

Naše zn. 92531/2026-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

„Nákup mobilního datového centra“

(dále jen „Zadávací dokumentace“ a/nebo „ZD“)

Identifikační údaje Zadavatele a osoby zastupující Zadavatele:

Název: Správa železnic, státní organizace
Sídlo: Dlážďená 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. Tomášem Tóthem**, generálním ředitelem
Profil Zadavatele: <https://zakazky.spravazeleznic.cz/>

1. Informace o osobě, která zpracovala část Zadávací dokumentace

Na zpracování Zadávací dokumentace se nepodílela osoba odlišná od Zadavatele.

2. Informace o předběžné tržní konzultaci:

1.1. 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](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 projeví 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.

1.2. 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 Petržilkova 2565/23, Stodůlky, 158 00 Praha 5, IČO: 60487291,
- Conteg, spol. s r.o., se sídlem Štětškova 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.

1.3. 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 požadovaného řešení, včetně možnosti realizace jako komplexní dodávky „na klíč“
- b) rozsah spolupráce dodavatelů při zpracování dokumentace, testování řešení, přejímkách, uvedení do provozu a předání do užívání,
- c) soulad navrhovaných řešení s relevantními právními a technickými předpisy,
- d) časovou náročnost na výrobu a dodání,
- e) zkušenosti dodavatelů s veřejnými zakázkami,
- f) možnosti financování, rámcové ceny,
- g) předchozí realizace obdobného plnění,
- h) technické kompetence dodavatelů a jejich schopnost zajištění provozní a servisní podpory po celou dobu životnosti řešení.

Na základě informací zjištěných v rámci předběžné tržní konzultace Zadavatel:

- a) ověřil, že trh je připraven dodat požadované plnění v plném rozsahu a většina dodavatelů má relevantní zkušenosti, avšak že pro přesné návrhy, ceny a srovnatelnost nabídek je nezbytné upřesnit technickou specifikaci a vymezit předmět plnění podrobněji. Zadavatel proto vytvořil dokument Bližší specifikace, který je přílohou závazného vzoru smlouvy, kde své požadavky blíže popsal,
- b) stanovil časový Harmonogram plnění,
- c) upravil údaj o předpokládané hodnotě veřejné zakázky,
- d) rozhodl nezahrnout do této veřejné zakázky realizaci systému Zabezpečeného úložiště v prostředí Správy železnic a tuto část realizovat formou samostatné

veřejné zakázky, a to zejména s cílem zajistit vyšší úroveň hospodářské soutěže.

- 1.4. 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. Účelem veřejné zakázky je výběr dodavatele na uzavření smlouvy na dodávku mobilního datového centra, kde budou v souladu se záměrem Zadavatele umístěny informační technologie, jako jsou servery, datová úložiště a síťové prvky.
- 4.2. Předmětem veřejné zakázky je návrh, zajištění stavební připravenosti, dodávka, instalace a uvedení do provozu mobilního datového centra (dále jen jako „**MDC**“) včetně zajištění jeho následné provozní údržby.
- 4.3. Podrobné vymezení předmětu veřejné zakázky je uvedeno v přílohách této Zadávací dokumentace.
- 4.4. Klasifikace předmětu veřejné zakázky (CPV) :

Hlavní kód CPV: 44211100-3 | Stavebnicové a mobilní buňky

Kód CPV: 32580000-2 | Datová zařízení

Kód CPV: 32424000-1 | Síťová infrastruktura

Kód CPV: 32523000-5 | Telekomunikační prostory

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

- 4.5. Zadavatel provozuje informační systémy kritické informační infrastruktury a předmět plnění veřejné zakázky je určen pro jejich provozování. Zadavatel je proto povinen řídit se zákonem č. 264/2025 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „**ZoKB**“).

Dne 17. prosince 2018 vydal Národní úřad pro kybernetickou a informační bezpečnost (dále jen „**NÚKIB**“), na základě zákona č. 181/2014 Sb., o kybernetické bezpečnosti 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“.

V souladu s § 71 odst. 3 ZoKB přitom platí, že: „*Varování vydaná přede dnem nabytí účinnosti tohoto zákona podle zákona č. 181/2014 Sb., ve znění pozdějších předpisů, se považují za varování vydaná podle tohoto zákona.*“

Dne 4. ledna 2019 vydal NÚKIB Metodiku k varování ze dne 17. prosince 2018, 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 ZoKB 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 zvládnutí, spočívající v nepřipuštění použití těchto prostředků v rámci plnění veřejné zakázky, a to 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 ZoKB **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.**

K ověření výše uvedeného je dodavatel povinen učinit přílohou nabídky **vyplněné čestné prohlášení**, jehož vzor je Přílohou č. 10 této Zadávací dokumentace.

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 **vyločení takového dodavatele ze zadávacího řízení.**

4.6. **Vyhrazená změna závazku**

4.7. Zadavatel si v souladu s § 100 odst. 1 ZZVZ vyhrazuje změnu závazku ze smlouvy na veřejnou zakázku, a to za podmínek uvedených v čl. 22 Závazného vzoru smlouvy.

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 nabytí účinnosti smlouvy.

Termín ukončení plnění: 10 let od ukončení fáze F4 (v této době bude prováděna profylaxe MDC a poskytovány související Služby na vyžádání).

Podrobnosti ohledně doby plnění Veřejné zakázky stanoví Harmonogram plnění, který je přílohou č. 8 dokumentu Příloha č. 4 této Zadávací dokumentace.

6.2. Místo plnění veřejné zakázky

Dodání a instalace MDC bude provedena na adrese: Ústřední stavědlo triangl, Plzeň.

Služby na vyžádání, jakož i další části Veřejné zakázky mohou probíhat rovněž v sídle Zadavatele či jeho organizačních jednotek.

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 vymezené 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.

- 7.2. Zadavatel aplikuje v zadávacím řízení níže uvedené prvky odpovědného zadávání.
- 7.2.1. Zadavatel v rámci zásady sociálně odpovědného zadávání za účelem usnadnění přístupu k plnění veřejné zakázky, případně její části, malým a středním podnikům minimalizuje administrativní náročnost při podání žádosti o účast/nabídky možností využití vzorových formulářů a čestných prohlášení, které jsou součástí Zadávací dokumentace k této veřejné zakázce.
- 7.3. Použití jiných prvků odpovědného zadávání, které byly zadavateli známy při vytváření této zadávací dokumentace, není vzhledem k povaze a smyslu zakázky vhodné z těchto důvodů:
 - 7.3.1. V oblasti sociálně odpovědného zadávání zadavatel neshledal potřebu použití dalších dílčích aspektů odpovědného zadávání s ohledem na předmět plnění bez typických rizikových činností spojených s porušováním pracovněprávních předpisů a mezinárodních úmluv o lidských právech, sociálních či pracovních právech.
 - 7.3.2. V oblasti inovací zadavatel nestanovil dílčí kritéria odpovědného zadávání, jelikož zadavateli není známo žádné inovativní řešení předmětu veřejné zakázky.

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, je-li níže požadována;
 - d) svou technickou kvalifikaci dle § 79 ZZVZ, je-li níže požadována;
 - e) jiná kritéria kvalifikace dle § 167 ZZVZ, je-li níže požadována.
- 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* 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 předkladu, je oprávněn si vyžádat předložení úředně ověřeného překladu dokladu tlumočnickem zapsaným do seznamu soudních tlumočnicků a soudních překladatelů podle zákona č. 354/2019 Sb., o soudních tlumočnicích 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 předchází vyloučení účastníka zadávacího řízení zruší.

10. Profesionální způsobilost dle § 77 ZZVZ

- 10.1. Zadavatel v souladu s ustanovením § 73 ZZVZ požaduje prokázání profesionální způsobilosti dle § 77 ZZVZ následujícím způsobem:
- 10.1.1. Dodavatel prokazuje splnění profesionální 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 profesionální způsobilosti předložením **výpisu z obchodního rejstříku či jiné obdobné evidence**.
- 10.2. Doklady k prokázání profesionální způsobilosti dodavatel nemusí předložit, pokud právní předpisy v zemi jeho sídla obdobnou profesionální způsobilost nevyžadují.

11. Ekonomická kvalifikace dle § 78 ZZVZ

- 11.1. Zadavatel požaduje, aby minimální obrát dodavatele dosahoval za každé ze 3 bezprostředně předcházejících účetních období minimální úrovně **průměrného ročního obrátu alespoň 40 mil. Kč bez DPH**.
- 11.2. Jestliže dodavatel vznikl později, postačí, předloží-li údaj o svém obrátu 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**.

12. Technická kvalifikace dle § 79 ZZVZ

- 12.1. Seznam významných zakázek
- 12.1.1. K prokázání kritéria technické kvalifikace požaduje Zadavatel doložení **Seznamu**

významných dodávek a prací 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. 2 této Zadávací dokumentace.

12.1.2. Ze seznamu významných zakázek musí vyplývat, že dodavatel v uvedeném období realizoval minimálně **3 významné zakázky**, z toho:

- i. **1 významnou službu/dodávku**, jejímž předmětem byl **návrh a dodávka datového centra ICT** či **obdobného technologického provozu**¹
- ii. **2 služby/dodávky**, z nichž každá zahrnovala **dodávku a implementaci alespoň 2 různých technologických celků** z následujícího výčtu:
 - a) **Nepřerušitelné zdroje napájení (UPS)** v redundantním zapojení **min. N+1**;
 - b) **Chladicí a klimatizační systém** s redundancí **min. N+1** (např. dvě a více nezávislých jednotek chlazení, z nichž každá zvládne zátěž při výpadku jiné);
 - c) **Slaboproudé bezpečnostní systémy**: elektronická požární signalizace (EPS), elektronická zabezpečovací signalizace (EZS), kamerový systém (CCTV) a systém kontroly vstupu (ACS);
 - d) **Speciální stavební prvky**: minimálně stabilní hasicí zařízení (SHZ) pro IT technologie, fyzické bezpečnostní prvky (např. bezpečnostní dveře a závory, zabezpečené vstupní zóny), stavební prvky jako kabelové žlaby nebo rošty dimenzované pro datovou kabeláž nebo zdvojená podlaha;

¹ Datovým centrem či obdobným technologickým provozem se pro účely pozouzení technické kvalifikace dodavatele rozumí jakýkoliv technologický prostor, ve kterém jsou instalovány a provozovány serverové technologie a v rámci něhož jsou implementovány minimálně všechny následující technologické celky:

- a) **Nepřerušitelné zdroje napájení (UPS)** v redundantním zapojení **min. N+1**;
- b) **Chladicí a klimatizační systém** s redundancí **min. N+1** (např. dvě a více nezávislých jednotek chlazení, z nichž každá zvládne zátěž při výpadku jiné);
- c) **Slaboproudé bezpečnostní systémy**: elektronická požární signalizace (EPS), elektronická zabezpečovací signalizace (EZS), kamerový systém (CCTV) a systém kontroly vstupu (ACS);
- d) **Speciální stavební prvky**: minimálně stabilní hasicí zařízení (SHZ) pro datový sál, fyzické bezpečnostní prvky (např. bezpečnostní dveře a závory, zabezpečené vstupní zóny), stavební prvky jako kabelové žlaby nebo rošty dimenzované pro datovou kabeláž nebo zdvojená podlaha;
- e) **IT infrastruktura nosných prvků**: datové rozvaděče (racky) včetně silnoproudých rozvodnic a rozvodů napájení (PDU) pro IT technologii;
- f) **Integrace do jednotného systému řízení a monitoringu** (např. BMS nebo DCIM) – tj. dodavatel má zkušenost s propojením chlazení, napájení a bezpečnostních systémů do centrálního dohledového systému.

Zadavatel nepožaduje, aby součástí významné dodávky byla dodávka prostoru samotného, postačí i jen dodání a implementace jednotlivých výše uvedených technologických celků do již existujícího prostoru.

- e) **IT infrastruktura nosných prvků:** datové rozvaděče (racky) včetně silnoproudých rozvodnic a rozvodů napájení (PDU) pro IT technologii;
- f) **Integrace do jednotného systému řízení a monitoringu** (např. BMS nebo DCIM) – tj. dodavatel má zkušenost s propojením chlazení, napájení a bezpečnostních systémů do centrálního dohledového systému.

přičemž každá z předložených významných zakázek musí mít hodnotu alespoň **8.000.000 Kč bez DPH**.

12.1.3. 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 odpovídajícím 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 **doložit jmenný seznam členů realizačního týmu** 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, uvede dodavatel rovněž údaje, z nichž bude ověřitelné splnění požadavku, včetně kontaktních údajů na objednatele příslušného referenčního projektu), jehož vzor je součástí této Zadávací dokumentace jako Příloha č. 8,
- 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. Realizační tým musí zahrnovat **alespoň 5 osob**, přičemž **kromě pozic Koordinátor BOZP a Projektový manažer mohou osoby v realizačním týmu zastávat i více pozic**, pokud budou pro tyto pozice splňovat veškeré kvalifikační požadavky stanovené touto Zadávací dokumentací.

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

Pracovní pozice	Minimální požadavky na kvalifikaci člena realizačního týmu
-----------------	--

<p>Vedoucí projektu (pouze 1 osoba)</p>	<ul style="list-style-type: none"> • Autorizovaný inženýr v oboru pozemní stavby dle zákona č. 360/1992 Sb., autorizační zákon <i>Tento požadavek dodavatel prokáže předložením osvědčení o autorizaci nebo výpisu z evidence autorizovaných osob ČKAIT (České komory autorizovaných inženýrů a techniků).</i> • Účast alespoň na 2 projektech realizace nebo rekonstrukce datových center nebo obdobných technologických provozů, v rámci kterých zajišťoval: <ul style="list-style-type: none"> ○ Komplexní řízení průběhu realizace projektu datového centra nebo obdobného technologického provozu. ○ Koordinace činností jednotlivých profesí – stavební, technologické, elektro, MaR, chlazení apod. ○ Sledování plnění harmonogramu ○ Kontrola kvality
<p>Specialista pro elektroinstalace a UPS (min. 1 osoba)</p>	<ul style="list-style-type: none"> • Požadována je odborná způsobilost v elektrotechnice dle § 7 nařízení vlády č. 194/2022 Sb. (Vedoucí elektrotechnik). <i>Tento požadavek dodavatel prokáže předložením Dokladu o složení zkoušky z odborné způsobilosti k výkonu činností v elektrotechnice.</i> • Účast na alespoň 2 projektech v rámci kterých prováděl instalaci UPS
<p>Specialista pro chlazení a VZT² (min. 1 osoba)</p>	<ul style="list-style-type: none"> • Praxe min. 5 let v oblasti chlazení a klimatizace datových center nebo obdobných technologických provozů. • Účast alespoň na 2 projektech, v rámci kterých zajišťoval realizaci chladicích systémů (např. instalace přesné klimatizace, free-cooling systémů, redundantních chillerů apod.) pro datová centra či obdobné technologické provozy.
<p>Specialista MaR (měření a regulace) (min. 1 osoba)</p>	<ul style="list-style-type: none"> • Praxe min. 3 roky v oblasti měření a regulace³ • Účast alespoň na 1 projektu, v rámci kterého zajišťoval integraci více technologických systémů (např. chlazení, napájení, environmentální čidla, PLC regulátory, atd.) do nadřazeného řídicího nebo monitorovacího systému (BMS, DCIM nebo obdobného). Integrace zahrnovala

² VZT = vzduchotechnika

³ Oblastí měření a regulace se pro účely pozouzení technické kvalifikace rozumí činnost spočívající v návrhu, konfiguraci, integraci, programování a uvádění do provozu systémů MaR zajišťujících dohled, řízení a automatizaci technologických celků, zejména chladicích, napájecích, vzduchotechnických a bezpečnostních systémů, včetně jejich propojení do centrálního dohledového systému.

	návrh nebo realizaci vazeb mezi systémy, jejich oživení a funkční testy.
Koordinátor BOZP (min. 1 osoba)	<ul style="list-style-type: none"> Kvalifikace koordinátora bezpečnosti a ochrany zdraví při práci na staveništi dle § 10 odst. 2 zákona č. 309/2006 Sb. <p><i>Tento požadavek dodavatel prokáže předložením osvědčení o získání odborné způsobilosti vydaným Ministerstvem práce a sociálních věcí.</i></p>
Specialista na datová centra ICT (min. 1 osoba)	<ul style="list-style-type: none"> Minimálně 5 let odborné praxe v oblasti návrhu, koordinace, provozu nebo implementace technologií v datových centrech nebo obdobných technologických provozech. Účast alespoň na 2 projektech, jejichž předmětem byla realizace nebo rekonstrukce datového centra či obdobného technologického provozu. V rámci těchto projektů vykonával minimálně tyto činnosti: <ul style="list-style-type: none"> Návrh rackových skříní Návrh osazení PDU Návrh optických propojů Účast alespoň na 1 projektu, jehož předmětem bylo poskytování provozní podpory⁴ datového centra či obdobného technologického provozu po dobu alespoň 3 let. <p><i>V případě, že jeden projekt splňuje parametry více druhů shora požadovaných významných projektů, lze jeho prostřednictvím prokázat splnění požadavku Zadavatele na realizaci těchto obou druhů projektů současně.</i></p>
Projektový manažer (min. 1 osoba)	<ul style="list-style-type: none"> Min. 5 let praxe na pozici projektového manažera (či obdobné, jejíž náplní bylo po stránce realizační vést projekty a řídit tým lidí), a to v oblasti řízení IT projektů, které zahrnovaly koordinaci více profesí (stavební, elektro, IT, bezpečnostní technologie, chladicí systémy, aj.). <p>Účast na alespoň 2 projektech, jejichž předmětem byla realizace nebo rekonstrukce datového centra či obdobného technologického provozu, a to v roli projektového manažera.</p> <ul style="list-style-type: none"> Držitel certifikátu odborné způsobilosti v oblasti projektového řízení (např. PRINCE2, IPMA, PMI nebo ekvivalent či vyšší).

⁴ Provozní podporou se pro účely pozouzení technické kvalifikace rozumí provádění profylaktických prohlídek či poskytování servisních služeb s cílem zajistit řádné fungování datového centra či obdobného technologického provozu.

13. Požadavky Zadavatele na způsob zpracování nabídkové ceny:

- 13.1. Zadavatel požaduje, aby účastník uvedl Celkovou nabídkovou cenu za plnění předmětu této veřejné zakázky, v české měně (Koruna česká), bez daně z přidané hodnoty (DPH), zaokrouhlenou maximálně na 2 desetinná místa.
- 13.2. Za účelem výpočtu Celkové nabídkové ceny v Kč bez DPH vyplní účastník Ceník, který je přílohou č. 2 dokumentu Příloha č. 4 této Zadávací dokumentace (dále také je „**Ceník**“). Za správnost provedení výpočtu Celkové nabídkové ceny odpovídá účastník.
- 13.3. Zadavatel požaduje, aby účastník uvedl také dílčí ceny za části předmětu veřejné zakázky (jednotlivé položky) v souladu s Ceníkem. Celková nabídková cena je pak dána součtem dílčích cen jednotlivých položek vynásobených jejich (předpokládaným) objemem.
- 13.4. Účastník je povinen vyplnit všechna požadovaná pole v Ceníku, která jsou označena k vyplnění dodavatelem.
- 13.5. Celková nabídková cena jakož i nabídková cena doplněná účastníkem do jednotlivých buněk v Ceníku 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 v dokumentu Příloha č. 4 této Zadávací dokumentace.

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 návrh smlouvy

- 16.1. Dodavatel je povinen využít Závazný návrh smlouvy, který tvoří dokument Příloha č. 4 Zadávací dokumentace.
- 16.2. Dodavatel není oprávněn činit změny či doplnění Závazného návrhu smlouvy, vyjma údajů, u nichž vyplývá z jejich obsahu povinnost doplnění (označené jako „*doplní dodavatel*“ či jiným obdobným způsobem). V případě nabídky podávané společně několika dodavateli je dodavatel oprávněn upravit Závazný návrh smlouvy toliko s ohledem na tuto skutečnost; totéž platí, je-li dodavatelem fyzická osoba.
- 16.3. Dodavatel je povinen Závazný návrh smlouvy doplněný dle výše uvedených pokynů učinit součástí nabídky. Nebude-li nabídka obsahovat přílohy smlouvy, do kterých nebyl účastník oprávněn zasahovat, má se za to, že se zněním takových příloh souhlasí, ledaže sdělil opak.

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 Ceníkem.
- 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 (buť 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. 3 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:
- Obsah nabídky (včetně nabídkové ceny),
 - Čestné prohlášení ve vztahu k zakázaným dohodám - Vzor čestného prohlášení je upraven jako Příloha č. 3 této Zadávací dokumentace,
 - Čestné prohlášení o střetu zájmů - Vzor čestného prohlášení je upraven jako Příloha č. 6 této Zadávací dokumentace,
 - Čestné prohlášení o splnění podmínek v návaznosti na mezinárodní sankce - Vzor čestného prohlášení je upraven jako Příloha č. 7 této Zadávací dokumentace,
 - Čestné prohlášení k ve vztahu k zákonu o registru smluv - Vzor čestného prohlášení

je upraven jako Příloha č. 5 této Zadávací dokumentace,

- f) Doklady prokazující splnění základní způsobilosti,
 - g) Doklady prokazující splnění profesní způsobilosti,
 - h) Doklady prokazující splnění ekonomické kvalifikace (jsou-li požadovány),
 - i) Doklady prokazující splnění technické kvalifikace (jsou-li požadovány),
 - j) Závazný vzor smlouvy doplněný dle pokynů v této Zadávací dokumentaci – Závazný vzor smlouvy je upraven jako Příloha č. 4 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 obrátu) 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.
- 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 sjednaném v rozsahu podrobně stanoveném v čl. 21. dokumentu Příloha č. 4, 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. 5 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. 23.2 této Zadávací dokumentace účastník nedokládá v případě, že neoznačí ve smlouvě, či rámcové dohodě, 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. 6 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 vyplýne, 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 předpisů⁵ (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 jednájí 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. 269/2014⁶, 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 ani nepřímo zpřístupněny fyzickým nebo právnickým osobám, subjektům či orgánům uvedeným v příloze I tohoto nařízení nebo v jejich prospěch (dále společně jen „**Osoby**

⁵ 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

⁶ 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.

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. 7 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 vyplývá, 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. Čestné prohlášení ke splnění technické kvalifikace
- Příloha č. 3. Čestné prohlášení ve vztahu k zakázaným dohodám
- Příloha č. 4. Závazný vzor smlouvy
- Příloha č. 5. Čestné prohlášení ve vztahu k zákonu o registru smluv
- Příloha č. 6. Čestné prohlášení o střetu zájmů
- Příloha č. 7. Čestné prohlášení o splnění podmínek v návaznosti na mezinárodní sankce
- Příloha č. 8. Vzor profesního životopisu
- Příloha č. 9. Výstupy z PTK
- Příloha č. 10. Čestné prohlášení v souladu s varováním NÚKIB

Ing. Tomáš Tóth
generální ředitel

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 „**Nákup mobilního datového centra**“, 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 vydaným 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]

Příloha č. 2 Zadávací dokumentace

Čestné prohlášení o splnění technické kvalifikace

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 „**Nákup mobilního datového centra**“, 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.

Významná zakázka č. 1	
Objednatel referenční zakázky IČO, sídlo/místo podnikání, kontaktní osoba k ověření realizované zakázky (tel. + e-mail)	[DOPLNÍ ÚČASTNÍK]
Popis předmětu referenční zakázky , z něhož vyplýne splnění <u>všech</u> podmínek kvalifikace, jak jsou zadavatelem požadovány v čl. 12.1.2 zadávací dokumentace <i>Dodavatel uvede podrobněji zejm. popis:</i> <ul style="list-style-type: none"> - napájení, - chlazení, - bezpečnostních systémů, - speciálních stavebních prvků, - IT infrastruktury nosných prvků, - integrace do jednotného systému řízení a monitoringu, <i>pokud byly tyto technologické celky součástí významné zakázky.</i>	[DOPLNÍ ÚČASTNÍK]
Finanční objem plnění ve vztahu, k němuž je kvalifikace prokazována (v Kč bez DPH)	[DOPLNÍ ÚČASTNÍK]
Doba realizace (datum od-do, v rámci 5 let nazpět před zahájením zadávacího řízení) <i>dodavatel doplní ve formátu MM/RRRR – MM/RRRR</i>	[DOPLNÍ ÚČASTNÍK]

Významná zakázka č. 2	
Objednatel referenční zakázky IČO, sídlo/místo podnikání, kontaktní osoba k ověření realizované zakázky (tel. + e-mail)	[DOPLNÍ ÚČASTNÍK]
Popis předmětu referenční zakázky , z něhož vyplývá splnění <u>všech</u> podmínek kvalifikace, jak jsou zadavatelem požadovány v čl. 12.1.2 zadávací dokumentace <i>Dodavatel uvede podrobněji zejm. popis:</i> <ul style="list-style-type: none"> - napájení, - chlazení, - bezpečnostních systémů, - speciálních stavebních prvků, - IT infrastruktury nosných prvků, - integrace do jednotného systému řízení a monitoringu, <i>pokud byly tyto technologické celky součástí významné zakázky.</i>	[DOPLNÍ ÚČASTNÍK]
Finanční objem plnění ve vztahu, k němuž je kvalifikace prokazována (v Kč bez DPH)	[DOPLNÍ ÚČASTNÍK]
Doba realizace (datum od-do, v rámci 5 let nazpět před zahájením zadávacího řízení) <i>dodavatel doplní ve formátu MM/RRRR – MM/RRRR</i>	[DOPLNÍ ÚČASTNÍK]

Významná zakázka č. 3	
Objednatel referenční zakázky IČO, sídlo/místo podnikání, kontaktní osoba k ověření realizované zakázky (tel. + e-mail)	[DOPLNÍ ÚČASTNÍK]
Popis předmětu referenční zakázky , z něhož vyplývá splnění <u>všech</u> podmínek kvalifikace, jak jsou zadavatelem požadovány v čl. 12.1.2 zadávací dokumentace <i>Dodavatel uvede podrobněji zejm. popis:</i> <ul style="list-style-type: none"> - napájení, - chlazení, - bezpečnostních systémů, - speciálních stavebních prvků, - IT infrastruktury nosných prvků, - integrace do jednotného systému řízení a monitoringu, <i>pokud byly tyto technologické celky součástí významné zakázky.</i>	[DOPLNÍ ÚČASTNÍK]
Finanční objem plnění ve vztahu, k němuž je kvalifikace prokazována (v Kč bez DPH)	[DOPLNÍ ÚČASTNÍK]
Doba realizace (datum od-do, v rámci 5 let nazpět před zahájením zadávacího řízení) <i>dodavatel doplní ve formátu MM/RRRR – MM/RRRR</i>	[DOPLNÍ ÚČASTNÍK]

V [DOPLNÍ ÚČASTNÍK] dne [DOPLNÍ ÚČASTNÍK]

Příloha č. 3 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 „**Nákup mobilního datového centra**“, tímto čestně prohlašuje, že:

- a) 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; a
- b) nepřipravoval části nabídek, které mají být hodnoceny podle kritérií hodnocení, ve vzájemné shodě s jiným účastníkem téhož zadávacího řízení, s nímž je spojenou osobou podle zákona o daních z příjmů.

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. 4 Zadávací dokumentace

Smlouva o dílo – návrh, dodávka a instalace mobilního datového centra

Číslo smlouvy Objednatele: [DOPLNÍ OBJEDNATEL PŘI PODPISU SMLOUVY]

Číslo smlouvy Zhotovitele: [DOPLNÍ ZHOTOVITEL]

číslo ISPROFOND: S602300325 / 5003520244

uzavřená podle ustanovení § 2586 a následujících 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, Dlážďená 1003/7, PSČ 110 00

IČ 70994234, DIČ CZ70994234

zastoupená **Ing. Tomášem Tóthem**, generálním ředitelem

(dále též jen „**Objednatel**“ nebo „**SŽ**“)

Zhotovitel:

Jméno osoby [DOPLNÍ ZHOTOVITEL]

Údaje o zápisu v evidenci

Údaje o sídlu

IČ , DIČ

Bankovní spojení:.....

Číslo účtu:.....

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 „Nákup mobilního datového centra“, 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.

Pokud nevyplývá z této Smlouvy jinak, mají pojmy s velkými počátečními písmeny význam definovaný v Příloze č. 5 – *Zvláštní obchodní podmínky pro Zakázky v oblasti ICT* (dále také jen „**ZOP**“ nebo „**Zvláštní obchodní podmínky**“), nebo Příloze č. 6 – *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; obdobně platí pro vztahy mezi jinými smluvními dokumenty.

1. Účel Smlouvy

- 1.1. Účelem Smlouvy je zajištění kapacitního, provozně spolehlivého a bezpečného zázemí pro umístění a provoz ICT technologií Objednatele, a to prostřednictvím mobilního datového centra (dále jen jako „**MDC**“). Účelem smlouvy je dále zajištění kontinuity provozu kritických informačních a telekomunikačních systémů Objednatele, zvýšení úrovně fyzické a provozní bezpečnosti těchto systémů a vytvoření podmínek pro jejich bezpečný provoz v souladu s platnými právními a technickými předpisy.
- 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 návrh, zajištění stavební připravenosti, dodávka, instalace a uvedení do provozu MDC včetně zajištění jeho následné provozní údržby za účelem zajištění kapacitního, provozně spolehlivého a bezpečného zázemí pro umístění a provoz ICT technologií Objednatele. Předmětem díla je rovněž provádění souvisejících Služeb na vyžádání.
- 2.3. V rámci provádění Díla je Zhotovitel povinen dodat Hardware alespoň v kvalitě a specifikacích uvedených v Příloze č. 1 této Smlouvy a další drobné hmotné pomůcky či předměty jinak nezbytné pro uvedení Hardware do běžného provozu (například propojovací kabely, napájecí kabely, šrouby, koncovky apod.) v místě instalace a dále poskytnout oprávnění užít případný Software (např. firmware, obslužné ovladače apod.), který je součástí Hardware uvedeného v Příloze č. 1 této Smlouvy.
- 2.4. Bližší požadavky na Předmět díla jsou vymezeny zejména, nikoliv však výlučně, v Příloze č. 1 této Smlouvy.
- 2.5. Součástí Předmětu díla je rovněž dodání Standardního software pro správu kamerového systému, blíže specifikovaného v čl. 7.2.3.4 Přílohy č. 1 této Smlouvy a pro monitoring a řízení MDC dle čl. 7.3.4 Přílohy č. 1 této Smlouvy. Ve vztahu ke Standardnímu software je Zhotovitel povinen:
 - a. zpřístupnit kódy, klíče či jiné prostředky umožňující využití Standardního software (včetně umožnění ověření originality a pravosti licence u autorizovaného distributora nebo výrobce),
 - b. udržovat aktuální a přístupné kódy a klíče po dobu trvání Smlouvy,
 - c. zajistit a udržovat originální maintenance výrobce Standardního Software, tj. zejména poskytnout Aktualizace, Modernizace, Zásadní modernizace a další patche či jiné

updaty tohoto Standardního Software včetně nejnovějších verzí tohoto Standardního Software Objednateli;

to vše po dobu 10 let od předání MDC k provedení akceptačního řízení Fáze F4.

- 2.6. 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.

3. Záruka za jakost

- 3.1. Jednotlivé části Předmětu díla by měly být provedeny tak, aby byla zajištěna jejich životnost po dobu alespoň 10 let od uvedení MDC do provozu. V souvislosti s tím je Zhotovitel povinen poskytnout Objednateli záruku za jakost Předmětu díla na dobu 10 let od jeho uvedení do provozu (dokončení Fáze 4).
- 3.2. Práva z vad budou po dobu trvání záruky za jakost uplatňována postupem dle části 15, 16 a 17 OOP.
- 3.3. Jako havarijní vadu ve smyslu části 17 OOP se rozumí zejména taková vada, která znemožňuje užívání Předmětu díla k účelu, pro který bylo pořízeno.
- 3.4. Odstranění havarijní vady ve lhůtě 5 dnů ve smyslu čl. 146 OOP je možné řešit i jen provizorním odstraněním vady (tj. takové nápravné opatření, které není finální, nýbrž zajistí možnost Díla sloužit svému účelu), za předpokladu, že ve lhůtě 30 dnů ode dne oznámení vady dojde k řádnému odstranění vady. O tomto provizorním odstranění vady musí být mezi stranami podepsáno písemné potvrzení.
- 3.5. Pro práva z vad týkající se Standardního Software se uplatní čl. 18.2. ZOP.

