SPRÁVA ŽELEZNIC

Naše zn. 80219/2025-SŽ-GŘ-O25

Výzva k podání nabídky

Správa železnic, státní organizace, se sídlem Praha 1, Nové Město, Dlážděná 1003/7, PSČ 110 00, generální ředitelství, Vás při splnění podmínek uvedených v ustanovení § 6 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „***ZZVZ***"),

vyzývá

k podání nabídky na realizaci veřejné zakázky s názvem

„Zavedení komplexního síťového řešení prevence úniku dat (DLP) pro non-Microsoft systémy v prostředí Správy železnic"

Správa železnic, státní organizace, zadává tuto veřejnou zakázku jako podlimitní sektorovou veřejnou zakázku v souvislosti s výkonem relevantní činnosti dle § 151 odst. 1 ZZVZ a v souladu s § 158 odst. 1 ZZVZ nepostupuje při zadávání této veřejné zakázky podle uvedeného zákona. Řízení na zadání této veřejné zakázky se dále v textu označuje jako „***výběrové řízení***".

Výše uvedená veřejná zakázka je dále v textu označována jen jako „***veřejná zakázka***". Výzva k podání nabídky je v textu označována též jako „***Výzva***".

Pro tuto zakázku jsou stanoveny následující podmínky:

1. Identifikační údaje zadavatele

Název:	Správa železnic, státní organizace
Sídlo:	Praha 1, Nové Město, Dlážděná 1003/7, PSČ 110 00
IČO:	709 94 234
DIČ:	CZ70994234
Zapsán:	v obchodním rejstříku vedeném Městským soudem v Praze, oddíl A, vložka 48384
Zastoupen:	Bc. Jiřím Svobodou, MBA, generálním ředitelem

2. Informace o osobě, která zpracovala část Výzvy

2.1. Zadavatel označuje následující části Výzvy, na jejichž zpracování se podílela osoba odlišná od zadavatele:

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

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

Část Výzvy	Identifikace osoby
Technická specifikace (Příloha č. 2 této Výzvy) Harmonogram plnění (Příloha č. 4 této Výzvy) Návrh dodávky (šablona) (Příloha č. 5 této Výzvy) Tabulka pro vyplnění nabídkové ceny (Příloha č. 6 této Výzvy) Popis prostředí SŽ (Příloha č. 7 této Výzvy) Informace k systémům SŽ (Příloha č. 8 této Výzvy) Výstupy z PTK (Příloha č. 11 této Výzvy) Tabulka pro vyplnění údajů pro dílčí hodnotící kritérium „Kvalita" (Příloha č. 15 této Výzvy)	s-boost s.r.o., IČO: 230 37 539, se sídlem Senovážné náměstí 978/23, 110 00 Praha 1
Výzva k podání nabídky Krycí list nabídky (Příloha č. 1 této Výzvy) Závazný vzor smlouvy (Příloha č. 3 této Výzvy) Čestné prohlášení k registru smluv (Příloha č. 10 této Výzvy) Dohoda o ochraně důvěrných informací (Příloha č. 13 této Výzvy) Tabulka pro vyplnění údajů pro dílčí hodnotící kritérium „Kvalita" (Příloha č. 15 této Výzvy)	PORTOS, advokátní kancelář s.r.o., IČO: 481 18 753, se sídlem Hvězdova 1716/2b, 140 00 Praha 4

3. Informace o předběžné tržní konzultaci:

3.1. Zadavatel analogicky v souladu s § 33 ZZVZ realizoval před zahájením výběrového řízení předběžnou tržní konzultaci (dále také jen „***PTK***").

3.2. 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 na veřejnou zakázku s názvem „Zavedení komplexního síťového řešení prevence úniku dat (DLP) pro non-Microsoft systémy v prostředí Správy železnic" (dále jen „***Pozvánka***") a zároveň zaslal Pozvánku 12 vybraným dodavatelům přímo prostřednictvím e-mailu. Dodavatelé, kteří projevili zájem účastnit se PTK, měli zadavateli v rámci prvního kola PTK zaslat odpovědi na otázky, které jim zadavatel zaslal ve lhůtě 10 dnů od ukončení registrace do PTK, a to na e-mailovou adresu: cnitptk@spravazeleznic.cz.

3.3. Prvního kola předběžné tržní konzultace se účastnili následující dodavatelé:

a) ALEF NULA, a.s., se sídlem Pernerova 691/42, Praha 8, PSČ 186 00, IČO: 618 58 579,

b) initMAX s.r.o., se sídlem Plynární 1617/10, Praha 7, PSČ 170 00, IČO: 119 23 652,

c) ICZ.INFRA a.s., se sídlem Na hřebenech II 1718/10, Praha 4, PSČ 140 00, IČO: 618 59 117,

d) IXPERTA s.r.o., se sídlem Lihovarská 1060/12, Praha 9, PSČ 190 00, IČO: 275 99 523.

3.4. V rámci prvního kola PTK zadavatel ověřil následující okruhy témat:

a) Specifikace předmětu plnění a nastavení jeho rozsahu, etap, dílčích kroků, nastavení parametrů poptávaných služeb, vhodnost rozdělení plnění na analyticko-přípravnou a implementační část.

b) Doba potřebná k realizaci předmětu plnění.

c) Předpokládaná hodnota veřejné zakázky, dostatečnost podkladů nezbytných pro stanovení nabídkové ceny (resp. nacenění).

3.5. S ohledem na potřebu objasnění dalších doplňujících dotazů zadavatel realizoval také druhé kolo PTK, které se týkalo následujících okruhů témat:

a) Předpokládaná hodnota veřejné zakázky, dostatečnost podkladů nezbytných pro stanovení nabídkové ceny (resp. nacenění).

b) Zmapování licenčních modelů používaných pro agentless DLP řešení.

c) Schopnosti systémů odhalovat informace v různých komunikačních protokolech.

3.6. Zadavatel v této souvislosti obeznámil neomezený okruh potenciálních dodavatelů se svým záměrem realizovat druhé kolo PTK prostřednictvím dokumentu Pozvánka k druhému kolu předběžné tržní konzultace ve věci přípravy zadávacích podmínek na veřejnou zakázku s názvem „Zavedení komplexního síťového řešení prevence úniku dat (DLP) pro non-Microsoft systémy v prostředí Správy železnic" (dále jen „***Pozvánka II***") a zároveň zaslal Pozvánku II 14 vybraným dodavatelům přímo prostřednictvím e-mailu.

3.7. Účastníci druhého kola PTK měli zadavateli zaslat odpovědi na dotazy uvedené v příloze č. 1 Pozvánky II, a to na e-mailovou adresu: cnitptk@spravazeleznic.cz.

3.8. Druhého kola předběžné tržní konzultace se účastnili následující dodavatelé:

a) ICZ.INFRA a.s., se sídlem Na hřebenech II 1718/10, Praha 4, PSČ 140 00, IČO: 618 59 117,

b) Aricoma a.s., se sídlem Vinohradská 1511/230, Praha 10, PSČ 100 00, IČO: 046 15 671,

c) Netfox s.r.o., se sídlem Hartigova 65/2755, Praha 3, PSČ 130 00, IČO: 275 74 032,

d) ALEF NULA, a.s., se sídlem Pernerova 691/42, Praha 8, PSČ 186 00, IČO: 618 58 579.

3.9. Konkrétní dotazy položené v rámci prvního a druhého kola PTK, jakož i shrnutí průběhu a výsledků obou kol PTK jsou uvedeny v příloze č. 11 této Výzvy.

4. Komunikace mezi zadavatelem a dodavatelem

4.1. Veškerá komunikace mezi zadavatelem a dodavateli ve výběrovém řízení musí být vedena pouze písemnou formou, a to elektronicky, s výjimkou případů vymezených v ustanovení § 211 odst. 5 ZZVZ. Jazyk pro komunikaci mezi zadavatelem a dodavatelem je výhradně český jazyk, není-li dále stanoveno jinak. Doručování písemností a komunikace mezi zadavatelem a dodavateli ve výběrovém řízení 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 dodavatele učiněnou elektronicky, avšak nikoliv prostřednictvím elektronického nástroje E-ZAK, bude tedy zadavatel vždy odpovídat prostřednictvím elektronického nástroje.

4.2. Zpracování osobních údajů včetně jejich zvláštních kategorií případně poskytnutých v průběhu výběrového řízení je zadavatelem prováděno pouze za účelem zadání předmětné 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. Podrobné informace týkající se zpracování osobních údajů, zadavatel uvedl na oficiálních webových stránkách https://www.spravazeleznic.cz/o-nas/sdeleni-o-zpracovani-osobnich-udaju-pro-verejnost.

5. Předmět veřejné zakázky

5.1. Informace o předmětu veřejné zakázky:

Předpokládaná hodnota: se nezveřejňuje

Druh veřejné zakázky: služby

Charakteristika veřejné zakázky: podlimitní sektorová

5.2. Předmětem veřejné zakázky je nasazení síťového DLP, jehož hlavním účelem bude ochrana a kontrola dat procházejících mezi technologickými sítěmi a uživatelskou sítí, a uživatelskou sítí a veřejnou sítí Internet. Součástí dodávky jsou následující fáze:

- Před-implementační analýza
- Implementace DLP řešení do prostředí Správy železnic (v případě, že bude v rámci řešení využita)
- Konfigurace a testování nasazeného DLP řešení
- Adopce řešení a školení administrátorů
- Post-implementační podpora nově implementovaných komponent do infrastruktury Správy železnic
- Služby na vyžádání

5.3. Požadavky na tyto fáze jsou podrobně popsány v Příloze č. 2 této Výzvy. Součástí dodávky musejí být také dokumentace skutečného provedení, evidence nasazených pravidel a jejich garantů, včetně evidence použitých signatur s jejich popisem. Dále musí být součástí dodávky veškeré případné licence pro plný běh DLP řešení. Součástí plnění je i testování dodaného řešení. Jedná se hlavně o výkonnostní testy a testy účinnosti jednotlivých pravidel před zavedením do plného provozu. Testování musí probíhat tak, aby neomezilo nebo neohrozilo produkční systémy Správy železnic.

5.4. Bližší specifikace předmětu veřejné zakázky je obsahem této Výzvy jako Příloha č. 2.

5.5. 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. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „***ZoKB***“).

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

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

– *ZTE Corporation, Šen-čen, Čínská lidová republika*“.

Dne 4. ledna 2019 vydal NÚKIB Metodiku k varování ze dne 17. prosince 2018 (dále jen „metodika“), kde jsou mj. určeny i postupy pro aktualizaci analýzy rizik. V souladu s vydanou metodikou zadavatel provedl analýzu rizik související s předmětnou veřejnou zakázkou, jak je jeho povinností podle § 5 a § 8 VoKB. V návaznosti na to zadavatel

identifikoval rizika spojená s výše uvedenými technickými a programovými prostředky jako neakceptovatelná a současně opatření k jejich zvládání, kterým je nepřipuštění použití těchto prostředků v rámci plnění veřejné zakázky.

5.6. V souladu s § 4 odst. 4 ZoKB zadavatel zohledňuje požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro Zadavatelem zajišťované služby informačních systémů v kategorii KII (Kritické informační infrastruktury).

5.7. Zadavatel tak na základě varování NÚKIB, navazující metodiky a provedené analýzy rizik, ve spojení s § 4 odst. 4 ZoKB, nepřipouští v rámci plnění veřejné zakázky použití technických nebo programových prostředků společností (výrobců), které jsou uvedené v současné době platném varování NÚKIB jako hrozba v oblasti kybernetické bezpečnosti.

5.8. Pokud by některý z dodavatelů ve své nabídce nerespektoval zákaz, resp. zadávací podmínku uvedenou v čl. 5.5 Výzvy, tzn. že by pro plnění veřejné zakázky navrhl použití technických nebo programových prostředků výše uvedených společností (výrobců), zadavatel bude postupovat analogicky podle § 48 odst. 2 písm. a) ZZVZ ve spojení s § 48 odst. 8 ZZVZ a přistoupí k vyloučení takového dodavatele z výběrového řízení.

5.9. Veřejná zakázka je spolufinancovaná prostřednictvím Integrovaného regionálního operačního programu (IROP), 5. výzva IROP – Kybernetická bezpečnost – SC 1.1 (ČR), v rámci projektu *„Kybernetická bezpečnost Správy železnic – Dohled a řízení bezpečnosti". Registrační číslo projektu: CZ.06.01.01/00/22_005/0000104*.

6. Předpokládaná hodnota veřejné zakázky

6.1. Předpokládaná hodnota předmětu veřejné zakázky se nezveřejňuje.

7. Doba a místo plnění veřejné zakázky

7.1. Termín zahájení plnění: od okamžiku účinnosti smlouvy

7.2. Termín ukončení plnění: Fáze F6 bude ukončena nejpozději do 42 týdnů od účinnosti smlouvy. Plnění nebude ukončeno dříve než za 5 let od skončení fáze F6. Harmonogram plnění předmětu veřejné zakázky tvoří přílohu č. 4 této Výzvy.

7.3. Místo plnění: Plnění veřejné zakázky bude probíhat především v sídle Zadavatele a sídlech jednotlivých organizačních složek Zadavatele, nebo na jakýchkoli jiných místech, pokud to bude potřebné či vhodné pro realizaci předmětu plnění veřejné zakázky.

8. Sociálně a environmentálně odpovědné zadávání, inovace

8.1. Zadavatel při vytváření zadávacích podmínek, včetně pravidel pro hodnocení nabídek, a výběru dodavatele, postupoval tak, aby v co nejvyšší možné míře naplnil zásady sociálně odpovědného zadávání, environmentálně odpovědného zadávání a inovací tak jak jsou definovány v § 28 odst. 1 písm. p) až r) ZZVZ (dále jen „***odpovědné zadávání***"). Vzhledem k tomu, že jednotlivé postupy odpovědného zadávání nebyly v ZZVZ ani v jiném zákoně taxativně vymezeny a současně je odpovědné zadávání stále se velmi dynamicky vyvíjejícím institutem veřejného zadávání, zadavatel při vytváření podmínek zvažoval použití zejména těch prvků odpovědného zadávání, které byly v době vytváření zadávacích podmínek jednoznačně vymezitelné a vymahatelné, a současně byla u nich vysoká míra jistoty, že zadavatel jejich aplikací neporuší ostatní zásady uvedené v § 6 ZZVZ a také principy 3E vyplývající ze zákona č. 320/2011 Sb. o finanční kontrole ve veřejné správě, ve znění pozdějších předpisů.

8.2. Zadavatel aplikuje ve výběrovém řízení níže uvedené prvky odpovědného zadávání.

8.2.1. Zadavatel pro snížení administrativní náročnosti při zpracování nabídek připravil pro dodavatele vzorové dokumenty (zejména čestná prohlášení), která mohou dodavatelé využít. Vzorové dokumenty (zejména čestná prohlášení) jsou přílohami této Výzvy.

8.2.2. Zadavatel požaduje, aby dodavatel při realizaci veřejné zakázky pro zadavatele zajistil pro své dodavatele (tj. poddodavatele) rovnocenné platební podmínky, jako má sjednány dodavatel se zadavatelem. Prvek odpovědného zadávání a povinnosti dodavatele s ním spojené zadavatel definoval v Závazném vzoru smlouvy, který je Přílohou č. 3 této Výzvy.

8.3. Použití jiných prvků odpovědného zadávání, které byly zadavateli známy při vytváření této Výzvy, není vzhledem k povaze a smyslu zakázky možné z těchto důvodů:

8.3.1. S ohledem na předmět plnění veřejné zakázky je nutné dbát na vysokou profesionalitu dodavatele, kvalifikovaný servis a kybernetickou bezpečnost. S poukazem na tyto skutečnosti není možné do plnění předmětu veřejné zakázky zapojit osoby s nízkou kvalifikací.

8.3.2. Při plnění veřejné zakázky nevznikají negativní dopady na životní prostředí.

9. Požadavky na prokázání splnění podmínek způsobilosti a kvalifikace dodavatele

Dodavatelé jsou povinni prokázat splnění základní a profesní způsobilosti a požadavků zadavatele obsažených v této Výzvě. V případě společné účasti dodavatelů prokazuje základní způsobilost dle čl. 9.1 této Výzvy a profesní způsobilost dle čl. 9.2.1 této Výzvy každý dodavatel samostatně. K prokázání základní a profesní způsobilosti postačí předložení dokladu ve formě prosté kopie. V případě cizojazyčných dokumentů zadavatel požaduje kopie předkládaných dokumentů s překladem do českého jazyka. Doklady ve slovenském jazyce a doklad o vzdělání v latinském jazyce se předkládají bez překladu. Pokud se podle příslušného právního řádu požadovaný doklad nevydává, může být nahrazen čestným prohlášením. Povinnost předložit doklad může dodavatel splnit odkazem na odpovídající informace vedené v informačním systému 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.

Dodavatel prokáže splnění základní a profesní způsobilosti tak, že ke své nabídce přiloží níže uvedené doklady, jimiž doloží:

9.1. **Základní způsobilost** dodavatel v nabídce prokáže ve vztahu k České republice předložením čestného prohlášení zpracovaného v souladu s kapitolou č. 3 přílohy č. 1 této Výzvy:

9.1.1. Způsobilý není dodavatel, který

a) byl v zemi svého sídla v posledních 5 letech před zahájením výběrového 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,

b) má v České republice nebo v zemi svého sídla v evidenci daní zachycen splatný daňový nedoplatek,

c) má v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na veřejné zdravotní pojištění,

d) 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,

e) 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.

9.1.2. Je-li dodavatelem právnická osoba, musí podmínku podle čl. 9.1.1 písm. a) této Výzvy splňovat tato právnická osoba a zároveň každý člen statutárního orgánu. Je-li členem statutárního orgánu dodavatele právnická osoba, musí podmínku podle čl. 9.1.1 písm. a) této Výzvy splňovat

a) tato právnická osoba,

b) každý člen statutárního orgánu této právnické osoby a

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

9.1.3. Účastní-li se výběrového řízení pobočka závodu

a) zahraniční právnické osoby, musí podmínku podle čl. 9.1.1 písm. a) této Výzvy splňovat tato právnická osoba a vedoucí pobočky závodu,

b) české právnické osoby, musí podmínku podle čl. 9.1.1 písm. a) této Výzvy splňovat osoby uvedené v čl. 9.1.2 této Výzvy a vedoucí pobočky závodu.

9.1.4. Účastník výběrového řízení může prokázat obnovení základní způsobilosti analogicky dle § 76 ZZVZ.

9.2. **Splnění profesní způsobilosti** prokáže dodavatel ve vztahu k České republice:

9.2.1. předložením výpisu z obchodního rejstříku nebo jiné obdobné evidence, pokud jiný právní předpis zápis do takové evidence vyžaduje.

9.2.2. Doklady podle čl. 9.2.1 této Výzvy dodavatel nemusí předložit, pokud právní předpisy v zemi jeho sídla obdobnou profesní způsobilost nevyžadují.

9.3. Stáří dokladů

9.3.1. Doklady prokazující základní způsobilost musí prokazovat splnění požadovaného kritéria způsobilosti **nejpozději v době 3 měsíců přede dnem zahájení výběrového řízení**. Den zahájení výběrového řízení je den odeslání této Výzvy prostřednictvím elektronického nástroje.

9.4. **Ekonomická kvalifikace**

9.4.1. Zadavatel nepožaduje.

9.5. **Technická kvalifikace**

9.5.1. Zadavatel požaduje, aby dodavatel ve své nabídce předložil seznam významných zakázek poskytnutých dodavatelem za posledních 5 let před zahájením výběrového řízení. Ze seznamu významných zakázek musí vyplývat, že dodavatel v uvedeném období realizoval:

- alespoň jednu významnou zakázku, jejímž předmětem byla před-implementační analýza, implementace, konfigurace a následná podpora agentless systému prevence úniku dat pro provozovatele kritické infrastruktury nebo pro subjekt provozující významný informační systém nebo informační systém základní služby ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, v minimálním finančním objemu (rozsahu) 3.000.000 Kč bez DPH za tuto významnou zakázku s tím, že cena zahrnuje i cenu licencí;

Splnění tohoto kvalifikačního kritéria dodavatel prokáže formou čestného prohlášení zpracovaného v souladu s kapitolou 5 přílohy č. 1 této Výzvy, z něhož budou vyplývat minimálně tyto informace:

- cena (resp. finanční objem) významné zakázky bez DPH;
- doba jejího poskytnutí;
- identifikace objednatele včetně kontaktu na zodpovědnou osobu, která může zadavateli realizaci významné zakázky potvrdit;
- popis předmětu plnění významné zakázky (v detailu potřebném pro posouzení splnění požadavku na předmět významné zakázky).

9.5.2. Doba „za posledních 5 let před zahájením výběrového řízení" se pro účely tohoto výběrového řízení považuje za splněnou, pokud významná zakázka byla v průběhu této doby dokončena alespoň v rozsahu odpovídajícímu požadavkům zadavatele uvedeným výše. Významná zakázka může být uznána výhradně tehdy, pokud subjekt dokládající poskytnutí příslušné referenční 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 výběrového 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 výběrového řízení, nebo pokud stále probíhají, za předpokladu splnění výše uvedených parametrů (tj. řádné dokončení příslušné části významné zakázky, která naplňuje požadavky Zadavatele na významné zakázky) ke dni konce lhůty pro prokázání kvalifikace. U následné podpory se doba „za posledních 5 let před zahájením zadávacího řízení" považuje za splněnou v případě, pokud následná podpora byla v období posledních 5 let před zahájením výběrového řízení veřejné zakázky poskytována alespoň po dobu 6 měsíců. 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 významné zakázky realizoval.

9.5.3. Zadavatel požaduje, aby dodavatel ve své nabídce předložil seznam osob, které se budou podílet na plnění předmětu veřejné zakázky, bez ohledu na to, zda se jedná o zaměstnance dodavatele nebo osoby v jiném vztahu k dodavateli (dále též „***realizační tým***").

Zadavatel požaduje, aby dodavatel prokázal splnění této části kvalifikace prostřednictvím níže uvedených osob s níže uvedenými požadavky. Splnění této části kvalifikace dodavatel prokáže formou čestného prohlášení zpracovaného v souladu s Přílohou č. 1 – kapitolou 6 přílohy č. 1 této Výzvy.

9.5.4. Jedna osoba nemůže zastávat více níže uvedených rolí. Dodavatel musí mít k dispozici realizační tým složený nejméně z 5 osob, přičemž každá z osob musí zcela splňovat požadavky, alespoň jedné z níže uvedených rolí. U rolí není rozhodné, jaký byl název role v praxi člena realizačního týmu, významný je její skutečný obsah. Požadavky na minimální počet osob pro jednotlivé role a požadavky na obsah role jsou stanoveny níže.

9.5.4.1 **Vedoucí realizačního týmu a garant řešení prevence úniku dat** – tuto roli bude zastávat minimálně 1 osoba

a) má minimálně jednu zkušenost s vedením realizačního týmu v rámci projektu implementace agentless DLP řešení s minimální cenou 2 000 000 Kč bez DPH, kterou získal za posledních 5 let před zahájením výběrového řízení;

b) je držitelem certifikátu CISSP (Certified Information Systems Security Professional) nebo obdobného certifikátu v oboru kybernetické bezpečnosti se zaměřením na ochranu dat a analýzu rizik (za předpokladu, že tento požadavek na certifikaci nesplňuje člen týmu na pozici Specialista ochrany dat a řízení rizik).

9.5.4.1 **Projektový manažer** – tuto roli bude zastávat minimálně 1 osoba

a) má minimálně jednu zkušenost s účastí na projektu implementace agentless DLP řešení s minimální cenou 2 000 000 Kč bez DPH, kterou získal za posledních 5 let před zahájením výběrového řízení.

9.5.4.1 **Seniorní produktový specialista** – tuto roli budou zastávat minimálně 2 osoby, přičemž každá samostatně

a) má minimálně jednu zkušenost s účastí na projektu implementace agentless DLP řešení s minimální cenou 2 000 000 Kč bez DPH, kterou získal za posledních 5 let před zahájením výběrového řízení;

b) je držitelem platné certifikace od výrobce dodávaného řešení, zaměřující se na design architektury a implementaci řešení.

9.5.4.1 **Specialista ochrany dat a řízení rizik** – tuto roli bude zastávat minimálně 1 osoba

a) má minimálně jednu zkušenost s účastí na projektu implementace agentless DLP řešení s minimální cenou 2.000.000 Kč bez DPH, kterou získal za posledních 5 let před zahájením výběrového řízení;

b) je držitelem certifikátu CISSP (Certified Information Systems Security Professional) uvedeného nebo obdobného certifikátu v oboru kybernetické bezpečnosti se zaměřením na ochranu dat a analýzu rizik (za předpokladu, že tento požadavek na certifikaci nesplňuje člen týmu na pozici Vedoucí realizačního týmu a garant řešení prevence úniku dat).

9.5.5. Zadavatel pro vyloučení všech pochybností uvádí, že postačuje, pokud požadavek na certifikaci (držitel uvedeného nebo obdobného certifikátu v oboru kybernetické bezpečnosti se zaměřením na ochranu dat a analýzu rizik: CISSP) splňuje pouze jedna z rolí Vedoucí realizačního týmu a garant řešení prevence úniku dat nebo Specialista ochrany dat a řízení rizik.

9.6. Pokud v účastníkem předložených dokladech k technické kvalifikaci bude finanční hodnota uvedena v jiné měně než CZK, bude částka přepočtena zadavatelem dle posledního čtvrtletního průměrného kurzu devizového trhu příslušné měny k CZK stanoveným a zveřejněným ČNB ke dni zahájení výběrového řízení.

9.7. Certifikáty vyžadované v rámci technické kvalifikace je možné předložit v rámci nabídky v anglickém jazyce bez jejich překladu do českého jazyka.

9.8. Jiný způsob prokázání základní a profesní způsobilosti

9.8.1. Předložením **Výpisu ze seznamu kvalifikovaných dodavatelů**, který je vydáván Ministerstvem pro místní rozvoj, prokáže dodavatel splnění základní způsobilosti dle čl. 9.1 této Výzvy a profesní způsobilosti dle čl. 9.2 této Výzvy v rozsahu, v jakém doklady pokrývají požadavky zadavatele pro plnění veřejné zakázky. V případě, že účastník bude prokazovat základní a profesní způsobilost prostřednictvím Výpisu ze seznamu kvalifikovaných dodavatelů, zadavatel uvádí, že je povinen přijmout výpis ze seznamu kvalifikovaných dodavatelů, pokud k poslednímu dni (viz čl. 15), ke kterému má být prokázána základní způsobilost nebo profesní způsobilost, není výpis ze seznamu kvalifikovaných dodavatelů starší než 3 měsíce. Zadavatel nemusí přijmout výpis ze seznamu kvalifikovaných dodavatelů, na kterém je vyznačeno zahájení řízení podle § 231 odst. 4 ZZVZ. Stejně jako výpisem ze seznamu kvalifikovaných dodavatelů může dodavatel prokázat kvalifikaci osvědčením, které pochází z jiného členského státu, v němž má dodavatel sídlo, a které je obdobou výpisu ze seznamu kvalifikovaných dodavatelů.

9.9. Prokázání kvalifikace prostřednictvím jiných osob

9.9.1. Dodavatel může ekonomickou kvalifikaci, technickou kvalifikaci nebo profesní způsobilost s výjimkou kritéria podle čl. 9.2.1 této Výzvy požadovanou zadavatelem prokázat prostřednictvím jiných osob. Dodavatel je v takovém případě povinen zadavateli předložit

a) doklady prokazující splnění profesní způsobilosti podle čl. 9.2 této Výzvy jinou osobou,

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

c) doklad o splnění základní způsobilosti podle čl. 9.1 této Výzvy 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.

9.9.2. Prokazuje-li dodavatel prostřednictvím jiné osoby kvalifikaci a předkládá doklady podle čl. 9.5 této Výzvy (v rozsahu požadavků na významné dodávky/služby nebo členy realizačního týmu) vztahující se k takové osobě, musí ze smlouvy nebo potvrzení o její existenci podle čl. 9.9.1 písm. d) této Výzvy vyplývat závazek, že jiná osoba bude vykonávat stavební práce či služby, ke kterým se prokazované kritérium kvalifikace vztahuje.

9.9.3. Má se za to, že požadavek podle čl. 9.9.1 písm. d) je splněn, pokud z obsahu smlouvy nebo potvrzení o její existenci podle čl. 9.9.1 písm. d) této Výzvy vyplývá závazek jiné osoby plnit veřejnou zakázku společně a nerozdílně s dodavatelem, to neplatí, pokud smlouva nebo potvrzení o její existenci podle 9.9.1 písm. d) této Výzvy musí splňovat požadavky dle čl. 9.9.2 této Výzvy.

9.9.4. Zadavatel požaduje, aby dodavatel a jiná osoba, jejímž prostřednictvím dodavatel prokazuje ekonomickou kvalifikaci podle čl. 9.4 této Výzvy, nesli společnou a nerozdílnou odpovědnost za plnění veřejné zakázky.

9.9.5. Na kvalifikaci osoby, jejímž prostřednictvím je prokazována kvalifikace, se vztahují pravidla stanovená touto Výzvou pro kvalifikaci dodavatele, za kterého je kvalifikace prokazována.

9.10. Dodavatel, který podal nabídku ve výběrovém řízení, nesmí být současně osobou, jejímž prostřednictvím jiný dodavatel v tomtéž výběrovém řízení prokazuje kvalifikaci.

9.11. Zadavatel si vyhrazuje právo postupovat analogicky k ustanovení § 48 odst. 5 ZZVZ.

10. Požadavky zadavatele na zpracování nabídky

10.1. Účastník předloží úplnou elektronickou verzi nabídky, 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

10.2. Pro tyto účely a v souladu se ZZVZ systém vyžaduje registraci dodavatelů a elektronický podpis založený na kvalifikovaném certifikátu. Podáním nabídky dodavatel 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.

