kontrolerů eliminuje řadu výrobců diskových polí.

ANO - Včetně integrace do stávající bezpečnostní a provozní architektury zadavatele	ČÁSTEČNĚ pro dodávku Mobilního kontejnerového datového centra.	ANO - Dodávku jsme schopni realizovat jako celek v rámci spolupráce s naším IT partnerem. Za předpokladu, že zadání a nastavená akceptační kritéria budou součástí zadání VŘ a budou jednoznačná. Pozn. Je možné navrhnout, dodat a naimplementovat řešení, které bude plnit požadavky na službu (SLA – RTO/RPO, výkonové a kapacitní požadavky apod.) aniž by zadavatel musel předepisovat detailní technologické
ANO - Z pohledu provozní odpovědnosti považujeme za rizikové řešení z hlediska kompatibility/funkčnosti, poskytovaných záruk včetně servisu a definice zodpovědností přes více různých dodavatelů.	ANO pro dodávku Mobilního kontejnerového datového centra.	ANO / ČÁSTEČNĚ Samostatně kontejner s NON-IT technologií, samostatně část IT. Další dělení těchto celků by nedávalo smysl, stírala by se odpovědnost za logický celek. Pro daný celek platí: Není možné obecně předpokládat, že „jiný" implementátor bude schopen implementovat řešení na technologiích, které nezná – a i kdyby technologie znal, svoje řešení může koncipovat jinak a dodané technologie mu nemusí vyhovovat. Pro Zadavatele bude jednoznačně výhodnější pokud bude Dodavatel garantovat řešení daného celku jako celek.

ANO	ANO	ANO - Součástí dodání je doprava do místa instalace, usazení kontejneru, jeho připojení na sítě a následné oživení. Vše je otázkou dohody na rozhraní dodávek.
ANO - Např. zátěžové testy, testovací provoz, orchestrace celkového řešení včetně testů dostupnosti, DR scénářů a bezpečnostních opatření	ANO pro dodávku Mobilního kontejnerového datového centra. Dle technické specifikace kompletní funkční zkouška po dobu 48 hodin s otestováním různých scénářů. Dodávka DA není součástí, pro kompletní otestování je nutná součinnost Zadavatele.	ANO - V rámci oživení a uvedení do provozu poskytujeme zátěžové testy, zkušební provoz, zaškolení obsluhy,…..

ANO - Dodavatel je připraven poskytnout součinnost při úpravě a doplnění interní dokumentace zadavatele v rozsahu odpovídajícím finálnímu technickému a bezpečnostnímu řešení. Konkrétní rozsah této součinnosti bude závislý na upřesnění architektury řešení a role jednotlivých komponent (viz Dotaz 3). Součinnost může zahrnovat zejména oblasti související s: – provozní a bezpečnostní architekturou mobilního kontejnerového datového centra, – návrhem a popisem technických a organizačních bezpečnostních opatření dle ZoKB a souvisejících prováděcích předpisů, – úpravami provozních postupů, havarijních a disaster recovery scénářů, – zapracováním změn vyplývajících z implementace technologií v oblastech IdM, PAM, HSM, DLP, XDR a centrálního logování. Konkrétní technologický i dokumentační rozsah bude možné jednoznačně stanovit až po upřesnění	NE - Týká se přílohy č. 3 – data storage. Tuto část nenabízíme	ANO - V tuto chvíli neznáme úroveň a rozsah vašich dokumentací, určitě jsme schopni poskytnout součinnost v této oblasti.