4. Místo plnění

- 4.1. Místem dodání a instalace MDC je Ústřední stavědlo triangl, Plzeň.
- 4.2. Služby na vyžádání, jakož i další části Předmět díla mohou probíhat v sídle Zadavatele či jeho organizačních jednotek.

5. Doba plnění

- 5.1. Doba trvání této Smlouvy činí 10 let od ukončení fáze F4 (v této době bude prováděna profylaxe MDC a poskytovány související Služby na vyžádání) (dále jen „**doba trvání Smlouvy**“).
- 5.2. 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.
- 5.3. Pokud není stanoveno jinak, je Zhotovitel povinen provádět Dílo a jeho části v termínech uvedených v závazném harmonogramu realizace Díla obsaženém v Příloze č. 8 této Smlouvy (dále jen „**Harmonogram**“).
- 5.4. Žádná ze Stran není oprávněna jednostranně měnit termíny uvedené v Harmonogramu.

6. Cena díla

- 6.1. Celková cena za splnění závazku Zhotovitele v rozsahu dle této Smlouvy (včetně Služeb na vyžádání), tj. Cena, je uvedena pod položkou Celková nabídková cena v Příloze č. 2 této Smlouvy – *Ceník*.
- 6.2. Ceny, a to jak jednotkové ceny, tak Celková nabídková cena, obsažené v Příloze č. 2 této Smlouvy, jsou uvedeny jako maximální, nejvýše přípustné, nepřekročitelné a zahrnující veškeré náklady Zhotovitele nutné k řádnému a včasnému provedení Předmětu 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. 2 této Smlouvy).
- 6.3. Součástí Ceny 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 Předmětu díla. Zhotovitel nese veškeré náklady nutně nebo účelně vynaložené při plnění závazku z této Smlouvy včetně správních poplatků.

- 6.4. Ceny obsažené v Příloze č. 2 této Smlouvy jsou uvedeny bez DPH. V případě změny zákonné sazby DPH není třeba uzavírat dodatek k této Smlouvě.
- 6.5. Změna Ceny dle části 5 odst. 19.2 OOP se nepřipouští.

7. Platební podmínky

- 7.1. 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 provedení Fáze 1 (F1), a to nejdříve po akceptaci (bez výhrad) této Fáze, jejímž předmětem jsou činnosti blíže specifikované v kapitole 5 Přílohy č. 1 této Smlouvy;

Druhý platební milník (**Platební milník B**): Výzva k úhradě ve výši ceny za provedení fází F2, F3 a F4, a to nejdříve po akceptaci (bez výhrad) těchto fází, které jsou tvořeny činnostmi uvedenými v kapitolách 6, 7, 8 a 9 Přílohy č. 1 této Smlouvy;

Třetí platební milník (**Platební milník C**): Výzva k úhradě ve výši ceny za provedení fáze F5, a to nejdříve po akceptaci (bez výhrad) této Fáze, jejímž předmětem jsou činnosti uvedené v kapitole 10 Přílohy č. 1 této Smlouvy;

Čtvrtý platební milník (**Platební milník D**): Výzva k úhradě ve výši ceny za provedení fáze F6, a to nejdříve po akceptaci (bez výhrad) této Fáze, jejímž předmětem jsou činnosti uvedené v kapitole 11 Přílohy č. 1 této Smlouvy;

- 7.2. Zhotovitel je dále oprávněn doručit Objednateli Výzvu k úhradě za každý kalendářní rok provádění Profylaxe MDC v souladu s kapitolou 12 Přílohy č. 1 této Smlouvy, a to nejdříve po akceptaci (bez výhrad) kompletního provedení všech profylaktických kontrol specifikovaných tamtéž a ve výši ceny ujednané v Příloze č. 2 této Smlouvy pro část Plnění „Profylaxe MDC“. Součástí Výzvy k úhradě musí být kopie Objednatelům podepsaných protokolů o provedených profylaktických kontrolách za daný kalendářní rok. Profylaxe MDC není Zhotovitelem prováděna v kalendářním roce, v němž došlo k akceptaci Fáze F4.
- 7.3. Zhotovitel je dále oprávněn doručit Objednateli Výzvu k úhradě vždy za každý měsíc, v němž došlo k akceptaci (bez výhrad) plnění na základě Objednávky Služeb na vyžádání dle čl. 11 této Smlouvy, a to ve výši součinu počtu MD dle Objednávky a ceny za jeden MD poskytování Služeb na vyžádání uvedené v Příloze č. 2 této Smlouvy.
- 7.4. Výzva k úhradě musí být fakturou nebo daňovým dokladem.
- 7.5. 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.
- 7.6. 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.
- 7.7. 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.
- 7.8. 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.

- 7.9. 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.

8. Akceptační řízení

- 8.1. Akceptačnímu řízení dle čl. 8.1 ZOP a tohoto článku této Smlouvy podléhají všechny Fáze F1 až F5, přičemž každá z těchto fází je součástí některého z platebních milníků A až C, jak stanoví kapitola 14 Přílohy č. 1 této Smlouvy. Lhůta dle čl. 8.1.9 ZOP se stanovuje v délce 7 kalendářních dnů.
- 8.2. Fáze plnění F1 až F5 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.
- 8.3. Akceptačnímu řízení dle čl. 8.4 ZOP a tohoto článku této Smlouvy podléhá Fáze F6, přičemž tato Fáze představuje platební milník D, jak stanoví kapitola 14 Přílohy č. 1 této Smlouvy
- 8.4. Plnění Fáze F7 (Profylaxe MDC) bude akceptováno postupně vždy po provedení dílčí profylaktické kontroly. O této dílčí profylaktické kontrole bude na místě vyhotoven protokol, který bude obsahovat výstupy z kontroly a případné další dokumenty, specifikované v kapitole 12 Přílohy č. 1 této Smlouvy. Podpisem tohoto protokolu ze strany Objednatele je příslušná profylaktická kontrola akceptována. Akceptace s výhradou není pro Fázi F7 možná.
- 8.5. Akceptačnímu řízení dle části 8.1 ZOP a tohoto článku této Smlouvy podléhají rovněž výstupy z poskytování Služeb na vyžádání (Fáze F8) dle čl. 11 této Smlouvy, které budou realizované na základě Objednávek. Akceptační kritéria budou v tomto případě vyplývat ze specifikace prací uvedených v Objedávce.
- 8.6. Posuzování jakýchkoliv Akceptačních kritérií je nutno provádět s ohledem na účel této Smlouvy.

9. Práva duševního vlastnictví

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

10. Školení

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

11. Služby na vyžádání

- 11.1. Zhotovitel se zavazuje poskytovat Služby na vyžádání, které jsou blíže vymezeny v části 8 Přílohy č. 1 této Smlouvy.
- 11.2. Maximální souhrn Služeb na vyžádání činí 100 MD za celou dobu trvání této Smlouvy. Objednatel není povinen Služby na vyžádání čerpat.
- 11.3. Objednatel v případě zájmu o provedení prací v rámci Služeb na vyžádání doručí Zhotoviteli objednávku prostřednictvím e-mailu Kontaktních osob uvedených v čl. 13 této Smlouvy se specifikací požadovaných prací, termínem provedení těchto prací a předpokládanou časovou náročností vyjádřenou v MD (dále jen „**Objedávka**“).
- 11.4. Zhotovitel se zavazuje bez zbytečného odkladu projednat s Objednatelem své případné připomínky k Objedávce, 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 Objedávky.

- 11.5. 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. 13 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.
- 11.6. Pro vyloučení všech pochybností Smluvní strany uvádí, že Objednávka nepředstavuje uzavření samostatné dílčí smlouvy na základě rámcové dohody dle § 131 ZZVZ.
- 11.7. 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. 8 této Smlouvy a poskytnout ve vztahu k těmto pracím Objednateli licenci či jiná práva z duševního vlastnictví v rozsahu v souladu s čl. 9 této Smlouvy.

12. Účast poddodavatelů a realizační tým

- 12.1. Zhotovitel je oprávněn plnit tuto Smlouvu výlučně prostřednictvím Poddodavatelů uvedených v Příloze č. 4 této Smlouvy – *Poddodavatelé*.
- 12.2. Před zapojením nového Poddodavatele do plnění této Smlouvy musí být Objednateli předložen nový seznam Poddodavatelů, který bude tvořit Přílohu č. 4 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.
- 12.3. Seznam členů realizačního týmu je Přílohou č. 7 této Smlouvy. Pravidla pro realizační tým se řídí částí 15 ZOP.
- 12.4. Změna v osobě Poddodavatele či ve složení realizačního týmu nepředstavuje podstatnou změnu závazku ze smlouvy ve smyslu § 222 ZZVZ a nepodléhá povinnosti uzavření dodatku ke Smlouvě.

13. Kontaktní osoby

- 13.1. Kontaktními osobami za účelem plnění této Smlouvy jsou za Zhotovitele **[DOPLNÍ ZHOTOVITEL: titul, jméno, příjmení, telefon a e-mail]**.
- 13.2. Kontaktními osobami za účelem plnění této Smlouvy jsou za Objednatele **[DOPLNÍ OBJEDNATEL: titul, jméno, příjmení, služební telefon a služební e-mail]**.
- 13.3. Kontaktní osobou Objednatele pro oblast kybernetické bezpečnosti je **[DOPLNÍ OBJEDNATEL: titul, jméno, příjmení, služební telefon a služební e-mail]**.
- 13.4. Změna kontaktních osob uvedených výše nepředstavuje podstatnou změnu závazku ze smlouvy ve smyslu § 222 ZZVZ a nepodléhá povinnosti uzavření dodatku ke Smlouvě.

14. Smluvní pokuty

- 14.1. Cenou pro účely stanovení výše smluvních pokut dle části 17 ZOP, části 21 ZOP a části 20 OOP se rozumí Cena ve smyslu čl. 6.1 této Smlouvy, není-li výslovně stanoveno jinak.
- 14.2. Jedná-li se o smluvní pokutu za prodlení s provedením části Předmětu díla, bude se při výpočtu smluvní pokuty vycházet z ceny příslušné části Předmětu díla, jak je stanovena v příloze č. 2 této Smlouvy.

15. Servicedesk

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

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: [doplň Zhotovitel x nemá-li Zhotovitel výše uvedené dokumenty, celý tento bod 20.3 odstraní].

21. Další povinnosti Zhotovitele

21.1. 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 10.000.000,- 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.

21.2. 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 smlouvy více jak 30 kalendářních dnů, je Objednatel oprávněn odstoupit od Smlouvy.

22. Vyhrazená změna závazku ze smlouvy

Objednatel si vyhrazuje postupovat dle § 100 odst. 1 ZZVZ, a to za následujících podmínek:

Případně-li okamžik uplynutí trvání Smlouvy dle čl. 5.1 této Smlouvy na měsíce leden či únor, není Zhotovitel povinen (ani oprávněn) v daném kalendářním roce (v němž skončí trvání smlouvy) provést profylaktické kontroly v souladu s kapitolou 12 Přílohy č. 1 této Smlouvy. Cena za Fázi F7 sjednaná v Příloze č. 2 této Smlouvy se v takovém případě ponížší o částku odpovídající ceně za provedení veškerých profylaktických kontrol v 1 kalendářním roce.

Smluvní strany jsou povinny o této skutečnosti uzavřít dodatek k této Smlouvě.

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* mají přednost před zněním Přílohy č. 3 *Platforma SŽ* (včetně jejích příloh). Ustanovení Přílohy č. 1 *Bližší specifikace předmětu plnění* a Přílohy č. 3 *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 | Ceník |
| Příloha č. 3 | Platforma SŽ (včetně jejích příloh) |
| Příloha č. 4 | Poddodavatelé |
| Příloha č. 5 | Zvláštní obchodní podmínky k ICT zakázkám |
| Příloha č. 6 | Obchodní podmínky ke smlouvě o dílo |
| Příloha č. 7 | Seznam členů realizačního týmu |

Za Objednatele:

Za Zhotovitele:

.....
Ing. Tomáš Tóth
generální ředitel

.....
[DOPLNÍ ZHOTOVITEL]

Klasifikace: Veřejný dokument



Bližší specifikace předmětu plnění

Příloha č. 1 Smlouvy



Obsah

1	Seznam zkratk	3
2	Úvod	7
3	Obecný popis mobilního datového centra	7
4	Požadavky na plnění	8
5	Projektová dokumentace (Fáze 1)	8
6	Stavební řešení pro umístění kontejneru	10
6.1	Dočasné umístění	10
6.2	Finální umístění	10
7	Výroba mobilního datového centra + stavební připravenost (Fáze 2)	10
7.1	Konstrukční řešení kontejneru	13
7.1.1	Vizuální provedení	13
7.1.2	Obvodový plášť	14
7.1.3	Svislé konstrukce	14
7.1.4	Vodorovné konstrukce	14
7.1.5	Nosné konstrukce	14
7.1.6	Vnitřní dělicí konstrukce	15
7.1.7	Nosné konstrukce stropu	15
7.1.8	Podlahy	15
7.1.9	Tepelné a zvukové vlastnosti	15
7.1.10	Výplně otvorů	16
7.1.11	Venkovní provedení	16
7.1.12	Vnitřní prostupy – dveře	16
7.1.13	Zámečnické konstrukce	17
7.1.14	Bleskosvodná a uzemňovací soustava	17
7.1.15	Dispoziční a provozní řešení	17
7.1.16	Bezbariérové užívání datového centra	18
7.2	Technologické řešení	18
7.2.1	Napájení	19
7.2.2	Chlazení a vzduchotechnika	22
7.2.3	Bezpečnostní technologie	24
7.2.4	Osvětlení	28
7.3	ICT technologie mobilního datového centra	29
7.3.1	Datové rozvaděče	29



7.3.2	PDU lišty.....	29
7.3.3	Strukturovaná kabeláž.....	30
7.3.4	Monitoring a řídicí systémy.....	31
8	Dodávka mobilního datového centra do místa instalace (Fáze 3).....	34
9	Zprovoznění mobilního datového centra (Fáze 4).....	35
10	Dokumentace (Fáze 5)	36
11	Školení (Fáze 6)	37
12	Profylaktické kontroly a revize (Fáze 7)	37
12.1	Profylaktická kontrola kontejneru MDC	39
12.2	Profylaktické kontroly a revize zdroje nepřetržitého napájení (UPS)	39
12.3	Profylaktické kontroly a revize elektrozařízení	40
12.3.1	Provozní kontrola jednotek PDU (Power Distribution Unit)	40
12.3.2	Provozní kontrola rozvaděčů.....	41
12.3.3	Provozní kontrola ATS	41
12.4	Profylaktické kontroly a revize jednotek chlazení	42
12.5	Profylaktické kontroly a revize monitorovacího systému.....	43
12.6	Profylaktické kontroly a revize stabilního hasicího zařízení (SHZ)	43
12.7	Profylaktické kontroly a revize bleskosvodné a uzemňovací soustavy	45
12.8	Profylaktické kontroly a revize nouzového osvětlení	45
13	Služby na vyžádání (Fáze 8)	46
14	Fáze dodávky a platební milníky	47
15	Ideologická schémata serverovny SŽT.....	48
15.1	Ideologické schéma zapojení napájení serverovny	48
15.2	Ideologické schéma zapojení chlazení serverovny	49
15.3	Ideologické schéma vizualizace monitorovaného prostředí serverovny	50

1 Seznam zkratk

Níže uvedená tabulka obsahuje seznam zkratk a pojmů použitých v rámci této Technické specifikace.

Přehled zkratk a pojmů:

Zkratka	Význam	Překlad/popis
ANSI	American National Standards Institute	Americký národní normalizační institut
API	Application Programming Interface	Programové rozhraní pro komunikaci mezi aplikacemi
ASHRAE	American Society of Heating, Refrigerating and Air-Conditioning Engineers	Profesní organizace zaměřená na normy HVAC
ATS	Automatic Transfer Switch	Automatický přepínač zdrojů napájení
BMS	Building Management System	Systém řízení budovy
BOZP	Bezpečnost a ochrana zdraví při práci	Oblast pracovně-bezpečnostních pravidel
CCTV	Closed-Circuit Television	Kamerový bezpečnostní systém
CETRIS	Cement-bonded particle board	Cementotřísková deska
CMOS	Complementary Metal-Oxide Semiconductor	Typ polovodičové technologie (snímače kamer, chipy)
CO ₂	Carbon Dioxide	Oxid uhličitý
ČSN	Česká technická norma	Národní standard technických norem
DCIM	Data Center Infrastructure Management	Systém pro správu a monitoring infrastruktury datového centra
DDTS	Dálková Diagnostika Technologických Systémů.	Interní diagnostický systém SŽ
DOCX	Microsoft Word Open XML Document	Formát dokumentu MS Word
DPA	Decentralized Parallel Architecture	paralelní zapojení výkonových modulů



DWG	Drawing	Formát technických výkresů Autodesk
DX	Direct Expansion	chlazení metodou přímé expanze, výparník je v přímém kontaktu s proudem chlazeného vzduchu
EKV	Elektronická Kontrola Vstupu	elektronický přístupový systém
EN	European Norm	Evropská technická norma
EPS	Elektrická požární signalizace	Systém detekce a hlášení požáru
FAT	Factory Acceptance Test	Přejímací test u výrobce
FC	Free Cooling	volné chlazení (využívá se příznivě nízké venkovní teploty)
GPS	Global Positioning System	Globální polohový systém
GSM	Global System for Mobile Communications	Mobilní komunikační standard
HD	High Definition	Vysoké rozlišení obrazu
HOP	hlavní ochranné přípojnice	hlavní ochranné přípojnice
HTTPS	Hypertext Transfer Protocol Secure	Šifrovaný komunikační protokol webu
HVAC	Heating, Ventilation and Air Conditioning	Vytápění, větrání a klimatizace
IR	Infrared	Infračervený signál / záření
ISO	International Organization for Standardization	Mezinárodní organizace pro normalizaci
ISTA	International Safe Transit Association	Normy pro testování balení a přepravy
IT / ICT	Information Technology / Information and Communication Technology	Informační technologie / informační a komunikační technologie
LCD	Liquid Crystal Display	Displej z tekutých krystalů
LiFePO ₄	Lithium Iron Phosphate	Typ lithiové baterie
LPS	Lightning Protection System	Systém ochrany před bleskem



MaR	Měření a Regulace	Technologie pro řízení a regulaci objektů
MD	Man-day	Člověkoden
MDC	Mobile Data Center	Mobilní datové centrum
NN	Nízké napětí	Elektrická síť do 1 kV
OS	Operating System	Operační systém
PBZ	Požárně bezpečnostní zařízení	Technické prostředky pro požární ochranu
PC	Personal Computer	Osobní počítač
PDF	Portable Document Format	Standardizovaný formát dokumentů
PDU	Power Distribution Unit	Jednotka pro distribuci napájení (v racku)
PIN	Personal Identification Number	Osobní identifikační kód
PIR	Passive Infrared Sensor	Pasivní infračervený detektor pohybu
PLC	Programmable Logic Controller	Programovatelný logický automat
PNG	Portable Network Graphics	Bitmapový grafický formát
PoE	Power over Ethernet	Napájení po ethernetové síti
PUE	Power Usage Effectiveness	Ukazatel energetické efektivity datového centra
PUR		
PVC	Polyvinyl Chloride	Polyvinylchlorid
PZTS	Poplachový zabezpečovací a tísňový systém	Elektronický zabezpečovací systém
RC3	Resistance Class 3	Třída odolnosti proti vloupání
RUPS	Redundant UPS	Redundantní nepřerušitelný zdroj napájení
SHZ	Stabilní hasicí zařízení	Automatický hasicí systém
SNMP	Simple Network Management Protocol	Síťový protokol pro správu zařízení



SŽ	Správa železnic	Správa železnic
SŽT	Správa železniční telematiky	Správa železniční telematiky
TB	Terabyte	Jednotka velikosti dat
TIA	Telecommunications Industry Association	Asociace vydávající normy pro telekomunikační infrastrukturu
TIER III	Data Center Tier III	Úroveň dostupnosti datového centra (N+1)
TIFF	Tagged Image File Format	Grafický formát pro bezztrátové obrázky
UPS	Uninterruptible Power Supply	Nepřerušitelný zdroj napájení
VZ	Veřejná zakázka	Proces zadávání veřejných zakázek
VZT	Vzduchotechnika	Větrací a klimatizační systémy
WDR	Wide Dynamic Range	Technologie pro kamerové snímače při vysokém kontrastu
XLSX	Microsoft Excel Open XML Spreadsheet	Formát tabulek MS Excel
ZABBIX	Dohledový systém	Open-source systém pro monitoring infrastruktury

2 Úvod

Tato technická specifikace definuje komplexní požadavky na návrh, konstrukci, technologické vybavení, instalaci, bezpečnostní prvky, provoz a údržbu mobilního kontejnerového datového centra. Cílem dokumentu je zajistit jednotné technické, funkční a kvalitativní podmínky pro dodávku řešení mobilního datového centra (dále jen „**MDC**“), které bude splňovat standardy vysoké dostupnosti, bezpečnosti, modularity a provozní spolehlivosti. Všechny dále uvedené části specifikace vycházejí z principu integrace veškerých technologií do jednoho kompaktního kontejnerového modulu a z požadavku na jeho dlouhodobý bezobslužný provoz.

3 Obecný popis mobilního datového centra

Mobilní datové centrum bude definováno jako trvale bezobslužné pracoviště bez stálé fyzické obsluhy, realizované v kontejnerovém provedení. Vzhledem k prostorovým možnostem je požadováno řešení s mobilní samonosnou konstrukcí, která umožní snadné usazení, opakovaný transport a přemístění na jinou lokalitu. MDC musí být navržen tak, aby jeho konstrukce umožňovala flexibilní manipulaci bez nutnosti zásadních stavebních úprav.

Datové centrum bude dodáno jako kompaktní „all-in-one“ řešení, v němž budou veškeré technologie integrovány přímo uvnitř MDC. Instalace bude provedena na předem připravený betonový základ, bez nutnosti složitých stavebních nebo instalačních prací – pouze s připojením na připravené napájecí a komunikační kabeláže.

Součástí řešení musí být pokročilý systém dálkového monitoringu, který umožní reálný časový sběr, vyhodnocování a vizualizaci klíčových provozních dat z technologií a senzorů. Zhotovitel musí zajistit integraci požadovaných dat v definovaném formátu do nadřazeného monitorovacího systému provozovaného Objednatelem.

Níže jsou stručně popsány základní požadované technické parametry mobilního datového centra, které jsou dále rozpracovány v navazujících kapitolách:

- **Vizuální identita:** Barevné provedení MDC a umístění identifikačních prvků (např. logo provozovatele) musí být v souladu s vizuálním stylem Objednatele, uvedeným na webových stránkách Objednatele ([Logomanuál - www.spravazeleznic.cz](http://www.spravazeleznic.cz));
- **Rozměrové požadavky:** MDC musí být navrženo tak, aby umožňoval bezpečné a funkční umístění všech požadovaných technologií a transportovatelnost, bez nutnosti pevně stanovených rozměrů;
- **Konstrukce:** MDC bude vybaveno ocelovou samonosnou konstrukcí s tepelnou izolací a plechovým opláštěním, která zajistí mechanickou stabilitu při osazení, přepravě a manipulaci;
- **Vstupní komora:** Součástí MDC bude integrovaná vstupní komora (podpůrná místnost), která bude fyzicky oddělovat datový sál od venkovního prostředí, čímž se zajistí ochrana proti klimatickým vlivům;
- **Umístění technologií:** Technologické komponenty, jako je například systém chlazení, musí být umístěny tak, aby nebyly pohledově exponované. Preferovaným řešením je jejich instalace ve střešní části;



- **Klasifikace infrastruktury:** Vnitřní Non-IT infrastruktura musí odpovídat klasifikaci dle Uptime Institute, přičemž řešení musí splňovat požadavky na úroveň **TIER III** (Objednatel nevyžaduje doložení certifikátu);
- **Instalace elektro a datové infrastruktury:** Elektrická instalace a datová kabeláž musí být realizovány v souladu s platnými technickými a požárními normami, s důrazem na zajištění mechanické stability během přepravy a manipulace;
- **Osvětlení:** Osvětlení bude realizováno pomocí energeticky úsporných svítidel. V jednotlivých místnostech bude osvětlení ovládáno místními nástěnnými vypínači, umístěnými u vstupních dveří. Venkovní osvětlení bude řízeno automatizovaným systémem;
- **Chlazení:** Chladicí systém bude navržen pro spolehlivý provoz v kontejnerovém prostředí, s požadavkem na redundanci minimálně v konfiguraci N+1. Umístění venkovních chladicích jednotek bude řešeno s ohledem na prostorové a provozní nároky; preferováno je střešní umístění, integrované do konstrukce MDC tak, aby nebyly pohledově exponované. Chladicí systém musí mít minimálně dva oddělené chladicí okruhy, umožňující provádět údržbu bez ovlivnění provozu. Jednotky spolu musí komunikovat a předcházet cyklování.
- **Napájení:** Pro napájení MDC proběhne harmonizace požadavků mezi Zhotovitelem a Objednatелеm a konkrétní požadavky budou upřesněny až v rámci realizace VZ.

4 Požadavky na plnění

Plnění veřejné zakázky se skládá z níže uvedených částí:

- Vyhotovení projektové dokumentace mobilního datového centra
- Stavební připravenost v místě instalace
- Výroba mobilního datového centra
- Dodávka MDC do místa instalace
- Zprovoznění MDC
- Dodání Dokumentace
- Školení
- Poskytování profylaxe
- Služby na vyžádání

5 Projektová dokumentace (Fáze 1)

Projektová dokumentace představuje klíčový výstup úvodní fáze projektu. Slouží jako závazný technický a stavební podklad pro výrobu, instalaci a následný provoz mobilního datového centra. Jejím cílem je zajistit jednoznačné určení technických parametrů, rozsahu prací, připojovacích bodů a požadavků na stavební připravenost tak, aby navazující fáze realizace mohly proběhnout bez rizik, nejasností a nutnosti dodatečných úprav. Z Projektové dokumentace musí být zřejmé, že dodávané MDC bude odpovídat veškerým požadavkům Objednatel specifikovaným v této příloze, zejména v kapitole 6 a 7 této přílohy.

Oblast	Výstupy Zhotovitele
Projektová dokumentace	<p>Vytvoření projektové dokumentace k MDC, která bude odpovídat požadavkům Objednatele specifikovaným níže v této příloze. Projektová dokumentace musí být zpracována v takovém detailu, aby z ní vyplývalo splnění požadavků Objednatele minimálně v rozsahu:</p> <ul style="list-style-type: none"> • Konstrukční řešení (rozměry, hmotnost, konstrukce a další technické parametry) včetně výkresů ve formátu PDF a dalších editovatelných formátech např. DWG • Technologické řešení <ul style="list-style-type: none"> ○ Napájení ○ Chlazení a vzduchotechnika ○ Bezpečnostní technologie ○ ICT technologie ○ Monitoring a řízení ○ Profylaxe a provozní údržba • Stavební řešení <ul style="list-style-type: none"> ○ Realizace místního šetření dočasného i finálního umístění MDC včetně fotodokumentace ○ Zhodnocení stavu stavební připravenosti, zejm.: <ul style="list-style-type: none"> - základové desky (rovinnost, nosnost, rozměry) - elektrického připojení - datové konektivity - uzemnění - možnosti dopravy ○ Vytvoření dokumentace ke stavební přípravě dočasného umístění MDC (a to včetně kótovaného návrhu umístění v místě dodání, z něhož budou patrné veškeré stavební prvky) ○ Plán a technologický postup přesunu MDC do finální lokality po jejím dokončení • Tabulkový seznam navrhovaných komponent MDC (konstrukční prvky, elektrické napájení, chlazení, IT rozvaděče, strukturovaná kabeláž) a jejich technických parametrů (Zhotovitel není povinen uvádět ty komponenty, které neurčují funkční vlastnosti MDC, zejm. takové komponenty, pro něž touto přílohou nejsou stanoveny konkrétní požadavky).

Jednotným výstupem výše uvedených požadavků bude samostatný dokument s názvem „Projektová dokumentace“. Dokumentace musí být předána v **elektronické podobě** (ve formátu PDF a také v editovatelném formátu, např. DWG, DOCX, XLSX)

6 Stavební řešení pro umístění kontejneru

Stavební řešení stanovuje technické a prostorové podmínky pro umístění MDC včetně požadavků na přípravu základové plochy, provedení dočasných zpevněných povrchů, zajištění silového napájení a vymezení prvků, které nejsou součástí této dodávky. Tato kapitola specifikuje jak parametry finální lokality, tak i minimální standardy přístupové infrastruktury a stavebních opatření nezbytných pro bezpečný provoz a instalaci MDC.

6.1 Dočasné umístění

Pro **dočasné** umístění MDC na nezpevněném pozemku v lokalitě Plzeň, provede Zhotovitel zpevnění a vyrovnaní povrchu pomocí silničních panelů o tloušťce minimálně 150 mm. Panely budou použity ve dvou úrovních nosnosti:

- o **20 t** v místech uložení MDC,
- o **6 t** v plochách určených pro pochozí komunikaci. Objednatel požaduje, aby před vstupem do MDC byla vybudována zpevněná plocha.

Silniční panely mohou být, dle místních možností, uloženy tak, aby navazovaly na okolní terén a nevytvářely výškové rozdíly. Rovinnost uložených panelů musí odpovídat požadavkům na zpevněné povrchy, tj. ± 5 mm. MDC musí být usazeno ve vodorovné poloze, přičemž maximální přípustný sklon nesmí překročit 1° .

V rámci dodávky je Zhotovitel povinen zajistit vhodná opatření pro bezpečný přístup do MDC, v souladu s platnými normami – například protiskluzovou nástupní plochu nebo schodiště.

Lokalita dočasného umístění je specifikována následujícími souřadnicemi:(GPS: 49.7462450N, 13.3982083E).

6.2 Finální umístění

MDC bude finálně umístěno v lokalitě Plzeň na zpevněném pozemku SŽ (betonová plocha) se zpevněnou přístupovou komunikací a přivedenými inženýrskými sítěmi (elektro, data). Přípravné stavební práce finální lokality budou realizovány Objednatelem v jiném projektu (tento projekt nebude z časových důvodů dokončen pravděpodobně dříve, než ve 1Q/2027).

Předmětem Smlouvy není doprava MDC do místa finálního umístění.

7 Výroba mobilního datového centra + stavební připravenost (Fáze 2)

Výroba mobilního datového centra vychází z technických a konstrukčních požadavků definovaných v kapitole 7 této přílohy. Požadavky na stavební připravenost jsou definovány v kapitole 6 této přílohy. Tyto kapitoly blíže specifikují technické parametry MDC požadované Objednatelem, ze kterých musí Zhotovitel při výrobě vycházet. Veškeré

požadavky uvedené v této kapitole musí být rovněž plně zohledněny při vyhotovování Projektové dokumentace dle kapitoly 5 této přílohy, která slouží jako závazný podklad pro realizaci výroby a stavební připravenosti.

V odůvodněných případech se může Zhotovitel v rámci výroby MDC odchýlit od schválené projektové dokumentace, ovšem pouze za předpokladu, že Zhotovitel o tuto změnu Objednatele písemně požádá a Objednatel tuto změnu schválí. Požadavek na změnu technických či funkčních parametrů MDC deklarovaných v projektové dokumentaci je Zhotovitel povinen vznést nejpozději 4 týdny před uplynutím lhůty pro splnění fáze 2 (výroba mobilního datového centra) a současně před provedením FAT testů (resp. protokol o úspěšném provedení FAT testů předložený pro účely akceptace fáze 2 musí zohledňovat technické a funkční parametry MDC uvedené v projektové dokumentaci, případně změněné po dohodě stran dle tohoto odstavce). Součástí žádosti musí být prohlášení Zhotovitele, že tato změna je v souladu s technickými požadavky na MDC stanovenými ve Smlouvě (zejm. v této příloze), označení zaměňované položky a specifikace nové položky. Objednatel tuto změnu schválí, pokud o ni bude požádáno předepsaným způsobem a změna bude v souladu s požadavky Smlouvy (zejm. této přílohy). Nevyjádří-li se Objednatel do 1 týdne od doručení žádosti o změnu tak, že změnu schvaluje, má se za to, že se změnou nesouhlasí. Zhotoviteli nevzniká nárok na provedení takové změny akceptované projektové dokumentace.