10.3. Dodavatel je oprávněn podat pouze jednu nabídku.

10.4. Nabídka musí obsahovat:

a) identifikační údaje účastníka analogicky dle ustanovení § 28 odst. 1 písm. g) ZZVZ, kontaktní osobu účastníka pro účely této veřejné zakázky, včetně jejích kontaktních údajů (telefon, e-mail),

b) čestné prohlášení k prokázání základní způsobilosti – účastník výběrového řízení v této souvislosti použije kapitolu 2 přílohy č. 1 této Výzvy,

c) doklady prokazující splnění profesní způsobilosti,

d) doklady prokazující splnění technické kvalifikace – účastník výběrového řízení v této souvislosti použije kapitolu 5 a 6 přílohy č. 1 této Výzvy,

e) návrh smlouvy. Závazný vzor smlouvy je uveden jako příloha č. 3 této Výzvy, přičemž účastník není oprávněn vkládat do návrhu smlouvy a jeho obchodních podmínek jiné sankce a závazky vůči zadavateli než ty, které obsahuje příloha č. 3 této Výzvy závazný vzor smlouvy a jeho obchodní podmínky. 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,

f) čestné prohlášení ve vztahu k zakázaným dohodám - účastník je povinen přiložit ke své nabídce čestné prohlášení o tom, že v souvislosti s výběrovým 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. Toto bude předloženo ve formě formuláře obsaženého v kapitole č. 5 přílohy č. 1 této Výzvy,

g) čestné prohlášení ve vztahu k zákonu o registru smluv – účastník výběrového řízení v této souvislosti použije přílohu č. 10 této Výzvy,

h) návrh dodávky, který bude zpracován dle článku 11 této Výzvy – účastník výběrového řízení v této souvislosti použije přílohu č. 5 této Výzvy,

i) seznam poddodavatelů – účastník výběrového řízení v této souvislosti použije kapitolu 8 přílohy č. 1 této Výzvy,

j) ostatní dokumenty, které mají dle účastníka výběrového řízení tvořit nabídku.

10.5. Analogicky dle ustanovení § 28 odst. 2 ZZVZ platí, že nebyla-li nabídka zadavateli doručena ve lhůtě nebo způsobem stanoveným v této Výzvě, k takové nabídce se nepřihlíží.

10.6. Zadavatel doporučuje a preferuje, aby nabídka byla podána za využití krycího listu uvedeného v příloze č. 1 této Výzvy.

11. Návrh dodávky

11.1. Zadavatel definoval v Technické specifikaci, která tvoří přílohu č. 2 této Výzvy, své požadavky na předmět plnění této veřejné zakázky, jejichž splnění je dodavatel povinen ve výběrovém řízení prokázat.

11.2. Každý dodavatel je povinen ve své nabídce předložit svůj návrh řešení a tento popsat. Návrh řešení přitom musí respektovat požadavky zadavatele uvedené v Technické specifikaci, tj. v příloze č. 2 této Výzvy. Dodavatel návrh řešení zpracuje do dokumentu, který je označen jako Návrh dodávky (šablona), a který tvoří přílohu č. 5 této Výzvy.

11.3. Zadavatel předložený návrh řešení v rámci posouzení splnění podmínek účasti ve výběrovém řízení posoudí, a to z toho pohledu, zda v něm byly zohledněny a respektovány všechny požadavky zadavatele uvedené v Technické specifikaci, tj. v příloze č. 2 této Výzvy.

11.4. Pokud dodavatelem předložený návrh řešení nebude vyhovovat požadavkům zadavatele (zadávacím podmínkám), zadavatel přistoupí k vyloučení takového dodavatele, z výběrového řízení (analogicky dle § 48 odst. 2 písm. a) ZZVZ).

12. Registr smluv

12.1. 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***").

12.2. 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.

12.3. Pokud účastník ve smlouvě, která bude nedílnou součástí nabídky, označí její části nebo určité informace dle čl. 12.2 této Výzvy, je účastník povinen předložit Čestné prohlášení. Vzor tohoto prohlášení je zpracován jako příloha č. 10 této Výzvy. 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 a takto znečitelněná smlouva by byla v důsledku toho uveřejněna způsobem odporujícímu ZRS, nese účastník veškerou odpovědnost.

12.4. Výše uvedené čestné prohlášení dle čl. 12.3 této Výzvy účastník nedokládá v případě, že neoznačí ve smlouvě, která bude nedílnou součástí nabídky, žádné takové časti nebo informace ve smyslu čl. 12.2 této Výzvy.

12.5. Účastník odpovídá za správnost a pravdivost veškerých údajů a skutečností, které jím budou uvedeny ve výše uvedeném čestném prohlášení. Zadavatel nebude přezkoumávat jejich pravdivost.

12.6. 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.

13. Poddodavatel

13.1. Zadavatel požaduje, aby účastník výběrového řízení v nabídce:

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

b) předložil seznam poddodavatelů, včetně jejich identifikačních údajů, pokud jsou účastníkovi výběrového řízení známi a uvedl, kterou část veřejné zakázky bude každý z poddodavatelů plnit.

14. Požadavky na způsob zpracování nabídkové ceny

14.1. Zadavatel požaduje, aby účastník výběrového řízení ve své nabídce uvedl celkovou nabídkovou cenu za plnění předmětu této veřejné zakázky, v české měně (Koruna česká), bez daně z přidané hodnoty (DPH).

14.2. Za účelem výpočtu celkové nabídkové ceny v Kč bez DPH bude účastníkem výběrového řízení vyplněna příloha č. 6 této Výzvy. Účastník výběrového řízení je povinen uvést nabídkovou cenou jednotlivých položek v Kč bez DPH - tento údaj účastník výběrového řízení doplní do sloupce E tabulky (pozn. místa určená k vyplnění účastníkem výběrového řízení jsou v tabulce označena oranžovou barvou). Nabídková cena za předpokládaný počet jednotek (pozn. předpokládaný počet jednotek je uveden ve sloupci F tabulky a

pokrývá celou dobu realizace veřejné zakázky) se ve vztahu ke každé části dodávky vypočte automaticky (viz sloupec H tabulky), to samé platí i pro celkovou nabídkovou cenu, která bude předmětem hodnocení nabídek.

14.3. Zadavatel požaduje, aby jednotkové nabídkové ceny byly dodavatelem stanoveny tak, aby byla respektována cenová omezení stanovená pro jednotlivé fáze veřejné zakázky tak, jak jsou uvedeny v příloze č. 6 této Výzvy – Tabulka pro vyplnění nabídkové ceny. Nerespektování těchto požadavků ze strany dodavatele bude považováno za nesplnění zadávacích podmínek.

14.4. Účastník výběrového řízení je povinen vyplnit jednotkovou nabídkovou cenu u všech položek, resp. jednotlivých částí dodávky, uvedených v tabulce. Nevyplnění ceny u některé z položek může být důvodem pro vyloučení dodavatele z výběrového řízení.

14.5. Celková nabídková cena stanovená v tabulce je cenou modelovou, tzn. že jde o předpokládaný objem plnění stanovený pro účely hodnocení nabídek. Pro plnění veřejné zakázky proto budou závazné jednotkové nabídkové ceny (tj. nabídkové ceny uvedené ve sloupci E tabulky).

14.6. Za správné vyplnění cenové tabulky (tj. tabulky, která je součástí přílohy č. 6 této Výzvy), které bude provedeno v souladu se zadávacími podmínkami, odpovídá účastník výběrového řízení.

14.7. Jednotkové ceny musí obsahovat veškeré náklady související s předmětem veřejné zakázky, včetně případné ceny podpory na novou infrastrukturu.

15. Lhůta a místo pro podání nabídky

15.1. Nabídka musí být podána elektronickými prostředky prostřednictvím elektronického nástroje E-ZAK, který je profilem zadavatele, a to v českém jazyce nebo analogicky k ustanovení § 45 odst. 3 ZZVZ. **Zadavatel nepřipouští podání nabídky v listinné podobě ani v jiné elektronické formě mimo elektronický nástroj E-ZAK**.

15.2. Dokumenty musí být do systému E-ZAK vkládány jako jeden soubor nebo více zkomprimovaných souborů ve formátu zip, rar nebo 7z, bez použití hesla. Zkomprimované soubory nesmí obsahovat žádný další zkomprimovaný soubor.

15.3. 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.

15.4. Nabídky podávané v elektronické podobě dodavatel doručí do konce stanovené lhůty pro podání nabídek, a to prostřednictvím elektronického nástroje E-ZAK na adrese https://zakazky.spravazeleznic.cz/

15.5. Lhůta pro podání nabídek je uvedena v elektronickém nástroji E-ZAK.

15.6. Nabídky podané po uplynutí lhůty pro podání nabídky nebudou otevřeny. Zadavatel bezodkladně vyrozumí účastníka o tom, že jeho nabídka byla podána po uplynutí lhůty pro podání nabídky.

16. Vysvětlení Výzvy

16.1. Zadavatel může Výzvu vysvětlit, pokud takové vysvětlení, případně související dokumenty, uveřejní stejným způsobem, jako uveřejnil tuto Výzvu, anebo pokud je zašle všem dodavatelům, kterým zaslal Výzvu nebo kteří si ji vyzvedli, v případě, že Výzva nebyla uveřejněna.

16.2. Dodavatel je oprávněn po zadavateli požadovat vysvětlení Výzvy. Žádost o vysvětlení Výzvy doručí dodavatel ve stanovené lhůtě písemnou formou, a to elektronicky. Zadavatel bude na žádosti o vysvětlení Výzvy odpovídat prostřednictvím elektronického

nástroje E-ZAK na adrese: https://zakazky.spravazeleznic.cz/. Pokud o vysvětlení Výzvy písemně požádá dodavatel, zadavatel vysvětlení uveřejní, odešle nebo předá včetně přesného znění žádosti bez identifikace tohoto dodavatele. Zadavatel není povinen vysvětlení poskytnout, pokud není žádost o vysvětlení doručena včas, a to alespoň 3 pracovní dny před uplynutím lhůty pro podání nabídek dle bodu 15.5 této Výzvy. Zadavatel se může rozhodnout vysvětlení poskytnout i na opožděnou žádost o vysvětlení.

16.3. Pokud je žádost o vysvětlení Výzvy doručena včas a zadavatel neuveřejní, neodešle nebo nepředá vysvětlení do 3 pracovních dnů, prodlouží lhůtu pro podání nabídek nejméně o tolik pracovních dnů, o kolik přesáhla doba od doručení žádosti o vysvětlení Výzvy do uveřejnění, odeslání nebo předání vysvětlení 3 pracovní dny.

16.4. Pokud by spolu s vysvětlením Výzvy zadavatel provedl i změnu zadávacích podmínek, postupuje podle následujícího článku této Výzvy.

17. Změna Výzvy

17.1. Zadávací podmínky obsažené ve Výzvě může zadavatel změnit nebo doplnit před uplynutím lhůty pro podání nabídek. Změna nebo doplnění Výzvy musí být uveřejněna nebo oznámena dodavatelům stejným způsobem jako zadávací podmínka, která byla změněna nebo doplněna.

17.2. Pokud to povaha doplnění nebo změny Výzvy vyžaduje, zadavatel současně přiměřeně prodlouží lhůtu pro podání nabídek. V případě takové změny nebo doplnění Výzvy, která může rozšířit okruh možných účastníků výběrového řízení, prodlouží zadavatel lhůtu tak, aby od odeslání změny nebo doplnění Výzvy činila nejméně celou svou původní délku.

18. Kritérium hodnocení nabídek

18.1. Kritéria hodnocení.

18.1.1. Hodnocení nabídek bude provedeno analogicky dle § 114 a násl. ZZVZ podle jejich ekonomické výhodnosti dle níže uvedených dílčích hodnotících kritérií.

18.1.2. Hodnotícím kritériem pro výběr nejvýhodnější nabídky v rámci ekonomické výhodnosti nabídek je nejvýhodnější poměr ceny a kvality, a to na základě následujících kritérií a vah, které představují podíl jednotlivých kritérií hodnocení na celkovém hodnocení:

Kritérium hodnocení	Váha
Nabídková cena	70 %
Kvalita	30 %

18.2. Nabídková cena

18.2.1. V rámci dílčího kritéria hodnocení „Nabídková cena" bude hodnocena celková nabídková cena stanovená způsobem dle čl. 14 této Výzvy. Nabídková cena relevantní pro hodnocení nabídky bude v nabídce uvedena v Tabulce pro vyplnění nabídkové ceny dle přílohy č. 6 této Výzvy na listu „Nabídková cena" v buňce H31, kde tato se vypočte automaticky.

18.2.2. Jako výhodnější bude v tomto kritériu hodnocena nabídka, která bude obsahovat nižší nabídkovou cenu za plnění v Kč bez DPH.

18.2.3. Nejvýhodnější nabídce, tj. nabídce s nejnižší celkovou nabídkovou cenou ze všech hodnocených nabídek bude přiřazeno 100 bodů. Ostatním nabídkám bude přiřazena bodová hodnota stanovená násobkem čísla 100 a poměru celkové nabídkové ceny předložené v nejvýhodnější nabídce (tj. v nabídce s nejnižší nabídkovou cenou) k celkové nabídkové ceně hodnocené nabídky. Takto získaný počet bodů bude vynásoben váhou dílčího hodnotícího kritéria „Nabídková cena" a následně matematicky zaokrouhlen na dvě desetinná místa.

18.2.4. Výpočet odpovídá následujícímu vzorci:

$$\frac{\text{Výše nejnižší celkové nabídkové ceny bez DPH}}{\text{Výše hodnocené celkové nabídkové ceny bez DPH}} * 100 * 0{,}7$$

18.3. Kvalita

18.3.1. Předmětem hodnocení nabídek v rámci dílčího hodnotícího kritéria „Kvalita" bude rozsah certifikace u osob na klíčových pozicích týmu dodavatele a dále rozsah výpočetního výkonu (tj. množství výpočetních prostředků, které dodavatel bude potřebovat zajistit mimo již využívané prostředky SŽ, a to minimálně v rozsahu celkového počtu procesorových jader a množství paměti RAM v jednotlivých prvcích, které poběží v prostředí SŽ). V rámci tohoto dílčího kritéria budou nabídce dodavatele přiřazeny body dle níže uvedené tabulky:

bodová škála: CPU (počet jader) + RAM(GB) = Výpočetní výkon	Výpočetní výkon min.	Výpočetní výkon max.	Počet bodů
	<	0	100
	1	5	80
	6	10	60
	11	15	40
	16	20	20
	21	>	0
Seniorní produktový specialista 1	Certifikace k produktům Cisco FirePower nebo Palo Alto na téma konfigurace, architektura, deployment.		10
Seniorní produktový specialista 2	Certifikace k produktům Cisco FirePower nebo Palo Alto na téma konfigurace, architektura, deployment.		10
Specialista ochrany dat a řízení rizik	Certifikace k produktům Cisco FirePower nebo Palo Alto na téma konfigurace, architektura, deployment.		10

18.3.2. Přidělování bodů v rámci dílčího hodnotícího kritéria „Kvalita" bude probíhat tak, že zadavatel přidělí body dle výše uvedené tabulky. Počet bodů bude dán součtem bodů získaných za rozsah výpočetního výkonu (tj. množství výpočetních prostředků, které dodavatel bude potřebovat zajistit mimo již využívané prostředky SŽ, a to minimálně v rozsahu celkového počtu procesorových jader a množství paměti RAM v jednotlivých prvcích, které poběží v prostředí SŽ) a rozsah certifikace jednotlivých členů týmu. Takto dosažené body se přepočtou tak, že každá hodnocená nabídka obdrží počet bodů, který

odpovídá poměru počtu získaných bodů k maximálnímu možnému zisku bodů v daném kritériu (tj. 130 bodů) a násobku čísla 100 při zohlednění váhy kritéria (30 %) a následném zaokrouhlení na dvě desetinná místa. Bodovým hodnocením se pro účely tohoto výpočtu rozumí celkový součet bodů, který získal příslušný účastník dle pravidel uvedených ve výše uvedené tabulce.

18.3.3. Celkový počet bodů v rámci dílčího hodnotícího kritéria „Kvalita" se vypočte dle následujícího vzorce:

$$\frac{\text{Bodové hodnocení hodnocené nabídky}}{130} * 100 \quad * 0{,}3$$

18.3.4. Zadavatel požaduje, aby účastník výběrového řízení ve své nabídce uvedl údaje o CPU (počet jader) a RAM (GB) (výpočetní výkon) a dále údaje o certifikaci členů týmu, které mají být předmětem hodnocení v rámci dílčího hodnotícího kritéria „Kvalita", a to ve formě vyplněné Tabulky pro vyplnění údajů pro dílčí hodnotící kritérium „Kvalita", jejíž závazný vzor tvoří přílohu č. 15 této Výzvy, a aby doložil příslušné certifikáty členů týmu, jež mají být předmětem hodnocení. Čl. 9.7 této Výzvy se pro tyto certifikáty uplatní obdobně.

18.4. Celkové hodnocení nabídek

18.4.1. Ekonomicky nejvýhodnější nabídkou bude nabídka, která získá nejvyšší počet bodů součtem výsledných hodnot dílčích hodnotících kritérií „Nabídková cena" a „Kvalita".

18.4.2. Zadavatel sečte u každého účastníka obdržené body z obou hodnotících kritérií. Jako nejvýhodnější nabídka bude vybrána nabídka účastníka, která v součtu obou hodnotících kritérií získá nejvíce bodů při splnění všech zákonných a zadávacích podmínek. Pro vyloučení pochybností zadavatel uvádí, že jednotlivé hodnoty budou při výpočtech hodnocení zaokrouhlovány vždy na 2 desetinná místa.

18.4.3. V případě celkové rovnosti bodů je ekonomicky nejvýhodnější nabídkou nabídka, která získala větší počet bodů v rámci kritéria „Nabídková cena". V případě celkové rovnosti bodů a rovnosti bodů v rámci kritéria „Nabídková cena" rozhodne o pořadí nabídky čas podání těchto nabídek, přičemž platí, že lépe se umístila ta nabídka, která byla podána dříve.

18.4.4. Pokud je v zadávacím řízení jediný účastník, může být zadavatelem vybrán bez provedení hodnocení.

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

19.1. 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.

19.2. 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 uvedeno v kapitole č. 4 přílohy č. 1 této Výzvy, ve své nabídce.

19.3. Vybraný dodavatel je povinen předložit k výzvě zadavatele analogicky dle § 122 odst. 3 písm. b) ZZVZ doklady a informace, z nichž nepochybně vyplyne, že vybraný dodavatel

i všichni poddodavatelé, jimiž vybraný dodavatel prokazuje kvalifikaci, splňují podmínku neexistence střetu zájmů ve smyslu § 4b Zákona o střetu zájmů a tohoto článku. 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 analogicky ve smyslu § 122 odst. 6 ZZVZ, a to i ve vztahu k příslušnému poddodavateli, prostřednictvím kterého vybraný dodavatel prokazoval část kvalifikace.

19.4. V případě postupu účastníka v rozporu s čl. 19 Výzvy bude účastník vyloučen z výběrového řízení.

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

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

20.2. Zadavatel nezadá veřejnou zakázku účastníku výběrového řízení, pokud je to v rozporu s mezinárodními sankcemi podle zákona upravujícího provádění mezinárodních sankcí.

20.3. Pokud se mezinárodní sankce podle čl. 20.2 této Výzvy vztahuje na:

a) účastníka výběrového řízení, může ho zadavatel vyloučit z účasti ve výběrovém řízení, nebo

b) vybraného dodavatele, vyloučí ho zadavatel z účasti ve výběrovém řízení.

20.4. Pokud se mezinárodní sankce podle čl. 20.2 této Výzvy vztahuje na poddodavatele:

a) účastníka výběrového řízení, může zadavatel požadovat nahrazení poddodavatele, nebo

b) vybraného dodavatele, musí zadavatel požadovat nahrazení poddodavatele.

20.5. Na základě požadavku zadavatele podle čl. 20.4 této Výzvy musí účastník výběrového řízení poddodavatele nahradit nejpozději do konce zadavatelem stanovené přiměřené lhůty. Pokud nedojde k nahrazení poddodavatele, platí, že se na účastníka výběrového vztahuje zákaz zadání veřejné zakázky.

20.6. 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[1] (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 čl. 20.6 písm. a) této Výzvy, nebo

c) fyzická nebo právnická osoba, subjekt nebo orgán, které jednají jménem nebo na pokyn některého ze subjektů uvedených v čl. 20.6 písm. a) nebo b) této Výzvy,

[1] 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

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

20.7. Zadavatel požaduje, aby účastník sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti ve výběrovém řízení, ani žádný z jeho poddodavatelů nebo jiných osob, jejichž způsobilost je využívána ve smyslu směrnic o zadávání veřejných zakázek, **nebyli** osobami dle čl. 20.6 této Výzvy a Nařízení č. 833/2014.

20.8. Dle čl. 2 nařízení Rady (EU) č. 269/2014 ze dne 17. března 2014, o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, ve znění pozdějších předpisů (dále jen „***Nařízení č. 269/2014***"), a dalších prováděcích předpisů k tomuto Nařízení č. 269/2014[2], 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 vedené na sankčních seznamech***").

20.9. Zadavatel dále požaduje, aby účastník sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti ve výběrovém 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.

20.10. Splnění zadávacích podmínek stanovených zadavatelem dle tohoto článku prokáže účastník předložením čestného prohlášení, jehož vzorové znění je uvedeno v kapitole č. 6 přílohy č. 1 této Výzvy, ve své nabídce.

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

20.12. V případě postupu účastníka v rozporu s čl. 20.6 až 20.11 Výzvy bude účastník vyloučen z výběrového řízení.

21. Další požadavky zadavatele

21.1. Zadavatel si vyhrazuje právo výběrové řízení až do okamžiku uzavření smlouvy kdykoliv zrušit bez uvedení důvodu.

21.2. Zadavatel si vyhrazuje právo změnit, upřesnit či doplnit tuto Výzvu k podání nabídky až do skončení lhůty pro podání nabídky.

---

[2] 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.

21.3. Zadavatel si vyhrazuje právo v průběhu výběrového řízení postupovat analogicky dle § 46 a § 113 ZZVZ.

21.4. Zadavatel si vyhrazuje právo vyloučit účastníka řízení analogicky dle ustanovení § 48 ZZVZ.

21.5. Další podmínky zadavatele pro uzavření smlouvy analogicky dle § 104 ZZVZ:

21.5.1. Vybraný dodavatel je povinen zadavateli na písemnou výzvu učiněnou analogicky dle § 122 odst. 3 písm. b) ZZVZ předložit doklady a informace dle čl. 19.3 a čl. 20.11 této Výzvy.

21.5.2. Neposkytnutí součinnosti vybraným dodavatelem dle tohoto článku je důvodem pro vyloučení vybraného dodavatele.

21.6. Zadavatel a vybraný dodavatel jsou povinni bez zbytečného odkladu po oznámení rozhodnutí o výběru uzavřít smlouvu. Vybraného dodavatele, který nesplnil povinnost dle tohoto článku, může zadavatel z výběrového řízení vyloučit. Zadavatel si vyhrazuje právo postupovat analogicky dle § 125 odst. 1 a 2 věta první ZZVZ.

21.7. Zadavatel nepřipouští varianty nabídek.

21.8. Zadavatel upozorňuje, že preferuje uzavírání smluv v elektronické podobě prostřednictvím kvalifikovaných elektronických podpisů. V případě, že dodavatel není schopen k takovému postupu zajistit zadavateli součinnost, sdělí tuto skutečnost ve své nabídce, a to prostřednictvím krycího listu, který je přílohou č. 1 této Výzvy.

22. Opatření k ochraně důvěrných informací

22.1. Zadavatel uvádí, že součástí Výzvy jsou rovněž informace, které mají charakter důvěrných informací (dále také jen „***Důvěrné informace***"). Jedná se o dokument s názvem „Popis prostředí", který tvoří přílohu č. 7 této Výzvy, o dokument s názvem „Informace k systémům SŽ", který tvoří přílohu č. 8 této Výzvy, o dokument s názvem "Interní předpis Zadavatele – Politika klasifikace aktiv", který tvoří přílohu č. 9 této Výzvy a o dokument s názvem "Interní předpis Zadavatele - Provozní politika prvků v působnosti systému řízení bezpečnosti informací", který tvoří přílohu č. 14 této Výzvy.

22.2. Zadavatel uveřejnil tyto části Výzvy na profilu zadavatele jako složku s názvem „Neveřejná část Výzvy" a tuto složku zahesloval.

22.3. Části Výzvy ve smyslu tohoto článku budou s ohledem na Důvěrné informace v nich obsažené poskytnuty dodavatelům pouze v elektronické podobě, a to výhradně na základě písemné žádosti dodavatele o jejich poskytnutí zaslané společně s podepsaným návrhem Dohody o ochraně důvěrných informací (dále jen „***NDA***") ze strany dodavatele, a to ve znění obsaženém jako příloha č. 13 této Výzvy.

22.4. Po doručení žádosti včetně podepsaného návrhu NDA umožní zadavatel dodavateli přístup k částem Výzvy obsahující Důvěrné informace způsobem podrobně popsaným v NDA. Za písemnou žádost dodavatele ve smyslu tohoto článku Výzvy je považováno doručení podepsaného návrhu NDA.

Přílohy tvořící nedílnou součást této Výzvy:

č. 1. Krycí list nabídky

č. 2. Bližší specifikace předmětu plnění (Technická specifikace)

č. 3. Závazný vzor smlouvy (vč. příloh)

č. 4. Harmonogram plnění

č. 5. Návrh dodávky (šablona)

č. 6. Tabulka pro vyplnění nabídkové ceny

č. 7. Popis prostředí SŽ

č. 8. Informace k systémům SŽ

č. 9. Interní předpis Zadavatele – Politika klasifikace aktiv

č. 10. Čestné prohlášení k zákonu o registru smluv

č. 11. Výstupy z PTK

č. 12. Platforma SŽ

č. 13. Dohoda o ochraně důvěrných informací

č. 14. Interní předpis Zadavatele – Provozní politika prvků v působnosti systému řízení bezpečnosti informací

č. 15. Tabulka pro vyplnění údajů pro dílčí hodnotící kritérium „Kvalita"

Jiří Svoboda
15.09.2025 14:14
Podepsáno elektronicky

.....

Bc. Jiří Svoboda, MBA
generální ředitel

SPRÁVA ŽELEZNIC

Příloha č. 1 Výzvy k podání nabídky

Krycí list nabídky k veřejné zakázce s názvem „Zavedení komplexního síťového řešení prevence úniku dat (DLP) pro non-Microsoft systémy v prostředí Správy železnic“ vedené pod č.j. 80219/2025-SŽ-GŘ-O25

Obsah

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

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

Kapitola 1. Základní údaje k nabídce

Zadavatel: **Správa železnic, státní organizace**

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

IČO 70994234, DIČ CZ70994234

Účastník: *jméno osoby/název firmy*

Sídlo:

IČO ……, DIČ …….

Zastoupená *údaje o statutárním orgánu nebo jiné oprávněné osobě*

Kontaktní osoba ve věci podání nabídky: xxxxxxxxxxxxxxxxxx

Email kontaktní osoby: xxxxxxxxxxxxxx

Účastník prohlašuje, že veškeré údaje uvedené v tomto krycím listu, který je Přílohou č. 1 Výzvy k podání nabídky na veřejnou zakázku zadávanou jako podlimitní sektorovou veřejnou zakázku, jsou pravdivé, úplné a odpovídají skutečnosti. Účastník si je vědom důsledků záměrného uvedení nepravdivých údajů, které v rovině tohoto výběrového řízení mohou vést až k vyloučení Účastníka z výběrového řízení.

ÚDAJE O MOŽNOSTI ELEKTRONICKÉHO UZAVŘENÍ SMLOUVY:

Účastník disponuje platným zaručeným elektronickým podpisem ve smyslu zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů[1]?	Zvolte položku.[2]
(pokud na výše uvedenou otázku odpověděl dodavatel kladně)	
Účastník je ochoten použít platný zaručený elektronický podpis pro uzavření smlouvy se zadavatelem v elektronické formě?	Zvolte položku.[3]

[1] Takový certifikát v českém prostředí vydávají následující poskytovatelé: a) **Česká pošta, s. p.,** b) **eIdentity a.s.,** c) **První certifikační autorita, a.s.**

[2] Účastník vybere jednu z možností.

[3] Účastník vybere jednu z možností.

Kapitola 2. Čestné prohlášení o splnění základní způsobilosti

Účastník, který podává tuto nabídku, tímto čestně prohlašuje, že není účastníkem, který:

a) byl v zemi svého sídla v posledních 5 letech před zahájením výběrového řízení pravomocně odsouzen pro trestný čin uvedený v příloze č. 3 k zákonu č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, nebo obdobný trestný čin podle právního řádu země sídla účastníka; k zahlazeným odsouzením se nepřihlíží,

b) má v České republice nebo v zemi svého sídla v evidenci daní zachycen splatný daňový nedoplatek,

c) má v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na veřejné zdravotní pojištění,

d) 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,

e) 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 účastníka.

Výše uvedené podmínky splňuje jak účastník (coby právnická osoba), tak každý člen jeho statutárního orgánu.

Kapitola 3. Čestné prohlášení účastníka o střetu zájmů

Účastník, který podává tuto nabídku, tímto čestně prohlašuje, že:

f) **není** obchodní společností, ve které veřejný funkcionář uvedený v § 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

g) žádní poddodavatelé, jimiž prokazuje kvalifikaci ve výběrovém řízení, **nejsou** obchodní společností, 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.