Orientační doba dodání řešení od podpisu smlouvy, včetně výroby mobilního kontejnerového datového centra, dodávky a instalace technologického vybavení, integrace, testování a uvedení do produkčního provozu, se pohybuje v rozmezí 9–12 měsíců. Konkrétní harmonogram realizace bude záviset zejména na včasném upřesnění technického rozsahu řešení, roli mobilního kontejnerového datového centra v rámci disaster recovery, rozsahu bezpečnostních a síťových komponent a integračních vazbách na stávající prostředí zadavatele.	Na základě našich zkušeností s obdobnými projekty je dodání vč. zprovoznění Mobilního datového centra dle přílohy č. 2 v délce 8 měsíců.	Výsledný termín dodání se odvíjí od konečné požadované konfigurace jak v oblasti kontejneru, tak IT části. Předpokládaná doba dodání je u kontejneru 4 – 8 měsíců od objednání. U IT části bohužel nelze komentovat rychlost dodávek, když z dodaných podkladů nelze ani určit, co bude součástí dodávek… Budeme-li předpokládat, že Zadavatel vyspecifikuje ve VŘ požadavky na „obvyklé“ zálohovací řešení, pak dodávka technologií může být v řádu 4-6týdnů, instalace, analýza a implementace řešení řádově 2- 3měsíce podle možností Zadavatele poskytovat

Architektura zabezpečení komunikace dodávaného zabezpečeného úložiště by byla navržena v souladu s principy obrany do hloubky (defence-in-depth) a s ohledem na požadavky technické specifikace a provoz kritické infrastruktury. Na vysoké úrovni lze předpokládat oddělení jednotlivých bezpečnostních zón (produkční prostředí, management, integrační a záložní/DR zóna), řízení komunikace prostřednictvím bezpečnostních síťových prvků (firewally, segmentace sítě), šifrování komunikace mezi lokalitami i jednotlivými komponentami a centrální řízení přístupů. Součástí architektury by bylo řízení identit a přístupů prostřednictvím IdM/PAM, využití vícefaktorové autentizace, centralizované logování a dohled nad bezpečnostními událostmi, včetně integrace s nástroji typu SIEM/XDR. Konkrétní topologie, použité technologie a detailní bezpečnostní opatření bude možné jednoznačně	Týká se přílohy č. 3 – tuto část nenabízíme.	V této fázi projektu nejsme připraveni tuto část jakýmkoliv způsobem komentovat více do hloubky.

ANO - Dodavatel má dlouhodobé praktické zkušenosti s realizací a provozem řešení pro subjekty působící v oblasti kritické infrastruktury, včetně organizací veřejné správy a státních institucí. Tyto zkušenosti zahrnují návrh, implementaci a provoz infrastruktury a aplikačních platforem s vysokými nároky na dostupnost, bezpečnost, geografickou redundanci a kontinuitu provozu. Realizovaná řešení byla navrhována s ohledem na požadavky kladené na kritické informační systémy, včetně souladu s příslušnými bezpečnostními a legislativními požadavky. Konkrétní zákaznické reference a detailní popisy projektů nelze z důvodu	ANO - Např. DC zdroje pro drážní aplikace.	ANO

ANO - Navrhované řešení je koncipováno s ohledem na požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti, a souvisejících prováděcích předpisů, zejména vyhlášky o kybernetické bezpečnosti. Soulad s těmito požadavky je zajišťován kombinací technických a organizačních opatření odpovídajících charakteru provozu kritické infrastruktury. V oblasti mobilního kontejnerového datového centra se jedná zejména o technická opatření v oblasti fyzické bezpečnosti, řízení přístupů, redundance klíčových komponent a kontinuity provozu. V oblasti zabezpečeného úložiště pak o opatření v oblasti ochrany dat, šifrování, řízení identit a přístupů, auditovatelnosti a bezpečnostního dohledu. Konkrétní rozsah a forma doložení souladu (např. certifikace, audity nebo prohlášení o shodě) bude vycházet z finální zvolené technologie a architektury řešení. Více bude možné specifikovat až po upřesnění technického rozsahu řešení, viz Dotaz 3.	ANO - Naše společnost je držitelem certifikace dle ISO 27001 – Dodávky prvků pro výstavbu telekomunikačních a datových sítí a poskytování kompletních systémových řešení.	V tuto chvíli s ohledem na nejasnosti v zadání není finální řešení známé, každopádně můžeme garantovat, že bude postupováno tak, aby byly tyto požadavky splněny.