Oblast	Výstup Zhotovitele
Fotodokumentace MDC	<ul style="list-style-type: none">Fotodokumentace jednotlivých výrobních celků včetně interiéru (minimálně ve Full HD rozlišení 1920x1080 pix, v běžném bezztrátovém formátu PNG, TIFF)
Stavební připravenost	<ul style="list-style-type: none">Zajištění (provedení) stavební připravenosti dočasného umístění, zejm.:<ul style="list-style-type: none">dodávka a umístění silničních panelů dle požadavků kapitoly 6.1 této přílohyPříprava povrchu (dočasného umístění) pro následné dodání MDCFotodokumentace připraveného místa pro dočasné umístění MDC

FAT testy (Factory Acceptance Tests)

Součástí závěru výrobní fáze jsou také FAT testy, jejichž provedení ověřuje shodu vyrobeného MDC s požadovanými parametry. O výsledcích FAT musí být zpracován protokol, který bude tvořit závěrečný potvrzující dokument této fáze plnění.

FAT testy budou provedeny minimálně v rozsahu:

1) Kontrola konstrukčního řešení

- Rozměry a hmotnost MDC
- Kvalita svárů, antikorozi ochrana, povrchové úpravy
- Nosnost podlahy pro racky (kg/m²)



- Tepelná izolace (PUR/PIR, minerální vata) – tloušťky a parametry
- Zátěžové testy konstrukce (vibrace, transport simulation)

2) Dveře a přístupové body

- Funkčnost zámků
- Těsnost dveří, gumové profily
- Požární odolnost podle specifikace projektu

3) ICT prostor

- Umístění a mechanika racků
- Počet racků, ukotvení (výsuvné systémy)
- Kabelové trasy
- Oddělení silové, datové a optické trasy
- Kvalita průchodek a zaslepení
- Konektorová výbava dle projektu

4) Napájecí systém

- Primární/sekundární přívody
- Měření napětí, proudů, fáze, zátěžové testy
- Ověření N+1 redundance
- Ověření správného jištění
- Označení a dokumentace
- Test jednotlivých okruhů
- Kontrola baterií UPS, stáří a kapacity
- Přepnutí na baterii při simulovaném výpadku, měření doby přepnutí
- Nabíjecí křivky baterií, autonomní testy
- Ověření bypassu UPS

5) Klimatizace a chlazení (HVAC)

- Výkonové parametry (kW chladu)
- Napojení na senzory a monitoring
- Test postupného startu
- Simulace tepelné zátěže (heat load dummy)
- Testování udržení teploty v rozsahu (např. 22 ± 2 °C)
- Redundance: odpojení jedné/více jednotek (N+1/N+2)

6) Bezpečnostní systémy (EPS/ PZTS)

- Funkčnost čidel (kouřová, teplotní, vlhkostní, dveřní)
- Kontrola tlaků lahví EPS
- Test ventilů, signálů, blokáci HVAC
- Simulace pre-alarm a alarm sekvence
- Přístupové systémy a zabezpečení
- Ověření výpadku – havarijní odemknutí

Oblast	Výstup Zhotovitele
FAT – Factory Acceptance Tests	Protokol o úspěšném provedení FAT testů, který bude obsahovat minimálně: <ul style="list-style-type: none">• Seznam testů a jejich výsledek• Výsledky z měření, která budou provedena

7.1 Konstrukční řešení kontejneru

Navržená konstrukce MDC musí splňovat aktuální požadavky na ochranu životního prostředí a být v souladu s platnými technickými normami, bezpečnostními, hygienickými a požárními předpisy. Exteriér modulu bude vizuálně zpracován pomocí fasádního opláštění z ocelových profilů.

Datové centrum bude realizováno jako modulární kontejnerová technologie, která poskytuje výkonné, flexibilní a energeticky efektivní řešení s možností rychlého nasazení v řádu několika týdnů. Předpokládá se využití hotové konfigurace optimalizované z hlediska výkonu a hustoty, která umožní agilní rozšíření kapacity nebo upgrade koncové infrastruktury.

MDC musí být navrženo tak, aby bylo jako celek kompletně sestaveno a technologicky integrováno ve výrobním závodě Zhotovitele. To zahrnuje instalaci všech non-IT technologií, jako jsou systémy napájení, záložní zdroje (UPS), rozváděče, chlazení, strukturovaná kabeláž, osvětlení, monitorovací a bezpečnostní systémy. Konstrukce musí umožnit bezpečnou přepravu s již nainstalovanými zařízeními ve stojanech. Mechanická odolnost musí odpovídat požadavkům pro kamionovou dopravu dle doporučení ISTA (International Safe Transit Association).

Veškerá ICT infrastruktura a související podpůrné technologie nezbytné pro provoz datového centra budou integrovány do jednoho konstrukčního celku. MDC tvoří uzavřený skelet, který zajišťuje ochranu a provozuschopnost zařízení během provozu i přepravy.

MDC bude mít samonosnou konstrukci, která umožní snadné usazení, opakovaný transport a přemístění na jinou lokalitu bez nutnosti zásadních stavebních úprav.

7.1.1 Vizuální provedení

Vizuální provedení musí odpovídat jednotnému vizuálnímu stylu provozovatele (SŽ), jak je definováno v manuálu vizuální identity ([Logomanuál - www.spravazeleznic.cz](http://www.spravazeleznic.cz)). MDC bude mít bílou barvu, přičemž podsvícené barevné logo Objednatele bude umístěno na obou delších stranách kontejneru (celkem 2 kusy) o rozměrech 80 x 40 cm. Zhotovitel je povinen zajistit zhotovení a umístění loga Objednatele na MDC formou trvalého fyzického prvku, který bude prostorově nebo reliéfně vyhotoven (např. plastický, 3D či jiný hmotný objekt). Logo nesmí být provedeno pouze povrchovou úpravou, jako je nástřik, nátěr, potisk, polep nebo aplikace fólie. Objednatel nestanoví konkrétní materiál, avšak požaduje, aby fyzická realizace loga byla odolná vůči povětrnostním podmínkám a vhodná pro dlouhodobé umístění v exteriéru.

Na vnější stěně, na levé straně venkovních vstupních dveří ve výšce 150 cm nad zemí bude umístěná památeční tabule - nerezová gravírovaná plaketa, o rozměru 30 x 20 cm. Text památeční tabule dodá Objednatel 2 týdny před avizovaným dodáním MDC Objednateli.

7.1.2 Obvodový plášť

Obvodový plášť MDC musí být navržen tak, aby odolával povětrnostním vlivům typickým pro klimatické podmínky České republiky dle ASHRAE. Konstrukce pláště bude provedena z vysoce odolné oceli, která zajistí mechanickou pevnost a dlouhodobou životnost při provozu i přepravě.

Panely tvořící obvodový plášť budou žebrované, vodotěsné a odolné vůči povětrnostním vlivům. Konstrukce musí splňovat požadavky na ochranu proti vlhkosti, teplotním výkyvům a mechanickému poškození, a zároveň zajistit bezpečné provozní podmínky pro vnitřní technologii.

7.1.3 Svislé konstrukce

Svislé konstrukce budou tvořeny z ocelových svařovaných ohýbaných profilů a tvarovaných plechů. Vnitřní strana konstrukce bude provedena z ocelových plechů, které budou pevně uchyceny k nosnému ocelovému rámu. Konstrukce musí zajistit dostatečnou tuhost, odolnost vůči mechanickému namáhání a splňovat požadavky na bezpečnost a životnost v souladu s platnými technickými normami.

7.1.4 Vodorovné konstrukce

Vodorovné konstrukce budou tvořeny svařovanými ocelovými ohýbanými profily a tvarovanými plechy. Nosný rám spodní a horní části bude vzájemně propojen ocelovými profily, které zajistí celkovou stabilitu a tuhost konstrukce.

Stěny budou tvořeny z profilovaných ocelových plechů, pevně uchycených k nosnému rámu. Konstrukce musí být navržena tak, aby odolávala mechanickému zatížení při provozu i přepravě, a zároveň umožňovala bezpečné osazení technologických komponent.

7.1.5 Nosné konstrukce

Nosná konstrukce bude tvořena svařovaným rámem z ocelových ohýbaných profilů a tvarovaných plechů. Spodní a horní rámová část jsou vzájemně propojeny ocelovými profily, které zajišťují celkovou tuhost a stabilitu konstrukce.

Stěny budou tvořeny z profilovaných ocelových plechů, pevně uchycených k nosnému rámu. Tloušťka použitých ocelových prvků se liší v závislosti na konkrétní části konstrukce a požadované mechanické odolnosti:

- **Stěny a střecha:** minimální tloušťka oceli je 1,6 mm,
- **Rám podlahy a příčníky:** zesílená ocel o tloušťce minimálně 4 mm pro zajištění nosnosti při vysokém zatížení,
- **Rohové sloupky:** nejvyšší konstrukční pevnost, tloušťka oceli minimálně 6 mm.

Konstrukce musí splňovat požadavky na statickou bezpečnost, odolnost vůči vibracím a nárazům při přepravě, a zároveň umožnit opakovanou instalaci bez ztráty funkčnosti.

7.1.6 Vnitřní dělicí konstrukce

Vnitřní dělicí konstrukce budou tvořeny sendvičovými panely s izolační vrstvou z polyuretanové pěny, překrytou lakovaným ocelovým plechem. Konstrukce stěn bude navržena tak, aby minimalizovala vznik tepelných mostů a tím omezila riziko kondenzace vlhkosti, zejména v zimních měsících.

Vnitřní dělicí konstrukce musí splňovat požární odolnost dle normy ČSN EN 13501-2 nebo obdobné.

Stěny budou vyztuženy pomocí ocelových plechů a profilů, které umožní instalaci zařízení s vyšší hmotností, jež nelze kotvit přímo do základní konstrukce. Celkové provedení musí zajistit mechanickou stabilitu, tepelnou izolaci a splňovat požadavky na bezpečný provoz ICT technologií.

7.1.7 Nosné konstrukce stropu

Nosná konstrukce stropu bude tvořena svařovaným rámem z ocelových ohýbaných profilů a tvarovaných plechů. Spodní a horní rámové části budou propojeny ocelovými profily, které zajišťují celkovou stabilitu konstrukce.

Střešní panely budou standardně vyrobeny z kovových materiálů, přičemž je možné využít i alternativní materiály za předpokladu, že splňují požadavky na tepelnou regulaci nebo přispívají ke snížení celkové hmotnosti.

Stropní konstrukce musí být navržena tak, aby:

- o zajistila dostatečnou nosnost pro plánované technologické vybavení, zejména venkovní jednotky chladicího systému,
- o umožnila rovnoměrné rozložení zatížení a provozní stabilitu,
- o poskytovala odpovídající tepelnou izolaci,
- o umožnila bezpečný pohyb obsluhy a instalaci zařízení na střeše.

7.1.8 Podlahy

Podlahová konstrukce bude tvořena vyztuženým ocelovým rámem, složeným z ohýbaných ocelových profilů. Povrch podlahy bude tvořen konstrukční deskou (např. CETRIS), která bude překryta antistatickým PVC povrchem, zajišťujícím bezpečný provoz ICT technologií.

Zateplení podlahy bude provedeno pomocí vrstvy polyuretanové pěny, která zajistí požadovanou tepelnou izolaci. Konstrukce podlahy musí být navržena tak, aby:

- o poskytovala dostatečnou nosnost pro plánované technologické vybavení,
- o umožňovala rovnoměrné rozložení zatížení a provozní stabilitu,
- o splňovala požadavky na tepelnou izolaci a bezpečný pohyb obsluhy,
- o umožňovala bezproblémovou instalaci zařízení.

7.1.9 Tepelné a zvukové vlastnosti

Stěny budou tvořeny sendvičovými panely s izolační vrstvou z polyuretanové pěny, překrytou lakovaným ocelovým plechem. Tepelná izolace bude navržena tak, aby účinně omezovala přenos tepla mezi vnějším a vnitřním prostředím, čímž přispěje ke stabilizaci

provozních podmínek ICT technologií. Všechny stěny musí být **tepelně izolovány** tak, aby vyhovovaly externím klimatickým podmínkám České republiky od **-19 °C do +39 °C** pro standardní HVAC návrhy dle ASHRAE institutu.

Součástí konstrukce bude také akustická izolace, která sníží přenos hluku z okolí a omezí dozvuk uvnitř MDC. Objednatel připouští použití kombinované tepelně-akustická izolace, která zajistí účinnou ochranu proti tepelným ztrátám i hlukové zátěži.

7.1.10 Výplně otvorů

Veškeré prostupy pro kabelové a potrubní vedení budou osazeny rozebíratelnými protiprachovými a protipožárními průchodkami. Každá průchodka bude dimenzována s minimální rezervou 30 % pro budoucí rozšíření technologické infrastruktury.

Prostupy pro napájecí a datové kabely budou vedeny buď spodní částí, nebo boční stěnou, v závislosti na konkrétním technickém řešení a umístění na lokalitě. Konstrukce prostupů musí být navržena tak, aby umožňovala bezpečnou instalaci, snadnou údržbu a splňovala požadavky na požární bezpečnost.

7.1.11 Venkovní provedení

Veškeré prostupy vzduchotechniky (VZT) skrz obvodový plášť budou osazeny venkovními protidešťovými žaluziemi. Žaluzie budou instalovány do rámců tvořených ocelovými profily a musí být navrženy tak, aby účinně zabránily vnikání dešťové vody do vnitřních prostor a zároveň neomezovaly funkčnost vzduchotechnického systému.

7.1.12 Vnitřní prostupy – dveře

Hlavní vstupní dveře (včetně zárubní) MDC budou mít minimální šířku 900 mm, výšku minimálně 2100 mm a budou odpovídat bezpečnostní třídě RC3 dle normy ČSN EN 1627. Dveře budou tepelně izolované, vybavené elektromechanickým zámkem s funkcí anti-panik, bezpečnostním kováním typu koule-klika (klika umístěna v chráněném prostoru), bezpečnostní cylindrickou vložkou a přístupovým systémem s bezkontaktní čtečkou karet s podsvícenou klávesnicí. Nad vstupem bude instalována ochranná stříška proti dešti a sněhu.

Vstupní místnost (podpůrná místnost) bude od datového sálu oddělena pevnou dělicí příčkou, která zajistí fyzickou bezpečnost, zabrání vniknutí nečistot a omezí nekontrolovanou výměnu vzduchu mezi prostory.

Vnitřní dveře mezi vstupní místností a datovým sálem budou rovněž mít minimální šířku 900 mm, výšku minimálně 2100 mm, vybaveny elektromechanickým zámkem s funkcí anti-panik, čtečkou karet s podsvícenou klávesnicí budou odpovídat bezpečnostní třídě RC3 dle normy ČSN EN 1627.

Pro zajištění efektivního řízení proudění vzduchu budou prostory teplé a studené uličky stavebně odděleny. Vstup do prostoru teplé uličky bude zajištěn posuvnými dveřmi s mechanickou aretací, pro kontrolovanou separaci proudění vzduchu a optimalizaci chlazení.

7.1.13 Zámečnické konstrukce

Zámečnické konstrukce budou instalovány uvnitř MDC jako pomocné konstrukční prvky pro upevnění technologického vybavení. Tyto prvky musí být navrženy tak, aby umožňovaly bezpečnou a stabilní montáž zařízení s různou hmotností a rozměry.

Zámečnické konstrukce budou rovněž využity pro mobilní instalaci technologických komponent na vnější straně MDC, v souladu s požadavky na provozní flexibilitu a technickou kompatibilitu.

7.1.14 Bleskosvodná a uzemňovací soustava

MDC bude chráněn proti atmosférickým vlivům pomocí systému ochrany před bleskem (LPS – Lightning Protection System), který zajistí maximální bezpečnost zařízení a minimalizaci rizik pro osoby i majetek.

Na střeše budou instalovány jímací tyče s možností snadné demontáže. Svody budou vedeny viditelně po obvodových stěnách a každý svod bude vybaven zkušební svorkou pro kontrolu funkčnosti.

Pro uzemnění hromosvodu a silnoproudých zařízení bude zřízena uzemňovací soustava tvořená zemnicími tyčemi umístěnými kolem MDC. Ze zemniců budou vyvedeny spoje pro svody hromosvodu a hlavní ochrannou přípojnicí. Veškeré kovové konstrukce v okolí MDC budou připojeny k této uzemňovací soustavě.

Uzemňovací soustava není součástí této veřejné zakázky a bude zajištěna samostatně Objednatelům v rámci přípravy konkrétní lokality.

7.1.15 Dispoziční a provozní řešení

Mobilní datové centrum je koncipováno jako trvale bezobslužné pracoviště, bez stálé fyzické obsluhy. Představuje řešení pro uživatele s požadavky na rychlou implementaci, mobilitu a nízké prostorové nároky. Veškerá infrastruktura MDC je integrována do **jednoho modulárního kontejneru**, který zahrnuje jak ICT zařízení, tak podpůrné technologie nezbytné pro jeho provoz.

MDC je dispozičně rozděleno na dvě hlavní části:

- **Přechodová místnost**, která slouží jako vstupní místnost z venku pro zamezení přenosu nečistot do vnitřní místnosti s ICT technologiemi, příruční sklad a také pro umístění některých technologických zařízení (např. elektrické rozvaděče);
- **Datový sál**, kde jsou umístěny datové rozvaděče.

Toto uspořádání zajišťuje dodatečnou úroveň zabezpečení datového sálu a zároveň minimalizuje vnikání vlhkosti, prachu a dalších nečistot do prostoru s ICT.

Vstupní koridor slouží jako přechodová zóna mezi vnějším prostředím a ICT částí. Z koridoru je umožněn přístup do ICT prostoru.

Vstup bude realizován přes dveře vybavené elektromechanickým zámkem s cylindrickou vložkou, ovládaným vnější bezkontaktní čtečkou s podsvícenou klávesnicí. Podpůrná místnost obsahuje podpůrné technologie a je vybavena kamerovým dohledem.

Přístup do ICT části je řízen pomocí elektronického přístupového systému ASSET provozovaným v infrastruktuře Objednatele, a to konkrétně čipovou kartou, v kombinaci s číselným PIN kódem. V této části se nachází jedna souvislá řada datových rozvaděčů, tvořící hlavní technologické jádro datového centra.

7.1.15.1 Přechodová místnost

Přechodová místnost plní funkci vstupní komory, která je konstrukčně oddělena od venkovního prostředí. Slouží jako ochranná bariéra proti vniknutí vody, prachu a dalších nečistot. Z této komory je zajištěn kontrolovaný přístup do prostoru s ICT technologiemi.

Současně tato místnost slouží jako přechodový prostor mezi exteriérem a datovým sálem, příruční sklad a místo pro instalaci vybraných technologických zařízení (např. elektrických rozvaděčů). Tímto uspořádáním se omezuje nutnost vstupu obslužného a servisního personálu přímo do datového sálu mobilního datového centra, čímž se zvyšuje bezpečnost a provozní efektivita.

7.1.15.2 Datový sál

V datovém sále budou instalovány datové rozvaděče (racky) dle průmyslového standardu **19"**, určené pro běžný IT hardware třetích stran. Proudění vzduchu bude řešeno z přední části do zadní, s cílem optimalizace chlazení.

Rozmístění rozvaděčů bude navrženo tak, aby vznikla oddělená ulička pro rozdělení chladného a ohřátého vzduchu. Součástí bude:

- 1 vstupní dveře do teplé uličky,
- Každý rozvaděč bude vybaven zamykacími jednodílnými dveřmi v přední části a dělenými dveřmi v zadní části.

7.1.16 Bezbariérové užívání datového centra

S ohledem na provozní charakter, konstrukční řešení a vnitřní dispozici MDC, není umožněn přístup osobám s omezenou schopností pohybu a orientace. MDC není navrženo pro bezbariérové užívání.

7.2 Technologické řešení

Infrastruktura mobilního datového centra musí splňovat požadavky pro úroveň **TIER III** dle klasifikace **Uptime Institute** nebo podle standardu **ANSI/TIA-942**. Systém musí být navržen tak, aby umožňoval servisovatelnost za plného provozu, tj. všechny klíčové komponenty MDC musí být vyměnitelné nebo opravitelné bez nutnosti odstávky IT systémů.

Hlavní požadavky na topologii infrastruktury zahrnují:

- **Plně redundantní napájecí systémy**, zajišťující nepřerušované napájení i při výpadku dodávky elektrické energie.
- **Redundantní chladicí systémy**, které udržují optimální provozní teplotu zařízení.



- **Redundance typu N+1** – každá kritická komponenta (napájení, chlazení) musí mít alespoň jednu záložní jednotku.
- Zajištění provozní kontinuity během údržby, díky použití redundantních prvků infrastruktury.
- Úroveň dostupnosti **minimálně 99,982 %**, což odpovídá maximálně přibližně 1,6 hodinám neplánovaného výpadku ročně.
- Průměrná roční hodnota PUE (Power Usage Effectiveness) nesmí překročit hodnotu **1,3**.

7.2.1 Napájení

Mobilní datové centrum bude vybaveno kompletním systémem elektrického napájení, který bude plně servisovatelný za provozu a navržen v souladu s požadavky úrovně **TIER III** dle Uptime Institute. Systém musí zajistit nepřetržité napájení všech ICT komponent, včetně záložních zdrojů a redundantních napájecích větví.

Hlavní požadavky na napájení zahrnují:

- **Příkon ICT:** Plánovaný příkon ICT technologií činí **100 kW**;
- **Celkový příkon:** Celkový příkon mobilního datového centra, včetně Non-IT technologií (např. chlazení, dobíjení baterií), nesmí překročit **180 kW**;
- **Energetická efektivita:** Průměrná roční hodnota PUE (Power Usage Effectiveness) nesmí překročit **1,3**

7.2.1.1 Hlavní systém napájení

Přívody elektrické energie budou zajištěny Objednatelem, včetně dodávky napájecích kabelů. Samotné napojení MDC na připravené elektrické rozvody zajistí Zhotovitel.

Distribuce elektrické energie bude zahájena v nadřazené rozvodně NN, kde bude zajištěno napájení i ze zálohované sítě prostřednictvím motorgenerátoru. Mobilní datové centrum bude napájeno prostřednictvím více napájecích větví, které zajistí provozní redundanci a vysokou dostupnost.

Pro napojení MDC bude ve finální lokalitě k dispozici samostatný třífázový přívod s jištěním 3 x 315 A, 400VAC. Na straně kontejneru musí být Zhotovitelem implementováno identické jištění.

Pro napojení MDC bude v dočasné lokalitě k dispozici samostatný přívod s jištěním minimálně 3 x 32 A, 400VAC

Systém napájení prioritně uvažuje s napojením z jednoho směru na úrovni 400V TN-C nebo TN-S vč. stacionárního zdroje el. energie – motorgenerátoru a zdroje nepřetržitého napájení na úrovni 230/400VAC. Provedení rozvaděčů musí umožňovat připojení systému datového centra také z druhého napájecího směru, včetně mobilního motorgenerátoru. Dodávka motorgenerátoru není součástí plnění Smlouvy.

Součástí projektu je ovšem realizace přípojného bodu pro napojení kabelu z druhého napájecího směru a přípojného bodu pro napojení mobilního motorgenerátoru.

Napájecí infrastruktura modulu MDC musí být navržena tak, aby umožňovala bezpečný provoz, snadnou údržbu a rozšíření v budoucnosti. Všechny komponenty musí být

kompatibilní s požadavky na provozní spolehlivost a energetickou účinnost a v souladu s platnými elektrotechnickými normami EN/ISO/ČSN.

7.2.1.2 Distribuce elektrické energie

Distribuce elektrické energie musí být navržena v konfiguraci dvojitého napájení (větev A / větev B) pro všechny spotřebiče v MDC. Z hlediska dostupnosti elektrického napájení budou spotřebiče v mobilním datovém centru rozděleny do následujících kategorií:

- Zálohovaná zařízení (napájená ze záložních zdrojů UPS)
 - Datové rozvaděče
 - Servery
 - Datová uložení
 - Síťová infrastruktura (switche, routery, firewally)
 - Řídicí systémy chlazení (např. řídicí jednotky klimatizací)
 - Bezpečnostní systémy (např. přístupové systémy, CCTV)
 - Ovládání motorgenerátoru (pokud je součástí dodávky)
 - Osvětlení nouzových zón (např. datový sál, podpůrná místnost)
- Nezálohovaná zařízení (napájené napřímo, bez podpory UPS, zálohované pouze motorgenerátorem)
 - Celý IT provoz (včetně toho, co je na UPS)
 - Chladicí systémy (CRAC jednotky, chillery)
 - Osvětlení celého objektu
 - Zabezpečovací systémy Nabíjení baterií UPS

Obě napájecí větve budou zakončeny samostatnými rozvaděči RH-A a RH-B, které budou zajišťovat distribuci elektrické energie pro technologické systémy, včetně chlazení a záložních zdrojů UPS.

Zálohované napájení ICT infrastruktury bude zajištěno prostřednictvím dvou samostatných rozvaděčů RUPS-A a RUPS-B, které budou připojeny k oběma napájecím větvím. Tím bude zajištěna redundance a vysoká dostupnost napájení.

- Zálohovaná ICT infrastruktura bude napájena přes **systém UPS**, který zajistí nepřerušované napájení v případě výpadku obou napájecích větví, po dobu nutnou k náběhu motorgenerátoru.
- Po spuštění motorgenerátoru bude napájení automaticky přepnuto na generovaný zdroj.

Nezálohovaná ICT infrastruktura bude napájena přímo z napájecích rozvaděčů bez použití UPS. V případě výpadku napájení bude jejich provoz obnoven po spuštění motorgenerátoru.

Pasivní napájecí větev bude také sloužit k napájení technologií během servisních zásahů na aktivní větvi, čímž bude zajištěna provozní kontinuita.

Všechny kovové části zařízení a vedení uvnitř MDC budou vodivě propojeny do jednotné zemnicí sítě, která bude vyvedena vně a připojena na vnější uzemňovací síť objektu. Uzemnění bude provedeno v souladu s normou **ČSN EN 50310 ed.4**.



Pro ochranné pospojování budou ve všech technických místnostech instalovány hlavní ochranné přípojnice (HOP), ke kterým budou připojeny všechny velké kovové hmoty v dosahu – včetně rozvaděčů, zařízení VZT, klimatizací, kovových konstrukcí, ústředen SLP apod. Tyto přípojnice budou propojeny s vnější uzemňovací sítí objektu, která není součástí této veřejné zakázky. MDC bude vybaveno svorkami pro jednoduché připojení k této síti.

Součástí systému napájení bude ochrana proti přepětí, realizovaná vhodnou instalací přepětových ochran v napájecí síti.

Pro případ dlouhodobé odstávky primárního napájení nebo fatální poruchy bude MDC vybaveno přívodem pro napájení z mobilního motorgenerátoru, napojeným do pasivní napájecí větve.

Celá distribuční soustava bude monitorována, včetně stavu jisticích a spínacích prvků. Měření spotřeby a sledování parametrů sítě bude přenášeno do monitorovacího systému, který umožní vyhodnocování provozních dat, včetně výpočtu PUE datového centra.

7.2.1.3 Záložní systém napájení

Objednatel zajistí záložní zdroj elektrické energie formou motorgenerátoru odpovídajícího výkonu, který nebude součástí MDC. Napájení datového centra bude realizováno prostřednictvím dvou nezávislých napájecích větví, přičemž jedna z nich bude napájena přes motorgenerátor a bude sloužit jako primární (aktivní) větev. Druhá větev bude napojena přímo na externí transformátor a bude sloužit jako sekundární (pasivní) napájecí směr.

7.2.1.4 Zdroj nepřerušitelného napájení (UPS)

Mobilní datové centrum bude vybaveno kompletním systémem zdrojů nepřerušitelného napájení, který bude navržený v souladu s požadavky úrovně **TIER III** dle Uptime Institute. Systém musí být plně servisovatelný za provozu a dimenzován pro zajištění nepřerušitelného napájení ICT infrastruktury, řídicího systému chlazení a systému monitoringu. Budou instalovány **dva modulární UPS systémy**, každý o výkonu **minimálně 100 kW**. Přičemž výkonové moduly napájecího systému budou dimenzovány v konfiguraci minimálně N+1.

Každý UPS systém bude tvořen výkonovými moduly o výkonu **min. 20 kVA / 20 kW**, které budou:

- o uživatelsky vyměnitelné („hot-swappable“),
- o instalovatelné za provozu bez přerušení napájení,
- o vybavené integrovaným statickým přepínačem (static switch),
- o vybavené samostatným řídicím systémem.

Pro zajištění nepřerušenoého provozu během startu motorgenerátoru bude každý UPS systém vybaven vlastní bateriovou sadou.

Požadovaná doba zálohování je **minimálně 10 minut při plné zátěži 100 kW** a provozu MDC a bateriových sad.

UPS systémy musí být schopny informovat správu IT o:

- o výpadku napájení



- kvalitě vstupního napětí (přepětí, podpětí, frekvence)
- kvalitě výstupního napětí (přepětí, podpětí, frekvence)
- přetížení, zkratu
- stavu bypassu
- vybití / nabití / kapacitě baterií
- času zálohování
- teplotě a chlazení
- ztrátě redundance
- poruše výkonového modulu a invertoru
- výpadku komunikace

prostřednictvím:

- e-mailu,
- SNMP trapu,
- webového rozhraní.

Komunikační SNMP karta bude součástí zařízení a napojena do systému monitoringu.

7.2.1.5 Základní požadavky na zdroje UPS

UPS systémy musí splňovat následující technické požadavky:

- **Modulární architektura DPA** (Decentralized Parallel Architecture) – paralelní zapojení výkonových modulů o min. výkonu 20 kVA / 20 kW
- **Hot-swappable moduly** – výměna a instalace za provozu bez nutnosti zásahu specializované techniky
- Baterie typu **LiFePO₄** (Lithium Iron Phosphate) s dlouhou životností, s nízkými nároky na údržbu, kompaktními rozměry, vhodné pro aplikace s vysokou dynamikou zátěže
- Každý modul musí obsahovat:
 - vlastní statický přepínač (static switch),
 - samostatný usměrňovač,
 - nezávislý řídicí systém,
 - LCD displej pro ovládání, monitoring a správu provozních parametrů
- Vysoká účinnost v on-line režimu s dvojitou konverzí
- Minimální efektivita **95,5 %** při zatížení 50–75 % nominálního výkonu při provozu ze sítě.
- Integrovaný manuální servisní bypass – umožňuje přesměrování napájení mimo UPS pro účely údržby bez přerušení dodávky energie
- Senzor pro teplotně kompenzované dobíjení – optimalizace nabíjecího napětí dle aktuální teploty baterií
- Rozhraní pro výstup do systému měření a regulace (MaR) – prostřednictvím SNMP protokolu a reléových kontaktů.

7.2.2 Chlazení a vzduchotechnika

Mobilní datové centrum bude vybaveno kompletním systémem chlazení a vzduchotechniky, navrženým v souladu s požadavky úrovně **TIER III** dle Uptime Institute. Systém musí být

plně servisovatelný za provozu a dimenzován pro chlazení IT vybavení s celkovým výkonem až **100 kW**.

Datové rozvaděče budou uspořádány tak, aby umožňovaly předozadní proudění vzduchu – klimatizovaný vzduch bude nasáván přední částí zařízení a teplý vzduch odváděn zadní částí. Pro zajištění účinného chlazení bude prostor teplé a studené uličky stavebně oddělen, čímž se zvýší efektivita systému.

Preferovaným řešením chlazení jsou alespoň 3 DX klimatizační jednotky, s podporou přímého, nebo nepřímého free coolingu (FC), s modulovatelným chladicím výkonem a vzájemnou komunikací zajišťující prevenci častého cyklování.

Tyto jednotky budou pracovat s cirkulačním oběhovým vzduchem a budou vybaveny EC ventilátory pro snížení spotřeby elektrické energie.

Systém chlazení bude navržen s **N+1 redundancí**, přičemž potřebný výkon musí být pokryt 100% chladicími jednotkami ve všech provozních režimech. Jednotky budou vybaveny integrovaným systémem řízení tlaku mezi teplou a studenou uličkou, který umožní přesné dávkování vzduchu dle aktuálních požadavků ICT zařízení.

Preferovaným řešením rozvodů pro distribuci chladiva jsou dva separované chladicí okruhy vedené jinou trasou do datového sálu. Jako příklad možného řešení rozvodů pro distribuci chladiva může posloužit níže uvedený koncepční návrh zapojení chlazení serverovny (kap. 15.2 - *Ideologické schéma zapojení chlazení serverovny*), který má sloužit jako podklad pro další technický návrh a neslouží jako závazný technický návrh.

Venkovní jednotky budou umístěny na střeše MDC a jejich konstrukce bude navržena tak, aby byly vizuálně integrovány do celkového vzhledu a nebylo zřejmé, jaké technologie jsou uvnitř umístěny.