Účastník dále čestně prohlašuje, že dostane-li se Účastník nebo poddodavatel, jímž prokazoval kvalifikaci ve výběrovém řízení, do střetu zájmů dle § 4b Zákona o střetu zájmů, a to kdykoliv až do okamžiku ukončení výběrového 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.

Kapitola 4. Čestné prohlášení účastníka k neuzavření zakázaných dohod

Účastník, který podává tuto nabídku, tímto čestně prohlašuje, že:

h) 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

i) nepřipravoval části nabídek, které mají být hodnoceny podle kritérií hodnocení, ve vzájemné shodě s jiným účastníkem téhož výběrového 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.

Kapitola 5. Čestné prohlášení o splnění technické kvalifikace – seznam významných zakázek

Účastník, který podává tuto nabídku, tímto čestně prohlašuje, že za posledních 5 let před zahájením výběrového řízení poskytoval významné zakázky definované v článku 9.5.1 Výzvy k podání nabídky, a že veškeré údaje níže uvedené jsou pravdivé.

Významná zakázka č. 1:

Název a popis předmětu plnění významné zakázky, z něhož bude vyplývat splnění všech požadavků Zadavatele dle článku 9.5.1 Výzvy k podání nabídky	**Doba realizace významné zakázky od - do (měsíc a rok)**	**Celkový finanční objem významné zakázky (v Kč bez DPH)**	**Identifikace objednatele**
			Název/obchodní firma: **Sídlo:** **IČO:** **Kontaktní osoba pro ověření údajů uvedených dodavatelem:** **Telefon:** **E-mail:**

Kapitola 6. Čestné prohlášení o splnění technické kvalifikace – seznam členů realizačního týmu

Účastník, který podává tuto nabídku, prohlašuje, že v případě, že se stane vybraným dodavatelem, bude plnit veřejnou zakázku v požadovaném rozsahu následujícím realizačním týmem, ledaže dojde k jeho změně v souladu se zadávacími podmínkami či uzavřenou smlouvou. Účastník dále prohlašuje, že veškeré údaje níže uvedené jsou pravdivé

Role č. 1 – Vedoucí realizačního týmu a garant řešení prevence úniku dat: [dodavatel na toto místo doplní jméno, příjmení a titul osoby, která bude tuto roli zastávat]

Vztah člena realizačního týmu k dodavateli[4]	[DOPLNÍ DODAVATEL]
Zkušenost s vedením realizačního týmu v rámci projektu implementace agentless DLP řešení s minimální cenou 2 000 000 Kč bez DPH za posledních 5 let před zahájením výběrového řízení	[DOPLNÍ DODAVATEL] Označení zkušenosti: Doba realizace zkušenosti: Označení objednatele včetně kontaktu pro ověření uvedených informací: Náplň zkušenosti:
Název certifikátu **(certifikát CISSP nebo jiný obdobný platný certifikát)**	[DOPLNÍ DODAVATEL – DODAVATEL OZNAČÍ CERTIFIKÁT, JEHOŽ JE TENTO ČLEN REALIZAČNÍHO TÝMU DRŽITELEM, A SOUČASNĚ PŘILOŽÍ KOPII CERTIFIKÁTU]

Role č. 2 – Projektový manažer: [dodavatel na toto místo doplní jméno, příjmení a titul osoby, která bude tuto roli zastávat]

Vztah člena realizačního týmu k dodavateli[5]	[DOPLNÍ DODAVATEL]
Zkušenost s účastí na projektu implementace agentless DLP řešení s minimální cenou 2 000 000 Kč bez DPH za posledních 5 let před zahájením výběrového řízení	[DOPLNÍ DODAVATEL] Označení zkušenosti: Doba realizace zkušenosti: Označení objednatele včetně kontaktu pro ověření uvedených informací:

[4] Dodavatel uvede některou z následujících alternativ: pracovní poměr, dohoda o pracovní činnosti, dohoda o provedení práce, člen statutárního orgánu, OSVČ, příp. další možnost. Pro vyloučení pochybností Zadavatel uvádí, že pokud je člen realizačního týmu OSVČ, bude považován 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.

[5] Dodavatel uvede některou z následujících alternativ: pracovní poměr, dohoda o pracovní činnosti, dohoda o provedení práce, člen statutárního orgánu, OSVČ, příp. další možnost. Pro vyloučení pochybností Zadavatel uvádí, že pokud je člen realizačního týmu OSVČ, bude považován 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.

	Náplň zkušenosti:

Role č. 3 – Seniorní produktový specialista: [dodavatel na toto místo doplní jméno, příjmení a titul osoby, která bude tuto roli zastávat]

Vztah člena realizačního týmu k dodavateli[6]	[DOPLNÍ DODAVATEL]
Zkušenost s účastí na projektu implementace agentless DLP řešení s minimální cenou 2 000 000 Kč bez DPH za posledních 5 let před zahájením výběrového řízení	[DOPLNÍ DODAVATEL] Označení zkušenosti: Doba realizace zkušenosti: Označení objednatele včetně kontaktu pro ověření uvedených informací: Náplň zkušenosti:
Název certifikátu **(platná certifikace od výrobce dodávaného řešení, zaměřující se na design architektury a implementaci řešení)**	[DOPLNÍ DODAVATEL – DODAVATEL OZNAČÍ CERTIFIKÁT, JEHOŽ JE TENTO ČLEN REALIZAČNÍHO TÝMU DRŽITELEM, A SOUČASNĚ PŘILOŽÍ KOPII CERTIFIKÁTU]

Role č. 3 – Seniorní produktový specialista: [dodavatel na toto místo doplní jméno, příjmení a titul osoby, která bude tuto roli zastávat]

Vztah člena realizačního týmu k dodavateli[7]	[DOPLNÍ DODAVATEL]
Zkušenost s účastí na projektu implementace agentless DLP řešení s minimální cenou 2 000 000 Kč bez DPH za posledních 5 let před zahájením výběrového řízení	[DOPLNÍ DODAVATEL] Označení zkušenosti: Doba realizace zkušenosti: Označení objednatele včetně kontaktu pro ověření uvedených informací: Náplň zkušenosti:

[6] Dodavatel uvede některou z následujících alternativ: pracovní poměr, dohoda o pracovní činnosti, dohoda o provedení práce, člen statutárního orgánu, OSVČ, příp. další možnost. Pro vyloučení pochybností Zadavatel uvádí, že pokud je člen realizačního týmu OSVČ, bude považován 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.

[7] Dodavatel uvede některou z následujících alternativ: pracovní poměr, dohoda o pracovní činnosti, dohoda o provedení práce, člen statutárního orgánu, OSVČ, příp. další možnost. Pro vyloučení pochybností Zadavatel uvádí, že pokud je člen realizačního týmu OSVČ, bude považován 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.

Název certifikátu **(platná certifikace od výrobce dodávaného řešení, zaměřující se na design architektury a implementaci řešení)**	[DOPLNÍ DODAVATEL – DODAVATEL OZNAČÍ CERTIFIKÁT, JEHOŽ JE TENTO ČLEN REALIZAČNÍHO TÝMU DRŽITELEM, A SOUČASNĚ PŘILOŽÍ KOPII CERTIFIKÁTU]

Role č. 4 – Specialista ochrany dat a řízení rizik: [dodavatel na toto místo doplní jméno, příjmení a titul osoby, která bude tuto roli zastávat]

Vztah člena realizačního týmu k dodavateli[8]	[DOPLNÍ DODAVATEL]
Zkušenost s účastí na projektu implementace agentless DLP řešení s minimální cenou 2 000 000 Kč bez DPH za posledních 5 let před zahájením výběrového řízení	[DOPLNÍ DODAVATEL] Označení zkušenosti: Doba realizace zkušenosti: Označení objednatele včetně kontaktu pro ověření uvedených informací: Náplň zkušenosti:
Název certifikátu **(certifikát CISSP nebo jiný platný certifikát s obdobným nebo vyšším rozsahem)**	[DOPLNÍ DODAVATEL – DODAVATEL OZNAČÍ CERTIFIKÁT, JEHOŽ JE TENTO ČLEN REALIZAČNÍHO TÝMU DRŽITELEM, A SOUČASNĚ PŘILOŽÍ KOPII CERTIFIKÁTU]

[8] Dodavatel uvede některou z následujících alternativ: pracovní poměr, dohoda o pracovní činnosti, dohoda o provedení práce, člen statutárního orgánu, OSVČ, příp. další možnost. Pro vyloučení pochybností Zadavatel uvádí, že pokud je člen realizačního týmu OSVČ, bude považován 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.

Kapitola 7. Čestné prohlášení účastníka o splnění podmínek v souvislosti se situací na Ukrajině

Účastník, který podává tuto nabídku, tímto čestně prohlašuje, že:

a) on sám jakožto dodavatel, ani jeho poddodavatelé, nejsou osobami, na něž se vztahuje zákaz zadání veřejné zakázky analogicky ve smyslu § 48a ZZVZ, tj. zejména, že

   i. on sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti ve výběrovém 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

   ii. on sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti ve výběrovém 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***")[9].

b) přestane-li on sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti ve výběrovém řízení, nebo některý z jeho poddodavatelů nebo jiných osob, jejichž způsobilost je využívána ve smyslu evropských směrnic o zadávání veřejných zakázek, splňovat výše uvedené podmínky, k nimž se toto četné prohlášení vztahuje, a to kdykoliv až do okamžiku ukončení výběrového řízení, oznámí tuto skutečnost bez zbytečného odkladu, nejpozději však **do 3 pracovních dnů** ode dne, kdy přestal splňovat výše uvedené podmínky, k nimž se toto četné prohlášení vztahuje, zadavateli veřejné zakázky.

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

[9] 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.

Kapitola 8. Seznam poddodavatelů

Účastník, který podává nabídku, tímto předkládá seznam poddodavatelů, s jejichž pomocí předpokládá plnění veřejné zakázky.

Identifikace poddodavatelů dodavatele[10]			**Část plnění veřejné zakázky, které má dodavatel v úmyslu zadat poddodavateli (specifikace a procentuální podíl)**
1.	**Obchodní firma / jméno a příjmení**	[doplní dodavatel]	[doplní dodavatel]
	Sídlo / Místo podnikání	[doplní dodavatel]	
	Identifikační číslo	[doplní dodavatel]	
	Prostřednictvím poddodavatele prokazována kvalifikace	ANO/NE [doplní dodavatel]	

[10] V případě více poddodavatelů zkopíruje dodavatel tabulku tolikrát, kolikrát bude třeba.

V …… dne ……

Jméno a Příjmení

funkce osoby

Příloha č. 2 Výzvy

SPRÁVA ŽELEZNIC

Bližší specifikace předmětu plnění (Technická specifikace)

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

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

Obsah

1 Seznam pojmů a zkratek

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

Přehled zkratek a pojmů:

Zkratka	Popis
Agent-based	DLP řešení založené na agentech
Agentless	DLP řešení bez instalace agentů na každé zařízení v síti
AS-IS	Stav v současnosti, zpravidla architektury, prostředí, informačního systému apod.
DLP	Řešení prevence uniku dat používaná zejména v rámci NGFW *(Data Loss Prevention)*
Dodavatel	Účastník, který bude vybrán SŽ, se stane Dodavatelem
HTTP, DNS, SNMP, SMTP, FTP, TFTP	Komunikační protokoly
HW	Hardware
ICT	Informační a komunikační technologie (Information and Communication Technologies)
IS	Informační systém
ISMS	Information Security Management System
KII	Kritická informační infrastruktura
LDAP, RADIUS, TACACS+, SAML	Autentizační protokoly
MD	Člověkoden, pracovní čas jedné osoby odpovídající jednomu pracovnímu dni, tedy typicky 8 hodin *(Man-Day)*
MPIP	Microsoft Purview Information Protection
MS	Microsoft Corporation, americký výrobce především SW a provozovatel cloudového prostředí MS Azure

OCR	Optické rozpoznávání znaků *(Optical Character Recognition)*
OS	Operační systém *(Operating System)*
PTK	Předběžná tržní konzultace je nástroj umožňující zadavateli veřejné zakázky oslovit dodavatele s požadavkem na informace ohledně zamýšlené připravované veřejné zakázky *(Request for Information)*
RBAC	Řízení přístupů na základě rolí
SaaS	Software jako služba, je model poskytování SW uživatelům formou předplatného, kde veškerá odpovědnost za údržbu je na straně dodavatele. *(Software as a service*)
SIEM	Řešení zabezpečení, které organizacím pomáhá detekovat bezpečnostní události, analyzovat je a reagovat na ně dříve, než způsobí škody v provozu firmy/organizace. *(Security Information and Event Management)*
SLA	Smluvní nastavení záruk, úrovně, dostupnosti a kvality služeb atd. *(Service-Level Agreement)*
Smlouva o dílo	Smlouva o dílo – Zavedení komplexního síťového řešení prevence úniku dat (DLP) pro non-Microsoft systémy v prostředí Správy železnic. Závazný vzor Smlouvy o dílo je přílohou č. 3 Výzvy k podání nabídky
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 („Zadavatel“)
TDS	Technologické datové sítě SŽ, jedná se o více VRF zpravidla vyhrazených pro OT, běžně se v prostředí SŽ nazývají také „Techlan“
UAS	Logická uživatelsko-aplikační síť SŽ, zahrnuje VRF v MPLS sítích a lokální VLAN, běžně se nazývá také „Intranet SŽ“
Účastník	Subjekt, který se účastní tohoto výběrového řízení o realizaci veřejné zakázky s názvem „Zavedení komplexního síťového řešení prevence úniku dat (DLP) pro non-Microsoft systémy v prostředí Správy železnic“

VZ	Veřejná zakázka „Zavedení komplexního síťového řešení prevence úniku dat (DLP) pro non-Microsoft systémy v prostředí Správy železnic“
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
ZoKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů

2 Úvod

Tento dokument je přílohou a nedílnou součástí Výzvy k podání nabídky na veřejnou zakázku s názvem „Zavedení komplexního síťového řešení prevence úniku dat (DLP) pro non-Microsoft systémy v prostředí Správy železnic", pro organizaci Správa železnic (SŽ). Dokument popisuje technické a jiné požadavky na veřejnou zakázku.

V rámci výběrového řízení je poptáváno provedení analýzy dat ve vyjmenovaných informačních systémech, dále ve spolupráci se SŽ určení klasifikace dat z těchto systémů a vytvoření knihovny detekčních signatur a reakčních pravidel pro detekci dat klasifikovaných jinak, než jako veřejná.

Dále je součástí poptávky návrh a implementace technických opatření pro zajištění prevence úniku dat v rámci prostředí SŽ. Tato opatření musí minimálně kontrolovat přenos dat mezi prostředím technologických sítí a uživatelskou sítí SŽ (interní perimetr) a mezi uživatelskou sítí a datovým provozem přecházejícím do veřejné sítě Internet (externí perimetr).

Navržené řešení nesmí modifikovat přenášená data jakýmkoliv způsobem, ani předpokládat jakoukoliv předchozí modifikaci dat (vyjma označení pomocí labelů s využitím nástroje Microsoft Purview Information Protection). Řešení dále nesmí ke své plné funkčnosti vyžadovat běh jakýchkoliv lokálních agentů. Případné použití lokálních agentů pro rozšíření funkcionalit DLP řešení na individuálních zařízeních je akceptovatelné pouze po dohodě se Zadavatelem. Je však vhodné, aby DLP řešení umělo pracovat s již označenými daty konkrétně se štítky vytvořené nástrojem Microsoft Purview Information Protection.

Dodavatel zaškolí administrátory, kteří na systém budou přistupovat. Současně se školením Dodavatel vytvoří návrh adopční (komunikační) kampaně, která představí implementované změny uživatelům SŽ, tzn. jaký má systém účel a co pro ně jeho nasazení obnáší.

2.1 Očekávání od DLP řešení

SŽ očekává dosažení následujících cílů v rámci plnění veřejné zakázky:

- Snížení rizik v souvislostí s narušením parametru důvěrnosti pro definovaný rozsah citlivých dat.
- Identifikace citlivých dat v rámci specifikovaných systémů v prostředí SŽ a vytvoření pravidel pro jejich ochranu.
- Naplnění legislativních požadavků v kontextu ochrany citlivých dat v klíčových systémech.
- Automatizovaný přístup k detekci a zamezení úniku citlivých dat.
- Definování a nastavení způsobu reportingu detekovaných událostí, řešení incidentů a způsob úpravy detekčních a blokovacích pravidel.
- Předání know-how ohledně správy a konfigurace na interní tým SŽ pro správu řešení a politik, které vyžadují detailní znalost interního prostředí a pravidel pro nakládání s citlivými údaji.

- Definovaní detekčních pravidel a politik, které budou svým přístupem minimalizovat invazivní zásahy do činnosti uživatelů a systémů při dodržení zásad ochrany informací.

Požadavky na rozsah řešení

Pro naplnění projektu ze strany Dodavatele je zapotřebí splnit následující:

- Vytvoření knihovny pravidel pro detekci klasifikovaných dat z vybraných systémů.
- Vytvoření knihovny signatur detekovaných dat.
- Ve spolupráci se Zadavatelem klasifikovat data v jednotlivých systémech.
- Zmapování toků dat z a do jednotlivých vybraných systémů.
- Návrh architektury řešení DLP (navržená architektura nesmí měnit celkovou cenu ani další hodnotící kritéria a musí být odsouhlasena Zadavatelem).
- Případná nová infrastruktura, potřebná pro DLP řešení, musí běžet ve virtualizované formě.
- Dodávka všech licencí potřebných k provozu navrhovaného DLP řešení.
- Implementace a konfigurace DLP řešení.
- Zaškolení vybraných zaměstnanců SŽ pro administraci a užívání DLP řešení.
- Vytvoření adopční kampaně pro zaměstnance SŽ.

2.2 Předmět plnění veřejné zakázky

Předmět plnění této veřejné zakázky je primárně založen na provedení analýzy a klasifikace informačních aktiv obsažených v systémech uvedených v rámci přílohy č. 8 Výzvy k podání nabídky s názvem – Informace k systémům SŽ z pohledu, a dále navržení, implementaci a konfiguraci DLP řešení do prostředí SŽ. Dodávka je rozdělena do následujících fází:

- Před-implementační analýza.
- Implementace DLP řešení do prostředí SŽ (v případě, že bude v rámci řešení využita).
- Konfigurace a testování nasazeného DLP řešení.
- Adopce řešení a školení administrátorů.
- Post-implementační podpora nově implementovaných komponent do infrastruktury SŽ.
- Služby na vyžádání.

Požadavky na tyto fáze jsou podrobně popsány v dalších částech tohoto dokumentu.

Součástí dodávky musejí být také dokumentace skutečného provedení, evidence nasazených pravidel a jejich garantů, včetně evidence použitých signatur s jejich popisem.

Dále musí být součástí dodávky veškeré případné licence pro plný běh DLP řešení.

Součástí plnění je i testování dodaného řešení. Jedná se hlavně o výkonnostní testy a testy účinnosti jednotlivých pravidel před zavedením do plného provozu. Testování musí probíhat tak, aby neomezilo nebo neohrozilo produkční systémy SŽ.

2.3 Oblasti, které nejsou předmětem plnění veřejné zakázky

Pro vyloučení pochybností SŽ uvádí, že následující oblasti **nejsou** předmětem plnění veřejné zakázky:

- Proxy servery či jiné zdroje dat pro DLP řešení.
- HW prostředky uvedené v rámci nabídky či jiné kapacity výpočetního výkonu (budou dodány ze strany Zadavatele). Dodavatel může maximálně požadovat celkový výpočetní výkon 160 jader a 768 GB RAM, kde jedna instance může být maximálně 128 jader a 512 GB, a zbylé instance pak maximálně 32 jader a 128 GB.
- Systém pro označování (štítkování) dokumentů a informací. Konfigurace IDS, IPS aj.

3 Současný stav a popis prostředí

Současný stav ICT prostředí, relevantní pro nasazení síťového DLP, je uveden v příloze č. 7 Výzvy k podání nabídky s názvem – Popis prostředí, kde jsou uvedeny základní informace k výchozímu stavu připravenosti prostředí SŽ pro nasazení řešení.

4 Požadavky na plnění

Plnění veřejné zakázky se musí skládat z níže uvedených fází:

1. Před-implementační analýza.
2. Implementace DLP řešení do prostředí SŽ (v případě, že bude v rámci řešení využita).
3. Konfigurace a testování DLP řešení.
4. Adopce DLP řešení a školení administrátorů.
5. Post-implementační podpora nově implementovaných částí DLP řešení a služby na vyžádání.

4.1 Požadavky na navrhované DLP řešení

Navrhované DLP řešení musí minimálně splňovat následující požadavky:

4.1.1 Funkční požadavky

- Inspekce přenášených dat, a to minimálně protokoly HTTP, DNS, SNMP, SMTP, FTP, TFTP, Telnet (s již odstraněným šifrováním).
- Na externím perimetru jsou definovány signatury na základě finger print, regex slovník. Systém musí být schopen pracovat s českým jazykem. Na interním perimetru stačí definice signatur na úrovni regex.
- Dešifrování provozu šifrovaného pomocí TLS, minimálně ve verzích 1.2 a 1.3 a jejich následná inspekce, viz výše.
- DLP řešení musí podporovat autorizaci uživatelů pomocí rolí (tzv. RBAC)
- Rozdělení přístupových rolí minimálně na:

  - Pouze náhled, pouze editace pravidel, plný administrátor.
- Řešení musí být schopno se napojit na externí poskytovatele identit, minimálně na Active Directory, Entra ID.
- Řešení musí podporovat minimálně následující autentizační protokoly - LDAP, RADIUS, TACACS+, SAML, Kerberos.
- Dodané řešení musí poskytovat možnost zapnutí vícefaktorové autentizace.
- Řešení musí logovat události, minimálně v rozsahu uvedeném v § 22 VoKB.
- Řešení musí být schopno odesílat logovací záznamy na vzdálený server pomocí protokolu Syslog ve formátu CEF nebo LEEF 2.0.
- V případě detekce musí být schopno minimálně následujících reakcí:
  - Nahlásit sepnutí pravidla
  - Změnit, nebo vymazat citlivý obsah
  - Zablokovat přenos dat.
- Řešení musí být schopno odesílat záznam bezpečnostní události o sepnutí pravidla do systému SIEM, nebo Log management systému, a to minimálně pomocí protokolu Syslog. Součástí události musí být minimálně jednoznačná identifikace zdrojového a cílového zařízení, identifikace detekčního pravidla, které bylo sepnuto, časová známka, data, která způsobila sepnutí pravidla a reakce systému.
- Na externím perimetru musí DLP řešení disponovat OCR.

4.1.2 Nefunkční požadavky

- Nesmí být omezena propustnost linky (min. propustnost stejná jako kapacita linky, tj. 7x 1 Gb/s a 1x 2 Gb/s na interním perimetru a 1x 5 Gb/s na externím perimetru).
- Musí běžet v módu HA, nebo v módu, kdy v případě výpadku není nijak omezena komunikace na síti.
- Řešení nesmí běžet plně v cloudovém prostředí, minimální forma musí být hybridní režim, kdy část systému DLP běží na lokální infrastruktuře Zadavatele a pro pokročilé funkce rozpoznání dat, které neodpovídají žádné ze zavedených signatur, může být využito cloudové prostředí.
- Datové centrum hostující případnou část řešení musí být na území EU.
- V případě využití open source komponent je nutné prokázat zasmluvněnou platnou podporu vývojáře a zavázat se k jejímu nákupu na minimálně dalších 5 let, nebo prokázat správou vlastní vývojové větve po dobu minimálně 5 let a její využití v jiných dodávkách s hodnotou min. 2 000 000,- Kč bez DPH.

4.2 Před-implementační analýza

Cílem před-implementační analýzy je popsat minimálně následující oblasti:

- Analýzu dat v rámci jednotlivých vybraných systémů a ve spolupráci se Zadavatelem jejich klasifikace.
- Analýzu toku dat z a do jednotlivých vybraných systémů a identifikace možných cest úniku dat, které nelze pokrýt stávajícími technologiemi SŽ.
- Vytvoření knihovny signatur pro detekci dat v rámci DLP klasifikovaných jinak než veřejná, včetně popisu jednotlivých signatur.

- Vytvoření knihovny pravidel, pro reakce na detekovaná data nasaditelná do DLP řešení.
- Analýzu aktuálně nasazeného systému Microsoft Purview, nasazovaných štítků a pravidel. Analýza by měla odhalit případné kolize provozu nezávislých DLP řešení.
- Dále pak součástí návrhu musí být dokumentované řešení případných nalezených kolizí se systémem MS Purview Information Protection (MPIP). Navržená architektura by měla klást důraz na co nejlepší spolupráci systémů již provozovaných v prostředí SŽ, a pokud je to žádoucí, i jejich vzájemnou integraci (např. využití štítků z MPIP).
- Nezbytnou součástí této fáze je pak vznik detailního harmonogramu dalších fází a z toho vycházející seznam předpokládaných požadavků na součinnost ze strany Dodavatele.
- Předložení testovacích scénářů a jejich schválení ze strany Zadavatele. Zadavatel se zároveň zavazuje dodat připravené sady testovacích dat nejpozději v den před plánovaným testováním (viz dodaný harmonogram).
- Předložení návrhu architektury. Navrhovaná architektura nesmí navyšovat cenu ani HW prostředky (CPU a RAM), které byly indikovány v rámci nabídky ve výběrovém řízení. Součástí návrhu architektury musí být detailní rollback scénář, popisující odstranění jednotlivých změn provedených na infrastruktuře SŽ a její uvedení do původního stavu před začátkem implementace nebo konfigurace DLP řešení.

4.2.1 Předmět akceptace fáze Před-implementační analýza

Předmětem akceptace této fáze je následující:

- Dokument zahrnující analýzu dat z vybraných systémů, obsahující minimálně popis vystupujících dat, jejich klasifikaci a šablony pro detekci.
- Dokument obsahující analýzu nasazení síťového DLP do prostředí s nasazeným MS Purview Information Protection. Analýza musí obsahovat identifikaci možných kolizí systémů a jejich odstranění a návrhy pro lepší spolupráci obou systémů.
- Dokument obsahující analýzu datových toků z a do vybraných informačních systémů s identifikací míst, která nejsou pokryta ochranou síťového DLP.
- Dokument obsahující katalog pravidel pro implementaci a jejich popis.
- Dokument obsahující detailní harmonogram implementace.
- Dokument obsahující seznam předpokládaných požadavků na součinnost Zadavatele.
- Dokument obsahující testovací scénáře.
- Dokument obsahující návrh architektury řešení.

Akceptace probíhá v souladu s dokumentem Zvláštní obchodní podmínky pro Zakázky v oblasti ICT (viz Příloha č. 5 Přílohy č. 3 Výzvy k podání nabídek (Závazný vzor smlouvy) - Zvláštní obchodní podmínky pro Zakázky v oblasti ICT).

4.3 Dodávka licencí

- Dodávka všech licencí potřebných k provozu navrhovaného DLP řešení, minimálně po dobu 5 let od akceptace fáze F6 a F7 ze strany SŽ (viz Příloha č. 4 Výzvy k podání nabídky s názvem – Harmonogram plnění).

4.3.1 Předmět akceptace fáze Dodávka licencí

- Potřebné licence k provozu navrhovaného DLP řešení pro plný běh v rámci SŽ, minimálně po dobu 5 let od akceptace fáze F6 a F7ze strany SŽ.

Akceptace probíhá v souladu s dokumentem Zvláštní obchodní podmínky pro Zakázky v oblasti ICT (viz Příloha č. 5 Přílohy č. 3 Výzvy k podání nabídek (Závazný vzor smlouvy) - Zvláštní obchodní podmínky pro Zakázky v oblasti ICT).

4.4 Implementace DLP řešení

Tato fáze závisí na návrhu DLP řešení. V případě, že navrhované DLP řešení nevyžaduje implementaci nové infrastruktury do prostředí SŽ a vystačí si s nástroji, které má SŽ již k dispozici, nebude tato fáze ze strany Dodavatele využita.

V opačném případě je v rámci této fáze nutné nasadit celé navrhované DLP řešení do infrastruktury SŽ a napojit ho na požadované zdroje dat, případně další nezbytnou infrastrukturu (NTP, identitní databáze aj.).

4.4.1 Předmět akceptace fáze Implementace DLP řešení

Předmětem akceptace této fáze je následující (pokud bude využita ze strany Dodavatele):

- Kompletně nasazené DLP řešení do infrastruktury SŽ (má k dispozici všechny specifikované funkcionality, má napojeny všechny zdroje dat a veškeré další vyžadované činnosti jsou pouze konfiguračního charakteru).
- Nasazeným DLP řešením musí procházet všechna data, která jsou v rámci analýzy identifikována jako data, která je zapotřebí monitorovat a data překračující jeden z určených perimetrů (interní, externí).

4.5 Konfigurace DLP řešení

Tato fáze obnáší hlavně nasazení vyspecifikovaných pravidel a konfiguraci řešení pro jejich plné fungování a maximální efektivitu. Konečná konfigurace musí zvládnout dešifrovat provoz šifrovaný protokolem SSL/TLS ve verzích minimálně 1.2 a 1.3. Musí také umět odhalit klasifikovaná data, minimálně v protokolech HTTP, DNS, TFTP, SMTP, SNMP, FTP, TFTP a Telnet.

4.5.1 Předmět akceptace fáze Konfigurace DLP řešení

Předmětem akceptace této fáze je následující:

- Dokument popisující stav skutečného provedení. Dokument musí obsahovat aktuální architekturu systému a popis předávané konfigurace systému se zachycením všech aktuálních schopností systému (ne pouze minimálního rozsahu).
- Systém, kerý je plně nakonfigurovaný a připravený k otestování ze strany SŽ a následně připraven k ostrému spuštění. Součástí i je zavedení potřebných úživatelů, přidělení oprávnění a předání administrátorských účtů zástupcům SŽ atd.