ANO - Dodavatel má dlouhodobé praktické zkušenosti s realizací projektů pro zákazníky, na které se vztahuje zákon č. 181/2014 Sb., o kybernetické bezpečnosti, a související prováděcí předpisy. Tyto zkušenosti zahrnují návrh, implementaci a provoz řešení v prostředí kritické infrastruktury a kritických informačních systémů. V rámci realizovaných projektů se dodavatel podílel zejména na návrhu a provozu bezpečné infrastruktury, zavádění technických a organizačních bezpečnostních opatření, implementaci geografické redundance a disaster recovery, a na zajištění souladu provozu systémů s požadavky ZoKB a vyhlášky o kybernetické bezpečnosti. Konkrétní zákaznické reference a detailní popisy projektů nelze z důvodu smluv o mlčenlivosti (NDA)	ANO Dodávka produktů a řešení do oblasti energetiky, dopravy, telekomunikační infrastruktury, obrany.	Pracujeme na dodávkách pro klienty z oblasti státní správy, kteří spadají do kritické infrastruktury.

Řešení je navrhováno a realizováno v souladu s relevantními technickými normami, standardy a doporučeními vztahujícími se k provozu datových center, bezpečnosti informací, fyzické bezpečnosti a požární ochraně, a to s ohledem na charakter kritické infrastruktury. Typicky se jedná zejména o následující normy a standardy: – ISO 9001 – systém managementu kvality, – ISO/IEC 27001 a ISO/IEC 27002 – systém řízení bezpečnosti informací a bezpečnostní opatření, – TIA-942 / TIA-942-B – návrh a provoz datových center (včetně požadavků na redundanci), – ČSN EN 13501 – klasifikace reakce stavebních výrobků na oheň, – další související ČSN, EN a ISO normy dle konkrétní oblasti (elektroinstalace, fyzická bezpečnost, požární ochrana, klimatizace a energetika). Konkrétní výčet aplikovaných norem a jejich rozsah se bude odvíjet od finální zvolené technologie	Elektro – IEC 60364, EN 61140, EN 61439, EN 12464, EN 1838, EN 62305. Požární ochrana - EN 62305, EN 1634-1, EN 54, EN 12094, ISO 14520. Fyzická bezpečnost – konstrukce EN 10025 (S355J2).	V technické specifikaci jsou normy uvedeny.

Orientační cena plnění za část „Mobilní kontejnerové datové centrum“ se pohybuje od 35 000 000 Kč bez DPH. Uvedená cena představuje rámcový odhad vycházející z obvyklých konfigurací mobilních kontejnerových datových center obdobného charakteru a zahrnuje zejména dodávku samotného kontejneru, jeho technologické vybavení a základní instalační práce. V rámci předběžné tržní konzultace a s ohledem na dosud neupřesněný technický rozsah řešení není možné provést detailní cenový rozpad. Konkrétní cena a struktura nákladů se bude odvíjet od finální specifikace technologie, požadované úrovně redundance, bezpečnosti a provozních parametrů	Mobilní datové centrum vč. zprovoznění 36 098 800 Kč bez DPH Profylaxe dle Technické specifikace v částce na 1 rok 683 480 Kč bez DPH V ceně je zahrnuto umístění kontejneru a jeho obslužnost v okruhu 100 km od sídla společnosti.	Předpokládaná hodnota plnění je 18 – 26 mil. Kč bez DPH, finální cena je závislá na požadovaném rozsahu plnění (montážní služby, testovací služby, servisní služby, ….)

Orientační cenu plnění za část „Realizace systému zabezpečeného úložiště v prostředí Správy železnic“ nelze v této fázi předběžné tržní konzultace jednoznačně stanovit. Důvodem je zejména neupřesněný technický rozsah řešení, zejména v oblasti požadovaného výkonu úložiště, architektury replikace a zálohování, požadavků na integrační vazby, bezpečnostních opatření a provozních parametrů. Tyto skutečnosti mají zásadní vliv na volbu technologie i celkovou cenu řešení. Konkrétní cenový rámec a strukturu nákladů bude možné definovat až po upřesnění technických požadavků a cílové architektury řešení, viz Dotaz 3.	Týká se přílohy č. 3 – tuto část nenabízíme.	Nelze odhadnout - z dodaných podkladů nelze určit, co bude součástí dodávek…