Systém chlazení bude dimenzován s ohledem na klimatické podmínky České republiky, včetně teplotních extrémů, vlhkosti a sezónních výkyvů. Vnitřní mikroklima bude řízeno dle požadavků ICT zařízení, přičemž doporučené teplotní a vlhkostní pásmo bude definováno podle standardu ASHRAE. Je požadována funkce vysoušení a zvlhčování vzduchu.

Systém musí umožňovat monitoring a regulaci teploty a vlhkosti v reálném čase, včetně generování alarmů při překročení limitních hodnot. Informace o ztrátě redundance nebo závadě systému budou předávány Objednateli prostřednictvím e-mailu, SNMP trapu a webového rozhraní. Každá chladicí jednotka bude vybavena SNMP komunikační kartou, napojenou do monitorovacího systému.

Vnitřní i venkovní jednotky budou napájeny **ze dvou nezávislých zdrojů** s automatickým přepnutím v případě výpadku. Systém musí být navržen tak, aby umožňoval servisovatelnost za plného provozu – všechny klíčové komponenty chlazení musí být vyměnitelné nebo opravitelné bez nutnosti odstávky IT systémů.

Odvod kondenzátu z chladicích a klimatizačních zařízení bude napojen na systém odvodnění instalační plochy tak, aby bylo zajištěno bezpečné odvádění vody a nedocházelo k jejímu vsakování do podlahy nebo k poškození základové konstrukce.

Pro zvýšení bezpečnosti pracovníků uvnitř kontejneru musí být v obou místnostech (Přechodová místnost i hlavní sál ITC) instalován detektor oxidu uhličitého-CO₂ (monitor



'vydýchaného vzduchu') s LCD displejem pro přehled o úrovni CO₂ v místnosti a akustickou signalizací při překročení zdravotního limitu 1500ppm. Detektor musí být umístěn na dobře viditelném místě vedle dveří.

7.2.3 Bezpečnostní technologie

Přístup do MDC bude chráněn prostřednictvím selektivního systému kontroly přístupu, který umožní autorizaci vstupu pouze oprávněným osobám. Součástí bezpečnostního řešení bude také ústředna poplachového zabezpečovacího a tísňového systému (PZTS), která zajistí dohled nad stavem zabezpečení objektu a umožní reakci na bezpečnostní incidenty.

Systém musí být navržen tak, aby splňoval požadavky na fyzickou bezpečnost, integraci s ostatními technologiemi a umožňoval vzdálenou správu a monitoring. Systém musí být plně kompatibilní, integrovatelný a spravovaný stávajícím systémem ASSET, který je provozován v infrastruktuře Objednatele.

7.2.3.1 Parametry přístupového systému

Ústředna (lokální):

Ústředna pro PZTS, včetně zdrojů, sběrnic a dalšího nutného příslušenství pro správnou funkci systému kompatibilní s technologií ASSET, provozovanou v infrastruktuře Objednatele.

Čtečka venkovní:

Čtečka s PIN klávesnicí, karty HF 13,56 MHz Mifare Classic (zápis/čtení sektoru) a Mifare Desfire (šifrování karet EV2 na aplikační úrovni s využitím diverzifikovaných klíčů) a dalších typů karet, ISO14443A, ISO14443B, ISO15693 + Venkovní kryt čtečky (je-li třeba k zajištění funkcionalit v exteriéru).

Čtečka musí být kompatibilní s technologií ASSET, provozovanou v infrastruktuře Objednatele (např. čtečka ASSET 612 či obdobná).

Čtečka vnitřní (dveře + racky):

Čtečka bez PIN karty HF 13,56 MHz Mifare Classic (zápis/čtení sektoru) a Mifare Desfire (šifrování karet EV2 na aplikační úrovni s využitím diverzifikovaných klíčů) a dalších typů karet, ISO14443A, ISO14443B, ISO15693.

Čtečka musí být kompatibilní s technologií ASSET, provozovanou v infrastruktuře Objednatele (např. čtečka ASSET 612 či obdobná).

Zámek rackový:

Zámek racku kompatibilní s použitou čtečkou a s technologií ASSET, provozovanou v infrastruktuře Objednatele.



Magnetický kontakt dveří:

Magnetický kontakt povrchový čtyřdrátový polarizovaný s pracovní mezerou 22 mm, montáž nad dveřmi.

Zámek dveří:

Elektromechanický, kompatibilní s technologií ASSET, provozovanou v infrastruktuře Objednatele.

Dveřní kování:

Systém koule – klika (klika zevnitř)

Veškerý hardware (včetně firmware) potřebný pro zprovoznění přístupového systému dodá Zhotovitel jako součást MDC. Zhotovitel je dále povinen provést napojení dodaného hardware na centrální systém pro řízení přístupu (který je provozován na technologii ASSET a spravován externím subjektem), Objednatel je povinen v této souvislosti poskytnout Zhotoviteli potřebnou součinnost.

7.2.3.2 Poplachový zabezpečovací a tísňový systém (PZTS)

Vnitřní prostory MDC budou chráněny pomocí duálních detektorů pohybu s antimaskingem (kombinace PIR + MW), které budou umístěny ve studené uličce, teplé uličce a podpůrné místnosti.

Všechny vstupní dveře, včetně dveří datových rozvaděčů a dveří oddělujících teplou a studenou uličku, budou vybaveny magnetickými kontakty pro detekci otevření.

Plášťová ochrana kontejneru bude realizována pomocí CCTV kamer s videoanalytickou funkcí. Tato funkce bude integrována do stávajícího systému provozovaného Objednatelem.

Systém PZTS bude napojen na centrální monitorovací systém, který umožní sledování a vyhodnocování všech klíčových informací z bezpečnostních technologií a senzorů.

Při použití přístupové karty v kombinaci s číselným PIN kódem oprávněné osoby dojde k odblokování dveří a umožnění vstupu. Zastřežení a odstřežení systému bude prováděno prostřednictvím klávesnice umístěné ve vstupní chodbě. V případě narušení bude aktivován akustický alarm a informace o události bude předána do monitorovacího systému.

7.2.3.3 Systém elektrické kontroly vstupů (EKV)

MDC bude vybaveno systémem elektronické kontroly vstupů (EKV), který zajistí řízený a bezpečný přístup do jednotlivých částí objektu. Systém bude tvořen bezkontaktními čtečkami karet s podsvícenou klávesnicí, biometrickými prvky a elektromechanickými zámky s bezpečnostními funkcemi.

Přístupový systém (EKV) bude integrován do centrálního bezpečnostního systému ASSET Objednatele. Správu a řízení přístupu bude zajišťovat příslušný útvar Objednatele.

Vstupní dveře do MDC (vnější plášť):

- Bezkontaktní čtečka karet s podsvícenou klávesnicí,

- Elektromechanický zámek s bezpečnostním kováním typu koule–klika (klika umístěna v chráněném prostoru) s funkcí anti-panik,
- Bezpečnostní cylindrická vložka,
- Minimálně čtyřbodové uzamčení typu EL566.
- Dveře budou osazeny samozavíračem (s kluznou lištou s možností otevření až 180°)
- Detektor nezavření dveří s opticko-zvukovou signalizací a napojením na PZTS

Vstupní dveře do ICT sálu (vnitřní část):

- Bezkontaktní čtečka karet s podsvícenou klávesnicí,
- Elektromechanický zámek s bezpečnostním kováním typu koule–klika s funkcí anti-panik,
- Bezpečnostní cylindrická vložka,
- Čtyřbodové uzamčení typu EL566.
- Dveře budou osazeny samozavíračem (s kluznou lištou s možností otevření až 180°)
- Detektor nezavření dveří s opticko-zvukovou signalizací a napojením na PZTS

Dveře do prostoru teplé uličky:

- Posuvné dveře s gravitačním zavíráním a s mechanickou aretací.

Dveře IT stojanů (datové rozvaděče):

- Bezkontaktní čtečka karet.

Všechny dveře (s výjimkou dveří datových rozvaděčů a dveří do teplé uličky) budou vybaveny elektromechanickým zámekem s funkcí anti-panik a budou splňovat požadavky bezpečnostní třídy **RC3 dle ČSN EN 1627**.

7.2.3.4 Dohledový kamerový systém (CCTV)

Pro zajištění vizuální kontroly, sledování provozu a identifikaci osob bude MDC vybaveno kamerovým systémem (CCTV) s video analytickými funkcemi. Kamery budou instalovány ve vnitřních i vnějších částech, konkrétně:

- ve studené a teplé uličce,
- v podpůrné místnosti,
- prostor okolo kontejneru (všechny strany)

Použité kamery budou vybaveny pokročilou technologií s CMOS senzorem a vysokou světelnou citlivostí. Napájení kamer bude zajištěno prostřednictvím PoE (Power over Ethernet) switchů.

Záznam z kamer bude ukládán na záznamový server umístěný uvnitř MDC. Obsluha v dohledovém centru SŽ bude mít možnost vzdáleného přístupu k živému obrazu i archivovaným záznamům, včetně možnosti vyhodnocení situací v reálném čase. On-line přenos bude umožněn i dohledu ze strany Objednatelem pověřených osob.

Parametry dohledového systému CCTV:

Kamery (minimální požadované parametry):

- 4x venkovní kamera, 4MPix, IP66, WDR, IR přísvit, napájení PoE, 130° zorné pole, videoanalytika součástí kamery, kamery budou umístěny na konstrukci kontejneru tak, aby zabíraly okolí kontejneru a hlavně vstupní dveře



- 4x vnitřní kamera, 4MPix, WDR, IR přísvit, napájení PoE, 130° zorné pole, videoanalytika součástí kamery, jedna kamera bude umístěna uvnitř proti vstupním dveřím

Nahrávací zařízení:

- Rackové provedení, min. požadavek na OS - Win 11 nebo Windows Server 2022
- Disky min. 2 x 2TB jako úložiště (zrcadlené-RAID 1)

Software (systém pro správu CCTV):

- Zhotovitel je povinen dodat následující licence výrobce Milestone Systems, jež je provozován v infrastruktuře Objednatele, kdy dodávka těchto licencí představuje rozšíření stávajícího systému Objednatele:
 - 1 x XProtect Corporate Base License (BL) - bude umístěno v prostorách Objednatele v Praze
 - 8x XProtect Corporate Device License (DL) - 1 ks na každou kameru

7.2.3.5 Požární systém

Mobilní datové centrum bude vybaveno systémem elektrické požární signalizace (EPS) a samočinným hasicím zařízením (SHZ) na bázi chemického plynu. Systém SHZ bude navržen v souladu s normou **ČSN ISO 14520-1:2006**. Jako hasicí médium může být použito například NOVEC 1230 nebo Inergen.

Plynový SHZ bude konstruován tak, aby jeho funkčnost byla zachována i při úplném výpadku elektrické energie, včetně výpadku všech záložních zdrojů a akumulátorů.

Systém SHZ bude navržen bez nutnosti instalace přetlakových klapek pro odvod přetlaku/podtlaku při vypouštění hasiva do chráněného prostoru. Detekce požáru bude zajištěna kombinací opticko-kouřových detektorů a laserové nasávací detekce pro včasně odhalení požáru.

Ústředna SHZ bude napojena na monitorovací systém, který bude přijímat standardní signály:

- Porucha,
- Před-poplach,
- Poplach
- Hasivo vypuštěno.

V chráněném prostoru budou instalována tlačítka pro manuální spuštění a blokaci systému SHZ, doplněná o optickou a akustickou signalizaci.

7.2.3.6 Ochrana před požárem baterií UPS

Pro ochranu před požárem baterií UPS bude použity vhodné optické a ionizační detektory kouře a senzory plamene v prostoru UPS.

SHZ pro baterie UPS bude konstruován tak, aby jeho funkčnost byla zachována i při úplném výpadku elektrické energie, včetně výpadku všech záložních zdrojů a akumulátorů.

Pro ochranu před požárem baterií UPS bude použit autonomní hasicí systém (např. Vermikulitový nebo F-500 systém) používající zónové hašení pouze v postižené části.

7.2.4 Osvětlení

Řešení provozního osvětlení bude navrženo s ohledem na členění prostor dle architektonických, provozních a hygienických požadavků. Osvětlení bude realizováno v souladu s normou **ČSN EN 12464-1**, tak aby byly splněny požadované hodnoty osvětlenosti v jednotlivých rovinách a prostorech, a zároveň byla zajištěna maximální světelná pohoda.

Použita budou **energeticky úsporná LED svítidla** s odpovídajícím krytím dle charakteru prostoru.

7.2.4.1 Vnitřní

Napájení osvětlení bude rozděleno rovnoměrně:

- 50 % z rozváděče RUPS-A
- 50 % z rozváděče RUPS-B

Požadované minimální hodnoty osvětlenosti dle ČSN:

- Technické prostory, strojovny – min. 200 lx
- Místnost s datovými rozvaděči – min. 500 lx

Ovládání svítidel bude realizováno místními vypínači umístěnými u dveří jednotlivých místností.

7.2.4.2 Vnější

Venkovní osvětlení bude zajištěno pomocí minimálně 4 ks LED reflektorů, umístěných na mobilních konzolách na střeše kontejneru. Ovládání reflektorů bude:

- Manuální
- Automatické – na základě signálu z minimálně 4 ks pohybových čidel umístěných v exteriéru nebo na základě analytických funkcí venkovních kamer.

7.2.4.3 Nouzové

Nouzové osvětlení bude navrženo tak, aby:

- jasně a jednoznačně vyznačovalo únikové cesty,
- zajistilo viditelnost překážek a bezpečný přesun osob k nouzovým východům,
- označovalo poplachová, protipožární a důležitá ovládací zařízení.

Nouzové osvětlení bude realizováno pomocí LED svítidel s integrovanou baterií, s předpokládanou dobou provozu v nouzovém režimu **min. 1 hodinu**.

Požadované hodnoty osvětlenosti dle **ČSN EN 1838**:

- Únikové cesty – min. 1 lx v osách
- Požárně bezpečnostní zařízení mimo únikové cesty – min. 5 lx

7.3 ICT technologie mobilního datového centra

Veškerá IT infrastruktura datového centra je integrována do **jednoho kontejnerového modulu**, který bude obsahovat:

- o všechna ICT zařízení,
- o podpůrné technologie nutné pro provoz.

7.3.1 Datové rozvaděče

Pro instalaci IT technologií bude Zhotovitelem dodáno **minimálně 8 ks datových rozvaděčů (racků)** typu **19"**, každý o rozměrech:

- o šířka: 800 mm
- o hloubka: 1200 mm
- o výška: 42U

Rozvaděče budou mít stabilní rámovou konstrukci s nosností **min. 1300 kg** (dynamické zatížení). Ukotvení rozvaděčů bude provedeno do rámu kontejneru s ponecháním mezer mezi stojany, čímž vznikne prostor pro:

- o kabeláž,
- o PDU lišty,
- o vyvazovací příslušenství,
- o každý rozvaděč bude vybaven zamykacími jednodílnými dveřmi v přední části a dělenými dveřmi v zadní části.

Rozmístění rozvaděčů musí umožnit:

- o bezproblémovou instalaci zařízení ze strany studené uličky,
- o podporu montáže zařízení s různou hloubkou.

Součástí dodávky budou:

- o záslepky pro uzavření min. **80 %** volných U pozic, v provedení pro beznástrojovou montáž,
- o separační rám pro oddělení teplé a studené uličky,
- o šrouby a klecové matice pro uchycení zaslepovacích panelů.

Každý datový rozvaděč bude vybaven samostatným elektronickým kartovým přístupovým systémem, který bude integrován do centrálního bezpečnostního systému ASSET, provozovaného v infrastruktuře Objednatele. Správu a řízení přístupu bude zajišťovat příslušný útvar Objednatele.

7.3.2 PDU lišty

Maximální garantovaný výkon na jeden RACK bude **10 kW**, každý datový rozvaděč bude vybaven **minimálně čtyřmi vertikálními měřenými PDU lištami** se zásuvkami **C13 a C19**, které:

- o nezasahují do U pozic,
- o nebrání instalaci kabeláže ani hlubokých IT zařízení,



- budou vnořeny do rámu skříně a instalovány na zadní straně rámu.
- Dvě třífázové PDU (32 A) ve spodní části racku:
 - Minimálně 8x C19 zásuvek a minimálně 8x C13 zásuvek
- Dvě jednofázové PDU (16 A) v horní části racku:
 - Minimálně 4x C19 zásuvek a minimálně 12x C13 zásuvek

Napájení PDU lišt:

- dvě lišty z napájecí větve A
- dvě lišty z napájecí větve B

PDU lišty budou **měřené a monitorované**, s možností sledování odběru a stavu napájení, musí obsahovat dostatečný počet zásuvek pro připojení všech ICT zařízení v plně osazeném racku, napojené do systému monitoringu pro účely sledování:

- spotřeby elektrické energie,
- výpočtu PUE datového centra.

Do PDU lišt budou integrována teplotně-vlhkostní čidla:

- 4 ks ve studené uličce,
- 2 ks v teplé uličce

Každé čidlo bude připojeno samostatně do jedné PDU lišty.

7.3.3 Strukturovaná kabeláž

Součástí dodávky mobilního datového centra bude předkonektorovaná strukturovaná kabeláž, zahrnující:

Vzájemně propojení racků:

- Optická strukturovaná kabeláž
 - OM4, MM, Duplex, SC/UPC, minimálně 12 portů/rack
 - OS2, SM, Simplex, E2000/APC, minimálně 12 portů/rack
- Metalická strukturovaná kabeláž:
 - kategorie CAT6a, minimálně 12 portů/rack
- Optické a metalické datové kabely požadujeme oddělit do vlastních kabelových žlabů (každý typ kabelu do vlastního žlabu)

7.3.3.1 Racková výbava

Každý serverový rozvaděč (rack) bude standardně osazen:

- 1 patch panelem s minimálně:
 - **12** optickými porty typu LC duplex (OM4)
 - **6** metalickými porty kategorie CAT6a.

7.3.3.2 LAN rozvaděče

Jeden z datových rozvaděčů bude vyhrazen jako LAN datový rozvaděč pro:

- o ukončení síťové konektivity,
- o správu datové infrastruktury.

V tomto rozvaděči budou instalovány:

- o odpovídající počet 1U panelů pro zakončení na optických a metalických kazetách.

7.3.3.3 Rozšiřitelnost

Patch panely musí obsahovat volné pozice pro budoucí rozšíření datové infrastruktury.

7.3.4 Monitoring a řídicí systémy

Pro potřeby sledování a řízení funkcionality podpůrné infrastruktury mobilního datového centra musí být Zhotovitelem dodán a instalován monitorovací a řídicí systém, který bude sledovat parametry a události v reálném čase. Monitorovací a řídicí systém musí shromažďovat, analyzovat, zpracovávat, integrovat, vyhodnocovat trendy ve všech kritických parametrech Non-IT infrastruktury a pomáhat tak udržet nejvyšší možnou dostupnost datového centra.

Systém monitoringu bude sloužit pro monitorování kompletní infrastruktury mobilního datového centra a bude koncipován jako autonomní ucelený.

7.3.4.1 Rozsah monitoringu

Monitorovací systém musí zajišťovat dohled nad všemi Non-IT technologiemi a prostředím vybraných prostor. Sběr dat z jednotlivých technologií bude realizován prostřednictvím komunikačních protokolů přímo monitorovacím systémem. Veškeré informace z technologií, senzorů a chladicích jednotek budou načítány pomocí PLC jednotky, která bude umístěna v samostatném rozvaděči. PLC musí obsahovat algoritmy pro vyhodnocování alarmových stavů, trvalé ukládání logů událostí a uchovávání trendových dat na lokálním úložišti (např. SD karta) v případě nedostupnosti centrální části systému. Návrh kabelových tras včetně použitých kabelů bude v kompetenci zhotovitele, který musí zajistit plnou kompatibilitu s dodávaným systémem a garantovat požadovanou funkcionality.

Monitorovací systém musí zajišťovat sběr a sledování následujících parametrů:

- o **Komunikace s technologiemi:** Sběr dat ze všech monitorovaných zařízení a technologických celků musí být realizován prostřednictvím komunikačních rozhraní integrovaných v jednotlivých technologiích nebo jejich nadřazených řídicích systémech
- o **Napájecí systém:** Monitoring musí zahrnovat dohled nad zdroji UPS, řídicím systémem energetiky, polohou všech jisticích a spínacích prvků, měřením odběru a spotřeby elektrické energie na vstupu do datového centra i pro napájení IT technologií. Dále musí být sledovány elektrické veličiny (napětí, proud, výkon, účinník) samostatně pro každý rozvaděč
- o **Chladicí systém:** Systém musí umožňovat datovou komunikaci se všemi chladicími jednotkami a jejich nadřazeným řídicím systémem



- **Fyzická bezpečnost:** Monitoring musí zahrnovat systémy SHZ (stabilní hasicí zařízení), PZTS (elektronický zabezpečovací systém) a EKV (elektronická kontrola vstupu)
- **Prostředí datové a energetické části:** Sledování teploty a relativní vlhkosti musí být zajištěno jak ve studené, tak v teplé zóně datové části, stejně jako v energetické části
- **Detekce úniku kapalin:** Systém musí monitorovat případné úniky kapalin ve všech relevantních místnostech

Monitorovací systém musí umožňovat archivaci událostí a trendových hodnot všech sledovaných parametrů tak, aby byly efektivně dostupné pro další uživatele nebo systémy (např. pro integraci do nadřazených systémů nebo pro reporting v rámci SLA). Systém musí rovněž podporovat evidenci externích informací vzniklých mimo vlastní monitorovací infrastrukturu, jako jsou:

- Reakce obsluhy na incidenty,
- Konfigurace prahových hodnot pro alarmový systém,
- Parametry automaticky prováděných eskalačních procesů,
- Související evidenční databáze.

— Součástí databáze musí být také správa přístupových oprávnění jednotlivých uživatelů systému.

Monitorovací systém musí splňovat následující funkční požadavky:

- **Centrální zpracování dat:** Veškeré informace musí být zpracovávány v centrální serverové části systému. Ta musí zajišťovat vyhodnocování dat v reálném čase, jejich archivaci po dobu minimálně 18 měsíců a eskalaci vzniklých událostí dle definovaného schématu.
- **Vizualizace provozních ukazatelů:** Systém musí umožňovat vizualizaci klíčových provozních hodnot, jako je ukazatel PUE (Power Usage Effectiveness), aktuální doba autonomie baterií UPS a další relevantní parametry.
- **Zobrazení pro různé typy uživatelů:** Rozhraní musí být optimalizováno pro zobrazení na monitorech s rozlišením FullHD pro operátory, a zároveň musí být dostupné pro vzdálené uživatele prostřednictvím standardního webového rozhraní nebo mobilní aplikace.
- **Definice odvozených alarmů:** Systém musí umožňovat uživatelskou konfiguraci odvozených alarmů na základě primárních alarmových stavů, jejich limitních hodnot a provozních podmínek.
- **Eskalace alertů:** Musí být zajištěna spolehlivá eskalace výstrah prostřednictvím SMS zpráv, a to bez závislosti na externí infrastruktuře – pomocí GSM modemu integrovaného přímo do jádra systému
- **Integrace s nadřazeným systémem:** Systém musí být schopen předávat data prostřednictvím API do nadřazeného monitorovacího systému Objednatele, založeného na platformě ZABBIX. A zároveň musí poskytnout možnost napojení na systém dálkové diagnostiky (DDTS) provozovaného Objednatelem.

- **Lokální server:** Lokální dohledový server musí být fyzicky umístěn v mobilním datovém centru.
- **Webový přístup:** Po zprovoznění komunikační trasy a konfiguraci musí být výstupy z monitorovacího systému okamžitě dostupné prostřednictvím zabezpečeného webového rozhraní (HTTPS) z libovolného PC vybaveného webovým prohlížečem

7.3.4.2 Požadavky na uživatelské rozhraní systému

Monitorovací systém musí být vybaven webovým rozhraním určeným pro práci operátorů a dalších oprávněných uživatelů. Rozhraní musí být dostupné z libovolného počítače s připojením k serveru monitorovacího systému. Navigace mezi jednotlivými schémata a detaily technologií musí být intuitivní, s využitím hypertextových odkazů pro přechod mezi zobrazeními.

Jako příklad možného řešení vizualizace monitorovaného prostředí datového centra a aktuálního stavu prostředí datového centra může posloužit níže uvedený koncepční návrh (kap. 15.3 - Ideologické schéma vizualizace monitorovaného prostředí serverovny), který má sloužit jako podklad pro další technický návrh a neslouží jako závazný technický návrh.

Rozhraní musí dále poskytovat následující funkce:

- **Grafické zobrazení průběhu teploty a vlhkosti** na jednotlivých senzorech, včetně vyznačení časových intervalů, kdy byly překročeny nastavené mezní hodnoty. Uživatelé s příslušným oprávněním musí mít možnost tyto meze upravovat.
- Grafické zobrazení průběhu sledovaných elektrických veličin, jako jsou napětí, proud, výkon apod.
- **Seznam událostí** s rozlišením jejich závažnosti a aktuálního stavu, včetně detailního zobrazení jednotlivých událostí a souvisejících systémových i uživatelských aktivit.
- **Monitoring polohy vývodových jističů**, včetně možnosti uživatelského popisu jednotlivých vývodů.

Bez ohledu na aktuálně zobrazený detail musí být vždy dostupný seznam aktivních poplachů, který bude obsahovat čas vzniku a ukončení poplachu, čas potvrzení obsluhou, počet opakování a popis události. Seznam musí umožňovat přímý přechod na zobrazení technologie, která poplach vyvolala, na detail události a (v případě odpovídajícího oprávnění) potvrzení jednotlivých nebo všech nevyřešených poplachů.

Systém nesmí omezovat počet vytvořených uživatelských účtů ani počet současně připojených uživatelů z hlediska licencování.

Uživatelské rozhraní musí podporovat vícejazyčné zobrazení, minimálně v českém a anglickém jazyce, s možností nastavení preferovaného jazyka individuálně pro každého přihlášeného uživatele.

Systém musí umožnit jednotlivým uživatelům nastavení nebo deaktivaci akustické signalizace aktivních událostí, s výjimkou uživatelů s rolí operátora, u nichž musí být signalizace trvale aktivní.



Správa uživatelských účtů a přidělování oprávnění bude plně v kompetenci Objednatele. Systém musí umožňovat definici a správu minimálně následujících uživatelských rolí:

- **Běžný uživatel:** Přístup k systému a zobrazení všech nebo vybraných informací dle přiděleného kontextu. Možnost přístupu k logům událostí a reportům. Umožnění zápisu komentářů k událostem a na evidenční karty jednotlivých technologií.
- **Operátor:** Oprávnění pro práci s alarmy a evidencí technologií v rámci odpovědnosti za provoz a reakci na vzniklé události.
- **Správce provozu:** Oprávnění ke konfiguraci provozních parametrů, včetně nastavení limitních hodnot pro vyhledávání událostí, definice alarmů druhé úrovně na základě primárních alarmů nebo kombinace provozních podmínek, a blokování alarmů pro odstavené technologie.
- **Správce systému:** Oprávnění pro globální správu uživatelů, konfiguraci systémových parametrů, zálohování dat, provádění off-line operací a další systémové činnosti.

8 Dodávka mobilního datového centra do místa instalace (Fáze 3)

Dodávka mobilního datového centra zahrnuje proces jeho bezpečné přepravy na místo určení a kontrolu neporušenosti po transportu. Tato fáze navazuje na výrobu MDC. Zhotovitel je v rámci této fáze povinen MDC dopravit do místa instalace a umístit jej v souladu s odsouhlasenými stavebními úpravami. Objednatel v rámci této fáze ověří, že MDC dorazilo bez mechanického poškození a co do stavební připravenosti v rozsahu odpovídajícím projektové dokumentaci (či jejím odsouhlaseným úpravám). Součástí této etapy je také zpracování protokolu o dodání a předložení kompletní fotodokumentace prokazující stav MDC při převzetí.

Oblast	Činnost
Dodávka	<ul style="list-style-type: none">• Dodávka MDC bude provedena v termínu po dohodě s Objednatelem do stanovené lokality (Zhotovitel je povinen oznámit Objednateli alespoň 14 dní předem, kdy bude MDC dodávat).• Ekologická likvidace obalových materiálů.
Kontrola	Po dodání MDC na místo určení bude: <ul style="list-style-type: none">• Ihned provedena přijímací kontrola stavu MDC (včetně fotodokumentace) v přítomnosti zástupce SŽT a dokumentace případných závad (zjevných).• Kontrola nepoškozenosti během transportu.• Kontrola, že kontejner byl usazen dle stavební části projektové dokumentace.• Ověření stability, roviny, kotvení a mechanického stavu.

	<ul style="list-style-type: none"> • Zkontrolována těsnost, stav rámu, zavírání dveří
Fotodokumentace	<ul style="list-style-type: none"> • Fotodokumentace vnějšku i vnitřku bude minimálně v HD kvalitě (rozlišení 1920x1080 pix) v bezztrátovém formátu PNG, nebo TIFF.

Výstupem výše uvedených požadavků bude samostatný dokument s názvem „Protokol o předání“, který zpracovává Zhotovitel.

9 Zprovoznění mobilního datového centra (Fáze 4)

Zprovoznění mobilního datového centra zahrnuje uvedení všech technologických, bezpečnostních a infrastrukturních systémů do plného provozu tak, aby bylo MDC uvedeno do provozu (tj. okamžitému a spolehlivému fungování v místě instalace).

Oblast	Činnost
Oživení systémů	<ul style="list-style-type: none"> • Připojení k elektrickému napájení • Kontrola rozfázování a jističů, • Aktivace UPS • Provedeno zemnění, pospojení, hromosvod • Kontrola správné instalace venkovních a vnitřních jednotek chlazení • Zprovoznění bezpečnostních technologií • Připojení na datové rozvody • Zprovoznění monitoringu a řídicích systémů
SAT - Site Acceptance Test	<p>Po dodání mobilního datového centra do místa instalace, proběhnou SAT testy, které ověří funkčnost zařízení při maximálním jmenovitém výkonu IT infrastruktury. Test bude proveden po dobu 48 hodin za použití simulované odporové zátěže a za účasti zástupce Objednatele.</p> <p>Testy proběhnou minimálně v těchto oblastech:</p> <ul style="list-style-type: none"> • test funkčnosti napájení (Start-up test) • test funkčnosti chlazení (Start-up test) • test výpadku napájení, přepnutí na UPS, alarmy • test škálování a výpadku chlazení • test bezpečnostních systémů EPS (požární detektory, sekvence pre-alarm / alarm, blokace, aktivace hašení) • test přístupových systémů PZTS • test funkčnosti dalších senzorů (teplota, vlhkost, únik vody, CO₂,...) • test simulované plné zátěže IT hardwarem • měření hodnot napětí a proudu za běhu MDC • monitoring a regulace systémů elektro a vzduchotechniky



Revize	<ul style="list-style-type: none">• provedení elektro revize, dle zákona č. 250/2021 Sb.• provedení revize požárně bezpečnostních zařízení (PBZ) dle vyhlášky č. 246/2001 Sb.
--------	--

Výstupem výše uvedených požadavků bude dokumentace obsahující minimálně:

- Protokol o úspěšném provedení SAT testů
- Protokoly o provedených revizích dle zákona č. 250/2021 Sb. a dle vyhlášky č. 246/2001 Sb.

10 Dokumentace (Fáze 5)

Objednatel požaduje, aby Zhotovitel po dokončení instalace a uvedení mobilního datového centra do provozu předal kompletní dokumentaci skutečného provedení díla. Dokumentace musí být předána v **elektronické podobě** (ve formátu PDF a editovatelném formátu, např. .DWG, .VSDX, .DOCX, .XLSX). Tato dokumentace musí obsahovat zejména:

Oblast	Výstupy Zhotovitele
Dokumentace	<ul style="list-style-type: none">• Popis konstrukce kontejneru a konstrukční plány.• Zapojovací schémata všech technologií (napájení, chlazení, bezpečnostní technologie, ICT technologie a další)• Konfigurační dokumentace napájení (primární, záložní)• Konfigurační dokumentace chlazení (topologie chlazení, typ chlazení, aj.)• Konfigurační dokumentace bezpečnostní technologií (EPS, SHS, PZTS, CCTV, aj.)• Konfigurace DCIM (Data center infrastructure management)• Tabulkový seznam instalovaných komponent, jejich technických parametrů, včetně výrobních čísel• Revizní zprávy a protokoly o funkčních zkouškách• Provozní, technické a údržbové manuály všech technologií• Záznamy o konfiguraci systémů (např. UPS, monitoring, SHZ)• Požární dokumentace• Kontaktní matice na podporu všech technologií• Fotodokumentace• A další relevantní dokumenty dle charakteru dodávky

11 Školení (Fáze 6)

Školení zaměstnanců určených k obsluze MDC je klíčovým prvkem bezpečného a spolehlivého provozu tohoto technologického celku. Mobilní datové centrum obsahuje komplexní systémy – elektrické, chladicí, požární, bezpečnostní i IT infrastrukturu – a jejich správná obsluha vyžaduje odborné znalosti, praktické dovednosti a povědomí o rizicích spojených s provozem.