Akceptace probíhá v souladu s dokumentem Zvláštní obchodní podmínky pro Zakázky v oblasti ICT (viz Příloha č. 5 Přílohy č. 3 Výzvy k podání nabídek (Závazný vzor smlouvy) - Zvláštní obchodní podmínky pro Zakázky v oblasti ICT).

4.6 Testování DLP řešení

V rámci této fáze také proběhne otestovaní funkčních schopností DLP řešení a detekčních schopností každého z nasazených pravidel.

Po otestování funkčnosti jednotlivých pravidel musí proběhnout zátěžové testy k ověření celkové konfigurace, viz akceptační kritéria.

4.6.1 Předmět akceptace fáze Testování DLP řešení

- Úspěšné otestování dekrypce provozu.
- Úspěšné otestování schopnosti detekce všech nasazených pravidel (každé pravidlo musí úspěšně detekovat informace, pro jejichž detekci bylo vytvořeno na základě dokumentace pravidla. Data pro testování budou poskytnuta ze strany SŽ). Otestování funkčnosti pravidla proběhne na všech protokolech vyjmenovaných v dokumentaci skutečného provedení, ve kterých má nástroj schopnost záchytu.
- Úspěšně provedené výkonnostní testy (systém musí zvládnout zpracovat min. 1 Gb/s na každém prostupu interního perimetru, v případě agregovaných linek pak součet kapacit těchto agregovaných linek a min. 5 Gb/s dat na externím perimetru).
- Úspěšně provedené testy výpadku DLP řešení.

Testování provede SŽ nebo subjekt, který bude určen ze strany SŽ.

4.7 Testovací provoz

Po ověření funkčnosti v rámci F5 bude následovat tříměsíční testovací provoz. Nálezy vzešlé z tohoto testovacího provozu musejí být následně, nebo ještě v době testovacího provozu, odstraněny.

4.7.1 Předmět akceptace fáze Testovací provoz

- Vypořádání všech nálzů vzniklých v rámci testovacího provozu

Akceptace probíhá v souladu s dokumentem Zvláštní obchodní podmínky pro Zakázky v oblasti ICT (viz Příloha č. 5 Přílohy č. 3 Výzvy k podání nabídek (Závazný vzor smlouvy) - Zvláštní obchodní podmínky pro Zakázky v oblasti ICT).

4.8 Adopce DLP řešení a školení administrátorů

Adopční část fáze spočívá ve vytvoření adopční kampaně pro zaměstnance SŽ. Adopční kampaň bude složena z pětiminutového videa a informačního emailu. Adopční kampaň má za účel informovat zaměstnance SŽ o účelu systému, jeho schopnostech a vlivu na práci zaměstnanců.

Školení zahrnuje:

- Školení administrátorů řešení v celkové délce školení 16 hodin (maximálně 25 účastníků).
- Účast na školení musí být stvrzena prezenční listinou.
- Všechna školení proběhnou v prostorách SŽ za přítomnosti školitele/školitelů Dodavatele v hybridním režimu (osobně, s možností vzdáleného přístupu), ze všech školení bude pořízen video záznam pro potřeby dalšího školení pracovníků SŽ.

4.8.1 Předmět akceptace fáze Adopce DLP řešení a školení administrátorů

Předmětem akceptace této Fáze je následující:

- Dokument (formátu informačního posteru) a video soubor (cca 5 min) pro adopční kampaň.
- Provedení školení administrátorů.

4.9 Post-implementační podpora nově nasazených komponent do infrastruktury SŽ a služby na vyžádání

Součástí dodávky bude i pětiletá podpora na celkové řešení vyjma komponent, které jsou již aktuálně součástí infrastruktury SŽ a aktuálně spadají pod smlouvu o podpoře. Podpora, která bude poskytována po ukončení fáze 3.5 (viz Příloha č. 4 Výzvy k podání nabídky s názvem - Harmonogram plnění), bude zahrnovat SLA na případně vyskytující se chyby a pravidelnou profylaxi celého řešení jednou za 3 měsíce. Součástí podpory jsou dále pravidelné upgrady systému a aplikace bezpečnostních patchů (či mitigace zranitelnosti), a to nejpozději do týdne od vydání výrobcem, a u kritických zranitelností nejpozději do 24 hodin po vydání patche, nebo mitigace.

Dodavatel poskytne SŽ služby na vyžádání, přičemž půjde o služby dvojího charakteru, což vyplývá z tabulky uvedené níže. Maximální souhrn těchto služeb bude činit 30 MD za celou dobu trvání smlouvy, čerpání bude probíhat dle konkrétních potřeb SŽ.

SŽ požaduje uvést cenu za následující položky ve formě ceny za 1 MD a celkové ceny za položku podle předpokládaného objemu čerpání:

Položka	Předpokládané čerpání v MD
Služba konzultační technické podpory dodaného řešení (technické a metodické otázky související s provozem a rozvojem řešení)	20
Změnová řízení, zakázkový vývoj, doplnění řešení	10

Celková cena za výše uvedené položky musí být součástí cenové nabídky Dodavatele.

SŽ není povinna služby na vyžádání čerpat.

5 Fáze dodávky a akceptační milníky

Dodávka má být dodána v níže uvedených fázích. Každá z níže uvedených fází musí být SŽ separátně akceptována nejpozději v termínu uvedeném v Harmonogramu, s výjimkou F8, kde post-implementační podpora bude akceptovaná na bázi měsíčních výkazů práce a akceptace služeb na vyžádání bude specifikována v rámci konkrétních objednávek. SŽ akceptuje výstupy dané Fáze, jestliže je Dodavatel provedl v šíři a kvalitě požadované v zadávacích podmínkách této veřejné zakázky. V opačném případě je Dodavatel povinen napravit nedostatky dodávky.

Fáze	Popis
F1	Fáze Před-implementační analýza
F2	Fáze Dodávka licencí
F3	Fáze Implementace DLP řešení (pokud bude ze strany Dodavatele využito)
F4	Fáze Konfigurace DLP řešení
F5	Testování DLP řešení
F6	Testovací provoz
F7	Fáze Adopce DLP řešení a školení administrátorů
F8	Fáze Post-implementační podpora nově nasazených komponent do infrastruktury SŽ a služby na vyžádání

Příloha č. 3 Výzvy

Smlouva o dílo – „Zavedení komplexního síťového řešení prevence úniku dat (DLP) pro non-Microsoft systémy v prostředí Správy železnic"

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

uzavřená podle ustanovení § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen **„Občanský zákoník"** nebo **„OZ"**).

Objednatel: **Správa železnic, státní organizace**
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze pod sp. zn. A 48384
Praha 1 - Nové Město, Dlážděná 1003/7, PSČ 110 00
IČO 70994234, DIČ CZ70994234
zastoupená **Bc. Jiřím Svobodou, MBA**, generálním ředitelem
(dále též jen „**Objednatel**" nebo „**SŽ**")

Zhotovitel: [DOPLNÍ DODAVATEL *jméno osoby/název firmy*]
[DOPLNÍ DODAVATEL *údaje o zápisu v evidenci*]
[DOPLNÍ DODAVATEL *sídlo*]
IČO [DOPLNÍ DODAVATEL], DIČ [DOPLNÍ DODAVATEL]
Bankovní spojení: [DOPLNÍ DODAVATEL]
Číslo účtu: [DOPLNÍ DODAVATEL]
[DOPLNÍ DODAVATEL *údaje o statutárním orgánu nebo jiné oprávněné osobě*]
(dále též jen „**Zhotovitel**" nebo „**Dodavatel**")

(dále jednotlivě též jen „**Strana**" nebo společně „**Strany**" a **„Smlouva"**)

Tato Smlouva byla uzavřena na základě výsledku výběrového řízení veřejné zakázky s názvem „Zavedení komplexního síťového řešení prevence úniku dat (DLP) pro non-Microsoft systémy v prostředí Správy železnic", č.j. veřejné zakázky 80219/2025-SŽ-GŘ-O25 (dále jen „**Veřejná zakázka**" a „**Zadávací řízení**") Objednatelem jako zadavatelem, neboť nabídka Dodavatele podaná na Veřejnou zakázku (dále jen **„Nabídka"**) byla Objednatelem vyhodnocena jako ekonomicky nejvýhodnější.

Veřejná zakázka je spolufinancovaná prostřednictvím Integrovaného regionálního operačního programu (IROP), 5. výzva IROP – Kybernetická bezpečnost – SC 1.1 (ČR), v rámci projektu *„Kybernetická bezpečnost Správy železnic – Dohled a řízení bezpečnosti". Registrační číslo projektu: CZ.06.01.01/00/22_005/0000104*.

Jednotlivá ustanovení této Smlouvy tak budou vykládána s ohledem a v souladu se zadávacími podmínkami Veřejné zakázky. V případě kolize ustanovení obsažených v jednotlivých

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384
Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČ: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

dokumentech smluvní dokumentace mají přednost ustanovení obsažená v následujících dokumentech v uvedeném pořadí (pokud není výslovně uvedeno jinak):

1) Vlastní text této Smlouvy;
2) Přílohy č. 1 až 3 této Smlouvy;
3) Příloha č. 5 této Smlouvy – Zvláštní obchodní podmínky pro Zakázky v oblasti ICT (dále jen „**ZOP**");
4) Příloha č. 6 této Smlouvy – Obchodní podmínky ke Smlouvě o dílo (dále jen „**OOP**");
5) Příloha č. 7 této Smlouvy – Platforma SŽ
6) Ostatní dokumenty zadávací dokumentace, resp. Výzvy k podání nabídek na Veřejnou zakázku či zmiňované v této Smlouvě vč. Návrhu dodávky předloženého v rámci Nabídky Dodavatele.

Pokud nevyplývá z této Smlouvy jinak, mají pojmy s velkými počátečními písmeny význam definovány v ZOP, nebo OOP. Pro vyloučení jakýchkoliv pochybností Strany uvádějí, že pokud je v této Smlouvě obsažen článek se shodným názvem jako v ZOP, OOP nebo jiném smluvním dokumentu, neznamená to, že by článek této Smlouvy plně nahrazoval příslušné články v jiných smluvních dokumentech, pokud není výslovně uvedeno jinak; obdobné platí pro vztahy mezi jinými smluvními dokumenty.

1 Účel Smlouvy

1.1 Objednatel jako subjekt povinný v souladu s ustanoveními § 3 písm. c) a d) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále také „**ZoKB**"), musí provádět bezpečnostní opatření (§ 5 ZoKB) v rozsahu nezbytném pro zajištění kybernetické bezpečnosti informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury. Jedním ze způsobů, jak naplnit tyto povinnosti, je zavedení komplexního síťového řešení prevence úniku dat (DLP) pro non-Microsoft systémy v prostředí SŽ.

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:

1.3.1 právních předpisů;

1.3.2 Smlouvy a jejích příloh;

1.3.3 zadávací dokumentace, resp. Výzvy k podání nabídek Veřejné zakázky;

1.3.4 Nabídky a

1.3.5 Interních předpisů SŽ (dále jen „**Interní předpisy**"), přičemž se za Interní předpisy pro účely této Smlouvy považují 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 provedení analýzy dat ve vyjmenovaných informačních systémech, dále ve spolupráci se SŽ určení klasifikace dat z těchto systémů a vytvoření knihovny

detekčních signatur a reakčních pravidel pro detekci dat klasifikovaných jinak, než jako veřejná. Dále je součástí dodávky návrh a implementace technických opatření pro zajištění prevence úniku dat v rámci prostředí SŽ, konfigurace a testování nasazeného DLP řešení, adopce řešení a školení administrátorů, post-implementační podpora nově implementovaných komponent do infrastruktury SŽ a služby na vyžádání.

Součástí dodávky musejí být také dokumentace skutečného provedení, evidence nasazených pravidel a jejich garantů, včetně evidence použitých signatur s jejich popisem. Dále musí být součástí dodávky veškeré případné licence pro plný běh DLP řešení. Součástí plnění je i testování dodaného řešení. Jedná se hlavně o výkonnostní testy a testy účinnosti jednotlivých pravidel před zavedením do plného provozu. Testování musí probíhat tak, aby neomezilo nebo neohrozilo produkční systémy SŽ.

2.3 Bližší požadavky na Předmět díla jsou vymezeny zejména, nikoliv však výlučně, v příloze č. 1 *Specifikace plnění dle této Smlouvy* (dále jen „**Příloha č. 1**").

2.4 Provedení Díla spočívá v provedení následujících **oblastí** dílčích činností ze strany Zhotovitele podrobně definovaných v části 4 Přílohy č. 1 této Smlouvy:

2.4.1 Před-implementační analýza.

2.4.2 Implementace DLP řešení do prostředí SŽ (v případě, že bude v rámci řešení využita).

2.4.3 Konfigurace a testování DLP řešení.

2.4.4 Adopce DLP řešení a školení administrátorů.

2.4.5 Post-implementační podpora nově implementovaných částí DLP řešení a služby na vyžádání.

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

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

2.7 Zhotovitel se zavazuje vyřešit Požadavky Objednatele dle servisního modelu C1 vymezeného v části 12 ZOP. Nezvolí-li Objednatel výslovně v rámci požadavku jinou kategorii, jedná se o požadavek kategorie B. Zhotovitel bude poskytovat Helpdesk v režimu 3 ve smyslu čl. 10.3 ZOP.

3 Místo plnění

3.1 Místem plnění této Smlouvy je především sídlo Objednatele a sídla jednotlivých organizačních složek Objednatele, nebo jakákoliv jiná místa, pokud je to potřebné či vhodné pro provedení Díla.

3.2 Přípravné práce je Zhotovitel oprávněn realizovat na svém vlastním technickém vybavení, což však nezakládá jakýkoliv nárok Zhotovitele na navýšení Ceny díla v souvislosti s následnou realizací Díla u Objednatele.

4 Doba plnění

4.1 Fáze F6 bude ukončena nejpozději do 42 týdnů od účinnosti Smlouvy. Plnění dle této Smlouvy nebude ukončeno dříve než za 5 let od skončení fáze F6. (dále jen „**doba trvání Smlouvy**")

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

4.3 Pokud není stanoveno jinak, je Zhotovitel povinen provádět Dílo v termínech uvedených v závazném harmonogramu realizace Díla obsaženém v příloze č. 3 této Smlouvy (dále jen „**Harmonogram**").

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

5 Cena díla

5.1 Celková cena za splnění závazku Zhotovitele provést Dílo v rozsahu dle této Smlouvy, tj. Cena díla, je uvedena pod položkou Nabídková cena celkem v příloze č. 2 této Smlouvy (dále jen „**Příloha č. 2**").

5.2 Ceny, a to jak jednotkové ceny, tak nabídková cena celkem, 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 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).

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

5.4 Ceny obsažené v Příloze č. 2 této Smlouvy jsou uvedeny bez DPH. V případě změny zákonné sazby DPH není třeba uzavírat dodatek k této Smlouvě, ledaže o to Objednatel požádá.

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

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

6 Platební podmínky

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

6.1.1 První platební milník: Výzva k úhradě ve výši jednotkové ceny za položky označené v Příloze č. 2 této Smlouvy takto: Fáze F1 - Před-implementační analýza a Fáze F2 - Dodávka licencí – Dodávka veškerých licencí potřebných k provozu navrhovaného DLP řešení, která je tvořena činnostmi uvedenými v části 4.2 a 4.3 Přílohy č. 1 této Smlouvy;

6.1.2 Druhý platební milník: Výzva k úhradě ve výši jednotkové ceny za položky označené v Příloze č. 2 této Smlouvy takto: Fáze F3 - Implementace DLP řešení, Fáze F4 - Konfigurace DLP řešení, Fáze F6 - Testovací provoz, které jsou tvořeny činnostmi uvedenými v části 4.4, 4.5 a 4.7 Přílohy č. 1 této Smlouvy;

6.1.3 Třetí platební milník: Výzva k úhradě ve výši jednotkové ceny za položku označenou v Příloze č. 2 této Smlouvy takto: Fáze F7 - Adopce DLP řešení a školení administrátorů, která je tvořena činnostmi uvedenými v části 4.8 Přílohy č. 1 této Smlouvy;

6.2 Zhotovitel je dále oprávněn doručit Objednateli Výzvu k úhradě vždy za každý měsíc, v němž došlo k akceptaci (bez výhrad) plnění na základě Objednávky Služeb na vyžádání dle čl. 10 této Smlouvy, a to ve výši součinu počtu MD dle Objednávky či Objednávek a ceny za jednu MD dle příslušné položky ceny *Služby na vyžádání* uvedené Příloze č. 2 této Smlouvy. Zhotovitel je dále oprávněn doručit Objednateli Výzvu k úhradě za každý měsíc po akceptaci (bez výhrad) služeb Post-implementační podpora nově nasazených komponent do infrastruktury SŽ, a to ve výši ceny za příslušný měsíc dle příslušné položky ceny *Post-implementační podpora nově nasazených komponent do infrastruktury SŽ* uvedené Příloze č. 2 této Smlouvy.

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

6.4 Výzvu k úhradě doručí Zhotovitel Objednateli jedním z následujících způsobů:

6.4.1 V listinné podobě na adresu:

Správa železnic, státní organizace
Centrální finanční účtárna Čechy
Náměstí Jana Pernera 217
530 02 Pardubice

6.4.2 V elektronické podobě na adresu:

ePodatelnaCFU@spravazeleznic.cz

6.4.3 prostřednictvím datové schránky:

uccchjm

6.5 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.

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

6.7 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.

6.8 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.

6.9 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.

7 Akceptační řízení

7.1 Samostatnému akceptačnímu řízení dle části 8 ZOP a tohoto článku této Smlouvy podléhají všechny fáze F1, F2, F3, F4, F5, F6 a F7 dle Přílohy č. 2 této Smlouvy.

7.2 Každá Fáze plnění, podléhající samostatnému Akceptačnímu řízení, se považuje za ukončenou akceptací (bez výhrad) posledního dílčího plnění uvedeného pro příslušnou Fázi v části 4 Přílohy č. 1 této Smlouvy. Akceptační kritéria pro každou dílčí část jednotlivých Fází vyplývají z části 4 Přílohy č. 1 této Smlouvy, přičemž se jedná o výstupy, které jsou uvedeny u každé fáze plnění.

7.3 Smluvní strany stanovují, že 30denní lhůta dle čl. 8.1.9 ZOP se pro účely této Smlouvy zkracuje na 5 kalendářních dní, s výjimkou fáze F2, u které je tato lhůta zkrácena na 2 kalendářní dny.

7.4 Zhotovitel bere na vědomí, že v rámci Předmětu díla může dojít k upřesnění Předmětu díla, resp. Akceptačních kritérií jednotlivých Fází. Vzhledem ke skutečnosti uvedené v předchozí větě nemohou být veškerá Akceptační kritéria vymezena zcela vyčerpávajícím způsobem. Zhotovitel proto bere na vědomí skutečnosti uvedené v tomto odstavci a zavazuje se v tomto ohledu postupovat v souladu s principy „best practice" a zohledňovat veškeré připomínky Objednatele, které lze s ohledem na účel této Smlouvy považovat za oprávněné. Zhotovitel dále bere na vědomí, že vzhledem ke skutečnostem uvedeným v tomto odstavci mohou být v rámci Akceptačního řízení vzneseny Objednatelem výhrady, jejichž povaha bude bránit akceptaci a jejichž důsledkem tak může být prodloužení doby Akceptačního řízení. Objednatel se zavazuje poskytnout Zhotoviteli součinnost při projednání připomínek k Předmětu díla i ve fázích přípravy.

7.5 Akceptačnímu řízení dle části 8 ZOP a tohoto článku této Smlouvy podléhají rovněž Služby na vyžádání, které budou realizované na základě Objednávek. Akceptační kritéria budou v tomto případě vyplývat ze specifikace prací uvedených v Objednávce. Akceptačnímu řízení dle části 8 ZOP a tohoto článku této Smlouvy podléhá rovněž Post-implementační podpora nově nasazených komponent do infrastruktury SŽ.

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

8 Licenční ujednání

8.1 Pokud jsou výstupy dílčích činností ze strany Zhotovitele, které jsou podrobně definované v části 4 Přílohy č. 1 této Smlouvy, Autorským dílem, uplatní se čl. 6.3. ZOP, a to včetně Dokumentace vztahující se k těmto výstupům.

8.2 V případě, že ze strany Zhotovitel je plněním Standardní Software namísto čl. 8.1 této Smlouvy se uplatní čl. 6.5 ZOP.

8.3 Zhotovitel prohlašuje a zavazuje se, že je a bude plně oprávněn disponovat právy duševního vlastnictví týkajícími se Díla, včetně práv autorských, a zavazuje se zajistit řádné a nerušené užívání Díla Objednatelem, včetně zajištění souhlasů všech nositelů práv duševního vlastnictví. Zhotovitel je povinen Objednateli uhradit jakékoli majetkové a nemajetkové újmy, vzniklé v důsledku toho, že by Objednatel nemohl Dílo nebo jakoukoli jeho část užívat řádně a nerušeně.

8.4 Zhotovitel se zavazuje, že při provádění Díla neporuší práva třetích osob, která těmto osobám mohou plynout z práv k duševnímu vlastnictví, a to po celou dobu trvání autorských práv k Dílu. Za případné porušení této povinnosti, a to i nastalé v průběhu užívání Díla Objednatelem, bude vůči takovým třetím osobám odpovědný výhradě Zhotovitel. Pokud budou práva třetích osob váznout na podkladech, materiálech a dalších předmětech, které Zhotoviteli poskytne Objednatel bez toho, aby jej na tyto skutečnosti upozornil, ponese odpovědnost za případné porušení práv třetích osob Objednatel.

9 Školení

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

10 Služby na vyžádání

10.1 Zhotovitel se zavazuje poskytovat Služby na vyžádání, které jsou blíže vymezeny v části 4.6 Přílohy č. 1 této Smlouvy.

10.2 Maximální rozsah Služeb na vyžádání činí 30 MD za celou dobu trvání této Smlouvy. Objednatel není povinen Služby na vyžádání čerpat.

10.3 Objednatel v případě zájmu o provedení prací v rámci Služeb na vyžádání doručí Zhotoviteli objednávku prostřednictvím e-mailu Kontaktních osob uvedených v čl. 12 této Smlouvy se specifikací požadovaných prací ve smyslu části 4.6 Přílohy č. 1 této Smlouvy, termínem provedení těchto prací a předpokládanou časovou náročností vyjádřenou v MD (dále jen „**Objednávka**").

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

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

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

11 Účast poddodavatelů a realizační tým

11.1 Zhotovitel je oprávněn plnit tuto Smlouvu výlučně prostřednictvím Poddodavatelů uvedených v příloze č. 4 této Smlouvy – Seznam poddodavatelů.

11.2 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 13 ZOP.

11.3 Zhotovitel plní tuto Smlouvu prostřednictvím realizační týmu, který je uveden v příloze č. 9 této Smlouvy. Pravidla pro realizační tým se řídí částí 14 ZOP.

12 Komunikace Stran

12.1 Každá ze Stran jmenuje Kontaktní osoby, které budou vystupovat jako zástupci Stran a prostřednictvím kterých bude probíhat veškerá komunikace předpokládaná touto Smlouvou nebo ZOP. Kontaktní osoby zastupují Stranu ve smluvních a technických záležitostech souvisejících s plněním předmětu této Smlouvy, zejména podávají a přijímají informace o průběhu plnění této Smlouvy (dále jen „**Kontaktní osoby**").

12.2 Kontaktními osobami za Objednatele jsou:

- ve věcech smluvních: [BUDE DOPLNĚNO JMÉNO, TEL., EMAIL]
- ve věcech technických: [BUDE DOPLNĚNO JMÉNO, TEL., EMAIL]
- ve věcech kybernetické bezpečnosti: [BUDE DOPLNĚNO JMÉNO, TEL., EMAIL]

Kontaktními osobami za Zhotovitele jsou:

- ve věcech smluvních: [DOPLNÍ DODAVATEL JMÉNO, TEL., EMAIL]
- ve věcech technických: [DOPLNÍ DODAVATEL JMÉNO, TEL., EMAIL]
- ve věcech kybernetické bezpečnosti: [DOPLNÍ DODAVATEL JMÉNO, TEL., EMAIL]

12.3 Každá ze Stran má právo změnit jí jmenované Kontaktní osoby, musí však o každé změně vyrozumět písemně druhou Stranu. Změna Kontaktních osob je vůči druhé Straně účinná okamžikem, kdy o ní byla písemně vyrozuměna; v případě změny Kontaktní osoby není třeba uzavírat dodatek k této Smlouvě.

13 Smluvní pokuty

13.1 Cenou pro účely stanovení výše smluvních pokut dle části 16 ZOP, části 20 ZOP a části 20 OOP se rozumí Cena díla, není-li výslovně stanoveno jinak.

14 Ukončení smluvního vztahu

14.1 Objednatel je oprávněn odstoupit od této Smlouvy, pokud dojde k významné změně ovládání Dodavatele podle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů, nebo změně vlastnictví zásadních aktiv, využívaných Dodavatelem k plnění této Smlouvy a změně oprávnění nakládat s těmito aktivy, či dojde ke změně ekvivalentní změnám výše uvedeným 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.

14.2 Další pravidla pro ukončení Smlouvy stanoví část 18 ZOP.

15 Kybernetická bezpečnost

15.1 Zhotovitel se zavazuje k zachovávání požadavků kybernetické bezpečnosti zejména dle části 20 ZOP, přičemž Zhotovitel je považován za Významného dodavatele ve smyslu ZOP.

16 Ochrana osobních údajů

16.1 Zhotovitel bude jako zpracovatel zpracovávat pro Objednatele jako správce následující kategorie subjektů osobních údajů: zaměstnanci Objednatele, externí dodavatelé Objednatele, důchodci, bývalí zaměstnanci.

16.2 Zhotovitel bude u jednotlivých kategorií subjektů údajů zpracovávat pro Objednatele následující typy osobních údajů: jméno a příjmení, jméno, příjmení, osobní číslo, login(y), pracovní zařazení, pracovně-právní vztahy, e-mailová adresa, jednoznačný identifikátor identity.

16.3 Pokud bude v rámci plnění této Smlouvy docházet ke zpracování osobních údajů, zavazuje se Zhotovitel dodržovat opatření dle části 21 ZOP. Pokud by Zhotovitel zpracovával další osobní údaje, než které jsou uvedeny v čl. 16.1 a 16.2 této Smlouvy, bude tak Zhotovitel činit rovněž za podmínek dle části 21 ZOP.

17 Ochrana důvěrných informací

17.1 Zhotovitel se zavazuje k ochraně důvěrných informací dle části 22 ZOP.

18 Střet zájmů, povinnosti Zhotovitele v souvislosti s konfliktem na Ukrajině

18.1 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.

18.2 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 18.5 této Smlouvy (dále jen „***Sankční seznamy***“).

18.3 Je-li Zhotovitelem sdružení více osob, platí podmínky dle odstavce 18.1 a 18.2 této Smlouvy také jednotlivě pro všechny osoby v rámci Zhotovitele sdružené, a to bez ohledu na právní formu tohoto sdružení.

18.4 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.

18.5 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.

18.6 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.

18.7 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 a § 2050 Občanského zákoníku se nepoužijí.

19 Přímé platby poddodavatelům

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

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

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

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

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

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

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

19.8 V případě, že částka k úhradě již byla uhrazena Zhotoviteli, Objednatel ji uhradí poddodavateli, a následně bude o částku k úhradě snížena celková odměna Zhotovitele, a to formou započtení proti pohledávce nebo pohledávkám Zhotovitele vzniklých na základě plnění této Smlouvy. O zápočtu proti pohledávce Zhotovitele musí Objednatel Zhotovitele písemně informovat. Není-li již budoucí platba, kterou by Objednatel mohl započíst proti své pohledávce vůči Zhotoviteli, představuje částka k úhradě výši smluvní pokuty za nesplnění povinnosti dle čl. 19.1 této Smlouvy a Zhotovitel se zavazuje tuto smluvní pokutu uhradit nejpozději do 15 dnů ode dne doručení výzvy k zaplacení.

20 Další povinnosti Zhotovitele

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

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

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

20.4 Plnění povinností dle čl. 20.3 této Smlouvy je Zhotovitel povinen prokázat kdykoli do 5 pracovních dnů od doručení písemné výzvy Objednatele, a to prostřednictvím všech potřebných dokladů dle aktuálních právních předpisů, resp. též s příslušnými výstupy ze mzdového a účetního systému Zhotovitele.

20.5 Zhotovitel je povinen dodržet podmínky pro využití open source komponent dle části 4.1.2 Přílohy č. 1 této Smlouvy. V případě, že vyjde najevo, že tyto podmínky nejsou splněny, jedná se o vadu plnění a Objednateli přísluší veškerá z toho plynoucí oprávnění.

21 Compliance

21.1 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.

21.2 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.

21.3 Zhotovitel má výše uvedené dokumenty k dispozici na webových stránkách: [doplní Zhotovitel x nemá-li Zhotovitel výše uvedené dokumenty, celý bod 21.3 odstraní].

22 Závěrečná ujednání

22.1 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 Stran, předmětu této Smlouvy, jeho ceně či hodnotě a datu uzavření této Smlouvy.

22.2 Zaslání této Smlouvy správci registru smluv k uveřejnění v registru smluv zajistí Objednatel. Nebude-li tato Smlouva zaslána k uveřejnění a/nebo uveřejněna prostřednictvím registru smluv, není žádná ze Stran oprávněna požadovat po druhé Straně náhradu škody ani jiné újmy, která by jí v této souvislosti vznikla nebo vzniknout mohla.

22.3 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.