ANO - V případě dodávky obou částí řešení v rámci jednoho projektu (mobilní kontejnerové datové centrum včetně IT vybavení a realizace systému zabezpečeného úložiště) lze obecně předpokládat ekonomickou výhodnost pro zadavatele, zejména z pohledu optimalizace návrhu architektury, integrace jednotlivých komponent, sjednocení odpovědnosti dodavatele a snížení nákladů na koordinaci a provoz. Konkrétní celkovou cenu plnění ani její detailní rozpad však nelze v této fázi předběžné tržní konzultace stanovit, a to z důvodu dosud neupřesněného technického rozsahu řešení, zejména v oblasti role mobilního kontejnerového datového centra, architektury zabezpečeného úložiště, požadované úrovně redundance a bezpečnostních opatření. Přesný cenový rámec a strukturu nákladů bude možné definovat až na základě finální specifikace technických	Nenabízíme kompletní řešení obou částí	Předpokládáme že ne, jedná se o natolik rozdílná plnění, že efekt sloučení těchto dvou oblastí nepovede ke snížení celkové ceny.

ANO - Dodavatel nabízí možnost pořízení řešení formou jednorázové investice (CapEx). Tento model je vhodný zejména v případech, kdy zadavatel preferuje vlastnictví technologických prostředků a jejich zařazení do dlouhodobého majetku. Konkrétní struktura CapEx modelu bude vycházet z finální specifikace řešení, rozsahu dodávky a zvoleného způsobu financování a bude možné ji detailně definovat	ANO	ANO - Technologie lze objednat včetně všech souvisejících nákladů na 5let provozu.
ANO - Dodavatel nabízí možnost pořízení řešení formou průběžných plateb (OpEx). Tento model umožňuje rozložení investičních nákladů do provozních výdajů a může být vhodný zejména v případech, kdy zadavatel preferuje flexibilitu financování a postupné čerpání služeb. Konkrétní podoba OpEx modelu, včetně struktury plateb, rozsahu zahrnutých služeb a délky trvání smluvního vztahu, bude vycházet z finální specifikace řešení a bude možné ji detailně definovat v rámci	NE	ANO - Pokud bude Zadavatel požadovat řešení, jehož součástí bude i část průběžně poskytovaných služeb (není však součástí tohoto průzkumu – např. průběžná administrace řešení, profylaktické služby apod.) v daném minimálním rozsahu, pak lze řešení nabídnout i jako službu.

NE - Vzhledem k povaze poptávaného řešení a jeho vysoké míře individualizace nelze poskytnout rámcový ceník ani univerzální ukázkovou konfiguraci s cenou. Dodávky tohoto typu jsou vždy navrhovány projektově na míru konkrétním požadavkům zadavatele, zejména s ohledem na požadovanou kapacitu, výkon, úroveň bezpečnosti, redundance a integrační vazby na stávající prostředí. Jakákoli vzorová konfigurace nebo ceník by v této fázi předběžné tržní konzultace neodrážely reálný rozsah ani cenu budoucího řešení a mohly by být zavádějící. Konkrétní konfiguraci a cenový rámec bude možné připravit až po upřesnění technických a provozních	NE - Jedná se o konfiguraci „na klíč“ dle Vaší technické specifikace, ne ceníkové položky.	NE - Z dodaných podkladů nelze určit, co bude součástí dodávek…

NE - Odhad provozních nákladů řešení v horizontu 1 roku, 5 let a 10 let nelze v této fázi předběžné tržní konzultace jednoznačně stanovit. Provozní náklady jsou zásadně ovlivněny finálním technickým řešením, zejména volbou technologií, požadovanou kapacitou a výkonem úložiště, úrovní redundance, bezpečnostními opatřeními, způsobem provozu (on-premise / managed služby) a zvoleným modelem financování (CapEx / OpEx). Konkrétní odhad provozních nákladů a model TCO bude možné zpracovat až po upřesnění technických a provozních požadavků zadavatele, viz	NE - Týká se i přílohy č. 3 – tuto část nenabízíme.	NE - Nelze odhadnout - z dodaných podkladů nelze určit, co bude součástí dodávek…