Oblast	Činnost
Školení	<ul style="list-style-type: none">• Zhotovitel zajistí pro vybrané zástupce Objednatele školení pro následující technologie, které budou součástí MDC a jejich obsluhu:<ul style="list-style-type: none">○ Technologie mobilního datového centra○ Bezpečnost práce (BOZP) a provozní rizika○ Přístupové a bezpečnostní systémy○ Požární ochrana a hašení○ Elektrická infrastruktura○ Chlazení○ Monitoring a dohled○ Provozní postupy a denní rutiny○ Postupy při havárii a krizové situaci○ Provozní dokumentace a její používání• Školení bude realizováno v rozsahu až 2 MD, Objednatel je oprávněn jej rozdělit do více dílčích školení pro více skupin.• Školení bude realizováno prezenční formou v místě dodávky kontejneru s praktickou ukázkou funkčních vlastností MDC a zodpovězením dotazů kladených zástupci Objednatele.• Objednatel je oprávněn 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 či jiným osvědčením.

Výstupem Zhotovitele bude samostatný dokument s názvem "Zpráva o školení zaměstnanců Správy železnic", obsahující výčet probraných a diskutovaných témat, jejíž přílohou bude rovněž prezenční listina.

12 Profylaktické kontroly a revize (Fáze 7)

Zhotovitel je povinen zajistit pravidelnou provozní kontrolu a revize podpůrných systémů mobilního datového centra v souladu s technickými specifikacemi výrobce. Kontrola bude prováděna kvalifikovaným servisním nebo revizním technikem podle specifikace a požadavků v podkapitolách níže. Cílem kontroly a revize je ověření provozuschopnosti systému, jeho souladu s definovanými technickými parametry, specifikacemi výrobce, s platnými právními předpisy a technickými normami.

Zhotovitel je povinen zajistit pravidelnou profylaktickou kontrolu a revize podpůrných systémů mobilního datového centra **po dobu 10 let** od skončení fáze 4 dle Harmonogramu.

Výstupem každé dílčí profylaktické kontroly bude **protokol o provedení profylaxe**. Protokol musí obsahovat seznam všech provedených činností, které jsou specifikovány v jednotlivých oblastech této kapitoly, dále naměřené hodnoty, zjištěné závady, fotodokumentaci (pokud je předepsána) a prohlášení příslušného technika o provedení profylaxe.

Zhotovitel je povinen provést profylaktickou kontrolu každého z dále v této kapitole uvedených technologických celků vždy 1x v daném kalendářním roce (ideálně v intervalu maximálně 12 měsíců). **Profylaxe ve smyslu této kapitoly nebude prováděna v kalendářním roce, v němž došlo ke zprovoznění mobilního datového centra (dokončení fáze 4).**

Zhotovitel je povinen informovat Objednatele o plánovaném termínu profylaktických kontrol minimálně 14 dní předem, a to písemnou formou.

Pro usnadnění plánování profylaktické činnosti Objednatel doporučuje, aby Zhotovitel prováděl jednotlivé profylaktické kontroly v souladu s níže uvedeným rozpisem úkonů. Datum realizace těchto úkonů může Zhotovitel stanovit dle svých možností, s přihlédnutím k minimálnímu intervalu provádění profylaktických kontrol.

Servisní úkon	Doporučené profylaktické kontroly
1.úkon	<ul style="list-style-type: none">• Profylaktická kontrola kontejneru MDC
2.úkon	Pro první větev: <ul style="list-style-type: none">• Profylaktické kontroly a revize monitorovacího systému• Profylaktické kontroly a revize elektrozařízení• Profylaktické kontroly a revize zdroje nepřetržitého napájení (UPS)
3.úkon	Pro druhou větev: <ul style="list-style-type: none">• Profylaktické kontroly a revize monitorovacího systému• Profylaktické kontroly a revize elektrozařízení• Profylaktické kontroly a revize zdroje nepřetržitého napájení (UPS)
4.úkon	<ul style="list-style-type: none">• Profylaktické kontroly a revize jednotek chlazení
5.úkon	<ul style="list-style-type: none">• Profylaktické kontroly a revize stabilního hasícího zařízení (SHZ)
6.úkon	<ul style="list-style-type: none">• Profylaktické kontroly a revize nouzového osvětlení
7.úkon	<ul style="list-style-type: none">• Profylaktické kontroly a revize bleskosvodné a uzemňovací soustavy

Cena za provedení profylaktických kontrol bude Zhotoviteli uhrazena vždy na základě řádného provedení všech profylaktických kontrol za daný kalendářní rok.

12.1 Profylaktická kontrola kontejneru MDC

Zhotovitel je povinen zajistit pravidelnou provozní kontrolu kontejneru MDC v souladu s technickými specifikacemi výrobce. Kontrola bude prováděna **1x ročně** kvalifikovaným servisním technikem. Cílem kontroly je ověření provozuschopnosti systému a jeho souladu s definovanými technickými parametry a podmínkami prostředí.

Vnější a vnitřní plášť:

- Kontrola koroze, deformací, prasklin nebo mechanického poškození
- Stav nátěru a antikorozi ochrany
- Kontrola, zda není porušená struktura dveří, pantů a zámků
- Kontrola těsnění dveří a kabelových průchodek (stárnutí, popraskání)
- Kontrola zatékání a kondenzace vlhkosti

Střecha:

- Kontrola poškození, uvolněných částí
- Kontrola hromadění vody
- Stav odvodnění a okapových systémů
- Kontrola UV degradace střešní vrstvy
- Očištění od listí a jiných nečistot

Okolní prostředí:

- Kontrola na přítomnost nežádoucí vegetace (dotyk větví stromů, zarůstání kontejneru vegetací) a případné odstranění
- Kontrola odtoků a drenáže kolem kontejneru
- Kontrola neporušenosti a funkčnosti přístupové cesty
- Kontrola, zda nedochází k pohybu MDC, sesedání podloží, nebo vyplavování okolí dešťovou vodou

12.2 Profylaktické kontroly a revize zdroje nepřetržitého napájení (UPS)

Zhotovitel je povinen zajistit pravidelnou provozní kontrolu a revizi UPS systému v souladu s technickými specifikacemi výrobce. Kontrola bude prováděna **1x ročně** kvalifikovaným servisním technikem. Cílem kontroly je ověření provozuschopnosti systému, jeho souladu s definovanými technickými parametry a podmínkami prostředí.

Rozsah provozní kontrola UPS:

- Ověření souladu provozního prostředí UPS s definovanými podmínkami
- Kontrola funkčnosti ventilátorů a proudění vzduchu
- Analýza registru událostí UPS na výskyt alarmových stavů
- Kontrola výkonových svorek UPS pod zátěží

- Kontrola zbývajících svorek, které nebyly zahrnuty v předchozím kroku
- Bodové měření teploty svorek interních a/nebo externích baterií
- Termovizní měření teploty výkonových svorek a komponent UPS
- Porovnání skutečných hodnot napětí a proudu s údaji na displeji (je-li k dispozici)
- Provedení testu vybíjení
- Ověření funkce přepnutí na bateriový provoz
- Test funkčnosti interního statického bypassu
- Vyčištění UPS od prachu a nečistot
- Kontrola kondenzátorových bank (je-li součástí systému)
- Vizuální a funkční kontrola vnitřních řídicích a výkonových vodičů
- Kontrola dotažení výkonových přípojek a jiných šroubových spojů uvnitř UPS
- Vizuální kontrola externích bateriových systémů (je-li tak zařízení vybaveno)
- Ověření aktuální verze firmware a případná aktualizace
- Měření izolačního odporu v rámci pravidelné elektro revize

Rozsah provozní kontroly bateriového systému:

- Vizuální kontrola zapojení baterií
- Test impedance/vodivosti baterií a vybíjení
- Kontrola a měření kapacity baterií
- Měření teploty svorek baterií, zvlnění AC napětí a proudu
- Dotažení svorek dle specifikace výrobce
- Kontrola výskytu koroze nebo úniku elektrolytu, včetně vyčištění systému
- Poskytnutí doporučení k výměně baterií, pokud jsou mimo toleranční hodnoty
- Analýza kapacity a dostatečnosti napájení z UPS a případné návrhy úprav

12.3 Profylaktické kontroly a revize elektrozařízení

Zhotovitel je povinen zajistit pravidelné revize všech elektrozařízení instalovaných v prostoru serverovny. Součástí této povinnosti je vedení kompletní dokumentační agendy revizních úkonů pro každé jednotlivé zařízení. Revize musí být prováděny v souladu s platnými právními předpisy, technickými normami a specifikacemi výrobce. Kontrola bude prováděna **1x ročně** kvalifikovaným revizním/servisním technikem.

12.3.1 Provozní kontrola jednotek PDU (Power Distribution Unit)

Servisní technik provede vizuální a elektronickou kontrolu jednotek PDU za účelem ověření jejich provozuschopnosti a souladu s technickými specifikacemi a podmínkami prostředí.

Rozsah provozní kontroly PDU:

- Ověření souladu provozního prostředí s definovanými podmínkami
- Kontrola registru událostí PDU na výskyt alarmových stavů
- Kontrola výkonových svorek pod zátěží (je-li k dispozici)
- Kontrola zbývajících svorek, které nebyly zahrnuty v předchozím kroku
- Termovizní měření teploty svorek, konektorů (včetně pořízení snímku)
- Porovnání skutečných hodnot napětí a proudu s údaji na displeji (je-li k dispozici)

- Vyčištění jednotky od prachu a nečistot
- Vizuelní kontrola vnitřních vodičů (řídících i výkonových, pokud to technicky lze)
- Kontrola dotažení výkonových přípojek (je-li k dispozici)
- Ověření verze firmware a případná aktualizace
- Měření izolačního odporu v rámci elektro revize
- Zápis zjištěných stavů do revizní dokumentace

12.3.2 Provozní kontrola rozvaděčů

Servisní technik provede vizuelní a funkční kontrolu rozvaděčů za účelem ověření jejich provozuschopnosti a souladu s technickými specifikacemi.

Rozsah provozní kontroly rozvaděčů:

- Ověření souladu provozního prostředí s definovanými podmínkami
- Kontrola registru událostí řídicího systému
- Kontrola výkonových svorek pod zátěží
- Kontrola zbývajících svorek, které nebyly zahrnuty v předchozím kroku
- Termovizní měření teploty svorek (včetně pořízení snímku)
- Porovnání skutečných hodnot napětí a proudu s údaji na displeji (je-li k dispozici)
- Vyčištění rozvaděče od prachu a nečistot
- Vizuelní kontrola vnitřních vodičů
- Kontrola dotažení výkonových přípojek
- Ověření verze firmware a případná aktualizace
- Měření izolačního odporu v rámci elektro revize
- Zápis zjištěných stavů do revizní dokumentace
- Analýza kapacity a dostatečnosti napájení a případné návrhy úprav

12.3.3 Provozní kontrola ATS

Servisní technik provede vizuelní a funkční kontrolu ATS rozváděče.

Rozsah provozní kontroly ATS:

- Ověření souladu provozního prostředí s definovanými podmínkami
- Kontrola registru událostí řídicího systému ATS
- Kontrola výkonových svorek pod zátěží
- Kontrola zbývajících svorek, které nebyly zahrnuty v předchozím kroku
- Termovizní měření teploty svorek (včetně pořízení snímku)
- Porovnání skutečných hodnot napětí a proudu s údaji na displeji (je-li k dispozici)
- Vyčištění jednotky od prachu a nečistot
- Vizuelní kontrola vnitřních vodičů
- Kontrola dotažení výkonových přípojek
- Ověření verze firmware a případná aktualizace
- Měření izolačního odporu v rámci elektro revize
- Zápis zjištěných stavů do revizní dokumentace

12.4 Profylaktické kontroly a revize jednotek chlazení

Zhotovitel je povinen zajistit pravidelnou vizuální a funkční kontrolu klimatizačního systému, a to včetně vnitřních i venkovních jednotek. Cílem kontroly je ověření provozuschopnosti systému, jeho souladu s technickými specifikacemi výrobce a podmínkami prostředí. Kontrola musí být prováděna **1x ročně** kvalifikovaným servisním technikem.

Rozsah provozní kontroly vnitřních klimatizačních jednotek:

- Ověření souladu provozního prostředí (prach, vlhkost, vibrace) s definovanými podmínkami
- Vizuální kontrola zařízení (poškození, opotřebení, nestandardní úpravy)
- Změření teplotní mapy termokamerou, detekce hotspotů
- Kontrola správného proudění vzduchu, (studená -> teplá ulička)
- Kontrola výkonových svorek pod zátěží (včetně krytů a úchytů)
- Kontrola chodu ventilátorů (hlučnost, doběh, rozběh)
- Kontrola otáček ventilátorů
- Kontrola mechanických částí motoru a dotažení spojů
- Kontrola čistoty lamel výměníku a průchodnosti vzduchu
- Kontrola odvodu kondenzátu a těsnosti chladicího okruhu
- Kontrola úkapů a čistoty okolí jednotky
- Kontrola odvodu kondenzátu (je-li zařízení vybaveno)
- Kontrola, vyčištění a výměna vzduchového filtru
- Kontrola funkce termostatu (nastavení a odezva systému)
- Kontrola funkce termického pohonu (je-li součástí)
- Kontrola stavové signalizace (logy, chybové hlášení, servisní intervaly)
- Kontrola registru událostí řídicího systému (je-li zařízení vybaveno)
- Měření teploty svorek pomocí termokamery nebo bezdotykového teploměru
- Porovnání skutečných hodnot napětí a proudu s údaji na displeji (je-li k dispozici)
- Vyčištění pomocných rozváděčů klimatizace (je-li součástí)
- Ověření verze firmware a případná aktualizace (je-li zařízení vybaveno)
- Analýza kapacity a dostatečnosti chlazení a případné návrhy úprav.

Rozsah provozní kontroly venkovních klimatizačních jednotek:

- Ověření souladu provozního prostředí (prach, vlhkost, vibrace) s definovanými podmínkami
- Vizuální kontrola zařízení (poškození, opotřebení, nestandardní úpravy)
- Kontrola výkonových svorek pod zátěží (včetně krytů a úchytů)
- Kontrola chodu ventilátorů (hlučnost, doběh, rozběh)
- Kontrola otáček ventilátorů
- Mytí výměníku tlakovou vodou
- Kontrola mechanických částí motoru a dotažení spojů
- Kontrola čistoty lamel výměníku a průchodnosti vzduchu
- Kontrola odvodu kondenzátu a těsnosti chladicího okruhu
- Kontrola úkapů a čistoty okolí jednotky
- Kontrola odvodu kondenzátu (je-li zařízení vybaveno)

- Kontrola kompresorové jednotky a jejího opotřebení

12.5 Profylaktické kontroly a revize monitorovacího systému

Zhotovitel je povinen zajistit pravidelnou vizuální a funkční kontrolu systému monitoringu prostředí, včetně hardwarových i softwarových komponent. Cílem kontroly je ověření provozuschopnosti systému, jeho souladu s technickými specifikacemi výrobce a podmínkami prostředí. Kontrola musí být **1x ročně** prováděna kvalifikovaným servisním technikem.

Rozsah provozní kontroly hardwarových komponent systému monitoringu:

- Kontrola funkčnosti čidel (teplotních, vlhkostních, záplavových)
- Ověření komunikace všech jednotek
- Kontrola komunikačních propojení
- Ověření aktuálnosti firmware komunikačních zařízení a případná aktualizace
- Kontrola funkčnosti kamerového systému monitoringu prostředí
- Kontrola spojů a všech signalizačních kontaktů
- Kontrola měření, komunikace a zatížení systému
- Úprava uživatelského nastavení systému monitoringu

— Rozsah provozní kontroly softwarových komponent systému monitoringu:

- Ověření komunikace všech jednotek – dostupnost a funkčnost monitorovaných zařízení
- Kontrola správnosti údajů ze senzorů (teplota, vlhkost, záplavy)
- Kontrola správného označení a nastavení provozních parametrů
- Kontrola uložených dat a jejich interpretace
- Záloha nastavení a uložených dat
- Kontrola správného nastavení data a času
- Ověření aktuálnosti softwarové verze a případná aktualizace
- Kontrola funkčnosti kamerového systému monitoringu prostředí
- Ověření aktivace a hlášení alarmových stavů
- Kontrola spojů a všech signalizačních kontaktů
- Ověření aktuálnosti firmware monitorovaných zařízení a případná aktualizace

12.6 Profylaktické kontroly a revize stabilního hasícího zařízení (SHZ)

Zhotovitel je povinen zajistit pravidelnou vizuální a funkční kontrolu plynového automatického hasícího systému (SHZ), včetně všech souvisejících komponent. Cílem kontroly je ověření provozuschopnosti systému, jeho souladu s technickými specifikacemi výrobce, projektovou dokumentací a podmínkami prostředí. Kontrola musí být prováděna **(1x ročně)** kvalifikovaným servisním technikem.

Rozsah provozní kontroly tlakové nádoby:



- Vizuální kontrola stavu systému
- Ověření umístění dle projektové dokumentace
- Kontrola výrobního čísla
- Kontrola uchycení systému, případná oprava
- Ověření přístupnosti systému, případná úprava
- Očištění systému od nečistot

Rozsah provozní kontroly manometru:

- Optická kontrola tlaku
- Kontrola aretace manometru
- V případě nízkého tlaku – dotlakování pomocí certifikovaného zařízení
- Kontrola plomby, případná výměna

Rozsah provozní kontroly tlakového spínače:

- Ověření přenosu signálu na rozhraní řídicí jednotky
- Funkční test pomocí kalibrovaného měřidla
- Kontrola plomby, případná výměna

Rozsah provozní kontroly záložního zdroje SHZ:

- Test funkce záložního akumulátoru – provoz na zálohu po dobu 1 hodiny,
- Kontrola spojů napájecího zdroje
- Měření napětí na konci napájecí větve
- Měření izolačního odporu dle elektro revize

Rozsah provozní kontroly nadřazeného systému EPS:

- Test aktivace hašení z centrály EPS
- Kontrola výstupních signálů (tlak, porucha)
- Test přenosu stavů na vyšší dozorová centra

Rozsah provozní kontroly detekce a ručního startu hašení:

- Test poruchy hlásicí linky vyjmutím hlásiče
- Test funkce hlásičů pomocí testovací sady
- Kontrola ručního hlásiče testovacím klíčem
- Měření impedance hlásicích linek

Rozsah provozní kontroly hlásičů tlaku v zásobnících hasiva:

- Vizuální kontrola tlakových spínačů
- Simulace stavu ztráty tlaku
- Měření impedance hlásicí linky

Rozsah provozní kontroly výstupních zařízení:

- Vizuální kontrola signalizačních prvků
- Funkční test optické a akustické signalizace
- Simulace stavu hašení
- Měření přídržné síly cívky magnetů
- Měření impedance ovládací linky
- Nasazení cívek magnetů



Rozsah provozního testu ústředny:

- Připojení k PC, test obslužným SW po dobu 1 hodiny, vyhodnocení výsledků

Rozsah provozní kontroly kontrolního štítku:

- Kontrola umístění a stavu štítku
- Nalepení štítku dle vyhlášky č. 246/2001 Sb., §7 odst. 4

Garanční zápis:

- Zápis do provozního deníku, který je Zhotovitel povinen evidovat a na žádost Objednatele jej předložit ke kontrole či nahlédnutí
- Vyhotovení protokolu o kontrole provozuschopnosti

12.7 Profylaktické kontroly a revize bleskosvodné a uzemňovací soustavy

Zhotovitel je povinen zajistit pravidelnou vizuální a funkční kontrolu bleskosvodné a uzemňovací soustavy (LPS), včetně všech souvisejících komponent. Cílem kontroly je ověření provozuschopnosti systému, jeho souladu s technickými specifikacemi výrobce, projektovou dokumentací a podmínkami prostředí. Kontrola musí být prováděna **1 x ročně** kvalifikovaným servisním technikem.

Zhotovitel je povinen zajistit pravidelné revize bleskosvodné a uzemňovací soustavy (LPS) definované pro objekty kritické infrastruktury v ČR, podle normy **ČSN EN 62305-3 ed.2** a souvisejících předpisů. Kontrola musí být prováděna kvalifikovaným revizním technikem, a to v minimálně v rozsahu:

- Kontrola jímací soustavy (tyče, lana, mříže)
- Kontrola svodů – neporušenost, uchycení, vedení
- Kontrola uzemňovací soustavy – přístupnost, značení
- Kontrola spojů – mechanické poškození, koroze
- Kontrola ekvipotenciálního pospojování
- Zkouška a měření rozpojení zkušebních svorek
- Měření zemního odporu
- Kontrola přepětových ochran – funkčnost, stav
- Vyhotovení protokolu o kontrole provozuschopnosti

12.8 Profylaktické kontroly a revize nouzového osvětlení

Zhotovitel je povinen zajistit pravidelnou vizuální a funkční kontrolu a údržbu nouzového osvětlení, včetně všech souvisejících komponent dle normy **ČSN EN 50172**. Cílem kontroly je ověření provozuschopnosti systému, jeho souladu s technickými specifikacemi výrobce, projektovou dokumentací a podmínkami prostředí.

Kontrola musí být prováděna kvalifikovaným servisním technikem nebo automatickým testovacím systémem, s výstupem do trvalého záznamového média (provozní deník).

Rozsah provozní kontroly nouzového osvětlení (**1x měsíčně**):

- Funkční test každého svítidla – simulace výpadku napájení
- Ověření, že svítidla se rozsvítí a fungují po stanovenou dobu
- Záznam výsledků do provozního deníku

Rozsah provozní kontroly nouzového osvětlení (**1x ročně**):

- Dlouhodobý test – simulace výpadku napájení na celou dobu autonomie (např. 1 hodina)
- Kontrola kapacity baterií, funkčnosti centrálního napájení
- Záznam do provozního deníku + vystavení dokladu o provedení zkoušky

13 Služby na vyžádání (Fáze 8)

Služby na vyžádání jsou jednorázové, individuálně sjednané činnosti poskytované zákazníkovi nad rámec standardních služeb provozu a údržby mobilního datového centra. Tyto služby jsou realizovány pouze na základě explicitního požadavku zákazníka a mohou zahrnovat zejména odborné konzultace, technické úpravy, modernizace, testování, konfigurace, měření, školení nebo aktualizaci dokumentace nad rámec plnění ujednaného ve Smlouvě. Služby na vyžádání mohou být sjednány maximálně v rozsahu 100 MD za celou dobu trvání Smlouvy.

Oblast	Činnost
Konzultační a poradenské služby	<ul style="list-style-type: none"> • poradenství v oblasti kybernetické, fyzické nebo provozní bezpečnosti související s provozem MDC, • konzultace související s doplněním nebo výměnou technologií, rozšířením rackové kapacity nebo přidáním nových modulů, • konzultace k možnému upgrade chladicích jednotek, UPS, PDU nebo DCIM, • konzultace k možnosti integrace dalších bezpečnostních prvků (kamery, přístupové systémy), • konzultace specifik souvisejících s přípravou MDC pro přesun na jinou lokalitu.
Konfigurační a implementační práce	<ul style="list-style-type: none"> • úpravy konfigurací DCIM/BMS a dohledových systémů, • konfigurace bezpečnostních scénářů (EPS, hašení, alarmy).
Analýzy, měření a testování	<ul style="list-style-type: none"> • provedení zátěžových nebo integračních testů mimo běžný provoz, • prověrky funkčnosti před/po modernizaci nebo před/po přemístění MDC, • provádění revizí specifikovaných v kap. 12 nad rámec ujednaných intervalů.
Školení a rozvoj personálu	<ul style="list-style-type: none"> • nadstandardní nebo rozšířené školení obsluhy,

	<ul style="list-style-type: none"> zaškolení na nové technologie po modernizaci, součinnost na provedení (řízení) cvičného scénáře havarijních stavů nebo krizového řízení za účasti zaměstnanců Objednatele. tvorba havarijního plánu.
Tvorba a aktualizace Dokumentace	<ul style="list-style-type: none"> doplnění nebo revize technické a provozní dokumentace, úpravy havarijního plánu, interních provozních řádů, tvorba / úprava schémat, výkresů nebo konfiguračních dokumentů.

14 Fáze dodávky a platební milníky

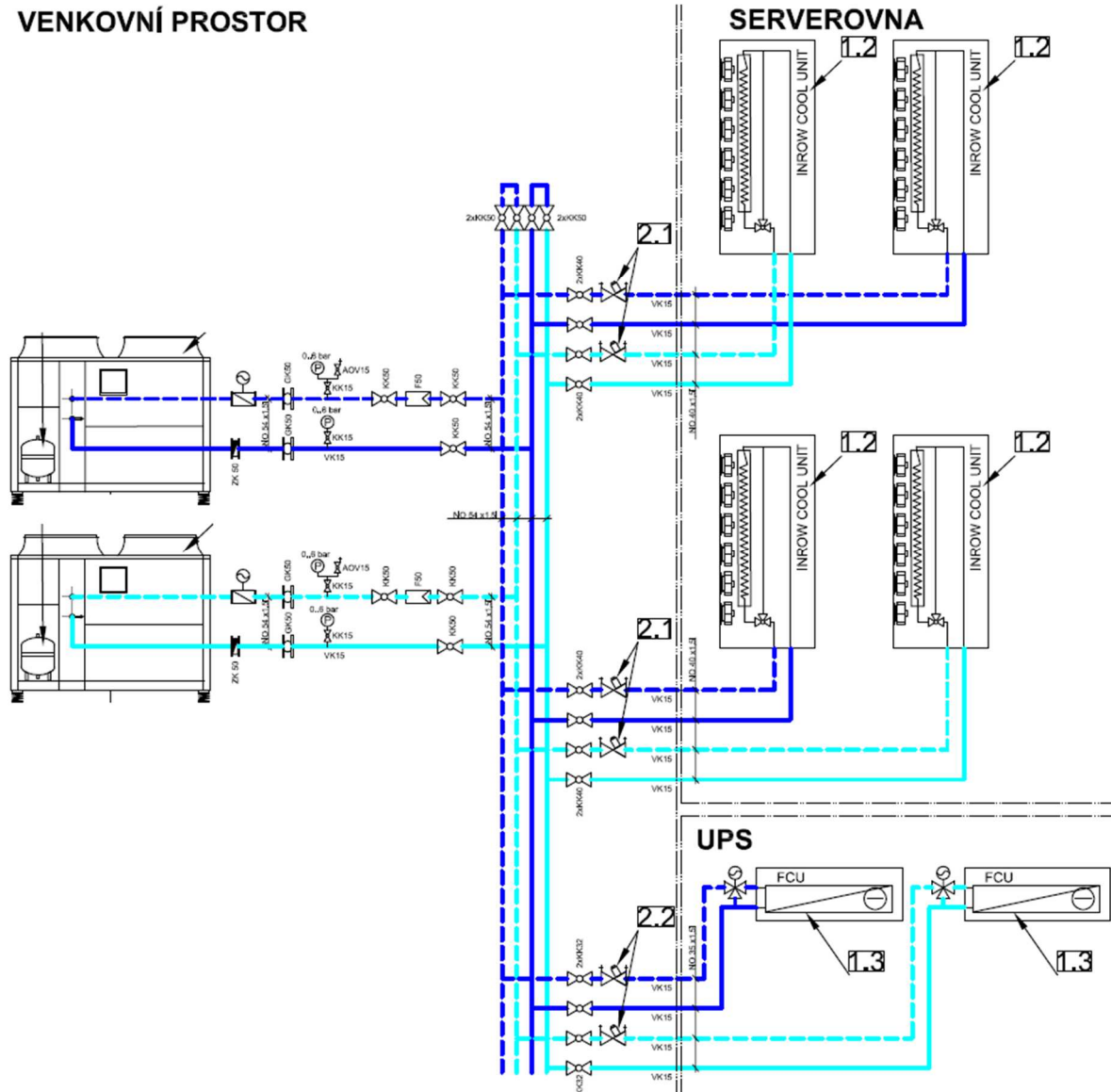
Plnění musí být prováděno v souladu s přílohou č. 8 Smlouvy (Harmonogram). Každá z níže uvedených fází (tj. každý řádek níže uvedené tabulky) je součástí jednoho z uvedených platebních milníků (A až D) a musí být Zhotovitelem provedena nejpozději v termínu uvedeném v Harmonogramu (do tohoto termínu musí být provedeno akceptační řízení ve vztahu k dané fázi). Objednatel akceptuje výstupy dané fáze, jestliže je Zhotovitel provedl v šíři a kvalitě požadované ve Smlouvě.

Platební milník	Fáze	Popis	Kapitola obsahující požadavky
A	F1	Projektová dokumentace	5, 6
B	F2	Výroba mobilního datového centra + Stavební připravenost	6, 7
B	F3	Dodávka mobilního datového centra	8
B	F4	Zprovoznění mobilního datového centra	9
C	F5	Dokumentace	10
D	F6	Školení	11
Bude hrazeno ročně na základě protokolů o provedených profylaktických kontrolách	F7	Profylaxe MDC	12
Plnění bude hrazeno na základě skutečného čerpání ze strany Objednatele.	F8	Služby na vyžádání	13

15.2 Ideologické schéma zapojení chlazení serverovny

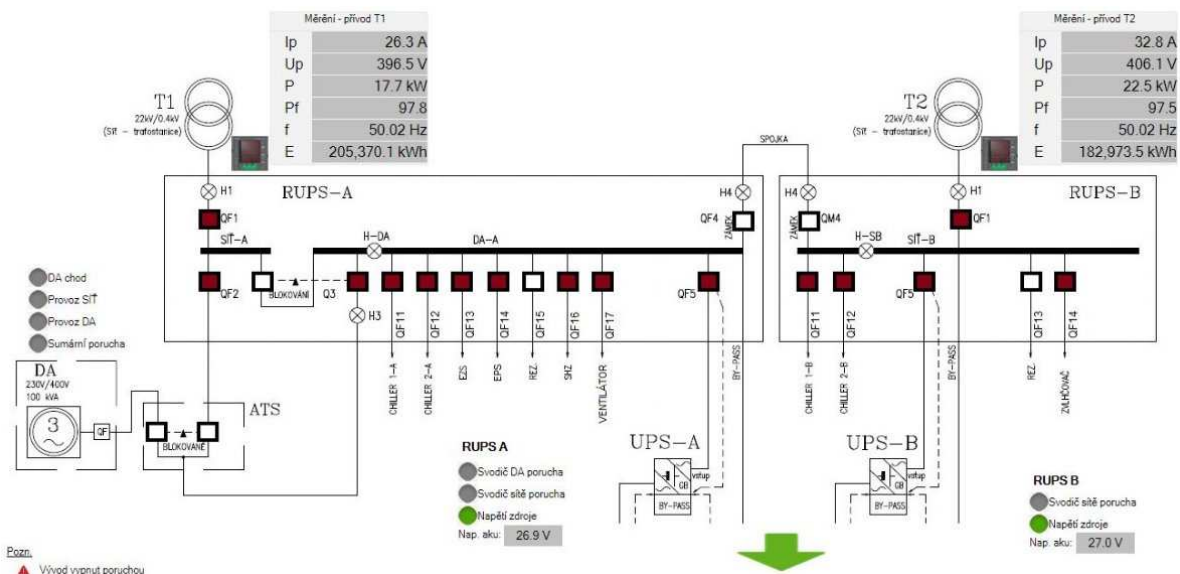
Schéma níže je koncepčním návrhem zapojení chlazení serverovny, má sloužit jako podklad pro projektovou a technickou dokumentaci a neslouží jako závazný technický návrh.

VENKOVNÍ PROSTOR



15.3 Ideologické schéma vizualizace monitorovaného prostředí serverovny

Schéma níže je koncepčním návrhem vizualizace monitorovaného prostředí datového centra, má sloužit jako podklad pro projektovou a technickou dokumentaci a neslouží jako závazný technický návrh.