22.4 Jestliže Strana označí za své obchodní tajemství část obsahu této Smlouvy, která v důsledku toho bude pro účely uveřejnění této Smlouvy v registru smluv znečitelněna, nese tato Strana odpovědnost, pokud by tato Smlouva v důsledku takového označení byla uveřejněna způsobem odporujícím ZRS, a to bez ohledu na to, která ze Stran tuto Smlouvu v registru smluv uveřejnila. S částmi této Smlouvy, které druhá 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 Strany Objednateli obsahujícího přesnou identifikaci dotčených částí této Smlouvy včetně odůvodnění, proč jsou za obchodní tajemství považovány. Druhá 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.

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

22.6 Tato Smlouva je vyhotovena v elektronické podobě, přičemž obě 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 Dodavatel a dvě vyhotovení Objednatel.

22.7 Veškerá práva a povinnosti Stran vyplývající z této Smlouvy se řídí českým právním řádem.

22.8 Smluvní vztahy neupravené touto Smlouvou se řídí Občanským zákoníkem a dalšími právními předpisy.

22.9 Všechny spory vznikající z této Smlouvy a v souvislosti s ní budou dle vůle Stran rozhodovány soudy České republiky, jakožto soudy výlučně příslušnými.

22.10 Je-li nebo stane-li se jakékoli ustanovení této Smlouvy neplatným, nezákonným nebo nevynutitelným, netýká se tato neplatnost a nevynutitelnost zbývajících ustanovení této Smlouvy. Strany se tímto zavazují nahradit do 5 (slovy: pěti) pracovních dnů po doručení výzvy druhé Strany jakékoli takové neplatné, nezákonné nebo nevynutitelné ustanovení ustanovením, které je platné, zákonné a vynutitelné a má stejný nebo alespoň podobný obchodní a právní význam.

22.11 Tuto Smlouvu lze měnit pouze písemnými a řádně označenými dodatky.

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

Přílohy

1. Specifikace plnění této Smlouvy (*jedná se o přílohu č. 2 Výzvy k podání nabídky – Bližší specifikace předmětu plnění (Technická specifikace), přílohu č. 7 Výzvy k podání nabídky – Popis prostředí SŽ a přílohu č. 8 Výzvy k podání nabídky – Informace k systémům SŽ*)
2. Specifikace nabídkové ceny *(bude doplněno v souladu s Nabídkou Dodavatele podle Dodavatelem vyplněného vzoru obsaženého v příloze č. 6 Výzvy k podání nabídky – Tabulka pro vyplnění nabídkové ceny)*
3. Harmonogram plnění *(jedná se o přílohu č. 4 Výzvy k podání nabídky – Harmonogram plnění)*
4. Seznam poddodavatelů *(bude doplněno v souladu s Nabídkou Dodavatele podle Dodavatelem vyplněného vzoru obsaženého kapitole č. 8 přílohy č. 1 Výzvy k podání nabídky – Seznam poddodavatelů)*
5. Zvláštní obchodní podmínky pro Zakázky v oblasti ICT
6. Obchodní podmínky ke Smlouvě o dílo
7. Platforma SŽ *(jedná se o přílohu č. 12 Výzvy k podání nabídky)*
8. Plná moc *(pouze v případě zastoupení Dodavatele osobou na základě plné moci)*
9. Realizační tým (*bude doplněno v souladu s Nabídkou Dodavatele podle Dodavatelem vyplněného vzoru obsaženého v kapitole 6 přílohy č. 1 Výzvy k podání nabídky – Čestné prohlášení o splnění technické kvalifikace – seznam členů realizačního*)

Za Objednatele:	Za Zhotovitele:
V …… dne ……	V …… dne ……
……	……
Bc. Jiří Svoboda, MBA generální ředitel	[*DOPLNÍ DODAVATEL*]

SPRÁVA ŽELEZNIC

Příloha č. 5 Smlouvy

Zvláštní obchodní podmínky pro Zakázky v oblasti ICT

OBSAH

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

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

1. VÝKLAD POJMŮ

1.1. **Akceptační kritéria** představují podmínku anebo vlastnost výstupu provádění Plnění dle Smlouvy, která musí být splněna, aby bylo Plnění dle Smlouvy provedeno, přičemž Akceptační kritéria jsou uvedena v Příloze Smlouvy, která obsahuje specifikaci Plnění (dále jen „**Specifikace Plnění**").

1.2. **Akceptační protokol** je protokol, který jsou zavázáni podepsat Objednatel i Dodavatel po provedení všech nezbytných činností v rámci Akceptačního řízení, potvrzující provedení výstupu provádění Plnění anebo výsledek Testů výstupů provádění Plnění. Protokol je připravený ze strany Dodavatele a následně upravený a vyplněný Objednatelem. Akceptační protokol obsahuje:

a. Specifikaci provedeného Plnění;

b. Akceptační kritéria;

c. informace o průběhu Testů, jsou-li prováděny;

d. další informace a dokumenty nezbytné pro provedení Akceptačního řízení provedeného Plnění.

1.3. **Akceptační řízení** je postupné provedení akceptačních procesů a podepsání Akceptačního/ch protokolu/ů pro Plnění dle Smlouvy.

1.4. **Aktualizace** je dílčí změna verze Softwaru, zpravidla odstraňující zranitelnosti či drobné nedostatky Softwaru většinou neprojevující se navenek uživatelům, v IT obvykle označovaná jako „patch" nebo „security update" (v rámci IT se také často označuje jako změna třetí číslice v čísle verze Softwaru, tedy např. 4.1.1. na 4.1.2.). Aktualizace představuje takovou změnu Softwaru, která není Modernizací ani Zásadní modernizací.

1.5. **Autorské dílo** znamená dílo ve smyslu § 2 Autorského zákona; zejména nikoliv však výlučně Software, Databáze a jakékoliv výstupy předávané Objednateli na základě Smlouvy, které splňují podmínky stanovené v § 2 Autorského zákona.

1.6. **Autorský zákon** znamená zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

1.7. **Cena** je celková cena za Plnění bez DPH dle Smlouvy. V případě:

a. Smlouvy na dobu neurčitou, jejímž předmětem jsou výhradně pravidelně se opakující či trvající služby či činnosti, se cenou Plnění bez DPH rozumí cena bez DPH za 12 měsíců poskytování takových služeb či činností.

b. Smlouvy na dobu neurčitou, součástí jejíhož předmětu jsou mj. pravidelně se opakující či trvající služby či činnosti, které je Dodavatel povinen poskytovat na dobu neurčitou, se cenou Plnění bez DPH rozumí souhrn cen bez DPH ostatních částí Předmětu Smlouvy a ceny bez DPH za 12 měsíců poskytování takových služeb či činností.

c. Smlouvy, která je rámcovou dohodou, se cenou za Plnění bez DPH této Smlouvy rozumí limit stanovený v této Smlouvě jako maximální souhrnná hodnota bez DPH všech dílčích smluv uzavřených na základě této Smlouvy.

d. Smlouvy, která je zčásti rámcovou dohodou, se cenou za Plnění bez DPH této Smlouvy rozumí souhrn cen bez DPH ostatních části Předmětu Smlouvy a limitu stanoveného v této Smlouvě jako maximální souhrnná hodnota bez DPH všech dílčích smluv uzavřených na základě této Smlouvy.

1.8. **Čas nahlášení Incidentu** představuje časový údaj, vyjadřující datum a čas, kdy byl Incident nahlášen Dodavateli způsobem stanoveným ve Smlouvě a ZOP, tj. vytvořením ticketu v Helpdesku, vytěžením e-mailu z e-mailového serveru Objednatele a jeho vložením do Helpdesku jako ticketu anebo ukončením telefonátu.

1.9. **Data** jsou jakékoliv údaje či informace vznikající v souvislosti s Plněním dle Smlouvy.

1.10. **Databáze** znamená databázi splňující požadavky na Autorská díla, databázi ve smyslu § 88 Autorského zákona a jakoukoliv jinou Autorským zákonem neupravenou databázi.

1.11. **Doba vyřešení** je pro každou kategorii Incidentů uvedena ve Smlouvě a ZOP a znamená rozdíl mezi časem nahlášení Incidentu a dodáním řešení. Do Doby vyřešení Incidentu se nezapočítává doba, po kterou nemůže Dodavatel řešit Incident z důvodu:

a. neobdržení podkladů a informací vyžádaných Dodavatelem, které jsou nezbytně nutné pro lokalizaci nebo replikaci Incidentu, od Objednatele;

b. řešení Incidentu u třetí osoby (vyjma Poddodavatele), jejíž součinnost je dle Smlouvy povinen zajistit Objednatel (např. poskytovatele služeb podpory IT prostředí Objednatele anebo systémů, na které je Software napojen);

c. neposkytnutí jiné nezbytně nutné součinnosti Objednatele vyžádané Dodavatelem v souladu s těmito ZOP či Smlouvou a souvisejícími přílohami.

1.12. **Doba zpracování či Reakční doba** je doba, ve které Dodavatel musí reagovat prostředkem odpovídajícím způsobu nahlášení Incidentu či Požadavku o přijetí takového nahlášení a o zahájení činností směřujících k vyřešení Incidentu či Požadavku.

1.13. **Dodavatel** označuje rovněž Poskytovatele, Zhotovitele či Prodávajícího v závislosti na typu uzavřené Smlouvy.

1.14. **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).

1.15. **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 dle příslušného Servisního modelu dle ZOP.

1.16. **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.

1.17. **FOSS licence** znamená Free Open Source Software licence.

1.18. **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).

1.19. **GUI** znamená grafické uživatelské rozhraní.

1.20. **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

1.21. **Hardware** znamená veškeré hmotné součásti počítačových systémů a veškeré související vybavení hmotné povahy spolu se vším příslušenstvím, a včetně veškeré související dokumentace.

1.22. **Informační či komunikační systém** znamená informační či komunikační systém kritické informační infrastruktury Objednatele ve smyslu § 2 b) ZKB nebo jiný informační či komunikační systém, na který se vztahuje ZKB.

1.23. **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 Helpdesku, 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

1.24. **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.

1.25. **ISDS** znamená informační systém datových schránek ve smyslu zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů.

1.26. **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.*

1.27. **Insolvenční zákon** znamená zákon č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů.

1.28. **IT prostředí Objednatele** znamená veškerý Hardware ve vlastnictví Objednatele a Software, ve vztahu k němuž je Objednatel nositelem potřebných oprávnění, nebo Hardware a Software využívaný Objednatelem na základě jiného právního titulu než Smlouvy. 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*.

1.29. **Kvalifikovaná osoba** je člen Realizačního týmu, kterým Dodavatel prokazoval splnění kvalifikačních předpokladů v rámci Veřejné zakázky.

1.30. **Kybernetický bezpečnostní incident** je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací podle § 7 ZKB v důsledku Kybernetické bezpečnostní události.

1.31. **Kybernetická bezpečností událost** je událost podle § 7 ZKB, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.

1.32. **MD** znamená manday/člověkoden. Nestanoví-li Smlouva jinak, odpovídá jeden MD 8 MH.

1.33. **MH** znamená manhour/člověkohodinu. Nestanoví-li Smlouva jinak, odpovídá jedna MH 60 minutám práce.

1.34. **Modernizace** je změna verze Softwaru, která zpravidla představuje výraznější zásah do dílčí funkcionality Softwaru, přepracováním jeho vybrané funkcionality či doplnění funkcionality nové, zvýšení kompatibility Softwaru s jinými prvky informačních a komunikačních technologií, či jinou optimalizaci funkce Softwaru nad rámec Aktualizace, zpravidla v IT označovaná jako „update" (v rámci IT se také často označuje jako změna druhé číslice v čísle verze Softwaru, tedy např. 4.1. na 4.2.).

1.35. **NÚKIB** znamená Národní úřad pro kybernetickou a informační bezpečnost.

1.36. **Občanský zákoník** znamená zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

1.37. **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.

1.38. **Objednatel** je Správa železnic, státní organizace, IČO 70994234, se sídlem Praha 1 – Nové Město, Dlážděná 1003/7, PSČ 110 00, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze pod sp. Zn. A 48384.

1.39. **Ohlašovatel** znamená osobu určenou Objednatelem, zpravidla uživatel Předmětu Smlouvy.

1.40. **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.

1.41. **Osobní údaje** znamenají osobní údaje ve smyslu GDPR, včetně zvláštních kategorií osobních údajů ve smyslu článku 9 a rozsudků ve smyslu článku 10 GDPR.

1.42. **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.

1.43. **Paušální služby** jsou služby definované ve Smlouvě, jsou-li takové, zpravidla trvajícího či opakujícího se charakteru.

1.44. **Plnění** představuje plnění, které tvoří Předmět Smlouvy a k němuž se váže povinnost Dodavatele toto plnění Objednateli poskytovat. Plnění je blíže specifikované ve Smlouvě a v Příloze Smlouvy *Specifikace Plnění.*

1.45. **Poddodavatel** znamená kteroukoli třetí osobu realizující poddodávky pro Dodavatele v souvislosti s Předmětem Smlouvy. Poddodavatelé mohou být výslovně uvedeni v Příloze Smlouvy *Poddodavatelé*.

1.46. **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

1.47. **Produkční prostředí** znamená IT prostředí Objednatele v ostrém provozu běžně přípustnou uživatelům Software, vyjma Testovacího prostředí.

1.48. **Provozovatel** znamená provozovatel ve smyslu § 2 písm. g) ZKB.

1.49. **Předmět Smlouvy** znamená dle typu Smlouvy Software nebo Hardware, přičemž parametry a vlastnosti Předmětu Smlouvy jsou blíže specifikovány v Příloze Smlouvy *Specifikace Plnění*.

1.50. **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*.

1.51. **Příloha Smlouvy** je dokument, který tvoří nedílnou součást Smlouvy a obsahuje bližší specifikaci smluvních podmínek.

1.52. **Reakce** znamená kvalifikovanou a konkrétní odpověď na nahlášení Incidentu nebo na jiný požadavek, ve formě a způsobem dále definovanými v Příloze Smlouvy *Specifikace Plnění*.

1.53. **Reakční doba** je pro každou kategorii Incidentů uvedena v Příloze *Specifikace Plnění* a představuje dobu od Času nahlášení Incidentu do doručení Reakce Objednateli nebo Ohlašovateli.

1.54. **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.

1.55. **Recovery Point Objective (RPO)** je parametr, který vyjadřuje maximální ztrátu dat uživatelů při havárii systému a následné obnově.

1.56. **Recovery Time Objective (RTO)** je parametr, který vyjadřuje dobu nutnou k obnově chodu služby do akceptované úrovně provozu.

1.57. **Helpdesk** je Software provozovaný Dodavatelem nebo Objednatelem sloužící ke komunikaci Stran v průběhu provádění Plnění dle Smlouvy, v rámci něhož bude evidován postup Dodavatele při provádění Plnění dle Smlouvy a zároveň bude sloužit jako kontaktní místo Dodavatele pro nahlašování Incidentů a Požadavků, vznášení dotazů k Plnění, získávání odpovědí ve vztahu k Plnění a další zaznamenávání průběhu provádění Plnění dle Smlouvy.

1.58. **Servisní model** je standardizovaný model provozu a podpory aplikace, systému nebo instance služby.

1.59. **SLA** znamená úroveň kvality Plnění představující dohodu o úrovni poskytovaných ICT služeb dle Smlouvy.

1.60. **Služby** jsou služby definované ve Smlouvě, jsou-li takové.

1.61. **Smluvní strany či Strany** jsou strany Smlouvy, tj. Objednatel a Dodavatel či jinak označené strany Smlouvy, jejíž součástí jsou tyto ZOP.

1.62. **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.

1.63. **Standardní Software** znamená Software, který je distribuován pod standardními licenčními podmínkami více třetím osobám. Mezi Standardní software patří:

a. Software renomovaných výrobců, jenž je na trhu běžně dostupný, tj. nabízený na území České republiky alespoň dvěma (2) na sobě nezávislými a vzájemně se neovládajícími subjekty, a který je v době uzavření Smlouvy prokazatelně užíván v produkčním prostředí nejméně u pěti (5) na sobě nezávislých a vzájemně nepropojených subjektů.

b. Software, u kterého je s ohledem na jeho (i) marginální význam, (ii) nekomplikovanou propojitelnost či (iii) oddělitelnost a nahraditelnost v IT prostředí bez nutnosti vynakládání větších prostředků (více než 50.000 Kč/rok) zajištěno, že další rozvoj Softwaru jinou osobou než tvůrcem/distributorem takového Softwaru je možné provádět bez toho, aby tím byla dotčena práva autorů takovéhoto Softwaru, neboť nebude nutné zasahovat do Zdrojových kódů takovéhoto Softwaru anebo proto, že případné nahrazení takovéhoto Softwaru nebude představovat výraznější komplikaci a náklad na straně Objednatele.

c. Software, jehož API („Application Programming Interface") pokrývá všechny moduly a funkcionality Softwaru, je dobře dokumentované, umožňuje zapouzdření Softwaru a jeho adaptaci v rámci měnících se podmínek IT prostředí Objednatele a Softwaru bez nutnosti zásahu do Zdrojových kódů Softwaru, a Dodavatel poskytne Objednateli právo užít toto rozhraní pro programování aplikací ve stejném rozsahu jako Software.

d. Software, o kterém to stanoví Smlouva.

1.64. **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.

1.65. **Testy** se rozumí provádění testovacího užívání Předmětu Smlouvy v Testovacím prostředí prostřednictvím simulace ostrého provozu v Produkčním prostředí a reálných situací a Testovacích scénářů.

1.66. **Testovací prostředí** znamená virtuální či fyzickou kopii Předmětu Smlouvy anebo IT prostředí Objednatele určenou Objednatelem k provádění Testů.

1.67. **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.

1.68. **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.

1.69. **Vada kategorie C** znamená vadu, která není Vadou kategorie A anebo B (např. špatná grafická úprava aplikace, špatný pravopis u nápovědy apod.).

1.70. **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.

1.71. **VKB** znamená vyhlášku 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.

1.72. **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.

1.73. **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).

1.74. **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.

1.75. **Významný dodavatel** znamená Dodavatel, který je Provozovatelem, jakož i každý, kdo s Objednatelem vstupuje do právního vztahu, který je významný z hlediska bezpečnosti Informačního či komunikačního systému ve smyslu § 2 odst. m) VKB.

1.76. **Významná změna** znamená změna, která má nebo může mít vliv na kybernetickou bezpečnost a představuje vysoké riziko, např.

a. změny pravidel ochranných systémů aplikačních firewallů a pravidel přepínání a směrování v sítích,

b. změny autentizačních mechanismů,

c. přidání, změna nebo odebrání služeb, informačních systémů/aplikací nebo ochranných systémů,

d. změny, které umožňují sdílení informací, služeb nebo zdrojů mimo provozní prostředí,

e. změny opatření pro zajištění bezpečnosti vzdáleného přístupu,

f. zavedení skriptů pro automatické přihlášení,

g. migrace dat do jiné Databáze, apod. ve smyslu § 2 odst. o) VKB.

1.77. **Zadávací dokumentace** je souborem dokumentů obsahujících zadávací podmínky, sdělované nebo zpřístupňované účastníkům zadávacího řízení na Veřejnou zakázku.

1.78. **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).

1.79. **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.

1.80. **ZKB** znamená zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.

1.81. **ZOP** znamená tento dokument, tedy zvláštní obchodní podmínky, které definují další parametry a upřesňují konkrétní podmínky a specifické požadavky Objednatele.

1.82. **ZZVZ** znamená zákon č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů.

1.83. Není-li výslovně uvedeno jinak nebo nevyplývá-li něco jiného z povahy věci, mají pojmy, které nejsou definovány v těchto ZOP, význam uvedený v Obchodních podmínkách či Smlouvě a jejích přílohách.

1.84. 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.

1.85. Pokud je uveden v ZOP čas, jedná se o čas SEČ.

1.86. 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. 20. 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 § 7 ZKB 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*. Podpisem Smlouvy Dodavatel prohlašuje, že měl možnost se seznámit s Interními předpisy Objednatele, jejichž seznam je uveden v Příloze Smlouvy *Seznam interních* předpisů, a dále bere na vědomí, že Interní předpisy mohou být přiměřeným způsobem jednostranně měněny či jinak doplňovány Objednatelem, přičemž každá nová verze je pro Dodavatele závazná vždy ode dne, kdy se s ní seznámil či měl prokazatelnou možnost se s nimi seznámit. Rozsah Interních předpisů může být Objednatelem jednostranně rozšířen o další dokumenty stanovující jeho interní procesy.

4. POVINNOSTI DODAVATELE

4.1. Dodavatel se zavazuje provádět pro Objednatele Plnění osobně, tj. prostřednictvím svých zaměstnanců, členů Realizačního týmu a prostřednictvím svých Poddodavatelů za podmínek stanovených ve Smlouvě a těchto ZOP. V případě, že je požadavek na složení Realizačního týmu uveden ve Smlouvě, je Dodavatel povinen provádět Plnění výhradně prostřednictvím členů Realizačního týmu, kterými prokázal splnění kvalifikace v průběhu zadávacího řízení na Veřejnou zakázku.

4.2. Dodavatel se během poskytování Plnění pro Objednatele zavazuje informovat Objednatele o Významné změně ovlivnění nebo ovládání Dodavatele podle ust. § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů (dále jen „ZOK"), nebo změně vlastnictví zásadních aktiv, využívaných Dodavatelem k Plnění Smlouvy a změně oprávnění nakládat s těmito aktivy.

4.3. Dodavatel se zavazuje poskytovat v rámci Plnění veškerou součinnost nezbytnou k provádění Plnění, zejména, nikoliv však výlučně:

a. poskytovat Plnění dle Smlouvy ve vysoké kvalitě s odbornou péčí odpovídající podmínkám sjednaným ve Smlouvě;

a. 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;

b. 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;

c. zajistit v souladu s podmínkami Smlouvy poskytnutí Dokumentace, a to rovněž vždy při každé Aktualizaci nebo jiné změně Předmětu smlouvy, nestanoví-li Objednatel jinak;

d. počínat si při provedení Plnění tak, aby nedošlo k infikaci Softwaru, Standardního Softwaru nebo IT prostředí Objednatele virem či jiným škodlivým kódem (malware apod.) způsobujícím narušení zabezpečení Softwaru a Standardního Softwaru za účelem jeho poškození či jiného narušení běhu;

e. bez zbytečného odkladu oznamovat Objednateli všechny Kybernetické bezpečnostní události a Kybernetické bezpečnostní incidenty s potenciálním negativním dopadem na Objednatele;

f. 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;

g. plnit Interní předpisy Objednatele a jeho pokyny v oblasti likvidace Dat (ať už Dat na papírových médiích, Dat zpracovávaných elektronicky nebo prostřednictvím jakýchkoli dalších nosičů Dat) a případně dále na výzvu Objednatele bez zbytečného odkladu zlikvidovat Data v souladu s těmito pravidly a pokyny. Dodavatel musí především postupovat tak, aby nebylo možné odstraněná data zneužít. Za odpovídající způsob likvidace dat je považováno odstranění, přepsání či fyzická likvidace nosiče informace v souladu se standardem US DoD 5220.22-M;

h. 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.

5. POVINNOSTI OBJEDNATELE

5.1. Objednatel je povinen zajistit Testovací a Produkční prostředí pro činnost Dodavatele v rámci IT prostředí Objednatele, pokud je to nezbytné pro provádění Plnění. Zajištění prostředí zahrnuje zajištění vzdáleného přístupu personálu Dodavatele do IT prostředí Objednatele, v přiměřeném rozsahu odpovídajícího možnostem Objednatele a Zadávací dokumentaci a při respektování bezpečnostních pravidel Objednatele, zejména bezpečnostní dokumentace, která je součástí Interních předpisů. Objednatel je povinen zajistit fungování Dodavatelem vytvořeného Testovacího prostředí, na kterém bude Software Testován, a Produkčního prostředí, na kterém Software poběží v ostrém provozu, přičemž všechna prostředí budou umístěna na IT prostředí Objednatele, není-li ve Smlouvě stanoveno jinak.

6. LICENČNÍ UJEDNÁNÍ

6.1. Smlouva stanoví, která licenční ujednání dle tohoto článku se použijí ve vztahu k Plnění. Neobsahuje-li Smlouva takový odkaz, použije se ve vztahu k Plnění vedle společných ustanovení k licenčním ujednáním dle odst. 6.7 tohoto článku též odst. 6.3 tohoto článku a ve vztahu k částem Plnění, která obsahují Standardní Software, též odst. 6.5 tohoto článku. Je-li součástí Plnění Hardware, použijí se též pravidla dle odst. 6.6 tohoto článku.

6.2. Odměna za oprávnění dle tohoto článku je zahrnuta v ceně Plnění.

6.3. **Postoupení výkonu autorských majetkových práv k Software**

6.3.1. V případě, že je Software Autorské dílo vznikající v průběhu Plnění, Dodavatel neodvolatelně postupuje na Objednatele oprávnění k výkonu majetkových práv autorských k takovému Autorskému dílu).

6.3.2. Dodavatel prohlašuje, že Software byl vytvořen zaměstnanci či Poddodavateli jako zaměstnanecké dílo ve smyslu § 58 odst. 1 a 7 Autorského zákona, a že je oprávněn k postoupení výkonu majetkových práv v souladu s tímto odst. 6.3 ZOP a má k takovému postoupení náležité souhlasy, přičemž Dodavatel se zavazuje na požádání Objednatele neprodleně předložit nebo jinak vhodným způsobem zpřístupnit dokumenty prokazující rozsah oprávnění Dodavatele. =

6.3.3. Objednatel je dále oprávněn postoupit oprávnění k výkonu majetkových práv na jakoukoli další třetí osobu dle volby Objednatele a udělovat licence a podlicence, s čímž Dodavatel výslovně souhlasí; pro zamezení pochybnostem je Dodavatel povinen podniknout veškeré kroky k získání náležitých oprávnění tak, aby mohl oprávnění k výkonu majetkového práva postoupit na Objednatele v souladu s tímto odst. 6.3 ZOP. S povinností převodu oprávnění k výkonu majetkových práv se pojí povinnost předání Zdrojového kódu dle čl. 7 ZOP.

6.3.4. Dodavatel dále prohlašuje, že má svolení autora/ů k zásahům do Software (včetně jeho Zdrojového a strojového kódu) ve smyslu § 58 odst. 4 Autorského zákona a tato svolení se vztahují na jakékoliv třetí osoby, jež budou vykonávat autorská majetková práva k tomuto Software.

6.3.5. Dodavatel dále prohlašuje, že vyloučil oprávnění autorů dle ustanovení § 58 odst. 3 Autorského zákona i vůči všem budoucím vykonavatelům autorských majetkových práv k Software.

6.3.6. Dodavatel dále převádí veškerá zvláštní práva pořizovatele k Databázím, jež tvoří součást Plnění. Nedojde-li z jakéhokoliv důvodu k převodu práva dle předchozí věty, uděluje Dodavatel Objednateli oprávnění k vytěžování a zužitkování celého obsahu takové Databáze nebo její kvalitativně nebo kvantitativně podstatné části a právo udělit jinému oprávnění k výkonu tohoto práva.

6.3.7. K ostatním majetkovým hodnotám, které spadají pod pojem Software a zároveň nespadají pod definici Autorského díla, uděluje Dodavatel Objednateli oprávnění v rozsahu dle odst. 6.3.8. ZOP. Ustanovení odst. 6.5 a 6.6 ZOP tímto nejsou dotčena.

6.3.8. Nevznikne-li Objednateli z jakéhokoliv důvodu ke kterékoliv části Softwaru oprávnění k výkonu autorských majetkových práv, uděluje Dodavatel Objednateli k dotčené části množstevně a územně neomezenou výhradní licenci ke všem známým způsobům užití, a to na dobu trvání autorských majetkových práv. Objednatel je oprávněn k dotčené části Softwaru udělovat licence, tyto dále postoupit a udělovat podlicence třetím osobám. Objednatel je dále oprávněn dotčené části upravovat a měnit (včetně Zdrojového a strojového kódu takové části Software), dokončovat, včetně práva takto upravené či dokončené části užívat, a dále tyto původní, upravené či dokončené

části zveřejňovat, spojovat s jiným dílem či zařazovat do díla souborného, zpracovávat, překládat či jinak zasahovat, a to vše i prostřednictvím třetí osoby.

6.4. **Nevýhradní licence k Software**

6.4.1. Ve vztahu k Software Dodavatel tímto uděluje Objednateli okamžikem akceptace Plnění ve smyslu čl. 8 ZOP, nebo jinak vymezeným okamžikem akceptace Plnění Smlouvou a jejími přílohami nevýhradní oprávnění k výkonu práva užít Software v souladu s dalšími podmínkami odst. 6.4 ZOP (dále „***Licence***"). Ustanovení tohoto odstavce se nevztahují na oprávnění Objednatele k Software, který je Standardním Software; tato oprávnění jsou upravena samostatně v odst. 6.5 ZOP. V případě, že je Plnění rozděleno na části, použije se tento odstavec na každou část Plnění.

6.4.2. Licence se uděluje jako nevýhradní a opravňuje Objednatele k výkonu práva užít veškerá Autorská díla a k výkonu práva vytěžovat a zužitkovat Databáze, jež tvoří Plnění, a to:

a. k jakémukoliv účelu;

b. na dobu trvání majetkových práv autorských;

c. na jakémkoliv území;

d. jakýmkoliv způsobem; a

e. bez množstevního omezení.

6.4.3. Dodavatel okamžikem dle odst. 6.3. ZOP uděluje rovněž oprávnění takový Software upravovat a měnit (včetně Zdrojového a strojového kódu), dokončovat, včetně práva takto upravený, změněný či dokončený Software užívat v rozsahu Licence, a dále tyto původní, upravené, změněné či dokončené části spojovat s jiným dílem či zařazovat do díla souborného, zpracovávat, překládat či jinak do nich zasahovat, a to vše i prostřednictvím třetí osoby

6.4.4. Objednatel má v rámci Licence právo udělit k Softwaru podlicenci třetím osobám a právo postoupit Licenci zcela či z části na třetí osoby, s čímž Dodavatel výslovně souhlasí.