Předpokládaná životnost jednotlivých technologických celků se odvíjí od jejich charakteru, intenzity provozu a způsobu údržby.
Mobilní kontejnerové datové centrum a podpůrné technologie (konstrukce kontejneru, napájecí systémy, chlazení, fyzická bezpečnost, požární ochrana) mají při pravidelné údržbě a provádění profylaktických kontrol předpokládanou životnost v rozmezí 7–10 let.
IT technologie (disková úložiště, servery, síťové a bezpečnostní prvky) je z hlediska provozní spolehlivosti, podpory výrobců a technologického vývoje vhodné plánovat k obnově v horizontu 5–7 let, včetně zajištění migrace na novou technologii.
Konkrétní životnost jednotlivých komponent se může lišit v závislosti na zvolené technologii a provozních podmínkách.

Kontejner – předpokládaná životnost je značně ovlivněna podmínkami v lokalitě umístění a pravidelnou údržbou. Pro zvýšení životnosti doporučujeme umístění na betonové pásy nebo patky z důvodu zamezení pronikání spodní vlhkosti do konstrukce způsobující korozi. Obecně lze uvést, že životnost se pohybuje v rozmezí 35 – 40 let.
Podpůrné technologie – životnost podpůrné technologie se pohybuje okolo 15 let, doporučená bezpečná doba provozu je však 10 let, kdy po jejím uplynutí se doporučuje provést výměnu nebo repasovat zařízení. Celková délka životnosti je podmíněna optimálními provozními podmínkami a pravidelnými servisními prohlídkami a výměnou spotřebního materiálu, jako jsou filtry, ventilátory atd. Používáme ventilátory, které mají v čistém prostředí životnost i 10

Kontejner – technologie jsou navrženy na 10-ti letý provoz, při správném servisním zabezpečení je životnost až 20 let.
IT - Typicky se živostnost předpokládá na 5let, protože to je doba po kterou výrobce garantuje servisní podporu na „ukončená" zařízení. Z toho také vyplývá, že lze systémy provozovat 7let i více.

ANO - Dodavatel je schopen zpracovat model celkových nákladů vlastnictví (TCO) pro různé varianty konfigurace řešení. TCO model může zahrnovat zejména investiční náklady, provozní náklady, náklady na údržbu, obnovu technologií a další relevantní položky v závislosti na zvoleném technickém a provozním modelu. Zpracování TCO je standardně poskytováno formou konzultačních služeb a vychází z finální specifikace technických a provozních požadavků zadavatele. Konkrétní rozsah a struktura TCO modelu bude možné definovat až po upřesnění cílové	ČÁSTEČNĚ - Jen pro část Mobilního kontejnerového datového centra.	NE - Z dodaných podkladů nelze určit, co bude součástí dodávek…

ANO - Dodavatel realizoval v posledních letech obdobná řešení pro různé typy zákazníků, zejména v oblasti veřejné správy, kritické infrastruktury a komerční sféry s vysokými nároky na dostupnost, bezpečnost a kontinuitu provozu. Realizace zahrnovaly zejména dodávky a integraci infrastruktury pro ukládání a zpracování dat, návrh a implementaci geografické redundance a disaster recovery, zabezpečení datových úložišť a jejich provozní podporu včetně SLA. Konkrétní zákaznické reference a detailní popisy jednotlivých projektů nelze z důvodu smluv o mlčenlivosti (NDA) uvádět. Uvedené zkušenosti však vycházejí z reálných produkčních nasazení a dlouhodobého provozu obdobných řešení	ANO - Jen pro část Mobilního kontejnerového datového centra.	ANO - Společně s výrobcem. Dodávali jsme samostatně stojící disková pole i celé řešení pro ukládání záloh. Pro relevantní odpověď bychom potřebovali lepší specifikaci zadání/očekávání Zadavatele.