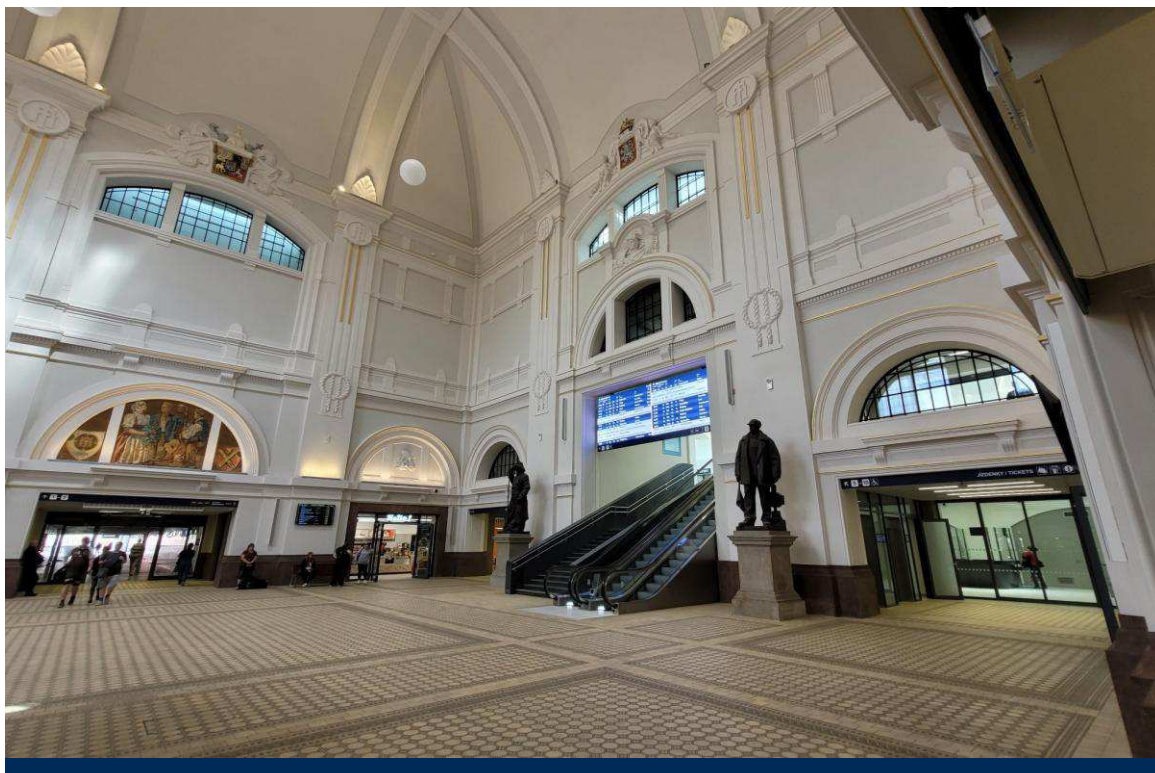


Ceník

Fáze	Část Plnění	Jednotka	Cena za jednotku (v Kč bez DPH)	Počet jednotek za dobu trvání Smlouvy	Cena za počet jednotek za dobu trvání Smlouvy (v Kč bez DPH)	Omezení ceny za platební milník	Vyjádření k zadaným hodnotám
F1	Projektová dokumentace	-		1	-	Maximální výše ceny za fázi F1 je omezena na 10 % z nabídkové ceny celkem po odečtení ceny za fáze F7 a F8.	
F2	Výroba mobilního datového centra	-		1	-		
F3	Dodávka mobilního datového centra	-		1	-		
F4	Zprovoznění mobilního datového centra	-		1	-		
F5	Dokumentace	-		1	-		
F6	Školení	-		1	-		
F7	Profylaxe MDC	rok	-	10			
z toho:							
	Profylaktická kontrola kontejneru MDC (kap. 12.1 Přílohy č. 1 Smlouvy)	kontrola/rok		10	-		
	Profylaktické kontroly a revize zdroje nepřetržitého napájení (UPS) (kap. 12.2 Přílohy č. 1 Smlouvy)	kontrola/rok		10	-		
	Profylaktické kontroly a revize elektrozařízení (kap. 12.3 Přílohy č. 1 Smlouvy)	kontrola/rok		10	-		
	Profylaktické kontroly a revize jednotek chlazení (kap. 12.4 Přílohy č. 1 Smlouvy)	kontrola/rok		10	-		
	Profylaktické kontroly a revize monitorovacího systému (kap. 12.5 Přílohy č. 1 Smlouvy)	kontrola/rok		10	-		
	Profylaktické kontroly a revize stabilního hasicího zařízení (SHZ) (kap. 12.6 Přílohy č. 1 Smlouvy)	kontrola/rok		10	-		
	Profylaktické kontroly a revize bleskosvodné a uzemňovací soustavy (kap. 12.7 Přílohy č. 1 Smlouvy)	kontrola/rok		10	-		
	Profylaktické kontroly a revize nouzového osvětlení (roční + měsíční) (kap. 12.8 Přílohy č. 1 Smlouvy)	kontrola/rok		10	-		
F8	Služby na vyžádání	MD		100	-		
Celková nabídková cena (v Kč bez DPH)						-	

Takto označená pole vyplní dodavatel

Jedná se o maximální počet jednotek, které lze na základě Smlouvy vyčerpat.



Platforma SŽ Základní dokument

Červen 2025

Obsah

1	Úvod	6
2	Platforma Správy železnic	6
3	Motivace Platformy SŽ	6
4	Architektonické principy	7
4.1	Bezpečnost a soulad s vnitropodnikovými předpisy	7
4.2	Auditní záznamy	7
4.3	Provozovatelnost řešení	8
4.4	Znovupoužitelnost řešení	8
4.5	Nezávislost na dodavatelích	9
4.6	Nákup a vývoj	9
4.7	Business kontinuita	10
5	Služby Platformy SŽ	10
5.1	Infrastrukturní služby	10
5.2	Platformní služby	10
5.3	Podpůrné služby	10
5.3.1	Bezpečnostní služby	10
5.3.2	Služby monitoringu	11
5.3.3	Služby patch managementu	11
5.3.4	Služby zálohování	11
5.3.5	Síťové služby	11
6	Technologie Platformy SŽ	12
7	Přílohy Platformy SŽ	13

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 (<i>Application Programming Interface</i>)
CEF	Datový formát pro uložení logů (<i>Common Event Format</i>)
CIFS	Síťový komunikační protokol pro přenos souborů. Kompatibilní se SMB verze 1.0 (<i>Common Internet File System</i>)
CSV	Jednoduchý textový souborový formát (Comma-separated values)
DB	Databázový software/aplikace/entita/instance, která je zpravidla provozována na databázovém serveru (<i>Database Entity</i>)
DB	Soubor datových objektů v elektronické formě uložených společně podle jednoho schématu a zpřístupňovaných počítačem (<i>Database</i>)
DB	Komponenta DBMS umožňující operace s daty v databázi. Mnohé DBMS podporují více DB enginů s různými vlastnostmi a specifiky (<i>Database Engine, Storage Engine</i>)
DBMS	Systém řízení databáze (<i>Database Management System</i>)
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 (<i>Hyper-text Transfer Protokol</i>)
HTTPS	Standardizovaný zabezpečený protokol pro přenos webových stránek (<i>Secured Hyper-text Transfer Protokol</i>)
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 (<i>Infrastructure as a Service</i>)
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 (<i>Internet Control Message Protocol</i>)
ICT	Informační a komunikační technologie (<i>Information and Communication Technology</i>)
IPMI	Standardizovaný protokol pro vzdálený dohled a management fyzických zařízení
IT	Informační technologie (<i>Information Technology</i>)
JDBC	API v jazyce Java pro jednotné rozhraní k relačním databázím (<i>Java Database Connectivity</i>)
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 (<i>JavaScript Object Notation</i>)
LEEF	Datový formát pro uložení logů (<i>Log Event Extended Format</i>)
MFA	Více-faktorové ověření identity uživatele (<i>Multi-Factor Authentication</i>)
NFS	Síťový souborový protokol primárně pro připojení vzdálených souborových systémů (<i>Network File System</i>)
OS	Operační systém (<i>Operating System</i>)
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 (<i>Platform as a Service</i>)

PAM	Řešení zabezpečení identit, které pomáhá chránit organizaci před kybernetickými hrozbami monitorováním, zjišťováním a prevencí neoprávněného privilegovaného přístupu k důležitým prostředkům (<i>Privileged Access Management</i>)
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 (<i>Proof of Concept</i>)
REST/API	Webově založené klient-server API (<i>Representational State Transfer</i>)
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 (<i>Request For Comments</i>)
S2S VPN	Šifrované VPN připojení zajišťující propojení dvou LAN (<i>Site-to-Site VPN, LAN-to-LAN VPN</i>)
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 (<i>System Center Configuration Manager</i>)
SFTP	Zabezpečený protokol pro přenos souborů. Pro zajištění šifrování využívá protokol SSH (<i>SSH File Transfer Protocol</i>)
SLA	Smluvní nastavení záruk, úrovně, dostupnosti a kvality služeb atd. (<i>Service-Level Agreement</i>)
SMB	Komunikační protokol pro přenos souborů. Lidově nazývaný Samba (<i>Server Message Block</i>)
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 (<i>Simple Network Management Protocol</i>)
SW	Programové vybavení počítače či jiného obdobného zařízení. Speciálním druhem software je <i>firmware</i> , který je úzce spjatý s konkrétním hardwarem (<i>Software</i>)
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 (<i>Virtual Private Network</i>)
WEC	Technologie předávání logů v prostředí Microsoft Windows (<i>Windows Event Collector</i>)
WEF	Technologie předávání logů v prostředí Microsoft Windows (<i>Windows Event Forwarder</i>)
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 (<i>Extended Detection and Response</i>)
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	System 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)

- o 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 regulačními 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 úložiště log management 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 vyjednávání 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. Integrovaní scénáře zajišťují, aby implementace nových funkcí v řídicí 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 služeb

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 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 jmenovanou VPN s MFA pro konkrétního externistu.
VPN S2S	Služba virtuální privátní sítě Site-to-Site.

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:

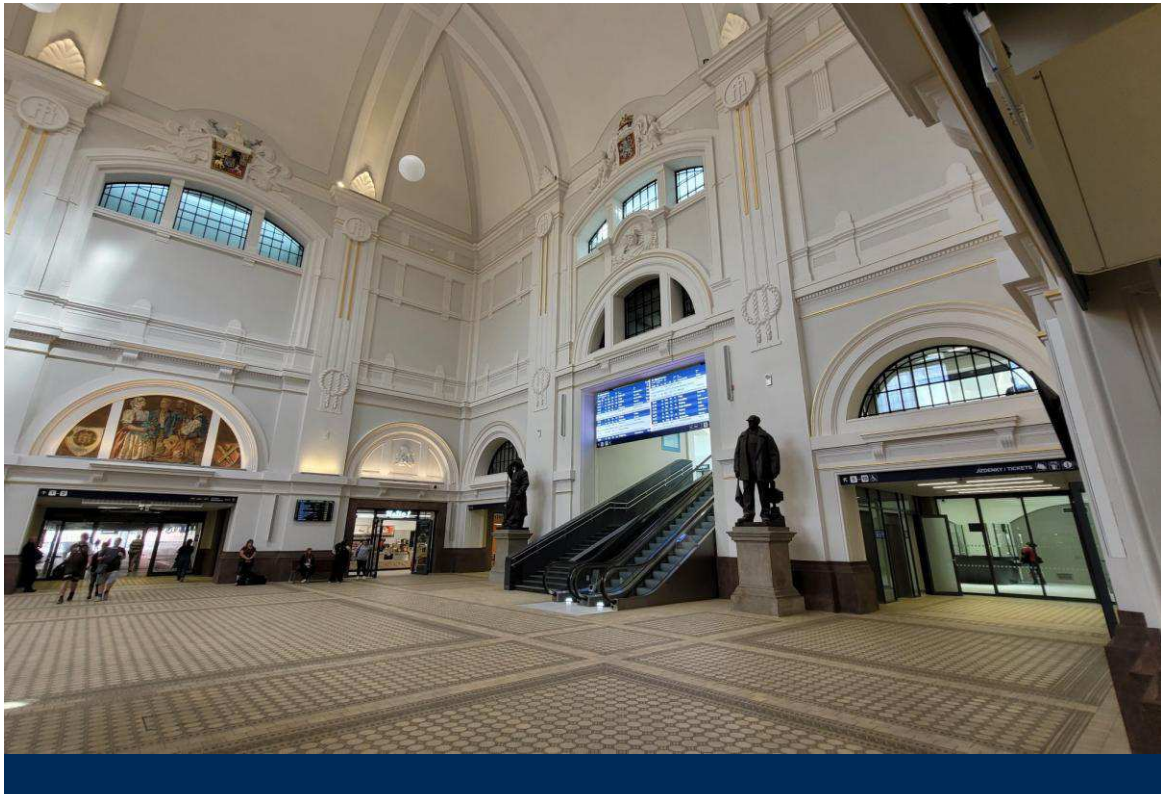
- Příloha 1 – Standardy softwarového vývoje
- Příloha 2 – Datová centra a serverovny
- Příloha 3 – Virtuální prostředí, serverové farmy a servery
- Příloha 4 – Konektivita a síťové prostředí
- Příloha 5 – Integrovaní standardy
- Příloha 6 – Komunikační standardy
- Příloha 7 – Standardy zálohování a disaster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

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

© 2025

Datum tisku
2025-07-30

spravazeleznic.cz



Platforma SŽ Standardy vývoje software

Červen 2025

Obsah

1	Úvod	5
2	Standardy vývoje informačních systémů Správy železnic	5
2.1	Prostředí	5
2.1.1	Vývojové prostředí	5
2.1.2	Testovací prostředí	5
2.1.3	Produkční prostředí	5
2.2	Dvouvrstvá architektura	5
2.2.1	Datová vrstva	6
2.2.2	Aplikační vrstva	6
2.3	Třívrstvá a vícevrstvá architektura	6
2.3.1	Datová vrstva	6
2.3.2	Aplikační vrstva	7
2.3.3	Prezentační vrstva	7
2.3.4	Integrační vrstva	7
2.4	Požadavky na prezentační vrstvu	8
2.4.1	Uživatelské rozhraní	8
2.4.2	Uživatelská zkušenost	8
2.5	Bezpečnost	9
2.5.1	Zabezpečení aplikací	9
2.5.2	Autentizace a autorizace	10
2.5.3	Zpracování osobních údajů	11
2.6	Dokumentace	11
2.6.1	Technická dokumentace jádra systému	11
2.6.2	E-R modely databáze	11
2.6.3	Objektový model pro aplikace	11
2.6.4	Procesní diagramy, schémata toků dat	11
2.6.5	Komunikační rozhraní	11
2.6.6	Drátové modely všech obrazovek uživatelského rozhraní aplikací	11
2.6.7	Popis konfigurace provozního prostředí	12
2.6.8	Uživatelská příručka	12
2.6.9	Příručka administrátora	12
2.6.10	Disaster Recovery postup (D/R Postup)	12
2.7	Modelování EA architektury	12
2.8	Předávání vývoje do provozu	12

Seznam zkratek

2FA	Dvou-faktorové ověření (<i>Two-Factor Authentication</i>)
3NF	Třetí normální forma návrhu tabulek databází řeší tranzitivní závislosti v rámci návrhu tabulek databází
DDL	(<i>Data Definition Language</i>)
EA	Podniková architektura (<i>Enterprise Architecture</i>)
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. (<i>General Data Protection Regulation</i>)
ICT	Informační a komunikační technologie (<i>Information and Communication Technology</i>)
IT	Informační technologie (<i>Information Technology</i>)
LDAP	(<i>Lightweight Directory Access Protocol</i>)
MFA	Více-faktorové ověření identity uživatele (<i>Multi-Factor Authentication</i>)
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 (<i>Service-Oriented Architecture</i>)
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 (<i>Structured Query Language</i>)
SSO	(<i>Single Sign-On</i>)
SW	Programové vybavení počítače či jiného obdobného zařízení. Speciálním druhem software je <i>firmware</i> , který je úzce spjatý s konkrétním hardwarem (<i>Software</i>)
SŽ	Správa železnic, státní organizace
SŽT	Správa železniční telematiky, organizační jednotka SŽ
UI	(<i>User Interface</i>)
UNICODE	Univerzální kódování znaků s možností reprezentace všech národních znakových sad
UX	(<i>User Experience</i>)
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 nejdříve 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 takového 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 prostřednictvím 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 popsána 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 systém bude zabezpečovat konzistenci aplikační logiky, napříč všemi desktopovými klienty.

Bez aktualizčních 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 služby¹ 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/zefektivnění 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 jsou²:
 - 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.

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

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

© 2025

Datum tisku
2025-07-30

spravazeleznic.cz



Platforma SŽ Datová centra a serverovny

Červen 2025

Obsah

1	Úvod	4
2	Datová centra	4
2.1	Datové centrum CDP Praha	4
2.2	Datové centrum CDP Přeřov	5
3	Serverovny	5
3.1	Významné serverovny	5
3.2	Serverovny dle geografických oblastí.....	5
3.3	Serverovny vybraných organizačních jednotek.....	5
3.4	Technologické serverovny	5
3.5	Technologické a sdělovací místnosti	5
4	Technologické vybavení	5
4.1	Stavební provedení	6
4.2	Napájení	6
4.3	Chlazení.....	6
4.4	Bezpečnost	7
4.5	Síťová infrastruktura	7
4.6	Ostatní vybavení.....	7

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 Přešov)
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 řídicí 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 (<i>Elektronická požární signalizace</i>)
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 (<i>Elektronická zabezpečovací signalizace</i>)
ICT	Informační a komunikační technologie (<i>Information and Communication Technology</i>)
IT	Informační technologie (<i>Information Technology</i>)
OJ	Organizační jednotka SŽ
OŘ	Oblastní ředitelství SŽ
OT	Provozní technologie (<i>Operations Technology</i>)
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 (<i>Uninterruptible Power Supply</i>)

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 umístěny 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

Dat centrum / 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 umístovány technologie jak IT, tak OT. Tato datová centra jsou součástí technologických řídicích 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 směrnici.

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 OR slouží primárně pro provoz ICT infrastruktury a aplikací určených pro jednotlivá OR.

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 budov 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 sítově odděleny od zbytku sítě pomocí firewallu. Pro místní sítové připojení je nutné používat výhradně sítové prvky detailně definované v Příloze 4 – *Konektivita a sítové 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

© 2025

Datum tisku
2025-07-30

spravazeleznic.cz

```
hdac0: <NVIDIA (0x0083) HDA CODEC> at cad 0
hdac0: <NVIDIA (0x0083) Audio Function Group
pem0: <NVIDIA (0x0083) (HDMI/DP 8ch)> at nid
pem1: <NVIDIA (0x0083) (HDMI/DP 8ch)> at nid
pem2: <NVIDIA (0x0083) (HDMI/DP 8ch)> at nid
pem3: <NVIDIA (0x0083) (HDMI/DP 8ch)> at nid
ugen0.1: <0x0086 XHCI root HUB> at usb0
uhub0: <0x0086 XHCI root HUB, class 9/0, rev
nvd0: <Samsung SSD 960 PRO 512GB> NVMe namesp
nvd0: 488386MB (100215216 512 byte sectors)
ada0 at ahcich0 bus 0 scbus0 target 0 lun 0
ada0: <ST320LT012-9WS14C 0001LVM1> ATAB-ACS S
ada0: Serial Number W0VDEFBC
ada0: 300.000MB/s transfers (SATA 2.x, UDMA6,
ada0: Command Queuing enabled
ada0: 305245MB (625142448 512 byte sectors)
ada0: quirks=0x1<4K>
ada1 at ahcich4 bus 0 scbus4 target 0 lun 0
ada1: <ST4000DM000-1F2168 CC52> ATAB-ACS SATA 3
ada1: Serial Number Z300YNB5
```

Platforma SŽ

Virtuální prostředí, serverové farmy, servery

Červen 2025

Obsah

1	Úvod	4
2	Virtualizační prostředí.....	4
2.1	Virtualizace serverů.....	4
2.2	Virtualizace koncových počítačů	4
2.3	Kontejnerizace.....	4
3	Serverové farmy.....	4
3.1	Konvergovaná infrastruktura	4
3.2	Hyper-konvergovaná infrastruktura	5
4	Fyzické servery	5
5	Datová úložiště.....	5
5.1	Datová úložiště farem.....	5
5.2	Datová úložiště pro zálohy a archivaci	5
5.3	Datová úložiště pro off-line zálohy	6
5.4	Kancelářská datová úložiště	6
6	Virtuální servery	6
6.1	Služba virtuálních strojů	6
6.2	Služby diskových uložišť	7
7	Databázové servery	7
8	Webové servery.....	7
9	Aplikační servery	8

Seznam zkratek

ACI	Technologie aplikačně orientované infrastruktury firmy Cisco (<i>Cisco ACI</i>)
CPU	Hlavní procesor zařízení či počítače, který je zodpovědný za plynulé spouštění software (<i>Central Processing Unit</i>)
DB	Databázová aplikace (<i>Database Engine</i>)
DR	Plán obnovy po havárii, součást kontinuity IT služeb (<i>Disaster Recovery</i>)
FC	Vysokorychlostní datové rozhraní primárně používané pro datová úložiště (<i>Fibre Channel</i>)
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 (<i>Hyperconverged Infrastructure</i>)
HTTP	Standardizovaný protokol pro přenos webových stránek (<i>Hyper-text Transfer Protokol</i>)
HW	Hardware označuje veškeré fyzicky existující technické vybavení počítače
ICT	Informační a komunikační technologie (<i>Information and Communication Technology</i>)
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 (<i>Internet Small Computer System Interface</i>)
IT	Informační technologie (<i>Information Technology</i>)
LTO	Otevřený formát magnetické pásky určené pro záznam velkých objemů dat (<i>Linear Tape Open</i>)
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 (<i>Network Attached Storage</i>)
OS	Operační systém
SAN	Oddělená datová síť pro připojení datových úložišť. Zpravidla používá protokol FC nebo iSCSI (<i>Storage Area Network</i>)
SAP	Modulární ERP systém od německé firmy SAP AG
SOHO	Obecné označení pro zařízení pro domácí a kancelářské použití (<i>Small Office / Home Office</i>)
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 (<i>Virtual Desktop Infrastructure</i>)
VM	Virtuální počítač (<i>Virtual Machine</i>)

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 umísťovat. 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:

- Umísťují 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:

- Umísťují 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:

- Umísťují 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 umístovaná mimo rackové skříně, typicky do kancelářských prostor, jsou nepřijatelná a nesmí být připojována do ICT prostředí Správy železnic.

Větší disková úložiště typu NAS umístovaná 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 úložišť

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 technologii 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

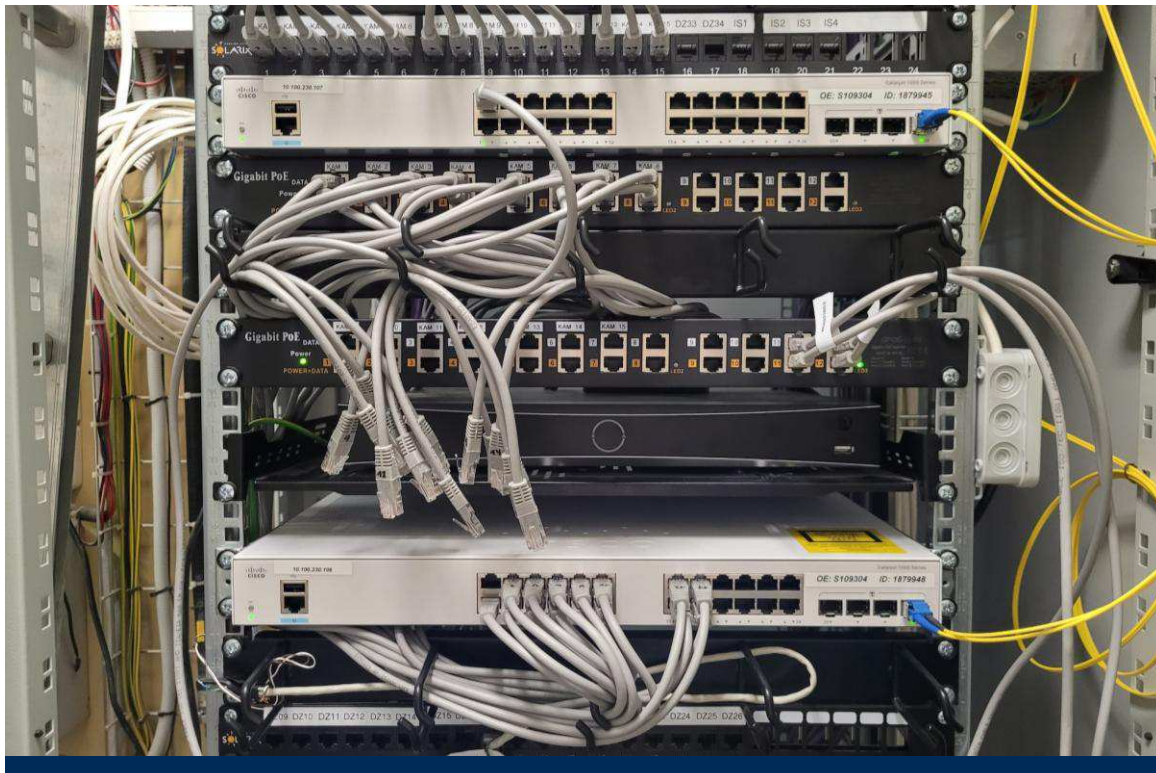
Služba	Popis
Liferay na Win.VMware.x86_64	Liferay je přední open-source podnikové portálové řešení založené na jazyce Java, které umožňuje správu dat, aplikací, procesů a integrace současných i nových aplikací z jednoho centrálního uživatelského rozhraní.

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

© 2025

Datum tisku
2025-07-30

spravazeleznic.cz



Platforma SŽ Konektivita a síťové prostředí

Červen 2025

Obsah

1	Úvod	8
2	Perimetr Správy železnic	8
2.1	Perimetr	8
2.2	Demilitarizovaná zóna	8
2.2.1	Demilitarizovaná zóna pro OT	8
2.3	Přístup přes VPN	8
2.3.1	Uživatelské VPN s MFA	9
2.3.2	Site to Site VPN	9
2.4	Komunikační směry	9
3	Fyzické sítě Správy železnic	10
3.1	Uživatelsko-aplikační síť	10
3.2	Technologické datové sítě	10
3.2.1	Segmentace sítě	10
3.2.2	Ostrovni oddělené sítě	10
4	Logické síťové prostředí	11
4.1	Komunikace mezi sítěmi	11
4.2	Georedundance	11
4.3	Řešení High Availability	11
5	Sítě APN	12
6	Síťová zařízení	12
6.1	Používané technologie	12
6.1.1	VLAN	12
6.1.2	VRF	12
6.1.3	Technologie DWDM	13
6.1.4	Sítě MPLS	13
6.1.5	Síťová spine-leaf topologie	13
6.1.6	Technologie Cisco ACI	13
6.1.7	Sítě OOB	14
6.2	Firewally	14
6.3	Routery	14
6.4	Switche	15
6.4.1	Switche pro datová centra	15
6.4.2	Switche pro fibre channel	15
6.4.3	Switche pro kamerové systémy	15
6.4.4	Switche pro management zařízení	16
6.4.5	Switche pro lokální sítě	16
6.5	Bezdrátová zařízení	16
6.6	Huby	16
6.7	Modemy a datová zařízení	16
6.8	Centralizovaná správa síťových prvků	17

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) (<i>Access Point Name</i>)
CLI	Příkazový řádek (<i>Command Line Interface</i>)
DB	Databáze
DC	Datové centrum v kontextu lokalit (<i>Datacenter</i>)
DCS	Distribuovaný systém řízení technologií (<i>Distributed Control System</i>)
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 útočnicků (<i>Distributed Denial of Service</i>)
DMZ	Část síťové infrastruktury organizace, ve které jsou soustředěny služby poskytované někomu z okolí, případně celému Internetu. Tyto vnější (veřejné) služby jsou obvykle nejněžším cílem internetového útoku; úspěšný útočník se ale dostane pouze do DMZ, nikoli přímo do vnitřní sítě organizace (<i>Demilitarized Zone</i>)
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 (<i>Denial of Service</i>)
DR	Plán obnovy po havárii, součást kontinuity IT služeb (<i>Disaster Recovery</i>)
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 (<i>Digital Subscriber Line</i>)
DWDM	Typ vlnového multiplexu, který je založený na multiplexování více optických signálů v jednom optickém vlákne na různých vlnových délkách nebo různých typech laserů (<i>Dense Wavelength Division Multiplex</i>)
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 (<i>General Packet Radio Service</i>)
HA	Vysoká dostupnost služeb. Předpokladem řešení je použití dvou a více nezávislých zařízení s cílem zajistit funkčnost v případě výpadku (<i>High Availability</i>)
HW	Hardware označuje veškeré fyzicky existující technické vybavení počítače
ICS	Průmyslové řídicí systémy (<i>Industrial Control System</i>)
ICT	Informační a komunikační technologie (<i>Information and Communication Technology</i>)
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 (<i>Industrial DeMilitarized Zone</i>)
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 (<i>Internet Protocol Security</i>)
IT	Informační technologie (<i>Information Technology</i>)
LAN	Místní počítačová síť (<i>Local Area Network</i>)
LTE	Řešení mobilního bezdrátového vysokorychlostního přenosu dat čtvrté generace (<i>4G / Long Term Evolution</i>)
MFA	Více-faktorové ověření identity uživatele (<i>Multi-Factor Authentication</i>)

MGMT	Řízení, dohled, konfigurace, sběr dat a vzdálený přístup k serverům a aktivním síťovým prvkům (<i>Management</i>)
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 (<i>Multiprotocol Label Switching</i>)
NGFW	Oproti běžným FW nabízí také doplňkové funkce jako AVC, AMP, IPS, IDS, DPI, DLP, TD, IdM a dešifrování a kontrolu TLS/SSL obsahu (<i>Next-Generation Firewall</i>)
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 (<i>Out-of-Band MGMT LAN</i>).
OŘ	Oblastní ředitelství SŽ
OS	Operační systém (<i>Operating System</i>)
OT	Provozní technologie (<i>Operations Technology</i>)
PAM	Řešení zabezpečení identit, které pomáhá chránit organizaci před kybernetickými hrozbami monitorováním, zjišťováním a prevencí neoprávněného privilegovaného přístupu k důležitým prostředkům (<i>Privileged Access Management</i>)
PLC	Programovatelný automat, typické koncové zařízení v OT (<i>Programmable Logic Controller</i>)
PoE	Technologie napájení zařízení přes standardní ethernetový kabel. PoE existuje v několika standardech, které se liší především přenášeným elektrickým výkonem (<i>Power over Ethernet</i>)
RJ45	Standardizovaný metalický konektor pro počítačové sítě (<i>Registered Jack 45</i>)
S2S VPN	Šifrované VPN připojení zajišťující propojení dvou LAN (<i>Site-to-Site VPN, LAN-to-LAN VPN</i>)
SAN	Oddělená datová síť pro připojení datových úložišť. Zpravidla používá protokol FC nebo iSCSI (<i>Storage Area Network</i>)
SCADA	Softwarové řešení zpravidla dispečerského dohledu a monitorování technologií (<i>Supervisory Control And Data Acquisition</i>)
SFP	Typ slotu a modulu pro datovou komunikaci zpravidla po optických vláknech. Podporuje rychlost maximálně 1 Gbps (<i>Small Form Factor Pluggable</i>)
SFP+	Typ slotu a modulu pro datovou komunikaci zpravidla po optických vláknech. Podporuje rychlost maximálně 10 Gbps (<i>Small Form Factor Pluggable Plus</i>)
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 (<i>Virtual Machine</i>)
VPN	Virtuální privátní síť (<i>Virtual Private Network</i>)
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 (<i>Virtual Routing and Forwarding</i>)
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 (<i>Web Application Firewall</i>)

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 řídicích 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 síť 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, síť 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 koncentrátoři 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 koncentrátoři, 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 firewallly.