6.4.5. Licence zahrnuje povinnost Dodavatele předat Objednateli Zdrojový kód a Dokumentaci k Software dle článku 7 ZOP.

6.4.6. Licence se vztahuje ve stejné míře a rozsahu jako k Software taktéž na:

a. Dokumentaci specifikovanou ve Smlouvě nebo jejích přílohách;

b. jakoukoliv jinou Dokumentaci předávanou k Software nad rámec Dokumentace dle předchozího písmene;

c. loga či jiné předměty duševního vlastnictví, které souvisí s Plněním a jsou vhodné či nezbytné k užití spolu s Plněním;

d. jakákoliv jiná Autorská díla či jiné předměty duševního vlastnictví, které souvisí s Plněním.

6.5. **Licence ve vztahu ke Standardnímu Software**

6.5.1. V případech, kdy je součástí Plnění Standardní Software, Dodavatel uděluje Objednateli okamžikem akceptace Plnění ve smyslu čl. 8 ZOP, jehož součástí je Standardní Software, k veškerému takovému Standardnímu Software nevýhradní oprávnění k výkonu práva užít příslušný Standardní Software v souladu s dalšími podmínkami odst. 6.5 ZOP (dále „***Licence k Standardnímu Software***"). V případě, že je Plnění rozděleno na části, použije se tento odstavec na každou část Plnění, jehož součástí je Standardní Software či jeho část.

6.5.2. Licence k Standardnímu Software se uděluje jako nevýhradní a opravňuje Objednatele k výkonu práva užít veškerý Standardní Software, a to:

a. všemi způsoby odpovídajícími účelu, pro který je takový Standardní Software určen;

b. na dobu trvání majetkových práv autorských, nebo alespoň na dobu trvání Smlouvy;

c. na jakémkoliv území; a

d. bez množstevního omezení.

6.5.3. Dodavatel je v rámci Licence k Standardnímu Software povinen zajistit poskytnutí podpory (subscription/license maintenance) k veškerému Standardnímu Software, tj. zajistit poskytování

nejnovějších verzí Standardního Software Objednateli a dalších služeb v souladu se standardními licenčními podmínkami Standardního Software, a to alespoň na dobu trvání Smlouvy.

6.5.4. Objednatel má v rámci Licence k Standardnímu Software oprávnění udělit ke Standardnímu Software podlicenci třetím osobám a právo postoupit Licenci k Standardnímu Software zcela či z části na třetí osoby, s čímž Dodavatel výslovně souhlasí.

6.5.5. Licence k Standardnímu Software se vztahuje ve stejné míře jako k Standardnímu Software taktéž na:

a. Aktualizaci, Modernizaci a Zásadní modernizaci Standardního Software, který je součástí Plnění;

b. Dokumentaci k Standardnímu Software specifikovanou ve Smlouvě nebo jejích přílohách;

c. Dokumentaci nad rámec Dokumentace k Standardnímu Software dle předchozího písm.;

d. právo zužitkovat a vytěžovat Databáze obsažené ve Standardním Software, který je součástí Plnění;

e. loga či jiné předměty duševního vlastnictví, které se Standardním Software, jež je součástí Plnění, souvisí a jsou vhodné či nezbytné k užití spolu s takovým Standardním Software.

6.5.6. V parametrech, které nejsou upraveny Smlouvou, jejími přílohami anebo jinou částí Zadávací dokumentace, se Licence k Standardnímu Software řídí příslušnými licenčními podmínkami výrobce Standardního Software.

6.5.7. V případě, že Dodavatel využije při plnění předmětu Smlouvy Standardní Software, je Dodavatel za účelem vyloučení vzniku proprietárního uzamčení Objednatele (tzv. vendor lock-in) povinen použít výlučně takový Standardní Software, u kterého jsou splněny podmínky dle definice Standardního Software dle odst. 1.63 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 povinnen, po dohodě s Objednatelem, a v případě, že tato dohoda nebude možná, pak dle volby Dodavatele:

a. na vlastní náklady dodat Objednateli Zdrojový kód předmětného Standardního Software a poskytnout Objednateli oprávnění užívat tento Standardní Software včetně Zdrojového kódu (včetně dalších způsobů nakládání) v rozsahu Licence dle odst. 6.4 ZOP; nebo

b. nahradit na vlastní náklady předmětný Standardní Software jiným Standardním Software, který bude mít alespoň srovnatelné funkcionality, kvalitu a technickou způsobilost jako nahrazovaný Standardní Software a zároveň splňovat podmínky stanovené v odst. 6.5.7 ZOP, a poskytnout k tomuto Standardnímu Software Objednateli Licenci k Standardnímu Software dle odst. 6.5 ZOP; nebo

c. nahradit na vlastní náklady předmětný Standardní Software vlastním Softwarem, tj. přeprogramovat část Díla představovanou předmětným Standardním Softwarem za využití vlastního Software vytvořeného na míru Objednateli, který bude mít alespoň srovnatelné funkcionality, kvalitu a technickou způsobilost jako nahrazovaný Standardní Software, a poskytnout k tomuto vlastnímu Softwaru Objednateli Licenci dle odst. 6.4 ZOP, a to včetně Zdrojového kódu.

6.5.9. Postupy dle odst. 6.5.8 písm. a) až c) ZOP podléhají samostatnému Akceptačnímu řízení. Vznikla-li Dodavateli povinnost dle odst. 6.5.8 ZOP, je Dodavatel povinen splnit povinnosti dle uvedeného odstavce i po ukončení Smlouvy. Ustanovení Smlouvy a ZOP relevantní pro splnění povinností dle předchozí věty se použijí i po ukončení Smlouvy.

6.5.10. Pokud v rámci Akceptačního řízení dle čl. 8 ZOP vyjde najevo, že Standardní Software nesplňuje podmínky odst. 6.5.7 ZOP, je Objednatel oprávněn Akceptační řízení přerušit, dokud Dodavatel nenapraví tento nedostatek předmětného Standardního Software jedním ze způsobů uvedených v odst. 6.5.8 ZOP. Objednatel není v takovém případě v prodlení.

6.5.11. Ustanovení odst. 6.3 a 6.6 ZOP se pro Standardní Software nepoužijí.

6.6. **Software vztahující se k Hardware**

6.6.1. V případech, kdy je k řádnému užívání dodaného Hardwaru potřebný určitý Software, je Dodavatel povinen poskytnout/zajistit Objednateli jako součást Plnění a za cenu zahrnutou v ceně Hardwaru, oprávnění užít tento Software v rozsahu, způsoby a za účelem obvyklým ve vztahu k Hardwaru, se kterým je spojen, nejméně však za podmínek dle Smlouvy a jejích příloh.

6.6.2. Ustanovení odst. 6.3 a 6.4 ZOP se pro Software vztahující se k Hardwaru nepoužijí.

6.7. **Společná ustanovení**

6.7.1. Nestanoví-li Smlouva a její přílohy či jiné části Zadávací dokumentace jinak, je Dodavatel při plnění Smlouvy oprávněn využít programy s otevřeným kódem či jejich části distribuovanými pod FOSS licencemi. Dodavatel však není oprávněn využít programy s otevřeným kódem či jejich části, které jsou distribuovány pod FOSS licencemi, jejichž podmínky by Objednateli ukládaly povinnost sdělovat nebo jinak šířit Software či jeho části, včetně Zdrojových kódů, třetím osobám, nebo umožnit jim změny, úpravy či jiné zásahy do Softwaru nebo jeho části.

6.7.2. Dodavatel je povinen zajistit Objednateli udělení oprávnění k veškerým programům s otevřeným kódem poskytnutým Objednateli v rozsahu takových FOSS licencí, které se na konkrétní program s otevřeným kódem, který je součástí Plnění, vztahují, přičemž konkrétní rozsah licence lze určit odkazem na soubor předávaný v rámci výstupu z Plnění anebo odkazem ve Zdrojovém kódu či jiným označením takové licence ve formátu vyžadovaném takovou veřejnou licencí, včetně odkazu na kompletní znění aktuálních licenčních podmínek příslušné FOSS licence; Dodavatel je dále povinen zajistit poskytnutí podpory k veškerým programům s otevřeným kódem, které jsou součástí Plnění, tj. povinnost Dodavatele zajistit poskytování nejnovějších verzí programů s otevřeným kódem a dalších služeb v souladu se standardními licenčními podmínkami programů s otevřeným kódem, a to alespoň na dobu trvání této Smlouvy. Ustanovení čl. 7 ZOP se pro programy s otevřeným kódem či jejich části, které jsou distribuovány pod FOSS licencemi, použije obdobně.

6.7.3. Dodavatel prohlašuje, že je oprávněn udělit Objednateli veškerá oprávnění v souladu s tímto článkem ZOP, má k takovému udělení veškeré potřebné souhlasy a jejich udělením Objednateli ani užíváním Plnění Objednatelem či uživateli Objednatele nebudou porušena práva duševního vlastnictví třetí osoby. Dodavatel odpovídá Objednateli za zajištění všech nezbytných oprávnění a souhlasů autora či autorů Software či Standardního Software k oprávněním udělovaným Objednateli dle tohoto článku ZOP. Dodavatel se zavazuje poskytnout Objednateli o zajištění oprávnění a veškerých souhlasů dle tohoto článku ZOP písemné prohlášení a na výzvu Objednatele 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 Objednatele, která je součástí Smlouvy, a dále vlastnosti a funkcionality uvedené ve specifikaci plnění Dodavatele (je-li taková), 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 nejméně čtrnáct (14) dní předem o termínu předání Předmětu Smlouvy či její části.

8.1.5. Dodavatel předá Objednateli Předmět Smlouvy k realizaci Akceptačního řízení. Akceptační řízení může být zahájeno pouze v případě, že Předmět Smlouvy byl Dodavatem 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 Helpdesku, 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 vady (zejména vady, pro které není vhodné dělení Vad dle ZOP -> např. některý HW měly-li být dle Návrhu řešení provedeny), 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 třiceti (30) kalendářních dnů ode dne zahájení Akceptačního řízení posoudit Předmět Smlouvy postupem dle odst. 8.1.2 ZOP a v případě dle odst. 8.1.6 ZOP podepsat Akceptační protokol a vyznačit na něm „**Akceptováno**", nebo „**Akceptováno s výhradou**" včetně vyznačení Vad/y či vad/y. V opačném případě je Objednatel povinen ve výše uvedené lhůtě podepsat Akceptační protokol společně s vyznačením „**Neakceptováno**" včetně vyznačení nesplněných Akceptačních kritérií nebo vyznačení Vad/y a jejich/její kategorizace (A, B nebo C) nebo vyznačení dalších vad.

8.1.10. Okamžikem podpisu Akceptační protokolu společně s vyznačením „**Akceptováno**", nebo „**Akceptováno s výhradou**" je Předmět Smlouvy proveden.

8.1.11. Podpis Akceptačního protokolu s vyznačením „**Akceptováno s výhradou**" nezbavuje odpovědnosti Dodavatele odstranit vyznačené Vady či vady. Dodavatel je povinen takové Vady či vady odstranit ve lhůtě určené Objednatelem, jinak do třiceti (30) kalendářních dnů od podpisu Akceptačního protokolu s vyznačením „**Akceptováno s výhradou**". Neodstranění Dodavatel Vady či vady ve lhůtě dle tohoto odstavce, jedná se porušení této Smlouvy podstatným způsobem. Do doby odstranění vyznačených Vad či vad dle tohoto odstavce není Objednatel povinen zaplatit Dodavateli část Ceny (či ceny příslušné části Plnění, je-li plněno po částech) odpovídající její padesáti (50) procentní výši. Objednatel není v takovém případě v prodlení se zaplacením části Ceny (či ceny příslušné části Plnění, je-li plněno po částech) dle předchozí věty. Pro účely ověření splnění povinností Dodavatele dle tohoto odstavce, je Dodavatel Objednateli povinen prokázat, že Plnění již nemá Vady či vady. Povinnost odstranit Vady či vady dle tohoto odstavce není splněna, neodstranil-li Dodavatel Vady či vady nebo objeví-li se v průběhu ověření:

a. nové Vady či vady, které vznikly v souvislosti s odstraňováním původních Vad či vad, nebo

b. Vady či vady, které v důsledku existence původních Vad či vad nebylo možné v Akceptačním řízení odhalit, nebo které bylo možno odhalit pouze s výraznými obtížemi.

8.1.12. V případě neakceptování Předmětu Smlouvy vyznačením na Akceptačním protokolu „**Neakceptováno**" se Dodavatel zavazuje odstranit nesplněná Akceptační kritéria a Vady uvedené v Akceptačním protokolu ve lhůtách výslovně stanovených v Akceptačním protokolu Objednatelem, a pokud nejsou takové, pak lhůtách přiměřených. Do odstranění nedostatků bránících akceptování není Předmět Smlouvy proveden. Po odstranění nedostatků uvedených v Akceptačním protokolu Dodavatel opětovně předá Předmět Smlouvy Objednateli k dalšímu kolu Akceptačního řízení a Objednatel postupuje obdobně podle odst. 8.1.5 ZOP.

8.2. **Akceptační řízení ve vztahu ke Službám**

8.2.1. Řádné provedení Služeb bude Stranami písemně potvrzeno podpisem Akceptačního protokolu po ukončení Akceptačního řízení obdobně dle odst. 8.1 ZOP (s výjimkou odst. 8.1.3 ZOP). Pro účely akceptace Služeb se Předmětem Smlouvy rozumí příslušný výstup ze Služeb (např. rozvoj Software). Strany jsou oprávněny zkrátit lhůty Akceptačního řízení ve smyslu odst. 8.1 ZOP v dílčí smlouvě uzavřené na základě Smlouvy. Nestanoví-li dílčí smlouva Akceptační kritéria Služby, rozumí se jimi:

a. vlastnosti a funkcionality uvedené ve specifikaci plnění Objednatele, která je součástí dílčí smlouvy uzavřené na základě Smlouvy, a dále vlastnosti a funkcionality uvedené ve specifikaci plnění Dodavatele (je-li taková), která je součástí dílčí smlouvy, a

b. požadavky na Zdrojové kódy a Dokumentaci dle čl. 7 ZOP.

8.2.2. Jsou-li Služby plněny po částech, použijí se ustanovení pro Akceptační řízení ve vztahu ke Službám přiměřeně vždy na každou takovou dílčí část výstupu ze Služeb, nedohodnou-li se Strany výslovně jinak.

8.2.3. Akceptační řízení se neprovádí u Služeb, které z povahy věci nepodléhají Akceptačnímu řízení (např. konzultace apod.). Služby musí být v souladu s dílčí smlouvou a přílohou č. 1 této Smlouvy. Uvedeným postupem nejsou dotčena práva z vadného plnění ve vztahu k takovým Službám

8.3. **Akceptační řízení ve vztahu k Paušálním službám**

8.3.1. Řádné provádění Paušálních služeb bude každý měsíc potvrzováno podpisem výkazu Paušálních služeb za bezprostředně předcházející měsíc. Podpisem výkazu Paušálních služeb Objednatelem jsou Paušální služby za příslušný měsíc akceptovány/provedeny. Objednatel není povinen podepsat výkaz Paušálních služeb, nebyly-li jednotlivé Paušální služby v příslušném měsíci řádně provedeny (jedná se např. o Paušální služby, u nichž konec lhůty pro splnění - např. doba pro vyřešení Incidentu – spadá do příslušného měsíce).

8.3.2. Návrh výkazu dle předchozího odstavce připraví Dodavatel. Výkaz musí obsahovat soupis provedených Paušálních služeb za bezprostředně předcházející měsíc a soupis dosud neukončených činností Paušálních služeb. Výkaz Paušálních služeb je Dodavatel povinen doručit nejpozději do deseti (10) kalendářních dnů po skončení měsíce, ve které byly služby poskytnuty.

8.4. **Akceptační řízení ve vztahu ke školení**

8.4.1. Dokladem o řádném provedení školení je prezenční listina podepsána účastníky školení, případně vydání certifikátu, mělo-li být školení zakončené vydáním certifikátu.

8.4.2. Vznikají-li pro školení školící materiály, akceptují se v akceptačním řízení odst. 8.1 ZOP se použije přiměřeně. V takovém případě je školení řádně provedené dnem, v němž je akceptován poslední požadovaný výstup.

8.4.3. V případě, že předmětem školení je hands-on školení, je školení řádne 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 bude potvrzeno předávacím protokolem podepsaným odpovědnými zástupci smluvních stran.

8.5.3. Nestanoví-li Smlouva či její přílohy jinak, Objedantel 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 zařazenmí 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. 20. ZOP. Tuto skutečnost je povinen na vyžádání Objednateli prokázat.

10. HELPDESK

10.1. Dodavatel se zavazuje:

10.1.1. nejpozději v den účinnosti Smlouvy založit a po celou dobu trvání Smlouvy udržovat v provozu Helpdesk (včetně úhrady případných licenčních poplatků za aplikaci Helpdesk) a udělit náležitá oprávnění k přístupu do Helpdesku, a to v počtu přístupů pro Ohlašovatele dle určení Objednatele. Helpdesk bude fungovat prostřednictvím webové adresy;

nebo

10.1.2. po celou dobu trvání Smlouvy užívat Helpdesk provozovaný Objednatelem.

10.2. Provozovatele Helpdesku stanoví Smlouva. Pokud Smlouva provozovatele Helpdesku nestanoví, má se za to, že provozovatelem Helpdesku je Dodavatel. V případě, že provozovatelem bude Objednatel, poskytne Dodavateli nezbytnou součinnost k řádnému užívání Helpdesku včetně případného poskytnutí licencí.

10.3. Dodavatel se zavazuje zajistit Helpdesk prostřednictvím přímého přístupu do Helpdesku na webové adrese určené Dodavatelem/Objednatelem dle provozních podmínek aplikace Helpdesk, případně prostřednictvím přímého datového propojení Helpdesků Objednatele a Dodavatele, a to v jednom z následujících režimů, který je vymezen ve Smlouvě:

a. **Režim 1:**

7x24, tj. dvacet čtyři (24) hodin sedm (7) dní v týdnu.

b. **Režim 2:**

7x12, tj. dvanáct (12) hodin sedm (7) dní v týdnu.

c. **Režim 3:**

5x12, tj. dvanáct (12) hodin pět (5) dní v týdnu

d. **Režim 4:**

5×8, tj. osm (8) hodin pět (5) dní v týdnu.

10.4. Nestanoví-li Smlouva jinak, počíná časový rozsah dle zvoleného režimu dle odst. 10.3 ZOP (s výjimkou režimu 1) vždy zároveň s časový rozsahem dle zvoleného Servisního modelu dle odst. 12.2 ZOP (např. pokud doba Servisního modelu začíná každý pracovní den v 7:00, provoz Helpdesk v rámci příslušného režimu začíná rovněž v 7:00).

10.5. Helpdesk 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 Helpdesk provozován Dodavatelem musí být zabezpečen tak, aby odpovídal požadavkům vyplývajícím ze ZKB a Interních předpisů. Výstupem z Helpdesku je záznam o veškerých úkonech Helpdesku ve formě přehledného logu, jež umožňuje vyhledávání a uchovávání záznamů tak, aby byly naplněny požadavky ZKB a Interních předpisů na takové záznamy.

10.6. Helpdesk bude dostupný pouze pro Objednatele a Ohlašovatele.

10.7. Nestanoví-li Smlouva jinak, je Dodavatel povinen nezávisle na Helpdesk mít nejpozději k okamžiku nabytí účinnosti Smlouvy zřízenou elektronickou adresu a telefonní linku a tuto adresu a telefonní číslo linky sdělit Objednali, a to vše pro účely min. příjmu oznámení Incidentů a Požadavků, vznášení dotazů k Plnění, získávání odpovědí ve vztahu k Plnění a pro další komunikace dle Smlouvy. Doba provozu elektronické adresy a telefonní linky bude odpovídat zvolenému režimu Helpdesk dle odst. 10.3 ZOP.

11. NAHLÁŠENÍ INCIDENTU

11.1. Hlášení o Incidentu Dodavateli bude provedeno Ohlašovatelem, a to přímým zadáním Incidentu do Helpdesku (vytvoření ticketu v Helpdesku, 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, v takovém případě je Incident dle 11.3 ZOP nahlášen okamžikem doplnění požadované informace.

11.3. Je-li Incident nahlašován prostřednictvím Helpdesku, pak se za Čas nahlášení Incidentu považuje čas vytvoření ticketu v Helpdesku. Je-li Incident nahlašován písemně na e-mailovou adresu, pak se za Čas nahlášení Incidentu považuje čas odeslání e-mailu z e-mailového serveru Ohlašovatele, nebo v případě hlášení Incidentu telefonicky čas ukončení telefonického hovoru. Dodavatel je povinen prokazatelným způsobem bezodkladně potvrdit přijetí nahlášení Incidentu, a to vždy prostřednictvím Helpdesku. 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 Helpdesku 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.

12. SERVISNÍ MODELY

12.1. Servisní model představuje standardizovaný model provozu a podpory aplikace, systému nebo instance služby.

12.2. Pokud je součástí Smlouvy zajištění provozu a podpory Softwaru nebo Hardwaru, je ve Smlouvě vymezen jeden z níže uvedených Servisních modelů:

Servisní model	Dostupnost	Doba provozu		Doba zpracování Incidentu	Doba vyřešení Incidentů kategorie A	Doba vyřešení Incidentů kategorie B	RTO	RPO	Doba zpracování Požadavku	Doba vyřešení Požadavku kategorie A	Doba vyřešení Požadavku kategorie B
A1 Kritický	99.5%	7x24	(0-24)	1 hod	2 hod	2 hod	4 hod	< 5 min	1 PD	1 PD	3 PD
A2 Kritický	99.5%	7x12	(6-18)	1 hod	2 hod	2 hod	4 hod	< 5 min	1 PD	1 PD	3 PD
A3 Kritický	99.5%	5x8	(7-15)	1 hod	2 hod	2 hod	4 hod	< 5 min	1 PD	1 PD	3 PD
A4 Kritický	99.5%	7x24	(0-24)	1 hod	4 hod	12 hod	4 hod	< 5 min	1 PD	2 PD	5 PD
A5 Kritický	99.5%	5x8	(7-15)	1 hod	4 hod	12 hod	4 hod	< 5 min	1 PD	2 PD	5 PD
B1 Závažný	98.0%	7x24	(0-24)	1 PD	2 PD	3 PD	48 hod	30 min	2 PD	3 PD	5 PD

B2 Závažný	98.0%	7x12	(6-18)	1 PD	2 PD	3 PD	48 hod	30 min	2 PD	3 PD	5 PD
B3 Závažný	98.0%	5x8	(7-15)	1 PD	2 PD	3 PD	48 hod	30 min	2 PD	3 PD	5 PD
C1 Normální	97.0%	5x12	(6-18)	1 PD	3 PD	6 PD	96 hod	24 hod	3 PD	7 PD	10 PD
C2 Normální	97.0%	5x8	(7-15)	1 PD	3 PD	6 PD	96 hod	24 hod	3 PD	7 PD	10 PD
D Minoritní	94.0%	5x8	(7-15)	2 PD	10 PD	14 PD	96 hod	24 hod	5 PD	10 PD	14 PD
E1 Customizovaný											
E2 Customizovaný											

12.3. Doba řešení Incidentu a Požadavku kategorie C je pro veškeré Servisní modely stanovena na 15 PD.

12.4. Do měření úrovně Dostupnosti (Software) nejsou započítávány:

a. dočasné vyřazení Softwaru z provozu na základě předchozí dohody Objednatele a Dodavatele (odstávka),

b. pravidelná vyřazení Softwaru z provozu Dodavatelem v časech sjednaných ve Smlouvě nebo její příloze (servisní okna),

c. smluvními stranami předem dohodnutý časový úsek za účelem instalace upgradu,

d. výpadky Softwaru způsobené Objednatelem přímo v důsledku jím provedených zásahů do Softwaru, které nebyly Dodavatelem předem schváleny,

e. skutečnosti ve vztahu k Hardware dle odst. 12.9 ZOP za podmínek, že je takový Hardware součástí Plnění a současně je nezbytný pro fungování Software.

12.5. Nedostupnost Softwaru dle odst. 12.4. ZOP se nepovažuje za nedosažení sjednaných parametrů Dostupnosti dle Smlouvy a nebude započítána do výpočtu dle odst. 12.6. a 12.7. ZOP.

12.6. Nestanoví-li Smlouva jinak, bude Dostupnost Software měřena na základě následujícího vzorce:

$$Dostupnost\ (\%) = \frac{Doba\ provozu - Doba\ výpadku}{Doba\ provozu} \times 100$$

12.7. Doba výpadku Softwaru je časový úsek z Doby provozu v hodinách, kdy je služba nedostupná, a počítá se podle následujícího vzorce:

$$Doba\ výpadku = \sum_{i}^{n} T_i$$

kde:

Σ je celková doba všech výpadků Softwaru za vyhodnocované období

T_i je doba jednotlivého výpadku Softwaru

n je počet všech výpadků

12.8. Doba Provozu Softwaru definovaná pro účely tohoto článku je celková doba provozu Softwaru v hodinách za vyhodnocované období, kterým je kalendářní měsíc.

12.9. Do měření úrovně Dostupnosti (Hardware) nejsou započítávány:

a. dočasná vyřazení Hardware z provozu na základě předchozí dohody Objednatele a Dodavatele (odstávka),

b. pravidelná vyřazení Hardware z provozu Dodavatelem v časech sjednaných ve Smlouvě nebo její příloze (servisní okna)

c. výpadky Hardware způsobené Objednatelem přímo v důsledku jím provedených zásahů do Hardware, které nebyly Dodavatelem předem schváleny

12.10. Ustanovení odst. 12.5. až 12.8 ZOP se použijí obdobně s tím, že odkaz v odst. 12.5 ZOP na odst. 12.4 ZOP se nahrazuje odkazem na odst. 12.9 ZOP a slovo Software se nahrazují slovem Hardware.

13. ÚČAST PODDODAVATELŮ

13.1. 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.

13.2. 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 nebudou jednat v rozporu s ujednáními Smlouvy a jejími Přílohami, kterou mezi sebou uzavřeli Dodavatel a Objednatel.

13.3. Významný dodavatel je oprávněn využít k Plnění dle Smlouvy Poddodavatele neuvedené ve Smlouvě jen v případě, že to Smlouva výslovně připouští, a to za podmínek v ní uvedených. Nestanoví-li Smlouva jinak, podléhají jednotliví Poddodavatelé Významného dodavatele předchozímu písemnému schválení ze strany Objednatele. Dodavatel může ke schválení navrhnout nebo do Plnění Smlouvy zapojit pouze takové Poddodavatele, kteří nejsou v rozporu s požadavky Objednatele na Významného dodavatele.

14. REALIZAČNÍ TÝM

14.1. 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.

14.2. 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.

14.3. 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.

14.4. 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.

14.5. 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.

15. KOMUNIKACE STRAN

15.1. Objednatel a Dodavatel si pro vzájemnou komunikaci ohledně Smlouvy zvolí kontaktní osoby, jejichž seznam uvedou ve Smlouvě.

15.2. Jsou-li naplněny podmínky odst. 20.1. ZOP, vykonává kontaktní osoba na straně Dodavatele povinnosti kontaktní osoby pro kybernetickou bezpečnost vyplývající z článku 20. 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 20. ZOP).

15.3. Strany si navzájem oznámí jakékoliv změny v kontaktních osobách, přičemž taková změna je účinná uplynutím sedmého (7.) dne po jejím doručení.

15.4. 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.

16. NÁHRADA ŠKODY A SMLUVNÍ POKUTY

16.1. 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. 16.2. ZOP, pokud nejsou ve Smlouvě výslovně zakotveny jiné sankce, které vylučují aplikaci odst. 16.2. ZOP. Ustanovení § 2050 Občanského zákoníku se nepoužije. Objednatel je však oprávněn uplatnit po Dodavateli nárok na náhradu škody pouze do celkové souhrnné výše sta (100) procent Ceny. Pro vyloučení všech pochybností se limitace dle předchozí věty vztahuje i na souhrnnou výši smluvních pokut. Tímto není dotčena odpovědnost za škodu způsobenou úmyslně či hrubou nedbalostí.