Dodavatel má zkušenosti s realizací projektů v oblasti mobilních datových center, bezpečných datových úložišť a související infrastruktury, včetně návrhu, implementace a provozní podpory řešení s vysokými nároky na dostupnost, bezpečnost a kontinuitu provozu. Konkrétní seznam projektů, názvy zákazníků ani detailní popisy realizací nelze z důvodu smluv o mlčenlivosti (NDA) uvádět ani zpřístupňovat. Uvedené zkušenosti vycházejí z reálně realizovaných a provozovaných řešení, a to zejména v prostředí veřejné správy, kritické infrastruktury a u zákazníků s požadavky na geografickou redundanci a disaster recovery	Mobilní kontejnerové datové centrum – Orange 2 moduly	Viz. výše Smlouvy se zákazníky nám neumožňují poskytovat tyto informace.

Dodavatel má dlouhodobé zkušenosti s realizací projektů v oblasti kritické infrastruktury (KII), a to jak pro subjekty veřejné správy, tak pro komerční a průmyslové organizace s vysokými nároky na dostupnost, bezpečnost a kontinuitu provozu. Realizované projekty zahrnovaly zejména návrh, implementaci a provoz infrastruktury a aplikačních platforem, zabezpečených datových úložišť, řešení geografické redundance a disaster recovery, jakož i zavádění technických a organizačních bezpečnostních opatření v souladu s požadavky zákona o kybernetické bezpečnosti. Konkrétní zákaznické reference a detailní popisy jednotlivých projektů nelze z důvodu smluv o mlčenlivosti (NDA) uvádět	Dodávka produktů a řešení do oblasti energetiky, dopravy, telekomunikační infrastruktury, obrany.	Viz. výše Smlouvy se zákazníky nám neumožňují poskytovat tyto informace.

ANO - Dodavatel má praktické zkušenosti s integrací hardwarových bezpečnostních modulů (HSM) a systémů pro správu identit a přístupů (IdM) v prostředí zákazníků s vysokými nároky na bezpečnost a auditovatelnost. Realizované projekty zahrnovaly zejména návrh a implementaci správy šifrovacích klíčů prostřednictvím HSM, integraci HSM se systémy pro šifrování dat při ukládání i přenosu, a napojení těchto komponent na centrální IdM/PAM řešení včetně řízení oprávnění a auditních stop. Uvedené zkušenosti vycházejí z reálně provozovaných řešení, zejména v prostředí veřejné správy a kritické infrastruktury. Konkrétní zákaznické reference nelze z důvodu smluv o mlčenlivosti (NDA)	NE	ANO

ANO - Dodavatel má praktické zkušenosti s implementací a integrací řešení typu XDR, včetně technologií výrobce Fidelis, v prostředí zákazníků s vysokými nároky na kybernetickou bezpečnost a dohled nad bezpečnostními událostmi. Realizované projekty zahrnovaly nasazení XDR nástrojů pro detekci, korelaci a vyhodnocování bezpečnostních incidentů napříč síťovou, endpointovou a aplikační vrstvou, včetně integrace s dalšími bezpečnostními prvky (např. SIEM, IDS/IPS, DLP) a napojení na centrální bezpečnostní dohled (SOC). Uvedené zkušenosti vycházejí z reálně provozovaných řešení, zejména v prostředí veřejné správy a kritické infrastruktury. Konkrétní zákaznické reference a detailní popisy projektů nelze z důvodu smluv o mlčenlivosti	NE	NE

Dodavatel má zkušenosti s realizací projektů, jejichž předmětem byla dodávka mobilního datového centra a samostatně také dodávka diskových úložišť s kapacitou v řádu jednotek petabajtů, včetně zajištění provozní podpory. Tyto dodávky byly realizovány jako technologicky oddělené celky, které však byly integrovány do jednoho funkčního řešení. V rámci poskytovaných služeb je dodavatel schopen zajistit provozní podporu formou servisních a provozních smluv v úrovních L1–L3, včetně dohledu nad provozem, řešení incidentů, eskalačních mechanismů a pravidelného reportingu. Konkrétní zákaznické reference a detailní popisy projektů nelze z důvodu smluv o mlčenlivosti (NDA) uvádět	NE - Týká se přílohy č. 3 – tuto část nenabízíme.	V této kombinaci reference nemáme.