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 mohou 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 Síť 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 síť 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

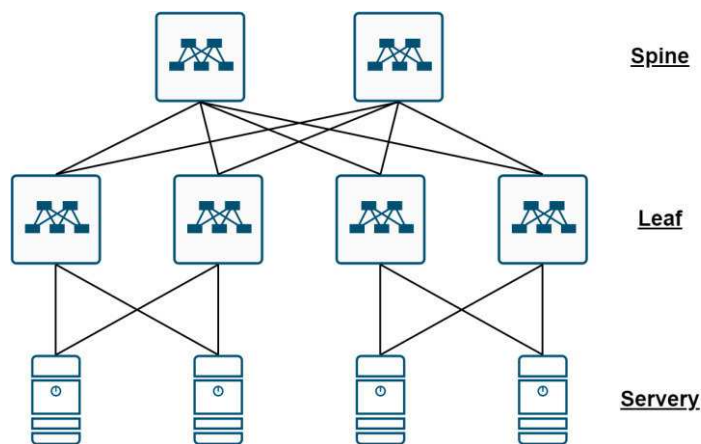
Typ zařízení	Popis	Konkrétní řady
DWDM	Přípojný bod	NCS 1000 NCS 2000

6.1.4 Síť 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 síť. 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 switchy 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 sítí 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 switchy v datových centrech již podporují integraci do Cisco ACI.

6.1.7 Síť 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 síť 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 síť.

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 síť	Cisco C9300 Cisco ISR
OT	Lokální routery pro OT síť	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 síť

Tyto switche pro lokální síť musí být umístitelné v 19" racku přímo na jeho ližiny. Redundantní zdroj není vyžadován.

Výčet používaných / preferovaných typů pro lokální síť

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 síť	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 síť

Typ zařízení	Popis	Konkrétní řady
Controller	Controller pro bezdrátové síť 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

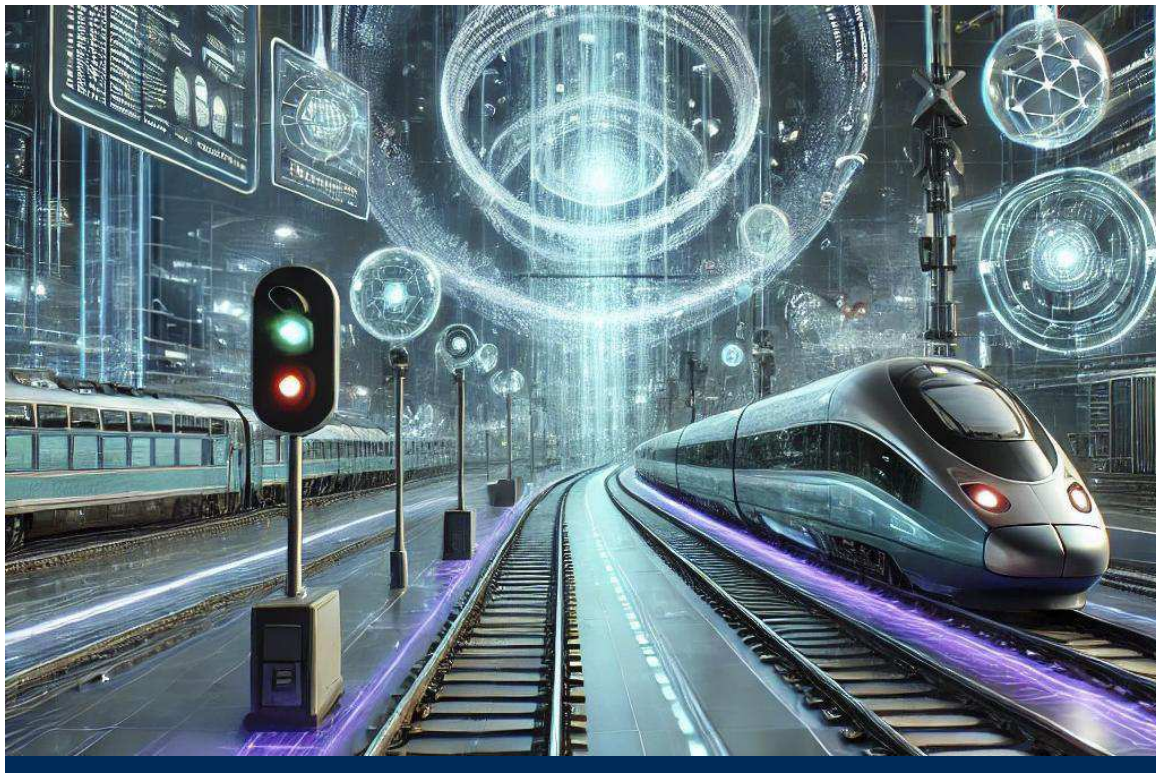
V prostředí Správy železnic se pro centralizovanou správu síťových prvků používají nástroje Cisco Catalyst Center (dříve Cisco DNA Center) a Cisco Nexus Dashboard Fabric Controller (dříve Cisco Data Center Network Manager). Tyto nástroje slouží pro správu, maintainance, aktualizace, zajištění jednotné konfigurace pomocí šablon i dohled nad celou sítí.

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

© 2025

Datum tisku
2025-07-30

spravazeleznic.cz



Platforma SŽ Integrační standardy

Červen 2025

Obsah

1	Úvod	4
2	Moderní architektonické rámce	4
2.1	Flexibilita	4
2.2	Škálovatelnost	4
2.3	Bezpečnost	4
2.4	Efektivita	4
3	Architektura integrací	5
3.1	Microservices Architecture	5
3.2	Event-Driven Architecture	5
3.3	API-First Approach	5
3.4	Hybridní architektura	5
4	Typy integrací	5
5	Softwarová architektura Enterprise Service Bus	6
6	Primární integrační scénáře	6
6.1	Integrační platforma	6
6.2	SAP Business Technology Platform	7
6.3	Microsoft nástroje a Azure	7
6.4	Integrace stávajících aplikací	7
7	Datové formáty	9
8	Metody	10
9	Dokumentace integračních scénářů	10
10	Řízení integračních scénářů	11

Seznam zkratk

API	Komplexně definované komunikační rozhraní aplikace (<i>Application Programming Inteface</i>)
CSV	Jednoduchý textový souborový formát (Comma-separated values)
ESB	Softwarová architektura a technologie používaná v oblasti podnikové integrace a správy služeb (<i>Enterprise Service Bus</i>)
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 (<i>Internet of Things</i>)
IT	Informační technologie (<i>Information Technology</i>)
ITIL	(<i>Information Technology Infrastructure Library</i>)
JSON	Datový formát primárně určený pro přenos dat (<i>JavaScript Object Notation</i>)
KII	Kritická informační infrastruktura
REST/API	Webově založené klient-server API (<i>Representational State Transfer</i>)
SAP	Modulární ERP systém od německé firmy SAP AG
SFTP	Zabezpečený protokol pro přenos souborů. Pro zajištění šifrování využívá protokol SSH (<i>SSH File Transfer Protocol</i>)
SMTP	Základní síťový protokol pro přenos elektronické pošty (<i>Simple Mail Transfer Protocol</i>)
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 (<i>Service-Oriented Architecture</i>)
SŽ	Správa železnic, státní organizace
XML	Standardizovaný jazyk používaný pro serializaci dat (<i>Extensible Markup Language</i>)

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 subsystemy 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 popsáných 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 orchestraci 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 (nešifované)	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

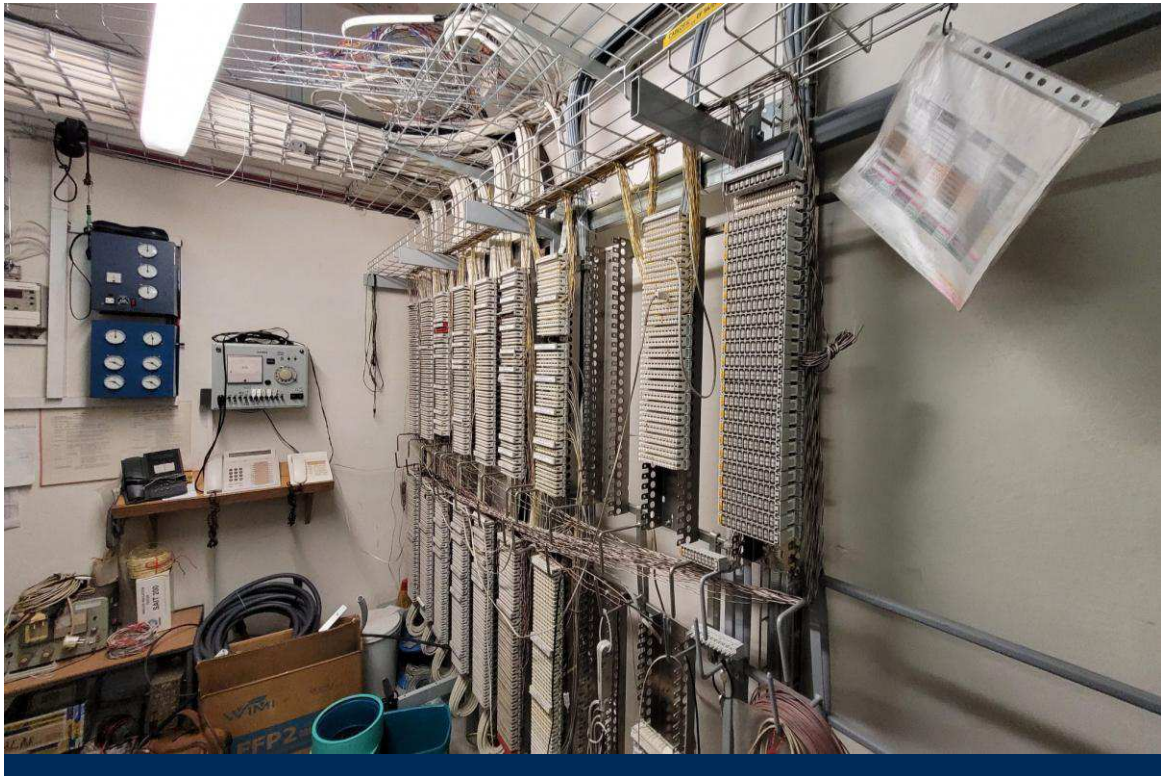
Jakékoliv nové Integrační scénáře, či změny Integračních scénářů musí projít skrze Architecture Board nebo Change management a být posouzeny v širším kontextu. Skrze jaký proces bude integrační scénář posuzován určí matice, která zahrnuje posouzení složitosti změny a její dopady. Integrační scénář následně 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

© 2025

Datum tisku
2025-07-30

spravazeleznic.cz



Platforma SŽ Komunikační standardsy

Červen 2025

Obsah

1	Úvod	4
2	Komunikační služby	4
3	SMS brána	4
4	Emailová komunikace.....	4
4.1	Z uživatelsko-aplikační sítě	4
4.2	Z technologických datových sítí	4
4.3	Z externích sítí Správy železnic.....	4
4.4	Mimo sítě Správy železnic	5
5	Komunikační platforma dispečerských pracovišť.....	5

Seznam zkratek

API	Komplexně definované komunikační rozhraní aplikace (<i>Application Programming Interface</i>)
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 (<i>Information and Communication Technology</i>)
O27	Odbor komunikace GŘ SŽ
SAP	Modulární ERP systém od německé firmy SAP AG
SMS	Krátká textová zpráva (<i>Short Message Service</i>)
SMTP	Základní síťový protokol pro přenos elektronické pošty (<i>Simple Mail Transfer Protocol</i>)
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 (<i>Virtual Private Network</i>)

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 branou 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 podporována.

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 síť 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

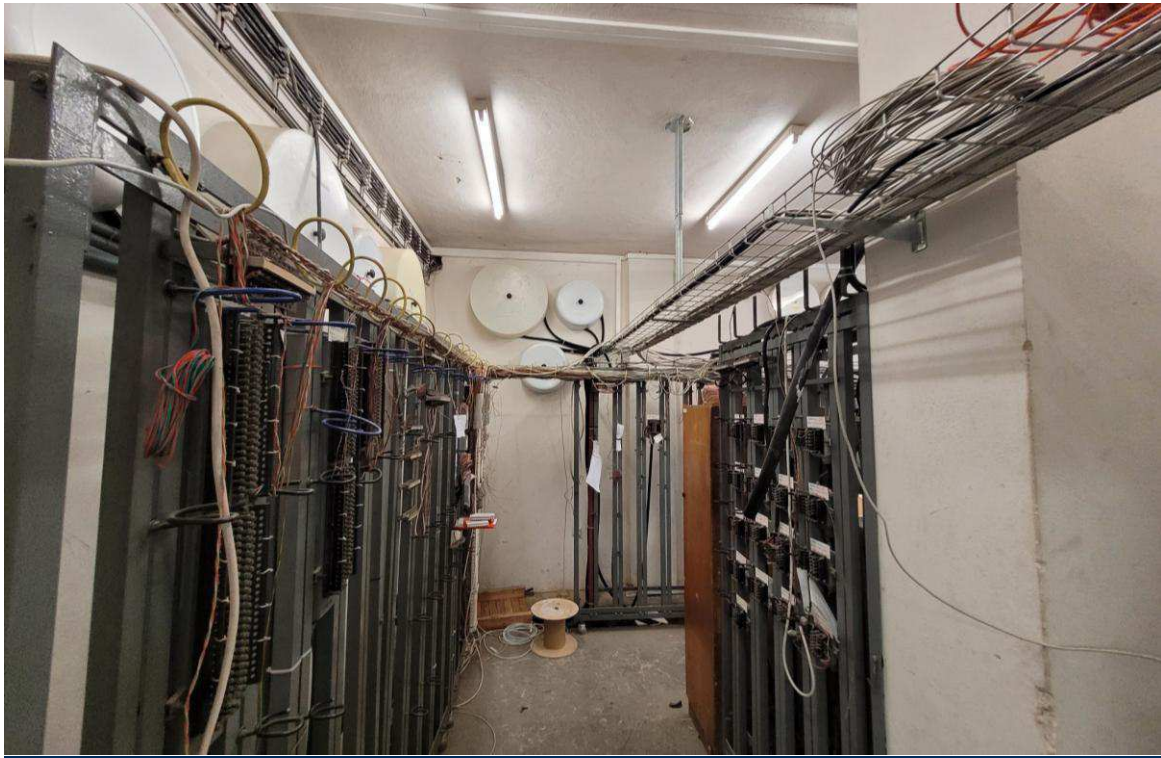
Komunikační platforma pro zajištění komunikace v rámci dispečerských pracovišť je Cisco Webex.

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

© 2025

Datum tisku
2025-07-30

spravazeleznic.cz



Platforma SŽ Standardy zálohování a disaster recovery

Červen 2025

Obsah

1	Úvod	4
2	Služby zálohování	4
3	Řešení Disaster recovery	4

Seznam zkratek

DB	Databázová aplikace (<i>Database Engine</i>)
DR	Plán obnovy po havárii, součást kontinuity IT služeb (<i>Disaster Recovery</i>)
IBM	Americká technologická společnost (<i>International Business Machines</i>)
ICT	Informační a komunikační technologie (<i>Information and Communication Technology</i>)
LTO	Otevřený formát magnetické pásky určené pro záznam velkých objemů dat (<i>Linear Tape Open</i>)
MSSQL	Databázový server od firmy Microsoft (<i>Microsoft SQL Server</i>)
OS	Operační systém (<i>Operating System</i>)
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 sintaxi (<i>Structured Query Language</i>)
SŽ	Správa železnic, státní organizace
TSM	Nástroj pro zálohování, v současné době již nese název IBM Storage Protect (<i>Tivoli Storage Manager</i>)
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.

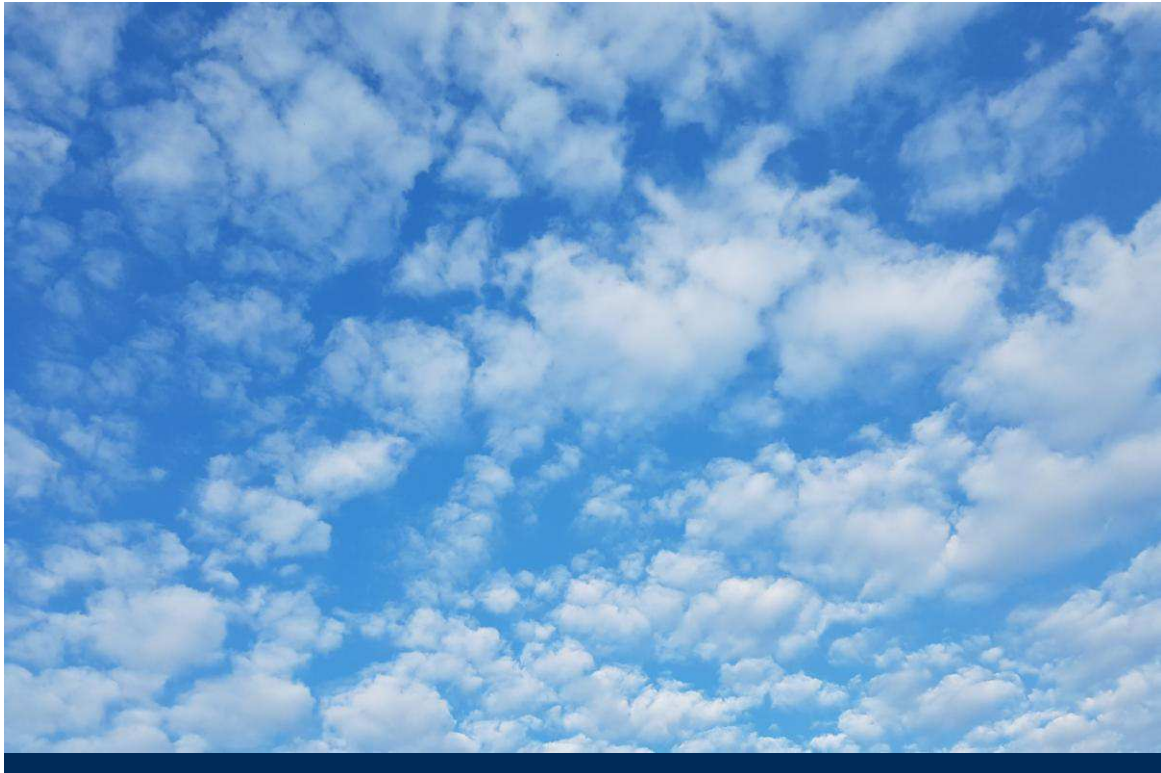
Všechny zálohy jsou pravidelně testovány a veškeré offline zálohy uložené na LTO páskách jsou pravidelně převáženy do zabezpečeného prostoru (do trezoru v jiné budově).

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

© 2025

Datum tisku
2025-07-30

spravazeleznic.cz



Platforma SŽ Cloudové prostředí

Červen 2025



Obsah

1	Úvod	5
2	Cloudové prostředí.....	5
2.1	Microsoft Entra ID	5
2.2	Služby M365	5
3	Cloudové služby	5
3.1	Služba ověření proti Microsoft Entra ID	5
3.2	Integrace s M365	5

Seznam zkratek

AAD	Služba AD provozovaná v cloudovém prostředí MS Azure. Nový název služby je „MS EntraID“ (<i>Azure Active Directory</i>)
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 (<i>Active Directory</i>)
AWS	Cloudové prostředí firmy Amazon (<i>Amazon Web Services</i>)
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 (<i>Domain Name System</i>)
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 (<i>Enterprise Resource Planning</i>)
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 (<i>Infrastructure as a Service</i>)
ICT	Informační a komunikační technologie (<i>Information and Communication Technology</i>)
IP	Jeden ze základních komunikačních protokolů používaných v počítačových sítích (<i>Internet Protocol</i>)
IT	Informační technologie (<i>Information Technology</i>)
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 (<i>Microsoft 365</i>)
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 (<i>Platform as a Service</i>)
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 (<i>pay-as-you-go</i>). To umožňuje uživatelům využívat software bez nutnosti investovat do hardware a IT infrastruktury (<i>Software as a Service</i>)
SAP	Modulární ERP systém od německé firmy SAP AG
SSO	Metoda jednotného přihlášení (<i>Single Sign-On</i>)
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 síť 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

© 2025

Datum tisku
2025-07-30

spravazeleznic.cz

Příloha č. 4 Smlouvy

Poddodavatelé

Dodavatel provádí předmět plnění dle Smlouvy prostřednictvím následujících Poddodavatelů:

[OBCHODNÍ FIRMA PODDODAVATELE – NÁZEV, IČO, SÍDLO – DOPLNÍ DODAVATEL]	
Část Plnění dle Smlouvy prováděná Poddodavatelem procentuálním 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.]

Zvláštní obchodní podmínky pro Zakázky v oblasti ICT

OBSAH

1. VÝKLAD POJMŮ.....	2
2. DOBA A MÍSTO PLNĚNÍ	8
3. PRÁVA A POVINNOSTI OBOU STRAN.....	9
4. POVINNOSTI DODAVATELE	9
5. POVINNOSTI OBJEDNATELE.....	10
6. LICENČNÍ UJEDNÁNÍ	10
7. ZDROJOVÝ KÓD A DOKUMENTACE.....	15
8. AKCEPTAČNÍ ŘÍZENÍ.....	16
9. ŠKOLENÍ	19
10. SERVICEDESK.....	19
11. NAHLÁŠENÍ INCIDENTU	20
12. SERVISNÍ MODELY	21
13. AKTUALIZACE PLNĚNÍ.....	22
14. ÚČAST PODDODAVATELŮ	22
15. REALIZAČNÍ TÝM	23
16. KOMUNIKACE STRAN	24
17. NÁHRADA ŠKODY A SMLUVNÍ POKUTY	24
18. ZÁRUKA ZA JAKOST A PRÁVA Z VADNÉHO PLNĚNÍ.....	26
19. UKONČENÍ SMLUVNÍHO VZTAHU	28
20. ZMĚNY SMLOUVY A ZMĚNOVÉ ŘÍZENÍ	29
21. KYBERNETICKÁ BEZPEČNOST.....	29
22. OCHRANA OSOBNÍCH ÚDAJŮ	36
23. OCHRANA DŮVĚRNÝCH INFORMACÍ	37

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 částí 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, obrázků, 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:
- neobdržení podkladů a informací vyžádaných Dodavatelem, které jsou nezbytně nutné pro lokalizaci nebo replikaci Incidentu, od Objednatele;
 - 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);
 - 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 nahlásování 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 optimalizací 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, Dlážďená 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 trvajících či opakujících 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 Ohlašovatelí.
- 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:
- 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.
 - 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 takového Softwaru, neboť nebude nutné zasahovat do Zdrojových kódů takového Softwaru anebo proto, že případné nahrazení takového Softwaru nebude představovat výraznější komplikaci a náklad na straně Objednatele.
 - 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.
 - 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 jejich 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 ovládnutí 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 infekci 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 vyzvu 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 možnosti 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 Poddodavatelem 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 náležitě souhlas, 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 nespádají 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 užití 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 užití veškerá Autorská díla a k výkonu práva vytěžovat a zužítkovat 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 užit 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 kalendářních 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 Akceptačního 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 nezaplátí 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 Objednatel 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 zakončeno 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 provedeno 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:
5x8, 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 časovým 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 Objednati, 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 nahlášován prostřednictvím Servicedesku, pak se za Čas nahlášení Incidentu považuje čas vytvoření ticketu v Servicedesku. Je-li Incident nahlášován 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:

- dočasné vyřazení Softwaru z provozu na základě předchozí dohody Objednatele a Dodavatele (odstávka),
- pravidelná vyřazení Softwaru z provozu Dodavatelem v časech sjednaných ve Smlouvě nebo její příloze (servisní okna),
- smluvními stranami předem dohodnutý časový úsek za účelem instalace upgradu,
- výpadky Softwaru způsobené Objednatelem přímo v důsledku jím provedených zásahů do Softwaru, které nebyly Dodavatelem předem schváleny,
- 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 závázání a nebudou jednat v rozporu s ujednáními Smlouvy a jejími Přílohami, kterou mezi sebou uzavřeli Dodavatel a Objednatel.
- 14.3. Významný dodavatel je oprávněn využit 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 odst. 8.1.11 ZOP za každý započatý den prodlení až do řádného odstranění poslední vytykávané 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 <u>odst. 12.8 ZOP</u>
Od 2 (včetně) do 5 %	15 % z ceny poskytovaného Plnění odpovídající vyhodnocovanému období dle <u>odst. 12.8 ZOP</u>
Od 5 (včetně) do 10 %	25 % z ceny poskytovaného Plnění odpovídající vyhodnocovanému období dle <u>odst. 12.8 ZOP</u>
Od 10 % (včetně) a více	50 % z ceny poskytovaného Plnění odpovídající vyhodnocovanému období dle <u>odst. 12.8 ZOP</u>

- 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 započít 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 nezabavuje 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 vyplývajících 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, ovládnutí 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 nenapravit 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 nenapravit.
- 19.4. Dodavatel není oprávněn odstoupit od Smlouvy ve vztahu k části Plnění, za kterou mu již bylo Objednatelem zapláceno.
- 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, protioopatření, 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 zvládnání Kybernetických bezpečnostních událostí a Kybernetických bezpečnostních incidentů obsahující činnosti, role, odpovědnosti a pravomoci k rychlému a účinnému zvládnání 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,

kteřá 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 protopatření 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 požadovat 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 ujednáno 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 knihovny 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 přístupových 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 **Dodavatel** 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 uchování 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 uchování 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](#).

Obchodní podmínky ke Smlouvě o dílo

OBSAH OBCHODNÍCH PODMÍNEK

Obchodní podmínky ke Smlouvě o dílo	1
ČÁST 1 - ÚVODNÍ USTANOVENÍ	2
ČÁST 2 - NÁVRH NA UZAVŘENÍ SMLOUVY O DÍLO	3
ČÁST 3 - DÍLO	3
ČÁST 4 - CENA DÍLA	4
ČÁST 5 - ZMĚNA CENY DÍLA	4
ČÁST 6 - PLATEBNÍ PODMÍNKY	4
ČÁST 7 - MÍSTO PLNĚNÍ	5
ČÁST 8 - DOBA PLNĚNÍ	6
ČÁST 9 - PROVÁDĚNÍ DÍLA	6
ČÁST 10 - ZKUŠEBNÍ PROVOZ	8
ČÁST 11 - PŘEPRAVA DÍLA	8
ČÁST 12 - PODDODAVATELÉ	9
ČÁST 13 - PŘEDÁNÍ A PŘEVZETÍ DÍLA	10
ČÁST 14 - VLASTNICKÉ PRÁVO A NEBEZPEČÍ ŠKODY	11
ČÁST 15 - VADY PLNĚNÍ A ZÁRUKA	11
ČÁST 16 - UPLATNĚNÍ PRÁV Z VADNÉHO PLNĚNÍ	12
ČÁST 17 - PODMÍNKY ODSTRANĚNÍ VAD	13
ČÁST 18 - POJIŠTĚNÍ	13
ČÁST 19 - DUŠEVNÍ VLASTNICTVÍ	14
ČÁST 20 - SANKCE	14
ČÁST 21 - OBECNÁ ODPOVĚDNOST ZHOTOVITELE	16
ČÁST 22 - Odstoupení od smlouvy o dílo	16
ČÁST 23 - OSTATNÍ UJEDNÁNÍ	17

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 ZoDHP 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 navrhuje 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 navrhuje Smluvní straně včas, kdyby její přeprava probíhala obvyklým způsobem, má pozdní přijetí účinky včasného přijetí, ledaže navrhuje 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, již 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 Objednatel.
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 Objednatel. 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 doručenu po obdržení notifikace doručení, která je automaticky odesílána odesílateli.**
33. Splatnost Výzvy k úhradě musí být stanovena tak, aby nastala 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 užití obdobně.
37. Ustanovení §2611, §2620–2622 a §2624 Občanského zákoníku se neuplatní.

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. Případně-li konec sjednané doby plnění na sobotu, neděli nebo svátek, není Zhotovitel v prodlení, dodá-li Dílo nejbližší 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 zneprístupněny.

54. Před zakrytím nebo zneprístupněním 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-GR-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 užití 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 užití 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 nevydává, 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 neomezuje.
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 nepřevzme, 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 použijí 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, použijí 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. Případně-li konec Záruční doby na sobotu, neděli nebo svátek, je vada včas uplatněna, je-li písemná forma reklamace odeslána Zhotoviteli nejbližší 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, užití 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 užití 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 Objednatel 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 zproští, 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 nezproští.

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 předvíдалa, 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 vyplývá, 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 dodatečně 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 částečné 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 přijímací 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 strany povinny plnit v době ode dne převzetí Díla Objednatelem, tedy zejm. ustanovení o vadách Díla.
202. Ustanovení §1977, §2002–2003 Občanského zákoníku se neuzijí.

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 tlumočnick.

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.

Příloha č. 7 Smlouvy

Realizační tým

Pozice	Kontaktní údaje	Činnosti prováděné členem realizačního týmu, zejm.:
Vedoucí projektu	<p>Jméno a příjmení: [DOPLNÍ ZHOTOVITEL]</p> <p>Telefon: [DOPLNÍ ZHOTOVITEL]</p> <p>E-mail: [DOPLNÍ ZHOTOVITEL]</p>	<ul style="list-style-type: none"> • Posuzuje a technicky vede stavební část projektu datového centra • Zajišťuje soulad stavebních řešení s technologickými požadavky • Koordinuje stavební práce a návaznosti ostatních profesí • Provádí dohled nad realizací stavebních prací • Kontroluje jejich soulad s dokumentací, standardy a požadavky Zadavatele • Monitoruje postup stavebních prací, vyhodnocuje rizika a navrhuje opatření • Zajišťuje stavební dokumentaci, záznamy a podklady • Spolupracuje s projektanty, dodavateli a technickým dozorem • Přípravuje technické podklady a účastní se kontrol, revizí a zkoušek
Odborník pro elektroinstalace a UPS	<p>Jméno a příjmení: [DOPLNÍ ZHOTOVITEL]</p> <p>Telefon: [DOPLNÍ ZHOTOVITEL]</p> <p>E-mail: [DOPLNÍ ZHOTOVITEL]</p>	<ul style="list-style-type: none"> • Zajišťuje technické vedení elektroinstalačních prací a instalací UPS • Zajišťuje návaznosti elektroinstalací na stavební, technologické, chladicí a MaR systémy • Kontroluje instalaci UPS systémů, rozvodů, záložních větví, jejich odzkoušení a integraci do ICT infrastruktury • Účastní se FAT/SAT testů a ověřuje funkčnost celého napájecího řetězce • Kontroluje provedení elektroinstalací v souladu s dokumentací, ČSN, interními standardy a technickými požadavky Zadavatele • Monitoruje průběh elektroinstalačních prací

		<ul style="list-style-type: none"> Zajišťuje související technickou dokumentaci, revizní zprávy a záznamy
Specialista pro chlazení a VZT	<p>Jméno a příjmení:</p> <p>[DOPLNÍ ZHOTOVITEL]</p> <p>Telefon:</p> <p>[DOPLNÍ ZHOTOVITEL]</p> <p>E-mail:</p> <p>[DOPLNÍ ZHOTOVITEL]</p>	<ul style="list-style-type: none"> Posuzuje a technicky vede řešení chlazení a VZT Koordinuje chladicí práce s ostatními profesemi Kontroluje realizaci chladicích zařízení Účastní se zkoušek, testů a ověřování funkčnosti při uvádění do provozu Sleduje správnost provedení, výkonové parametry, redundanci a splnění technických požadavků Kontroluje soulad se zpracovanou dokumentací a požadavky Zadavatele Zajišťuje vedení technické dokumentace, protokolů a podkladů pro předání
Specialista MaR (měření a regulace)	<p>Jméno a příjmení:</p> <p>[DOPLNÍ ZHOTOVITEL]</p> <p>Telefon:</p> <p>[DOPLNÍ ZHOTOVITEL]</p> <p>E-mail:</p> <p>[DOPLNÍ ZHOTOVITEL]</p>	<ul style="list-style-type: none"> Posuzuje, navrhuje a technicky vede řešení MaR pro technologické provozy, zejména v prostředí datových center Zajišťuje správnou funkci snímačů, regulátorů, řídicích jednotek a jejich návazností Koordinuje a realizuje propojení chlazení, napájení, environmentálních čidel, PLC a dalších technologií do systémů BMS, DCIM nebo obdobných Navrhuje komunikační vazby, signály a přenosy dat mezi systémy Zajišťuje uvádění MaR systémů do provozu, provádí funkční testy a ověřuje správnost integrace Účastní se FAT/SAT testů a řeší případné nedostatky Dozoruje provedení MaR instalací a kontroluje jejich soulad s projektovou dokumentací, normami a požadavky Zadavatele Sleduje správné nastavení regulačních prvků a logiky řízení Zajišťuje vedení dokumentace, protokolů a podkladů pro předání

Koordinátor BOZP	<p>Jméno a příjmení: [DOPLNÍ ZHOTOVITEL]</p> <p>Telefon: [DOPLNÍ ZHOTOVITEL]</p> <p>E-mail: [DOPLNÍ ZHOTOVITEL]</p>	<ul style="list-style-type: none"> • Zajišťuje bezpečnost práce při realizaci • Kontroluje pracovní postupy a podmínky • Zajišťuje dokumentaci a vyhodnocení BOZP
Specialista na datová centra ICT	<p>Jméno a příjmení: [DOPLNÍ ZHOTOVITEL]</p> <p>Telefon: [DOPLNÍ ZHOTOVITEL]</p> <p>E-mail: [DOPLNÍ ZHOTOVITEL]</p>	<ul style="list-style-type: none"> • Zajišťuje odborné vedení a technické zajištění ICT infrastruktury datového centra • Navrhuje a konfiguruje klíčové prvky DC infrastruktury • Zajišťuje návaznost ICT infrastruktury na technologie chlazení, napájení, bezpečnostní systémy, MaR a stavební části • Dozoruje realizaci a uvedení ICT infrastruktury do provozu • Kontroluje správnost instalace ICT prvků, kabeláže a rozvaděčových systémů • Podílí se na testování, validaci a ověřování provozních parametrů DC technologií
Projektový manažer	<p>Jméno a příjmení: [DOPLNÍ ZHOTOVITEL]</p> <p>Telefon: [DOPLNÍ ZHOTOVITEL]</p> <p>E-mail: [DOPLNÍ ZHOTOVITEL]</p>	<ul style="list-style-type: none"> • Řídí komplexně projekt datového centra • Vede projekt v celém jeho životním cyklu, řídí tým a interní zdroje • Zajišťuje plnění cílů projektu v oblastech rozsahu, času, nákladů a kvality • Koordinuje práce a návaznosti mezi stavebními, elektro, IT, bezpečnostními, chladicími a dalšími profesemi • Sleduje postup projektu a vyhodnocuje rizika • Kontroluje správnost realizace prací a jejich shodu s projektovou dokumentací a technickými požadavky • Zajišťuje komunikaci, dokumentaci a předání projektu

HARMONOGRAM

Fáze	Popis	Zahájení fáze	Ukončení (od zahájení fáze)
F1	Projektová dokumentace	Od nabytí účinnosti smlouvy	do 3 týdnů
F2	Výroba mobilního datového centra	Od ukončení F1	do 12 týdnů
F3	Dodávka mobilního datového centra	Od ukončení F2	do 2 týdnů
F4	Zprovoznění mobilního datového centra	Od ukončení F3	do 4 týdnů
F5	Dokumentace	Od ukončení F4	do 2 týdnů
F6	Školení	Od ukončení F4	do 1 týdne
F7	Profylaxe MDC	Od ukončení F4	120 měsíců
F8	Služby na vyžádání	Od ukončení F4	120 měsíců

Příloha č. 5 Zadávací dokumentace – **Účastník předloží pouze v případě postupu dle čl. 23.2. a 23.3 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 „**Nákup mobilního datového centra**“, tímto čestně prohlašuje, že

dále uvedené údaje a další skutečnosti uvedené či jinak řádně označené ve smlouvě na plnění předmětu veřejné zakázky/rámcové dohody, 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 vlastníky 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 doporučujícím ZRS, a to bez ohledu na to, zda byla smlouva uveřejněna prostřednictvím registru smluv ze strany zadavatele nebo účastníka.