16.2. Objednateli vzniká vůči Dodavateli právo na zaplacení smluvní pokuty:

a. poruší-li Dodavatel svoji povinnost řádně a včas provést Plnění ve výši 0,05 % z Ceny 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 řádně a včas provést jakoukoliv část Plnění ve výši 0,05 % z ceny takové části Plnění za každý započatý den prodlení až do řádného splnění této povinnosti; v případě, že by smluvní pokuty dle odst. 16.2. písm. a. a písm. b. ZOP měly běžet vůči Dodavateli zároveň, vzniká za takové období Objednateli nárok pouze dle odst. 16.2. písm. a. ZOP. Plnění se považuje pro účely této smluvní pokuty za řádně a včas provedené i v případě, že bylo akceptováno s výhradou;

c. poruší-li Dodavatel svoji povinnost dle odst. 8.1.11 ZOP ve výši 0,01 % z Ceny (případně ceny části Plnění, jedná-li se o akceptaci dílčí části Plnění) za každý započatý den prodlení až do řádného splnění této povinnosti;

d. 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;

e. 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;

f. poruší-li Dodavatel některou z povinností týkající se účasti Poddodavatelů anebo Realizačního týmu, ve výši 2 % z Ceny za každé jednotlivé porušení povinnosti;

g. 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;

h. 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;

i. 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;

j. V případě, že Dodavatel nedodrží Dostupnost stanovenou Servisním modelem dle odst. 12.2. ZOP, ve výši dle tabulky uvedené níže v závislosti na míře nedodržení požadované Dostupnosti:

Výše poklesu Dostupnosti oproti stanovené Dostupnosti Servisním modelem je	Výše smluvní pokuty
Do 2 %	10 % z ceny poskytovaného Plnění odpovídající vyhodnocovanému období dle odst. 12.8 ZOP
Od 2 (včetně) do 5 %	15 % z ceny poskytovaného Plnění odpovídající vyhodnocovanému období dle odst. 12.8 ZOP
Od 5 (včetně) do 10 %	25 % z ceny poskytovaného Plnění odpovídající vyhodnocovanému období dle odst. 12.8 ZOP
Od 10 % (včetně) a více	50 % z ceny poskytovaného Plnění odpovídající vyhodnocovanému období dle odst. 12.8 ZOP

k. 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;

l. ve výši a za podmínek dle článku 20. ZOP v oblasti kybernetické bezpečnosti;

m. ve výši a za podmínek dle článku 21. ZOP v oblasti ochrany osobních údajů;

n. ve výši a za podmínek dle článku 22. ZOP v oblasti ochrany Důvěrných informací; nebo

o. poruší-li Dodavatel svoji povinnost dle odst. 13.2. ZOP nebo 13.3. ZOP, ve výši 2 % z Ceny za každé jednotlivé porušení.

16.3. Pro smluvní pokuty stanovené v odst. 16.2. písm. 16.2.g. a 16.2.h. 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.

16.4. Zaplacením smluvních pokut není dotčeno právo Objednatele na náhradu Újmy v plném rozsahu.

16.5. Smluvní pokuta je splatná do 30 dnů ode dne doručení písemné výzvy Objednatele k jejímu uhrazení. Objednatel je oprávněn započíst nárok na zaplacení smluvní pokuty, i pokud ještě není splatný, proti jakémukoliv nároku Dodavatele na peněžité plnění vyplývajícímu ze Smlouvy.

16.6. 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.

17. ZÁRUKA ZA JAKOST A PRÁVA Z VADNÉHO PLNĚNÍ

17.1. Společná ustanovení

17.1.1. Dodavatel uděluje Objednateli záruku za jakost Plnění a všech jeho částí na dobu dvou (2) let ode dne akceptace výstupu Plnění.

17.1.2. 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.

17.1.3. 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.

17.1.4. Dodavatel neodpovídá za vady, pokud byly způsobeny zásahem do takových výstupů Plnění ze strany Objednatele nebo jím pověřené osoby, případně jiných dodavatelů Objednatele.

17.1.5. Objednatel je povinen oznámit vady Plnění Dodavateli prostřednictvím Helpdesku, nebude-li Stranami dohodnuto jinak.

17.1.6. 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.

17.2. Záruka vztahující se k Softwaru

17.2.1. Pokud výrobce Standardního Software poskytuje záruku za jakost, pak Dodavatel postupuje takovou záruku za jakost Objednateli. To nezbavuje Dodavatele povinnosti poskytnout Objednateli vlastní záruku za jakost ve smyslu tohoto článku.

17.2.2. 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

[1] Lhůta je stanovena v hodinách.
[2] Lhůta je stanovena ve dnech.
[3] Lhůta je stanovena ve dnech.

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]

17.3. Záruka vztahující se k Hardwaru

17.3.1. 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.

17.3.2. 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.

17.3.3. V případě, že odstranění reklamovaných vad bude trvat déle než dva (2) Pracovní dny, zavazuje se Dodavatel poskytnout Objednateli náhradní Hardware či jinou náhradní hmotnou věc po dobu trvání odstranění reklamované vady, nedohodnou-li se Strany jinak.

18. UKONČENÍ SMLUVNÍHO VZTAHU

18.1. 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.

18.2. 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. 20. ZOP opakovaně nebo závažným způsobem.

[4] Lhůta je stanovena v hodinách.
[5] Lhůta je stanovena ve dnech.
[6] Lhůta je stanovena ve dnech.

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. 13.2. ZOP nebo odst. 13.3. ZOP nebo Poddodavatel Dodavatele poruší některou z povinností vyplývající z požadavků dle odst. 13.2. ZOP.

f. Dodavatel podá insolvenční návrh jako dlužník ve smyslu § 98 Insolvenčního zákona nebo insolvenční soud nerozhodne o insolvenčním návrhu na Dodavatele do šesti (6) měsíců od zahájení insolvenčního řízení, nebo insolvenční soud vydá rozhodnutí o úpadku Dodavatele ve smyslu § 136 Insolvenčního zákona.

g. Je přijato rozhodnutí o povinném nebo dobrovolném zrušení Dodavatele (vyjma případů sloučení nebo splynutí).

h. Okolnost vylučující povinnost k náhradě Újmy kterékoli ze Stran trvá déle než 30 dnů;

i. dojde k Významné změně dle odst. 4.2. ZOP.

j. Dojde k Významné změně kontroly nad Dodavatelem nebo změny kontroly nad zásadními aktivy využívanými Dodavatelem k plnění Smlouvy, přičemž kontrolou se zde rozumí vliv, ovládání či řízení dle ust. § 71 a násl. ZOK, či ekvivalentní postavení.

k. Dojde k Významné změně ovlivnění nebo ovládání Dodavatele podle ust. § 71 a násl. ZOK nebo změně vlastnictví zásadních aktiv, využívaných Dodavatelem k plnění Smlouvy a změně oprávnění nakládat s těmito aktivy, či dojde ke změně ekvivalentní těmto změnám a tato změna bude Objednatelem vyhodnocena jako riziko bezpečnosti informací, které nelze odstranit jiným opatřením; toto ustanovení se uplatní i pro případ, že Dodavatel o takových změnách dopředu a včas neinformuje Objednatele.

18.3. Dodavatel je oprávněn odstoupit od Smlouvy pouze v případech jejího podstatného porušení, jestliže:

a. Objednatel nezaplatil jakoukoli dlužnou částku za Plnění dle Smlouvy řádně a včas a toto porušení nenapravil ani do 60 dnů ode dne obdržení písemné výzvy k nápravě; nebo

b. Objednatel poruší jinou povinnost dle Smlouvy podstatným způsobem a ve lhůtě 60 dnů ode dne obdržení písemné výzvy k nápravě toto své porušení nenapraví.

18.4. Dodavatel není oprávněn odstoupit od Smlouvy ve vztahu k části Plnění, za kterou mu již bylo Objednatelem zaplaceno.

19. ZMĚNY SMLOUVY A ZMĚNOVÉ ŘÍZENÍ

19.1. 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.

19.2. 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.

19.3. 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.

20. KYBERNETICKÁ BEZPEČNOST

20.1. Tento článek se uplatní v případě, kdy tak výslovně stanoví Smlouva, pokud je Předmětem Smlouvy Informační či komunikační systém, pokud má Plnění dopad na Informační či komunikační systém, nebo pokud je Smlouva uzavřena s Významným dodavatelem či Provozovatelem. Zda je Dodavatel Významným dodavatelem či Provozovatelem, stanoví Smlouva. Na jiné Smlouvy a vztahy se neuplatní, ledaže se Dodavatel stane Významným dodavatelem či Provozovatelem v průběhu plnění Smlouvy. V takovém případě se na něj čl. 20. uplatní v rozsahu v jakém to po něm lze spravedlivě požadovat.

20.2. Dodavatel se při plnění Smlouvy zavazuje postupovat v souladu se ZKB, VKB a souvisejícími právními předpisy, dodržovat zásady bezpečnosti informací, Interní předpisy Objednatele a z nich vyplývající povinnosti týkající se bezpečnostních opatření, provozní řády prostor Objednatele, rozhodnutí, 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 ZKB a VKB, včetně upozorňování a zajištění hlášení Kybernetických bezpečnostních událostí a Kybernetických bezpečnostních incidentů Objednateli, jakož i další bezpečnostní politiky, metodiky a postupy, se kterými byl Objednatelem seznámen.

20.3. 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. Kontaktní osoba Dodavatele je povinna splnění povinnosti dle předchozí věty Objednateli potvrdit do 30 dnů od uzavření Smlouvy. 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.

20.4. Není-li ve Smlouvě ujednáno jinak, je Dodavatel povinen vytvořit, pravidelně aktualizovat a vynucovat vůči osobám podílejícím se, byť i nepřímo, na Předmětu Smlouvy:

a. politiku řízení přístupu, na základě které přidělí oprávnění k výkonu činností jednotlivým rolím svých fyzických osob (přístup pro více osob na jednom účtu je nežádoucí a lze pouze se souhlasem Objednatele) podílejících se na plnění Smlouvy (zaměstnanci, programátoři podnikatelé apod.) 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; 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;

b. politiku zvládání Kybernetických bezpečnostních událostí a Kybernetických bezpečnostních incidentů obsahující činnosti, role, odpovědnosti a pravomoci k rychlému a účinnému zvládání Kybernetických bezpečnostních událostí a Kybernetických bezpečnostních incidentů.

20.4.2. Kontaktní osoba Dodavatele je povinna před započetím Plnění, nejpozději však do 30 dnů od uzavření Smlouvy, určit a popsat veškerá dotčená primární i podpůrná aktiva na straně Dodavatele potřebná pro plnění Smlouvy. 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. Dodavatel je povinen řídit rizika spojená s Plněním dle Smlouvy minimálně dle standardů požadovaných normou ISO 27001 a případně dle Interních předpisů, pokud obsahují závazná pravidla pro řízení rizik. Dodavatel je povinen bez zbytečného odkladu po uzavření Smlouvy kontaktní osobu Objednatele informovat o způsobu řízení rizik a o zbytkových rizicích souvisejících s Plněním Smlouvy a následně v pravidelných intervalech informovat o změnách.

20.5. Dodavatel je povinen zaslat kontaktní osobě Objednatele bez zbytečného odkladu všechna hlášení o událostech, která mají charakter Kybernetické bezpečnostní události nebo 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 této Kybernetické bezpečnostní události anebo Kybernetickému bezpečnostnímu incidentu, případně zvolí jinou formu dohodnutou mezi Objednatelem a Dodavatelem určenou ke včasnému hlášení Kybernetické bezpečnostní události nebo Kybernetického bezpečnostního incidentu a/nebo již učiněných opatření. Dodavatel je povinen veškeré Kybernetické bezpečnostní události a Kybernetické bezpečnostní incidenty zaznamenávat a po nezbytně dlouhou dobu uchovávat. Dodavatel je povinen poskytnout Objednateli veškerou nezbytnou součinnost k detekci, vyhodnocení či řešení Kybernetické bezpečností události nebo Kybernetického bezpečnostního incidentu, a to včetně případné realizace nutných opatření dle pokynů Objednatele. 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 jednotlivou Kybernetickou bezpečnostní událost nebo Kybernetický bezpečnostní incident jedním z následujících způsobů:

a. e-mailem na adresu kontaktní osoby uvedené ve Smlouvě; nebo

b. telefonicky na telefonní číslo kontaktní osoby uvedené ve Smlouvě; nebo

c. ohlášením do Helpdesku Objednatele.

20.6. Dodavatel je povinen pravidelně alespoň čtvrtletně předkládat Objednateli zprávu o počtu a druhu útoků a Kybernetických bezpečnostních událostí a Kybernetických bezpečnostních incidentů, které zaznamenal ve spojení s Plněním a/nebo Předmětem Smlouvy.

20.7. Dodavatel se zavazuje poskytnout Objednateli veškerou součinnost nezbytnou k tomu, aby Objednatel řádně naplňoval právní povinnosti stanovené ZKB, VKB a Interními předpisy. Zejména se Dodavatel zavazuje poskytnout Objednateli součinnost směřující k zavedení a provádění bezpečnostních opatření podle ZKB, VKB a Interních předpisů a řešení Kybernetických bezpečnostních událostí a Kybernetických bezpečnostních incidentů. Jestliže Dodavatel při plnění Smlouvy zjistí či jako odborník mohl a měl zjistit rozpor ustanovení Interních předpisů se ZKB, VKB anebo rozhodnutím či jiným pokynem NÚKIB v souladu se ZKB, je povinen takový rozpor Objednateli neprodleně ohlásit a poskytnout Objednateli součinnost k jeho odstranění.

20.8. Dodavatel bere na vědomí, že v rámci provádění Plnění může být podroben Interním předpisům Objednatele či jeho pokynům v oblasti řízení kontinuity činností, zejména může být zahrnut do havarijních plánů, úkolů při aktivaci řízení kontinuity činností, bezpečnostní politiky apod., a to v rozsahu, v jakém lze po Dodavateli spravedlivě požadovat s ohledem na předmět plnění.

20.9. 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.

20.10. 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.

20.11. Objednatel má právo prostřednictvím určených osob provádět v pravidelných intervalech (1x ročně, 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 ZKB a/nebo VKB, audit kybernetické bezpečnosti, tj. dodržování bezpečnosti informací dle Interních předpisů, ZKB a VKB 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:

a. nehlášená návštěva u Dodavatele v místě umístění členů Realizačního týmu či jiných osob podílejících se na plnění Smlouvy v rozsahu tří (3) hodin vždy nejčastěji čtyřikrát (4x) za rok; a

b. nehlášený telefonát 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.

20.12. 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.

20.13. 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 a bezodkladně informovat Objednatele do 7 dnů.

20.14. Je-li součástí Předmětu 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 NÚKIB.

20.15. 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:

a. provádět analýzy topologie sítě či skenování aktivních částí Předmětu Plnění; a

b. realizovat bezpečnostní opatření pro odstranění nebo blokování síťových spojení, která neodpovídají požadavkům na ochranu integrity komunikační sítě.

20.15.2. Významný dodavatel je dále povinen:

a. poskytnout Objednateli veškeré potřebné informace a součinnost v procesu řízení a evidence změn v souladu s § 11 VKB 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 dokumentace, souvisejícím testováním, zajištění možnosti navrácení do původního stavu a provedení dalších činností dle VKB);

b. strpět a poskytnout Objednateli veškerou potřebnou součinnost v případě nutnosti provést penetrační testování;

c. zpracovat a pravidelně aktualizovat bezpečnostní dokumentaci v rozsahu stanoveném ve Smlouvě;

d. průběžně detekovat známé zranitelnosti dotčených aktiv Objednatele a bezodkladně na ně upozorňovat Objednatele; a

e. vést v elektronické formě provozní deník obsahující veškeré podstatné okolnosti související s plněním povinností Dodavatele dle článku 20. ZOP a/nebo Plněním, provozní události důležitých aktiv a relevantní záznamy o plnění povinností Dodavatele dle článku 20. ZOP a zpřístupnit jej Objednateli prostřednictvím zabezpečeného vzdáleného přístupu, není-li ve Smlouvě ujednán jiný způsob; v provozním deníku Významný dodavatel dále do 20. dne následujícího měsíce uvede výstup z monitoringu dostupnosti, důvěrnosti a integrity aktiv

Objednatele, se kterými pracuje v rámci plnění Smlouvy, prováděného nejméně jedenkrát měsíčně a vyhodnocovaného vždy k 10. dni následujícího měsíce.

20.15.3. Provozovatel je dále povinen:

a. provádět pravidelné zálohy dat a programového vybavení vztahujících se k Plnění dle Smlouvy, zabezpečit je vhodnými prostředky proti neoprávněným přístupům nebo jejich ztrátě a v pravidelných intervalech testovat funkčnost těchto záloh, nejméně jedenkrát za měsíc, není-li ve Smlouvě ujednáno jinak;

b. plnit další povinnosti vyplývající pro Provozovatele ze ZKB a VKB.

20.16. Pokud Objednatel zjistí, že Dodavatel postupuje v rozporu s tímto článkem, je Objednatel v takovém případě oprávněn dožadovat se toho, aby Dodavatel odstranil vady vzniklé vadným postupem Dodavatele, zdržel se provádění postupů, které jsou v rozporu s tímto článkem, nebo konal, jak je od něj vyžadováno tímto článkem, a dále Smlouvou 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. Jestliže Dodavatel včas neodstraní nedostatky ve smyslu předchozí věty tohoto odstavce nebo se jedná o porušení povinnosti (bez ohledu na jeho závažnost), pak je Objednatel oprávněn od Smlouvy odstoupit.

20.17. 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 Kybernetické bezpečnostní události anebo 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.

20.18. Dodavateli nenáleží za plnění povinností souvisejících s bezpečností informací ve smyslu článku 20. ZOP jakákoliv další odměna, resp. taková odměna je součástí Ceny.

20.19. Objednatel je oprávněn požadovat na Dodavateli zaplacení smluvní pokuty:

a. za každý den prodlení při zavedení bezpečnostních opatření podle ZKB, VKB, 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 ZKB, VKB, 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 Kybernetické bezpečnostní události nebo Kybernetického bezpečnostního incidentu;

d. ve výši 2 % z Ceny za každý případ neumožnění nebo odepření provedení kontroly a auditu kybernetické bezpečnosti ve smyslu článku 20. ZOP;

e. ve výši 5 % z Ceny za každý případ porušení článku 20. 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 20. ZOP, dané porušení nebylo odstraněno a negativní následek porušení povinnosti stále trvá; a

g. ve výši 1 % z Ceny za každý případ jiného porušení článku 20. ZOP neuvedeného výše.

21. OCHRANA OSOBNÍCH ÚDAJŮ

21.1. 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.

21.2. 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.

21.3. 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.

21.4. 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.

21.5. 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.

21.6. 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.

21.7. 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.

21.8. 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.

21.9. 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.

21.10. Po ukončení zpracování Osobních údajů podle Smlouvy je Dodavatel povinen poskytnout Objednateli všechna Zařízení obsahující Osobní údaje, pokud je to možné, a vymazat všechny zpracovávané Osobní údaje ze všech svých systémů nebo databází, včetně vymazání všech záložních kopií, s výjimkou, kdy uchovávání vyžadují právní předpisy, nebo k tomu dal písemný souhlas Objednatel.

21.11. 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.

21.12. 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.

22. OCHRANA DŮVĚRNÝCH INFORMACÍ

22.1. 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.

22.2. Dodavatel se zavazuje použít Důvěrné informace pouze k plnění svých povinností vyplývajících ze Smlouvy. Dodavatel nesmí použít Důvěrné informace k jinému účelu.

22.3. 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.

22.4. Dodavatel nesmí Důvěrné informace bez předchozího písemného souhlasu Objednatele rozmnožovat, kopírovat či jakýmkoliv jiným způsobem reprodukovat. Dodavatel dále nesmí Důvěrné informace bez předchozího písemného souhlasu Objednatele uchovávat v jakékoliv databázi, počítačovém programu, úložišti či na datovém nosiči, vyjma případů, kdy je takové uchovávání Důvěrných informací nezbytné pro účel vyplývající ze Smlouvy.

22.5. 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.

22.6. 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.

22.7. 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. 22.6. ZOP

b. ve výši 100 000 Kč za každé jednotlivé jednání, které představuje porušení jakékoli z povinností stanovených v odst. 22.6. ZOP.

SPRÁVA ŽELEZNIC

Příloha č. 6 Smlouvy

Obchodní podmínky ke Smlouvě o dílo

OBSAH OBCHODNÍCH PODMÍNEK

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

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

ČÁST 1 - ÚVODNÍ USTANOVENÍ

1. Pro účely těchto Obchodních podmínek mají následující slova význam u nich uvedený:
   - 1.1. **Občanský zákoník** – zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.
   - 1.2. **ZoDPH** – zákon č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.
   - 1.3. **ZoÚ** – zákon č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů.
   - 1.4. **SZ** – zákon č. 283/2021 Sb., stavební zákon, ve znění pozdějších předpisů.
   - 1.5. **ZZVZ** – zákon č. 134/2016 Sb., o zadávání veřejných zakázkách, ve znění pozdějších předpisů.
   - 1.6. **Objednatel** – Správa železnic, státní organizace, IČO 70994234, se sídlem Praha 1 – Nové Město, Dlážděná 1003/7, PSČ 110 00, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze pod sp. zn. A 48384.
   - 1.7. **Zhotovitel** – osoba uvedená ve Smlouvě o dílo jako Zhotovitel; též všechny osoby, které jsou ve Smlouvě o dílo uvedené na straně Zhotovitele, je-li na straně Zhotovitele více než jedna osoba.
   - 1.8. **Smluvní strany** – Objednatel a Zhotovitel.
   - 1.9. **Smluvní strana** – Objednatel nebo Zhotovitel dle smyslu ujednání.
   - 1.10. **Nabídka** – souhrn dokumentů, které Zhotovitel podal jako návrh do zadávacího řízení, na jehož základě byla uzavřena Smlouva o dílo.
   - 1.11. **Smlouva o dílo** – smlouva uzavřená mezi Smluvními stranami, která odkazuje na Obchodní podmínky.
   - 1.12. **Obchodní podmínky** – tento text obchodních podmínek.
   - 1.13. **Předmět díla** – věc, která má být zhotovena, nebo činnost s jiným výsledkem, specifikovaná ve Smlouvě o dílo.
   - 1.14. **Související plnění** – další plnění (práce, dodávky, služby, činnosti a výkony), která je Zhotovitel povinen dle Smlouvy o dílo poskytnout vedle samotného provedení Předmětu díla.
   - 1.15. **Rozhodnutí Objednatele** – veškerá rozhodnutí, sdělení, souhlasy, povolení či jiné výsledky úkonů orgánů státní správy, samosprávy či jiných subjektů, které pro účely Díla nebo v souvislosti s ním získal nebo do doby dokončení Díla získá Objednatel a jež Objednatel Zhotoviteli předal nebo s nimiž se Zhotovitel jinak seznámil.
   - 1.16. **Rozhodnutí Zhotovitele** – veškerá rozhodnutí, sdělení, souhlasy, povolení či jiné výsledky úkonů orgánů státní správy, samosprávy či jiných subjektů, které je Zhotovitel povinen dle Smlouvy o dílo získat. Jakékoliv Rozhodnutí Zhotovitele, které není v českém jazyku, musí být do českého jazyka přeloženo a překlad musí být úředně ověřen.
   - 1.17. **Veřejnoprávní podklady** – souhrn Rozhodnutí Objednatele a Rozhodnutí Zhotovitele.
   - 1.18. **Doklady** – veškeré listiny, které se vztahují k Předmětu díla nebo Souvisejícímu plnění a které jsou třeba k jejich převzetí a užívání; veškerá Rozhodnutí Zhotovitele; veškeré další listiny, vyjma Výzvy k úhradě, které je Zhotovitel dle Smlouvy o dílo povinen předat Objednateli. Všechny Doklady musejí být v českém jazyku, nebo v původním jazyku s překladem do českého jazyka, není-li uvedeno jinak.
   - 1.19. **Dílo** – souhrn veškerých plnění, která je Zhotovitel povinen provést za účelem splnění Smlouvy o dílo; zahrnuje zejm. provedení Předmětu díla, poskytnutí či provedení Souvisejícího plnění a dodání Dokladů.
   - 1.20. **Cena díla** – cena za Dílo sjednaná ve Smlouvě o dílo (částka bez DPH).
   - 1.21. **Výzva k úhradě** – daňový doklad, je-li Zhotovitel povinen dle ZoDHP uhradit v souvislosti s provedením Díla nebo jeho části DPH, nebo faktura, pokud Zhotovitel v souvislosti s provedením Díla nebo jeho části není dle ZoDPH povinen uhradit DPH.

1.22. **Vícepráce** – práce, dodávky nebo služby nad rámec Smlouvy o dílo, na jejichž provedení se Smluvní strany dohodnou po uzavření Smlouvy o dílo.
1.23. **Méněpráce** – práce, dodávky nebo služby v rámci Smlouvy o dílo, na jejichž vypuštění se Smluvní strany dohodnou po uzavření Smlouvy o dílo.
1.24. **Obalový materiál** – palety, dřevěné desky či jiné věci, které slouží pro potřeby přepravy nebo ochrany Předmětu díla. Dle kontextu Smlouvy o dílo se rozumí Obalovým materiálem též jednotlivý kus palety, dřevěné desky nebo jiné věci.
1.25. **Přejímací řízení** – proces, při kterém Zhotovitel předává a Objednatel kontroluje a přebírá Dílo, nebo je odmítá.
1.26. **Předávací protokol** – listina osvědčující předání a převzetí Díla nebo jeho části, jejíž minimální náležitosti jsou uvedeny v části Předání a převzetí Díla.
1.27. **Záruční doba** – doba, do jejíhož uplynutí je Objednatel oprávněn uplatňovat práva z vad plnění poskytnutého Zhotovitelem na základě Smlouvy o dílo; Záruční doba činí 24 měsíců.
1.28. **CTD** – Centrum techniky a diagnostiky, organizační jednotka Objednatele.

ČÁST 2 - NÁVRH NA UZAVŘENÍ SMLOUVY O DÍLO

2. Odpověď Smluvní strany na návrh na uzavření Smlouvy o dílo učiněný druhou Smluvní stranou, která vymezuje obsah návrhu jinými slovy nebo která obsahuje jakékoliv, byť nepodstatné, dodatky, odchylky, výhrady nebo omezení není přijetím návrhu.
3. I pozdní přijetí návrhu na uzavření Smlouvy o dílo má účinky včasného přijetí, pokud navrhující Smluvní strana bez zbytečného odkladu alespoň ústně vyrozumí druhou Smluvní stranu, že přijetí považuje za včasné, nebo pokud se začne chovat ve shodě s návrhem.
4. Plyne-li z písemnosti, která vyjadřuje přijetí návrhu na uzavření Smlouvy o dílo, že byla odeslána za takových okolností, že by došla navrhující Smluvní straně včas, kdyby její přeprava probíhala obvyklým způsobem, má pozdní přijetí účinky včasného přijetí, ledaže navrhující Smluvní strana bez odkladu vyrozumí alespoň ústně druhou Smluvní stranu, že považuje návrh za zaniklý.
5. Bez ohledu na jakékoliv okolnosti nelze přijmout návrh na uzavření Smlouvy o dílo tak, že se Smluvní strana, jíž je návrh určen, podle návrhu zachová.
6. **Odkáží-li Smluvní strany v návrhu na uzavření Smlouvy o dílo i v přijetí návrhu na obchodní podmínky, které si odporují, je Smlouva o dílo přesto uzavřena s obsahem určeným v tom rozsahu, v jakém obchodní podmínky nejsou v rozporu; to platí i v případě, že to obchodní podmínky vylučují. Vyloučí-li to některá ze Smluvních stran nejpozději bez zbytečného odkladu po výměně projevů vůle, Smlouva o dílo uzavřena není.**
7. Smlouva o dílo může být uzavřena pouze v písemné podobě.

ČÁST 3 - DÍLO

8. Zhotovitel se zavazuje provést na svůj náklad a nebezpečí pro Objednatele Dílo a Objednatel se zavazuje Dílo převzít a zaplatit Zhotoviteli Cenu díla a příslušnou DPH, bude-li Zhotovitel povinen dle ZoDHP uhradit v souvislosti s provedením Díla nebo jeho části DPH.
9. Zhotovitel je povinen provést Dílo v jakosti, provedení a způsobem uvedeným ve Smlouvě o dílo a zároveň
   9.1. v jakosti, provedení a způsobem, jenž odpovídá vlastnostem a způsobu, které Zhotovitel popsal nebo které Objednatel očekával s ohledem na povahu Díla, a to v rozsahu, ve kterém není v rozporu s jakostí, provedením a způsobem sjednaným ve Smlouvě o dílo,
   9.2. v jakosti, provedení a způsobem, jenž se hodí k účelu vyplývajícímu ze Smlouvy o dílo a není-li v ní vyjádřen pak k účelu, ke kterému se Dílo obvykle používá, a to v rozsahu, ve kterém není v rozporu s jakostí, provedením a způsobem sjednaným ve Smlouvě o dílo,

9.3. v souladu s Veřejnoprávními podklady,
9.4. v souladu s požadavky právních předpisů a příslušných ČSN.

10. Je-li jakost či provedení Předmětu díla zároveň určeno vzorkem nebo předlohou, musí Předmět díla odpovídat jakostí nebo provedením vzorku nebo předloze. Liší-li se jakost nebo provedení určené ve Smlouvě o dílo a vzorek nebo předloha, rozhoduje Smlouva o dílo. Určuje-li Smlouva o dílo a vzorek nebo předloha jakost nebo provedení rozdílně, nikoliv však rozporně, musí Předmět díla odpovídat Smlouvě o dílo i vzorku nebo předloze.
11. Opatřuje-li Zhotovitel věc za účelem jejího zpracování při provádění Díla, je povinen opatřit věc novou, nepoužitou a neopotřebovanou.
12. Je-li součástí Díla povinnost Zhotovitele zajistit jakékoliv Rozhodnutí Zhotovitele, je Zhotovitel povinen provést veškeré činnosti, kterých je k získání příslušného Rozhodnutí Zhotovitele třeba.

ČÁST 4 - CENA DÍLA

13. Cena díla zahrnuje veškeré náklady Zhotovitele spojené se splněním jeho povinností vyplývajících ze Smlouvy o dílo a Obchodních podmínek a zisk Zhotovitele.
14. Objednatel není povinen hradit v souvislosti se Smlouvou o dílo žádné jiné finanční částky, než Cenu díla a případně příslušnou DPH, není-li uvedeno jinak (tím není dotčeno právo Zhotovitele na případnou úhradu smluvní pokuty, úroků z prodlení, či jiných sankcí, a právo na náhradu škody způsobené Objednatelem).
15. Cena díla obsahuje předpokládaný vývoj cen vstupních nákladů a předpokládané zvýšení ceny v závislosti na čase plnění, a to až do dokončení Díla.
16. Je-li Zhotovitel povinen dle ZoDHP uhradit v souvislosti s provedením Díla nebo jeho části DPH, je Objednatel povinen Zhotoviteli takovou DPH uhradit vedle Ceny díla.
17. Cenu díla lze měnit pouze za podmínek uvedených v části Změna ceny Díla (viz ČÁST 5 - Obchodních podmínek).
18. Konečné finanční částky na fakturách/daňových dokladech nesmí být zaokrouhlovány na celé Kč. Objednatel nebude akceptovat zaokrouhlení a haléřové vyrovnání v případě uvedení na faktuře/daňovém dokladu nebude hradit.