ANO - Dodavatel má praktické zkušenosti s realizací migrací dat v rozsahu jednotek petabajtů, a to jak v rámci jedné lokality, tak mezi geograficky oddělenými datovými centry. V rámci realizovaných projektů byly využívány standardní nástroje výrobců storage technologií a virtualizačních platforem, případně specializované migrační nástroje, v kombinaci s vlastním migračním postupem zahrnujícím plánování, testování, validaci a finální přepnutí. Konkrétní zákaznické reference a detailní popisy použitých nástrojů nelze z důvodu smluv o mlčenlivosti	NE - Týká se přílohy č. 3 – tuto část nenabízíme.	ANO - Bez znalosti informací o „zdrojových“ datech/systémech, nelze určit/navrhnout způsob migrace dat. Jinak se budou souborové systémy a jinak databáze (a i zde se každá databáze migruje jinak).

Provozujeme infrastrukturu typu IaaS v rámci více geograficky oddělených datových center společnosti, která jsou navrhována a provozována v souladu s principy metodiky TIER III (Uptime Institute), zejména v oblasti redundance klíčových technologických komponent a kontinuity provozu. Infrastruktura je zároveň provozována s ohledem na požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti, a souvisejících prováděcích předpisů. Architektura podporuje geografickou redundanci a scénáře disaster recovery a je využívána pro provoz systémů s charakterem kritické infrastruktury a kritických informačních systémů. Z důvodu smluv o mlčenlivosti (NDA) není možné uvádět ani zpřístupňovat konkrétní zákaznické reference či detailní popisy jednotlivých řešení

Týká se přílohy č. 3 – tuto část nenabízíme.

Máme několik zákazníků ve státní správě, bankovnictví i v ostatních oblastech. Informace poskytneme dle varianty cílového řešení.

ANO - Dodavatel poskytuje školení a kompletní technickou i provozní dokumentaci v českém jazyce. Dokumentace je standardně dodávána v rozsahu odpovídajícím charakteru řešení a zahrnuje zejména technickou dokumentaci architektury, provozní a bezpečnostní postupy, popis integračních vazeb, havarijní a disaster recovery scénáře a související provozní metodiky. Školení jsou realizována v rozsahu přiměřeném cílovým rolím zadavatele (např. administrátoři, provozní tým, bezpečnost) a jejich konkrétní obsah a forma budou upřesněny dle finálního technického řešení. Součástí podpory a školení může být rovněž využití nástrojů založených na AI jako doplňkové formy podpory, zejména pro interaktivní práci s technickou a provozní dokumentací, asistovanou orientaci v provozních a bezpečnostních postupech a podporu řešení standardních provozních situací. Využití těchto nástrojů bude případně specifikováno na základě	ANO	ANO - Možno i v AJ

ANO - Dodavatel má možnost zprostředkovat náhled vzorového řešení formou referenční návštěvy vybraného řešení nebo výrobního závodu, a to v rozsahu umožněném smluvními podmínkami a pravidly ochrany informací. Referenční návštěva může zahrnovat ukázku konstrukčního a technologického provedení mobilního kontejnerového datového centra, jeho základních infrastrukturních prvků a principů provozu. Konkrétní rozsah, forma a lokalita případné návštěvy budou upřesněny po dohodě se zadavatelem. Z důvodu smluv o mlčenlivosti (NDA) není možné zpřístupňovat detailní technickou dokumentaci ani plnohodnotné provozní prostředí zákazníků, nicméně je možné prezentovat řešení v obecné a demonstrační rovině	ANO Je možné navštívit jako výrobní závod, tak již instalovaná modulární datová centra	Kontejner - ANO IT - NE Váš komentář k navrhovanému řešení. Z dodaných podkladů nelze ani určit, co bude součástí dodávek