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 [DOPLNÍ ÚČASTNÍK] dne [DOPLNÍ ÚČASTNÍK]

Příloha č. 6 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/žádost o účast v řízení na zadání nadlimitní sektorové veřejné zakázky s názvem „**Nákup mobilního datového centra**“, (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 [DOPLNÍ ÚČASTNÍK] dne [DOPLNÍ ÚČASTNÍK]

Příloha č. 7 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/žádost o účast v řízení na zadání nadlimitní sektorové veřejné zakázky s názvem „**Nákup mobilního datového centra**“, (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 čestné 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 čtené 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. 8 Zadávací dokumentace

Vzor profesního životopisu

Předpokládaná **pozice** ze seznamu realizačního týmu dodavatele: **[DOPLNÍ DODAVATEL]**

- a. Příjmení: **[DOPLNÍ DODAVATEL]**
- b. Jméno: **[DOPLNÍ DODAVATEL]**
- c. Titul: **[DOPLNÍ DODAVATEL]**
- d. Kontaktní pracovní adresa (včetně pracovního tel/e-mail): **[DOPLNÍ DODAVATEL]**
- e. Současná funkce/pracovní pozice včetně uvedení osoby zaměstnavatele a vztahu k zaměstnavateli, příp. uvést OSVČ či jinak dle skutečného stavu: **[DOPLNÍ DODAVATEL]**

Pozn.: Dodavatel uvede některou z následujících alternativ: pracovní poměr na plný úvazek, pracovní poměr na částečný úvazek, dohoda o pracovní činnosti, dohoda o provedení práce, člen statutárního orgánu, OSVČ, příp. další možnost. Pro vyloučení pochybností zadavatel uvádí, že pokud je dokládána osoba OSVČ a zároveň není současně dodavatelem nebo není vůči dodavateli v pracovním či obdobném poměru, bude považována za jinou osobu ve smyslu § 83 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, se všemi důsledky z toho vyplývajícími, nikoliv za zaměstnance či za osobu v obdobném postavení.

- f. Osoba **je / není** **[DOPLNÍ DODAVATEL]** zaměstnancem dodavatele.
- g. Osoba **je / není** **[DOPLNÍ DODAVATEL]** současně zaměstnancem zadavatele.
- h. **Praxe** pro účely prokázání kvalifikace čl. 12.2.3. Zadávací dokumentace:

Doba profesní praxe na konkrétní pozici <i>(ve formátu mm/rrrr - mm/rrrr)</i>	Zaměstnavatel/OSVČ <i>Dodavatel doplní identifikaci zaměstnavatele či uvede, že byl OSVČ</i>	Popis vykonávaných činností <i>Dodavatel doplní označení <u>pozice</u> a rovněž stručný <u>popis</u> vykonávaných činností, ze kterého bude vyplývat naplnění požadavků dle čl. 12.2.3 Zadávací dokumentace</i>
[DOPLNÍ DODAVATEL]		[DOPLNÍ DODAVATEL]
[DOPLNÍ DODAVATEL]		[DOPLNÍ DODAVATEL]
[DOPLNÍ DODAVATEL]		[DOPLNÍ DODAVATEL]

i. **Účast na projektech** pro účely prokázání kvalifikace čl. 12.2.3. Zadávací dokumentace:

1)	Název projektu (činnosti/zakázky)	[DOPLNÍ DODAVATEL]
	Objednatel projektu (obch. firma/název a sídlo a kontaktní osoba objednatele - jméno, tel., email)	[DOPLNÍ DODAVATEL]
	Datum realizace projektu (MM/RRRR – MM/RRRR)	[DOPLNÍ DODAVATEL]
	Popis předmětu projektu	[DOPLNÍ DODAVATEL]
	Popis činností, které člen týmu prováděl v rámci projektu	[DOPLNÍ DODAVATEL]

2)	Název projektu (činnosti/zakázky)	[DOPLNÍ DODAVATEL]
	Objednatel projektu (obch. firma/název a sídlo a kontaktní osoba objednatele - jméno, tel., email)	[DOPLNÍ DODAVATEL]
	Datum realizace projektu (MM/RRRR – MM/RRRR)	[DOPLNÍ DODAVATEL]
	Popis předmětu projektu	[DOPLNÍ DODAVATEL]
	Popis činností, které člen týmu prováděl v rámci projektu	[DOPLNÍ DODAVATEL]

3)	Název projektu (činnosti/zakázky)	[DOPLNÍ DODAVATEL]
	Objednatel projektu (obch. firma/název a sídlo a kontaktní osoba objednatele - jméno, tel., email)	[DOPLNÍ DODAVATEL]
	Datum realizace projektu (MM/RRRR – MM/RRRR)	[DOPLNÍ DODAVATEL]
	Popis předmětu projektu	[DOPLNÍ DODAVATEL]
	Popis činností, které člen týmu prováděl v rámci projektu	[DOPLNÍ DODAVATEL]

V případě dalších zkušeností použije dodavatel tabulku opakovaně dle potřeby.

Přílohy:

- kopie certifikátů/osvědčení požadovaných v čl. 12.2.3. zadávací dokumentace

11	Máte zkušenosti s veřejnými zakázkami v oblasti kritické infrastruktury?	ANO	ANO	ANO	Tento dotaz nebyl zodpovězen.	ANO	ANO	ANO	ANO	ANO - Jsem dodavatelem technologických částí v oboru zabezpečovacích, sledovacích, řídicích a komunikačních technologií dopravní infrastruktury.	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 aplikací na platformě s vysokými nároky na dostupnost, bezpečnost, geografickou redundanci a kontinuální 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 ochrany o mlčenlivosti (NDA) uvést.	ANO - Např. DC zdroje pro drážní aplikace.	ANO
12	Spĺňuje řešení požadavky zákona o kybernetické bezpečnosti (ZokB) 264/2025 Sb. a vyhlášky o kybernetické bezpečnosti (VoKB) 409/2025 Sb.? Jaké certifikace nebo audity to dohlédá?	ANO ISO 27000 a příslušné podčásti. V případě auditu se musí zajistit provádění penetračních testů.	ANO - V tom kontextu, že s pomocí navrhovaného řešení je možné zajistit splnění vybraných požadavků ZokB a VoKB. Tato legislativa a priorit nestanovuje explicitní požadavky na řešení nebo technologii. Ani nespecifikuje postupy a způsoby certifikace technologie. 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.	Toto by měl prokázat navrhovatel, projektant nebo zpracovatel zadání.	Tento dotaz nebyl zodpovězen.	Nezodpovědět, není známo řešení.	ANO	ANO	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. Součástí řešení jsou také požadavky je zajišťován kombinací technických a organizačních opatření odpovídající 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 kontinuální provozu. V oblasti zabezpečeného úložiště pak o opatření v oblasti ochrany dat, šifrování, řízení identit a přístupů, auditovatelnosti a bezpečnostního dohledu. Konkrétní rozah 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 - Násle společnost je držitelem certifikace dle ISO 27001 - Dodávky prvky pro výrobu telekomunikačních a datových síť a poskytování komplexních systémových řešení.	V tuto chvíli s ohledem na nejasnosti v zadání není finální řešení známé, každopádně můžeme garantovat, že bude postaveno tak, aby byly tyto požadavky splněny.	
13	Máte praktické zkušenosti s projekty pro klienty, na kterých se vztahuje ZokB 181/2014 Sb. a VoKB? Pokud ano, stručně je popište.	ANO - V rámci XXX byl realizován návrh, implementace, provozování a údržba infrastruktury v rámci IT a OT.	ANO - Máme zkušenosti s dodávkou infrastrukturálních řešení pro klienty, na něž se vztahuje ZokB a VoKB. Máme zkušenosti i s dodávkou řešení do oblasti kritické infrastruktury a vyznamovaných informačních systémů. U vybraných projektů zpracováváme i bezpečnostní analýzy a bezpečnostní dokumentaci posuzující splnění požadavků VoKB při nasazení řešení, resp. dokumentující, jak implementace navrhovaného řešení jajiňuje splnění vybraných požadavků ZokB a VoKB kladených legislativou na zadavatele	ANO	Tento dotaz nebyl zodpovězen.	ISJR, NAKIT	ANO - Společnost XXX, má praktické zkušenosti s projekty pro klienty, na kterých se vztahuje ZokB 181/2014 Sb. a VoKB*	ANO	ANO	ANO - Dodavatel má dlouhodobé praktické zkušenosti s realizací projektů pro klienty, 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 podílí 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 vyhláškou o kybernetické bezpečnosti. Konkrétní zákaznické reference a detailní popisy projektů nelze z důvodu smluv o mlčenlivosti (NDA) uvést.	ANO - Dodávka prováděná z řešení do oblasti energetiky, dopravy, telekomunikační infrastruktury, obrany.	Pracujeme na dodávkách pro klienty z oblasti státní infrastruktury.	
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 m - Část 1: Základní hlediska, stanovení základních charakteristik, definice - ČSN 33 2000-4-41 ed.3 Ochrana před úrazem elektrickým proudem - ČSN 33 2000-4-44 Ochrana před EMC (elektromagnetickým rušením) - ČSN 33 2000-4-46 ed. Odstupování a spínání - ČSN 33 2000-4-42 ed.2 Ochrana před úrazem tepla - ČSN 33 2000-4-43 ed.2 Ochrana proti nebezpečím - 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 - ČSN 33 2000-5-54 ed.3 Uzemnění,	Není relevantní. Předmětem námi navrhovaného řešení není řešení samotného datového centra, k němuž se otázka vztahuje (elektro, fyzická bezpečnost, požární bezpečnost, ...). Jednotlivě navrhované technologie splňují požadavky norem a EU legislativy v oblasti elektrické bezpečnosti a dalších relevantních norem	Toto by měl prokázat navrhovatel, projektant nebo zpracovatel zadání.	Tento dotaz nebyl zodpovězen.	Z pohledu IT infrastruktury bude záležet na vybrané technologii	Řešení společnosti XXX je navrhováno dle norem ISO 9001:2015 a ISO 27001:2022 XXX splňují následující předpisy: • EN ISO 9001 • Evropské předpisy • Povinné certifikace pro Českou republiku týkající se instalovaných systémů	Jedná se o celý soubor norem pokrývajících jednotlivé části, jmenovitě nejdůležitější: Non-IT infrastruktura dle EN 50600 Konstrukce dle EN 1011, protikorozní ochrana dle ČSN EN 12944	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. Fyzicky 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 včet aplikovaných norem a jejich rozsah se bude odvíjet od finální zvolené	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 10225 (S3532).	V technické specifikaci jsou normy uvedeny.		

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 technické části na klíč: 21 000 000 Kč Realizace služeb: 1 500 000 Kč	Tuto část nenabízíme.	15-20 mil. Kč bez DPH	Tento dotaz nebyl zodpovězen.	Nenabízíme	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 POC, instalace, logistiky, uvedení do provozu, dokumentace a školení		Část dodávka, instalace a zpuštění – 39 200 000 Kč bez DPH v rámci České republiky. Část prolytacké kontroly a revize – 295 000 Kč bez DPH za 1 rok v rámci České republiky.	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 přihledem 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 řešení, viz Dotaz 3	Mobilní datové centrum vč. zprovoznění 36 098 800 Kč bez DPH Prolytace dle Technické specifikace v částce na 1 rok 663 480 Kč bez DPH V ceně je zahrnuto umístění kontejneru a jeho obsluhu v ohradu 100 km od sídla společnosti.	Předpokládáme hodnotu plnění je 18 – 28 mil. Kč bez DPH, finální cena je závislá na požadovaném rozsahu plnění (montážní služby, testovací služby, servisní služby, ...)
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 řádu nižších desítek milionů korun	Pokud budou požadávky na systém zabezpečeného úložiště konkrétnější budeme schopni orientační cenovou nabídku zpracovat.	V tuto chvíli nedokážeme odhadnout cenu za tuto část	Tento dotaz nebyl zodpovězen.	Záleží na vybraném řešení. Nemáme k dispozici potřebné podklady.	Náš odhad pro kompletní zajištění zabezpečeného úložiště včetně HW (storage, servery), síťové, instalace, uvedení do provozu, dokumentace, školení se pohybuje okolo 4 milionů EUR			Orientační cenu plnění za část „Realizace systému zabezpečeného úložiště v prostředí Správy železnic“ nelze v této fázi předběžně tržní konzultace jednoznačně stanovit. Důvodem je zejména neupřesněný technický rozsah řešení, zejména v oblasti požadovaného výkonu, úložiště, architektury replikace a zálohování, požadavků na integritační 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...
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 realizaci obou částí současně je možné předpokládat celkovou úsporu nákladů.	Kontejner nenabízíme.	Předpokládáme, že ANO	Tento dotaz nebyl zodpovězen.	Záleží na vybraném řešení. Nemáme k dispozici potřebné podklady.	ANO Konkrétní úsporu bychom byli schopni vyčíslit po bližším vyspecifikování technického řešení			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 11/19 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 předběžně 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 a provozních požadavků zadavatele, viz	Nenabízíme kompletní řešení obou částí	Předpokládáme že ne, jedná se o natolik rozdílné plnění že efekt sloučení těchto dvou oblastí nepovede ke snížení celkové ceny.
18	Nabízíte možnost pořízení formou jednorázové investice (CapEx)?	ANO	ANO - Obecně jsme schopni k navrhovaným řešením nabídnout model financování OpEx i CapEx	ANO	Tento dotaz nebyl zodpovězen.	ANO	ANO			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 v rámci následného zadávacího řízení.	ANO	ANO - Technologie lze objednat včetně všech souvisejících nákladů na Slet provozu.
19	Nabízíte možnost pořízení formou průběžných plateb (OpEx)?	ANO	ANO - Obecně jsme schopni k navrhovaným řešením nabídnout model financování OpEx i CapEx.	ČÁSTEČNĚ	Tento dotaz nebyl zodpovězen.	Záleží na vybraném řešení. Nemáme k dispozici potřebné podklady.	ANO			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 následného zadávacího řízení.	NE	ANO - Pokud bude Zadavatel požadovat řešení, jehož součástí bude i část průběžně poskytovaných služeb (není však součástí tohoto průzkumu – např. průběžná administrace řešení, prolytacké služby apod.), v daném minimálním rozsahu, pak lze řešení nabídnout i jako službu.

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	NE	Je možné získat rámcový ceník nebo ukázkovou konfiguraci s cenou? Pokud ano, uveďte prosím odkaz k nahlédnutí či stažení.	Fento dotaz nebyl zodpovězen.	Záleží na vybraném řešení. Nemáme k dispozici potřebné podklady.	ČÁSTEČNĚ - Pro získání ukázkové konfigurace a ceny bychom určitě potřebovali specifikovat požadované řešení	NE - Jedná se o specifický návrh odpovídající požadavkům Závadatele.	NE - Vzhledem k povaze požadovaného 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 vztahy na síťové úrovni. Každá 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 požadavků zadavatele, viz Dotaz 3	NE - Jedná se o konfiguraci „na klíč“ dle Vaší technické specifikace, ne ceníkové položky.	NE - Z dodaných podkladů nelze určit, co bude součástí dodávek...
21	Lze odhadnout provozní náklady řešení na 1 rok, 5 let a 10 let dopředu? Pokud ano, uveďte prosím číslo.	Cca 600 000 Kč/1 rok 3 000 000 Kč/5 let 8 000 000 Kč/10 let	NE	NE	Lze odhadnout provozní náklady řešení na 1 rok, 5 let a 10 let dopředu? Pokud ano, uveďte prosím číslo.	Fento dotaz nebyl zodpovězen.	Záleží na vybraném řešení. Nemáme k dispozici potřebné podklady.	ANO - Pro odhad provozních nákladů bychom ale potřebovali specifikovat požadované řešení	ČÁSTEČNĚ - Jedná-li se o provozní náklady vztahené 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, časnost transportů atd	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 úložišť, 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 Dotaz 3	NE - Týká se i přílohy č. 3 – tuto část nenabízíme.	NE - Nelze odhadnout - z dodaných podkladů nelze určit, co bude součástí dodávek...
22	Jaká je předpokládaná životnost jednotlivých technologií? kontejner + podřípné technologie data storage, servery	20 let kontejner 15 let podřípné technologie 5 let je standardní životní cyklus pro IT infrastrukturu Individuální HW komponenty mají životnost typicky do 7 let. Typicky je možné v iničiální 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 prodloužovat a HW je již zastaralý a dochází k jeho ovládnutí. U řešení s potřebou delšího životního cyklu je pak dlouhodobá životnost zajištěna na SW úrovni, která zajišťuje kontinuální provoz datového úložiska i v případě výměny částí HW komponent	Datastorage a servery	kontejner + podřípné technologie - min. 10 let data storage, servery - min. 5 let	Jaká je předpokládaná životnost jednotlivých technologií? kontejner + podřípné technologie data storage, servery	Fento dotaz nebyl zodpovězen.	Záleží na vybraném řešení. Nemáme k dispozici potřebné podklady.	Předpokládaná životnost kontejneru + podřípných technologií je 20 let pro hlavní sídlo. HW vybavení (data storage, servery) se nejlépe vyvíjí na dobu 5ti let, nicméně jeho životnost je samozřejmě delší. Z pohledu životního cyklu doporučujeme obnovu HW nejméně jednou za 5 let, doporučujeme však již zmíněných 5 let.	ČÁSTEČNĚ - Životnost kontejneru je až 50 let při pravidelné údržbě a zejména odpovídá antikoroznímu nádrhu. Celková délka životnosti je pak ovlivněna prostředím, ve kterém je kontejner umístěn z pohledu vlhkosti, větru, vody, sněhu. Podřípné 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.	Předpokládaná životnost jednotlivých technologií závisí na jejich charakteru, a pravidelnou údržbou. Pro zvýšení životnosti doporučujeme umístění na betonové pásy nebo patky z důvodu zamezení pronikání spodní vlhkosti do konstrukce způsobující korozí. Obecně lze uvést, že životnost se pohybuje v rozmezí 35 – 40 let. Podřípné technologie - životnost podřípné technologie se pohybuje okolo 15 let, doporučená bezpečná doba provozu je však 10 let, kdy po jejím uplynutí se doporučuje provést výměnu nebo reparovat zařízení. Celková délka životnosti je podmíněna optimálními provozními podmínkami a pravidelnými servisními prohlídkami a výměnou potřebného materiálu, jako jsou filtry, ventilátory atd. Používáme ventilátory, které mají v čistém prostředí životnost 110 let.	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 korozí. Obecně lze uvést, že životnost se pohybuje v rozmezí 35 – 40 let. Podřípné technologie - životnost podřípné technologie se pohybuje okolo 15 let, doporučená bezpečná doba provozu je však 10 let, kdy po jejím uplynutí se doporučuje provést výměnu nebo reparovat zařízení. Celková délka životnosti je podmíněna optimálními provozními podmínkami a pravidelnými servisními prohlídkami a výměnou potřebného materiálu, jako jsou filtry, ventilátory atd. Používáme ventilátory, které mají v čistém prostředí životnost 110 let.	Kontejner - technologie jsou navrženy na 10-ti letý provoz, při správném servisním zabezpečení je životnost až 20 let. IT - Typicky se životnost 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.
23	Nabízíte model TCO výpočtu pro různé varianty konfigurací?	ANO	ANO	ČÁSTEČNĚ	Nabízíte model TCO výpočtu pro různé varianty konfigurací?	Fento dotaz nebyl zodpovězen.	Záleží na vybraném řešení. Nemáme k dispozici potřebné podklady.	ANO	ANO - Dodávatel 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 architektury řešení.	ANO - Dodávatel 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 architektury řešení.	ČÁSTEČNĚ - Jen pro část Mobilního kontejnerového datového centra.	NE - Z dodaných podkladů nelze určit, co bude součástí dodávek...
24	Dodáváte jste v posledních 3 letech obdobné řešení svým subjektům?	ANO	ANO	ČÁSTEČNĚ	Dodáváte jste v posledních 3 letech obdobné řešení svým subjektům?	Fento dotaz nebyl zodpovězen.	NE	ANO	ČÁSTEČNĚ - Sdělovací a zabezpečovací místnosti pro digitální infrastrukturu.	ANO - Dodávatel realizoval v posledních letech obdobné řešení pro různé typy zákazníků, zejména v oblasti veřejné správy, kritické infrastruktury a komerční sféry s vysokými nároky na dostupnost, bezpečnost a kontinuální provoz. Realizace zahrnovaly zejména dodávky a integraci infrastruktury pro ukládání a zpracování dat, návrh a implementaci geografické redundance a disaster recovery, zabezpečení datových úložisk a jejich provozní podporu včetně SLA. Konkrétní zákaznické reference a detailní popis jednotlivých projektů nelze z důvodu ochrany o mlčenlivosti (NDA) uvádět. Uvedené vycházejí z reálných produkčních nasazení a dlouhodobého provozu obdobných řešení	ANO - Jen pro část Mobilního kontejnerového datového centra.	ANO - Společně s výrobcem. Dodávatel jme samostatně stojící diskové pole i celé řešení pro ukládání zázah. Pro relevantní odpověď bychom potřebovali lepší specifikaci zadané/žádávané Závadatele.

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 - 4 ks • XXX • XXX - 1ks • XXX - 1ks • XXX - 1ks Reference v oblasti zabezpečeného úložiště: • 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 úložiště (objektová storage ECS) (2024) - Dodávka, instalace, implementace a podpora objektové storage v mobilním kontejnerovém datovém centru XXX Dodávka zálohovacích zařízení (2024)	Vzhledem k mířenosti netze v tuto chvíli poskytnout - státní organizace	řento dotaz nebyl zodpovězen.	XXX		Technologické celky v oboru zabezpečovacích, sdělovacích, řídicích a komunikačních technologií dopravní infrastruktury ve střední Evropě	Dodávatel má zkušenosti s realizací projektů v oblasti mobilních datových center, bezpečných datových úložišť a související infrastruktury, včetně návrh, implementace a provozní podpory řešení s vysokými nároky na dostupnost, bezpečnost a kontinuitu provozu. Konkrétně seznam projektů, názvy zákazníků ani detailní popis realizací netze z důvodu smluv o mlčenlivosti (NDA) uvádět ani zptřístupovat. Uvedené zkušenosti vycházejí z reálné 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.	
26	Uveďte seznam vašich relevantních projektů v oblasti kritické infrastruktury (KI) včetně stručného popisu předmětu dodávky/ služby.	XXX 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 Dodávka zálohovacích zařízení (2024) - Dodávka zálohovacích zařízení (DataDomain, páskových knihoven, zálohovacího SW) včetně instalace a implementace. XXX Technická infrastruktura pro CMS 2.5 (2024,2025)	řento dotaz nebyl zodpovězen.	XXX	řento dotaz nebyl zodpovězen.	řento dotaz nebyl zodpovězen.	řento dotaz nebyl zodpovězen.	řento dotaz nebyl zodpovězen.	řento dotaz nebyl zodpovězen.	řento dotaz nebyl zodpovězen.	řento dotaz nebyl zodpovězen.
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.	ČÁSTEČNĚ	řento dotaz nebyl zodpovězen.	ANO	ANO - Některé integrace jsme zajišťovali přímo XXX technickými lidmi, u některých projektů spolupracujeme s našimi autorizovanými partnery	řento dotaz nebyl zodpovězen.	řento dotaz nebyl zodpovězen.	řento dotaz nebyl zodpovězen.	řento dotaz nebyl zodpovězen.	řento dotaz nebyl zodpovězen.
28	Máte zkušenosti s integrací XDR od výrobce Fidelis?	ČÁSTEČNĚ	NE	NE	řento dotaz nebyl zodpovězen.	ANO	ČÁSTEČNĚ - Na integraci XDR od výrobce Fidelis bychom byli schopni spolupracovat s některými z našich autorizovaných partnerů, kteří XDR řešení od společnosti Fidelis prodávají a implementují	řento dotaz nebyl zodpovězen.	řento dotaz nebyl zodpovězen.	řento dotaz nebyl zodpovězen.	řento dotaz nebyl zodpovězen.	řento dotaz nebyl zodpovězen.

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 uložení a cloudových služeb byly umístěny do fixního datového centra.	XXX Nové backup uložení (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 webových portálů, kde je možné sledovat průběh řešení incidentu. Technickou podporu je pak možné rozšířit o další služby – Proaktivní podporu, Patch management, Plánovací konzultace a konfigurační služby.	žádné	řento dotaz nebyl zodpovězen.	Nedodávali jsme			Dodávateľ má zkušenosti s realizací projektů, jejichž předmětem byla dodávka mobilního datového centra a kapacitou v řádu jednotek petabajtů, včetně záložního provozní podpory. Tyto dodávky byly realizovány jako technologicky oddělené celky, které však byly integrovány do jednoho funkčního řešení. V rámci poskytovatelských služeb je dodávateľ schopen zajistit provozní podporu formou servisních a provozních smluv v úrovních L1-L3, včetně dohledu nad provozem, řešení incidentů, esalobních mechanismů a pravidelného reportingu. Konkrétní zákaznické reference a detailní popis projektů nelze z důvodu smluv o mlčenlivosti (NDA) uvést	NE - Týká se přílohy č. 3 – tuto část nenabízíme.	V této kombinaci reference nemáme.
30	Máte zkušenosti s migrací dat v rozsahu petabajtů? Jaké nástroje jste použili?	ANO	ANO - Máme zkušenosti jak s migrací primárních dat mezi produkčními datovými úložišti, tak z migrace záloh mezi různými zálohovacími SIV. Konkrétní migrační postup a nástroj je zvolen na základě detailního posouzení zdrojové a cílové platformy pro uložení dat a specifík zákaznického prostředí.	NE	řento dotaz nebyl zodpovězen.	ANO - Z pohledu nástrojů využíváme například: VMware vMotion či Storage based migrace prostřednictvím XXX Peer Motion, VirtualDisc		ANO - Dodávateľ 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 využity standardní nástroje výrobců storage technologií a virtualizačních platform, případně specializované migrační nástroje, v kombinaci s vlastním migračním postupem zahrnujícím plánování, testování, validaci a finální přepnutí. Konkrétní zákaznické reference a detailní popis použitých nástrojů nelze z důvodu smluv o mlčenlivosti (NDA) uvést.	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 souborově spravovat a jinak i databáze (a i zde se každá databáze migruje jinak).	
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, datové úložiště a DPS. Součástí byla rovněž instalace, implementace a následná technická podpora řešení. XXX Odměna diskových polí (storage infrastruktury) v ústředí KVV 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 uložení (objektová storage ECS) (2024)	XXX	řento dotaz nebyl zodpovězen.	XXX		Provozujeme infrastrukturu typu Iaas v rámci více geograficky oddělených datových center společnosti, které 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 tedy i disaster recovery a je využívána pro provoz systémů s charakterem kritické infrastruktury a kritických informačních systémů. Z důvodu smluv o mlčenlivosti (NDA) není možné uvést ani aplikovat konkrétní zákaznické reference či detailní popis jednotlivých řešení	Týká se přílohy č. 3 – tuto část nenabízíme.	Máme několik zákazníků ve státní správě, jankovních i v ostatních oblastech. Informace poskytneme dle vnitřní cílové řešení.	
32	Poskytujete školení a dokumentaci v českém jazyce?	ANO	ANO - Pro řešení zabezpečeného uložení jsme schopni nabídnout školení i zpracování dokumentace v českém jazyce.	ANO	řento dotaz nebyl zodpovězen.	ANO	ANO	ANO - Dodávateľ 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 doplňková 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 AI	

33	Máte k dispozici náhled vzorového řešení? Například vzorový kontejner na ukázkou nebo zprostředkovaná návštěva za účelem prohlídky kontejneru u zákazníka. Případně byla by možná návštěva Vašeho výrobního závodu?	ANO	NE	NE	Tento dotaz nebyl zodpovězen.	NE	ANO - Určitě je možné domluvit si návštěvu XXX v továrně v Nizozemsku nebo v Customer Innovation Centru v Ženevě		ČÁSTEČNĚ	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 ukázkou konstrukčního a technologického provedení mobilního kontejnerového datového centra, jeho základních infrastrukturálních prvků a principů provozu. Konkrétní rozsah, forma a lokalita případné návštěvy budou upřesněny po dohodě se zadavatelem. Z důvodu smyslu a účelnosti (NOA) není možné přístupovat detailní technickou dokumentaci ani příslušné provozní prostředí zákazníků, nicméně je možné prezentovat řešení v obecné a demonstrační rovině.	ANO je možné navštívit jako výrobní závod, tak již instalovaná modulační datová centra	Kontejner - ANO IT - NE Všá komentář k navrhovanému řešení. Z šodaných podkladů netze ani určit, co bude součástí podávek
----	---	-----	----	----	-------------------------------	----	--	--	----------	---	--	--

Příloha č. 10 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 „**Nákup mobilního datového centra**“, (dále jen „**Veřejná zakázka**“ a „**Zadávací řízení**“), tímto čestně prohlašuje, že:

- a) ve smyslu varování Národního úřadu pro kybernetickou a informační bezpečnost, vydaného podle § 12 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů, ze dne 17. prosince 2018, č. j. 3012/2018NÚKIB-E/110, nevyužije pro účely plnění předmětu Veřejné zakázky technické či programové prostředky společností *Huawei Technologies Co., Ltd, Šen-čen, Čínská lidová republika* a *ZTE Corporation, Šen-čen, Čínská lidová republika*, ani jejich dceřiných společností, jejichž využití představuje hrozbu v oblasti kybernetické bezpečnosti.

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]