ČÁST 5 - ZMĚNA CENY DÍLA

19. Změna ceny díla je možná pouze v případě
    19.1. víceprací nebo méněprací,
    19.2. zjistí-li Zhotovitel při kontrole projektové dokumentace předané mu Objednatelem vady nebo její nevhodnost či neúplnost, které mají vliv na náklady Zhotovitele,
    19.3. v jiných případech jen pokud se na tom Smluvní strany dohodnou.
20. V případě víceprací i méněprací Zhotovitel provede ocenění jejich soupisu jednotkovými cenami položkového rozpočtu, je-li ve Smlouvě o dílo zahrnut.
21. Pokud práce, dodávky nebo služby nebudou v položkovém rozpočtu obsaženy nebo položkový rozpočet není ve Smlouvě o dílo zahrnut, užije se pro jejich ocenění cena obvyklá.
22. V případě vad, nevhodnosti nebo neúplnosti projektové dokumentace, kterou předal Objednatel Zhotoviteli, je-li taková projektová dokumentace součástí Smlouvy o dílo, mají-li takové vady, nevhodnosti nebo neúplnosti vliv na náklady Zhotovitele, postupují smluvní strany obdobně jako při oceňování víceprací nebo méněprací.
23. Změnu Ceny díla lze provést jen uzavřením dodatku ke Smlouvě o dílo.

ČÁST 6 - PLATEBNÍ PODMÍNKY

24. Objednatel neposkytuje zálohy.

25. Zhotovitel vyúčtuje Objednateli Cenu díla a případnou DPH Výzvou k úhradě.
26. Cenu díla a případnou DPH je Objednatel povinen uhradit Zhotoviteli do 60 dnů ode dne převzetí Díla; má-li být dle Smlouvy o dílo proveden též zkušební provoz, pak do 60 dnů ode dne úspěšného ukončení zkušebního provozu, nastane-li den skončení zkušebního provozu později než převzetí Díla Objednatelem.
27. Cena díla a případná DPH je uhrazena dnem jejich odepsání z bankovního účtu Objednatele.
28. Je-li Výzva k úhradě fakturou, musí obsahovat náležitosti účetního dokladu dle §11 ZoÚ a náležitosti stanovené v §435 Občanského zákoníku.
29. Je-li Výzva k úhradě daňovým dokladem, musí obsahovat náležitosti daňového dokladu dle §28 ZoDPH a náležitosti stanovené v §435 Občanského zákoníku.
30. Výzva k úhradě musí vždy obsahovat číslo Smlouvy o dílo, včetně uvedení uzavřených dodatků, její přílohou musí být vždy jedno vyhotovení Protokolu o převzetí potvrzeného Objednatelem. Ve výzvě k úhradě musí být vždy uvedeny jako identifikace Objednatele nejméně následující údaje:
    Správa železnic, státní organizace
    Dlážděná 1003/7, 110 00 Praha 1 – Nové Město
    IČO: 709 94 234
    Obchodní rejstřík u Městského soudu v Praze, sp. zn. A 48384
31. Výzvu k úhradě je Zhotovitel povinen doručit Objednateli nejpozději 15 dnů před uplynutím doby uvedené v odstavci 26 Obchodních podmínek.
32. Výzvy k úhradě, vč. všech příloh, budou Objednateli zasílány následovně:
    32.1. v digitální podobě na e-mailovou adresu ePodatelnaCFU@spravazeleznic.cz, nebo
    32.2. v digitální podobě do datové schránky s identifikátorem Uccchjm, nebo
    32.3. v listinné podobě **ve dvou vyhotoveních** na adresu Správa železnic, státní organizace, Centrální finanční účtárna Čechy, Náměstí Jana Pernera 217, 530 02 Pardubice, nebo
    32.4. prostřednictvím kontaktního formuláře na webových stránkách Objednatele https://www.spravazeleznic.cz/kontakty/podatelna.

    Objednatel upřednostňuje příjem Výzev k úhradě v digitální podobě ve formátu PDF/A, ISO 19005, min. verze PDF/A-2b, na výše uvedené emailové adrese. **V případě, že je Výzva k úhradě zasílána na výše uvedenou e-mailovou adresu, považuje se za doručenou po obdržení notifikace doručení, která je automaticky odesílána odesílateli**.

33. Splatnost Výzvy k úhradě musí být stanovena tak, aby nenastala dříve, než uplyne doba stanovená v odstavci 26 Obchodních podmínek.
34. Stanoví-li Výzva k úhradě splatnost delší, než je jako minimální stanovena v předchozím odstavci, je Objednatel oprávněn uhradit Cenu díla a případnou DPH ve lhůtě splatnosti určené ve Výzvě k úhradě.
35. Stane-li se zhotovitel nespolehlivým plátcem nebo daňový doklad zhotovitele bude obsahovat číslo bankovního účtu, na který má být plněno, aniž by bylo uvedeno ve veřejném registru spolehlivých účtů, je objednatel oprávněn z finančního plnění uhradit daň z přidané hodnoty přímo místně a věcně příslušnému správci daně zhotovitele.
36. Je-li ve Smlouvě o dílo výslovně stanoveno, že Zhotovitel bude předávat Objednateli Dílo po částech, je Zhotovitel oprávněn vystavit Výzvu k úhradě předávané části Díla poté, co Objednatel převezme příslušnou část Díla. Ustanovení odstavců 26 - 35 Obchodních podmínek se užijí obdobně.
37. Ustanovení §2611, §2620–2622 a §2624 Občanského zákoníku se neužijí.

ČÁST 7 - MÍSTO PLNĚNÍ

38. Zhotovitel je povinen předat Objednateli Dílo v místě, jež vyplývá ze Smlouvy o dílo. Nelze-li takto místo předání Díla zjistit, vyzve Zhotovitel Objednatele, aby sdělil, ve kterém místě má Zhotovitel Objednateli Dílo předat. Nesdělí-li Objednatel místo plnění

do 5 pracovních dnů ode dne doručení výzvy Zhotovitele, je Zhotovitel povinen Dílo předat Objednateli v sídle Objednatele.

ČÁST 8 - DOBA PLNĚNÍ

39. Zhotovitel je povinen zahájit provádění Díla bez zbytečného odkladu po uzavření Smlouvy o dílo.
40. Je-li součástí povinností Zhotovitele doprava Díla po jeho zhotovení do místa plnění dle Smlouvy o dílo, je Zhotovitel povinen dopravit Dílo do místa plnění v pracovní den v době od 8 do 15 hodin. Dodá-li Zhotovitel Dílo Objednateli v jiné než uvedené době, je Objednatel oprávněn odmítnout Dílo převzít a není zároveň v prodlení s převzetím Díla. Připadne-li konec sjednané doby plnění na sobotu, neděli nebo svátek, není Zhotovitel v prodlení, dodá-li Dílo nejblíže následující pracovní den v časovém rozmezí dle tohoto odstavce.
41. Není-li stanoveno jinak, je Zhotovitel povinen začít s plněním svých povinností vždy bez zbytečného odkladu.
42. Zjistí-li Zhotovitel jakékoliv skutečnosti, které by mohly mít vliv na dobu plnění, je Zhotovitel povinen bez zbytečného odkladu Objednatele o takových skutečnostech informovat.

ČÁST 9 - PROVÁDĚNÍ DÍLA

43. Zhotovitel provede Dílo s potřebnou péčí v ujednaném čase a obstará vše, co je k provedení Díla potřeba.
44. Při provádění Díla postupuje Zhotovitel samostatně, je však vázán příkazy Objednatele ohledně způsobu provádění Díla.
45. Zhotovitel se zavazuje brát v úvahu veškeré upozornění Objednatele, týkající se realizace Díla a upozorňující na možné porušování smluvních i právními předpisy stanovených povinností Zhotovitele.
46. Zhotovitel je povinen upozornit Objednatele bez zbytečného odkladu na nevhodnou povahu věcí převzatých od Objednatele nebo příkazů daných mu Objednatelem k provedení Díla, jestliže Zhotovitel mohl tuto nevhodnost zjistit při vynaložení odborné péče.
47. Překáží-li nevhodná věc nebo příkaz v řádném provádění Díla, Zhotovitel jej v nezbytném rozsahu přeruší až do výměny věci nebo změny příkazu; trvá-li Objednatel na provádění Díla s použitím předané věci nebo podle daného příkazu, má Zhotovitel právo požadovat, aby tak Objednatel učinil v písemné formě.
48. Doba stanovená pro dokončení Díla se prodlužuje o dobu vyvolanou přerušením dle předchozího odstavce.
49. Trvá-li Objednatel na provádění Díla s použitím předané věci nebo podle daného příkazu a zachová-li se Zhotovitel podle toho, nemá Objednatel práva z vady Díla vzniklé pro nevhodnost věci nebo příkazu.

Harmonogram

50. Je-li dle Smlouvy o dílo vyžadován Harmonogram provádění Díla, je Zhotovitel povinen jej předložit Objednateli bez zbytečného odkladu po uzavření Smlouvy o dílo, nejpozději však do 10 dnů ode dne uzavření Smlouvy o dílo.
51. Zhotovitel je povinen udržovat harmonogram v aktuálním stavu a v případě změny vždy předat Objednateli bezodkladně aktualizovaný harmonogram.

Kontrola provádění prací

52. Objednatel je oprávněn kontrolovat provádění Díla. Zjistí-li objednatel, že Zhotovitel provádí Dílo v rozporu s povinnostmi vyplývajícími ze Smlouvy o dílo, Obchodních podmínek, Veřejnoprávních podkladů, právních předpisů nebo příslušných ČSN, je Objednatel oprávněn dožadovat se toho, aby Zhotovitel odstranil vady vzniklé vadným prováděním a Dílo prováděl řádným způsobem. Jestliže tak Zhotovitel neučiní v přiměřené lhůtě, jedná se o podstatné porušení Smlouvy o dílo.

53. Zhotovitel je povinen písemně vyzvat Objednatele ke kontrole a prověření prací, které v dalším postupu budou zakryty nebo se stanou nepřístupnými. Zhotovitel je povinen vyzvat Objednatele nejméně 3 pracovní dny před termínem, v němž budou předmětné práce zakryty nebo znepřístupněny.
54. Před zakrytím nebo znepřístupněním prací je Zhotovitel povinen pořídit podrobnou fotodokumentaci prací a předat ji Objednateli v digitální podobě na CD nebo DVD nosiči bez zbytečného odkladu po pořízení fotodokumentace.
55. Pokud se Objednatel ke kontrole přes včasné písemné vyzvání nedostaví, je Zhotovitel oprávněn předmětné práce zakrýt. Bude-li se v tomto případě Objednatel dodatečně požadovat jejich odkrytí, je Zhotovitel povinen toto odkrytí provést na náklady Objednatele. Pokud se však zjistí, že práce nebyly řádně provedeny, nese veškeré náklady spojené s odkrytím prací, opravou chybného stavu a následným zakrytím Zhotovitel.
56. Obdobně bude-li Objednatel požadovat vykonání zvláštních zkoušek nebo ověření jakékoliv části Díla z důvodu podezření, že tato část Díla neodpovídá Smlouvě o dílo, Obchodním podmínkám, Veřejnoprávním podkladům, právním předpisům nebo příslušným ČSN, a bude-li zjištěno, že podezření bylo správné, nese náklady spojené s vykonáním zkoušek nebo ověřením Zhotovitel.
57. Zhotovitel je povinen umožnit výkon technického a autorského dozoru.

Kontrolní dny

58. Pro účely kontroly průběhu provádění Díla může Objednatel nebo jím pověřená osoba provést kontrolní dny v termínech nezbytných pro řádné provádění kontroly.
59. Kontrolních dnů se zúčastní zástupci Objednatele případně osob vykonávajících funkci technického dozoru a autorského dozoru.
60. Zástupci Zhotovitele jsou povinni se kontrolních dnů zúčastňovat. Zhotovitel má právo přizvat na kontrolní den své poddodavatele podílející se v souladu se Smlouvou o dílo a Obchodními podmínkami na provádění Díla.
61. Kontrolní dny vede Objednatel nebo jím pověřená osoba.
62. Obsahem kontrolního dne je zejména zpráva Zhotovitele o postupu prací, kontrola postupu prací, připomínky a podněty osob vykonávajících funkci technického a autorského dozoru a stanovení případných nápravných opatření a úkolů.
63. Objednatel nebo jím pověřená osoba pořizuje z kontrolního dne zápis, který předá všem zúčastněným.

Dodržování zákazu požívání alkoholických nápojů a užívání jiných návykových látek

64. Objednatel je oprávněn provádět u všech osob, které Zhotovitel používá při provádění díla, kontrolu, zda tyto osoby nejsou pod vlivem alkoholu nebo návykové látky.
65. Kontrola bude prováděna dle Směrnice SŽDC č. 120 Dodržování zákazu kouření, požívání alkoholických nápojů a užívání jiných návykových látek, č.j. 36503/2017-SŽDC-GŘ-O10 ze dne 3.11.2017, účinné od 7.11.2017 nebo dle jiného předpisu, který uvedenou směrnici případně nahradí.
66. Výše uvedená Směrnice je pro Zhotovitele a všechny osoby, které Zhotovitel používá při provádění Předmětu Díla závazná okamžikem platnosti a účinnosti Smlouvy o dílo. Zhotovitel a tím i všechny osoby, které Zhotovitel používá při provádění Předmětu Díla, se zavazují poskytnout Objednateli veškerou součinnost v souladu s výše uvedenou směrnicí.

Dodržování podmínek stanovisek příslušných orgánů a organizací

67. Zhotovitel se zavazuje dodržet při provádění Díla veškeré podmínky vyplývající z Veřejnoprávních podkladů.
68. Pokud nesplněním těchto podmínek vznikne Objednateli škoda, je Zhotovitel povinen nahradit škodu v plném rozsahu, ledaže prokáže, že škodě nemohl zabránit ani v případě vynaložení veškeré možné péče, kterou na něm lze spravedlivě požadovat.

Použité materiály a výrobky

69. Zhotovitel se zavazuje a odpovídá za to, že při realizaci Díla nepoužije žádný materiál, o kterém je v době jeho užití známo, že je škodlivý. Pokud tak Zhotovitel učiní, je povinen

na vyzvání Objednatele provést nápravu, přičemž veškeré náklady s tím spojené nese Zhotovitel.

70. Zhotovitel se zavazuje, že k realizaci Díla nepoužije materiály, které nemají požadovanou certifikaci či předepsaný průvodní doklad, je-li to pro jejich použití nezbytné podle Smlouvy o dílo, Obchodních podmínek, Veřejnoprávních podkladů, právních předpisů nebo příslušných ČSN. Certifikace a průvodní doklady Zhotovitele použitých materiálů jsou součástí Dokladů.

Částečné plnění

71. Nabízí-li Zhotovitel Objednateli částečné plnění Předmětu díla, aniž by částečné plnění bylo výslovně sjednáno ve Smlouvě o dílo, není Objednatel povinen částečné plnění přijmout. Přijme-li Objednatel částečné plnění, je Zhotovitel povinen nahradit Objednateli zvýšené náklady způsobené mu částečným plněním.

Ostatní ujednání

72. Vícepráce lze provést a méněpráce neprovést až poté, co budou vícepráce nebo méněpráce dohodnuty včetně změn Ceny díla dodatkem ke Smlouvě o dílo. Provede-li Zhotovitel vícepráce v rozporu s tímto odstavcem, ponese náklady na ně ze svého.
73. Dojde-li k jakémukoliv úrazu při provádění Díla nebo při činnostech souvisejících s prováděním Díla je Zhotovitel povinen zabezpečit vyšetření úrazu a sepsání příslušného záznamu. Objednatel je povinen poskytnout Zhotoviteli nezbytnou součinnost.
74. Žádný z podkladů, které Zhotovitel převzal od Objednatele v souvislosti s Dílem ani žádný Doklad není Zhotovitel oprávněn bez předchozího písemného svolení Objednatele užít k jiným účelům, než je provedení Díla, zejména je nesmí poskytnout třetím osobám.
75. Zhotovitel je povinen při provádění Díla postupovat v součinnosti s případnými jinými dodavateli Objednatele, a to dle pokynů udělených Objednatelem a nebudou-li pokyny uděleny, postupovat tak, aby umožnil ostatním dodavatelům v co největší míře plnit jejich závazky.
76. Objednatel se zavazuje poskytovat Zhotoviteli součinnost při provádění Díla v rozsahu a způsobem, ve kterém lze tuto součinnost po Objednateli spravedlivě požadovat. Bude-li Zhotovitelem požadována po Objednateli jakákoliv součinnost dle předchozí věty, je Zhotovitel povinen Objednatele k jejímu poskytnutí s dostatečným předstihem vyzvat a ve výzvě ji dostatečně specifikovat.
77. Zhotovitel na sebe přebírá nebezpečí změny okolností ve smyslu §1765 Občanského zákoníku.
78. Ustanovení §1912, §2595 Občanského zákoníku se neužijí.

ČÁST 10 - ZKUŠEBNÍ PROVOZ

79. Ustavení této části se užijí v případě, že ze Smlouvy o dílo nebo z povahy Předmětu díla vyplývá, že má být proveden zkušební provoz.
80. Zkušebním provozem se prověřuje, zda Předmět díla je za předpokládaných provozních a výrobních podmínek schopen dosahovat výkonů (parametrů) v kvalitě a množství stanovených Smlouvou o dílo, Obchodními podmínkami, Veřejnoprávními podklady, právními předpisy a příslušnými ČSN.
81. Zkušební provoz je Zhotovitel povinen provést před předáním Díla Objednateli, do doby úspěšného provedení zkušebního provozu není Dílo dokončeno.
82. Zkušební provoz musí trvat minimálně 48 hodin, nestanoví-li Veřejnoprávní podklady, právní předpisy nebo příslušné ČSN jinak.
83. Zhotovitel se zavazuje v průběhu zkušebního provozu neprodleně odstraňovat veškeré vady, které bude Předmět díla vykazovat.
84. Zkušební provoz bude úspěšně proveden, nebude-li Předmět díla k poslednímu dni doby stanovené pro zkušební provoz vykazovat vady bránící jeho užívání.
85. Bude-li k poslednímu dni doby zkušebního provozu Předmět díla vykazovat vady bránící užívání, prodlužuje se délka trvání zkušebního provozu o dobu dle dohody Smluvních stran, jinak o 24 hodin.
86. Úspěšné provedení zkušebního provozu je podmínkou převzetí díla Objednatelem.

ČÁST 11 - PŘEPRAVA DÍLA

87. Ustavení této části se užijí v případě, je-li Dílo po svém zhotovení za účelem předání Objednateli přepravováno.
88. Je-li dle Smlouvy o dílo nebo zvyklostí třeba Předmět díla zabalit, Zhotovitel Předmět díla zabalí dle Smlouvy o dílo; není-li ujednání o balení Předmětu díla ve Smlouvě o dílo, pak dle zvyklostí, a není-li jich, pak způsobem potřebným pro uchování Předmětu díla a jeho ochranu.
89. Jestliže Zhotovitel označí Obalový materiál nejpozději do doby převzetí Předmětu díla Objednatelem jako vratný, a to přímo na Obalovém materiálu, v Dokladech nebo jiným zřejmým způsobem, ze kterého bude zřejmé, který Obalový materiál je vratný, je Objednatel oprávněn předat Zhotoviteli při předávacím řízení (viz ČÁST 13 - Obchodních podmínek) stejné množství Obalového materiálu téhož druhu a srovnatelného nebo nižšího stupně opotřebení. V rozsahu předání Obalového materiálu Objednatelem Zhotoviteli dle předchozí věty zaniká právo Zhotovitele na vrácení Obalového materiálu.
90. V rozsahu, v němž Objednatel nevrátí vratný Obalový materiál Zhotoviteli dle předchozího odstavce, je Zhotovitel oprávněn Objednateli vyúčtovat zálohu na vratný Obalový materiál. Výše zálohy nesmí přesáhnout dvojnásobek pořizovací ceny Obalového materiálu.
91. Doposud nevrácený vratný Obalový materiál je Objednatel povinen na vlastní náklady dopravit do sídla Zhotovitele, a to nejpozději do jednoho roku od převzetí Předmětu díla Objednatelem. Objednatel je oprávněn nahradit nevrácený vratný Obalový materiál Obalovým materiálem stejného druhu a srovnatelného nebo nižšího stupně opotřebení. Bez zbytečného odkladu po převzetí vráceného Obalového materiálu nebo jeho náhrady Zhotovitelem, je Zhotovitel povinen vrátit Objednateli zaplacenou zálohu na vratný Obalový materiál. Nevrátí-li Objednatel dosud nevrácený vratný Obalový materiál nebo Obalový materiál stejného druhu a srovnatelného nebo nižšího stupně opotřebení ani do dvou let od převzetí Předmětu díla Objednatelem, stává se nevrácený vratný Obalový materiál vlastnictvím Objednatele a složená záloha se stává vlastnictvím Zhotovitele.
92. Pokud Zhotovitel Předmět díla Objednateli odesílá prostřednictvím dopravce, umožní Zhotovitel Objednateli uplatnit práva z přepravní smlouvy vůči dopravci, pokud o to Objednatel Zhotovitele požádá.
93. Pokud Zhotovitel Předmět díla Objednateli odesílá prostřednictvím dopravce, je Zhotovitel povinen zajistit dopravu u dopravce tak, aby Předmět díla byl dodán Objednateli v době uvedené v odstavci 40 Obchodních podmínek.
94. Je-li třeba provést vyložení Předmětu díla z dopravního prostředku, je vyložení povinen provést Zhotovitel na své náklady.
95. Je-li Objednatel v prodlení s převzetím Předmětu díla, uchová jej Zhotovitel, může-li s ním nakládat, pro Objednatele způsobem přiměřeným okolnostem. Převzal-li Objednatel Předmět díla, který zamýšlí odmítnout, uchová jej způsobem přiměřeným okolnostem. Smluvní strana, která uchovává Předmět díla pro druhou Smluvní stranu, má právo na náhradu účelně vynaložených nákladů spojených s uchováním Předmětu díla, nemůže jej však za účelem zajištění svého práva na úhradu nákladů zadržet.

ČÁST 12 - PODDODAVATELÉ

96. Zhotovitel je oprávněn pověřit provedením části Díla třetí osobu – poddodavatele. Zhotovitel odpovídá za činnost poddodavatele tak, jako by činnost prováděl sám.
97. Zhotovitel je oprávněn pověřit provedením části Díla poddodavatele pouze, pokud je poddodavatel uveden v příloze Smlouvy o dílo.
98. Zhotovitel se zavazuje, že poddodavatelé splní všechny povinnosti vyplývající Zhotoviteli ze Smlouvy o dílo, a to přiměřeně k povaze a rozsahu poddodávky.
99. Zhotovitel se zavazuje, že poddodavatelé, kterými prokazoval splnění kvalifikace v zadávacím řízení, se budou podílet na provedení příslušné věcně vymezené části Díla v rozsahu dle Nabídky Zhotovitele.

100. Zhotovitel je oprávněn změnit poddodavatele pouze s předchozím písemným souhlasem Objednatele. Objednatel vydá písemný souhlas se změnou do 10 dnů od doručení žádosti Zhotovitele. Objednatel souhlas se změnou nevydá, pokud
    100.1. prostřednictvím původního poddodavatele Zhotovitel v zadávacím řízení prokazoval kvalifikaci a nový poddodavatel nebude mít stejnou či vyšší kvalifikaci jako původní nahrazovaný poddodavatel nebo
    100.2. po Objednateli nelze spravedlivě požadovat, aby s takovou změnou souhlasil.

ČÁST 13 - PŘEDÁNÍ A PŘEVZETÍ DÍLA

101. Závazek Zhotovitele provést Dílo je splněn jeho dokončením a převzetím Díla Objednatelem, včetně převzetí veškerých Dokladů.
102. Součástí Dokladů je dle povahy a charakteru Díla též
    102.1. dodavatelská výrobní a dílenská dokumentace,
    102.2. atesty, záruční listy, prohlášení o shodě všech věcí, jež byly použity při provádění Díla,
    102.3. zápisy a osvědčení o všech předepsaných zkouškách, měřeních,
    102.4. dokumenty osvědčující průběh zkušebního provozu,
    102.5. servisní plán, návod k obsluze a návod k použití částí Díla,
    102.6. doklady o zabezpečení likvidace odpadů v souladu s právními předpisy,
    102.7. fotodokumentace z průběhu provádění Díla, zejména fotodokumentace prací a konstrukcí, které byly dalším postupem prací zakryté nebo jinak znepřístupněné,
103. V případě, že Smlouva o dílo, Obchodní podmínky, Veřejnoprávní podklady, právní předpisy nebo příslušné ČSN předepisují provedení zkoušek, revizí, atestů a měření či zajištění prohlášení o shodě týkajících se Díla, je Zhotovitel povinen zajistit jejich úspěšné provedení před předáním Díla Objednateli.
104. Objednatel Dílo převezme za předpokladu, že provedení Díla odpovídá Smlouvě o dílo, Obchodním podmínkám, Veřejnoprávním podkladům, právním předpisům a příslušným ČSN, je dokončeno (plně funkční), a je prosté vad s výjimkou ojedinělých drobných vad, které samy o sobě ani ve spojení s jinými nebrání užívání Díla funkčně nebo esteticky, ani jeho užívání podstatným způsobem neomezují.
105. Splnění podmínek pro předání Díla bude ověřeno v rámci přejímacího řízení. Zhotovitel je povinen písemně vyzvat Objednatele k převzetí Díla (zahájení přejímacího řízení). Přejímací řízení bude Objednatelem zahájeno do 5 pracovních dnů po obdržení písemné výzvy Zhotovitele.
106. Objednatel je oprávněn přizvat k účasti v přejímacím řízení i jiné osoby, jejichž účast pokládá za nezbytnou.
107. O průběhu přejímacího řízení bude Zhotovitelem pořízen zápis s identifikací vad Díla, pokud budou v průběhu přejímacího řízení zjištěny. Zápis bude použit jako podklad pro zpracování Předávacího protokolu. Zpracování návrhu Předávacího protokolu zajistí Zhotovitel.
108. Předávací protokol obsahuje
    108.1. výslovný souhlas Objednatele s převzetím Díla
    108.2. datum převzetí Díla,
    108.3. prohlášení Objednatele, zda přebírá Dílo bez výhrad, nebo s výhradami,
    108.4. soupis zjištěných vad nebránících řádnému užívání Díla,
    108.5. dohodnuté lhůty k odstranění zjištěných vad nebo jiná opatření (byla-li dohodnuta),
    108.6. soupis Dokladů předaných Zhotovitelem Objednateli.
109. Objednatel převezme Dílo bez výhrad, je-li v předávacím řízení zjištěno, že Dílo je prosté vad.
110. Převezme-li Objednatel Dílo s výhradami, postupují Smluvní strany dále obdobně dle ustanovení odstavců 139 - 153 Obchodních podmínek, přičemž pro odstranění vad platí doba sjednaná v Předávacím protokolu, jinak doba 15 dní od oboustranného

podpisu Předávacího protokolu a za reklamaci se považuje identifikace vad uvedená v Předávacím protokolu podepsaném Objednatelem.

111. V případě, že Objednatel Dílo nepřevezme, bude mezi Smluvními stranami sepsán záznam s uvedením důvodu nepřevzetí Díla a s uvedením stanovisek Smluvních stran. Zpracování záznamu zajistí Zhotovitel.
112. V případě nepřevzetí Díla Smluvní strany sjednají lhůtu pro odstranění zjištěných vad. Nebude-li vada odstraněna ve lhůtě sjednané, jinak do 15 dní, je Objednatel oprávněn zajistit odstranění vady jinou odborně způsobilou osobou na náklady Zhotovitele. Veškeré náklady vzniklé Objednateli v souvislosti s odstraněním vady způsobem dle předchozí věty je Zhotovitel povinen Objednateli uhradit. Zhotovitel je povinen ve stanovené lhůtě odstranit vady i v případě, kdy podle jeho názoru za vady neodpovídá. Náklady na odstranění v těchto sporných případech nese až do vyjasnění nebo do vyřešení rozporu Zhotovitel. Po odstranění vad vyzve Zhotovitel Objednatele k zahájení náhradního přejímacího řízení, které Objednatel zahájí bezodkladně, nejpozději do 2 pracovních dnů od obdržení výzvy Zhotovitele.
113. Podpisem Předávacího protokolu nebo záznamu o nepřevzetí Díla je přejímací řízení ukončeno.
114. Pro průběh náhradního přejímacího řízení se užijí ustanovení odstavců 104 - 113 Obchodních podmínek obdobně.
115. Připouští-li to povaha Předmětu díla, a není-li sjednán zkušební provoz, má Objednatel právo, aby byl Předmět díla před ním překontrolován nebo aby byly předvedeny jeho funkce.
116. Ustanovení §1921, §2112, §2605 odst. 2, §2606, §2609, §2618 a §2629 Občanského zákoníku se neužijí.

ČÁST 14 - VLASTNICKÉ PRÁVO A NEBEZPEČÍ ŠKODY

117. Vlastnické právo k Dílu náleží od počátku Objednateli.
118. Vlastnické právo k dodávkám materiálu a jiných hmotných movitých věcí nabývá Objednatel okamžikem jejich zapracování do Díla, učiněním součástí Díla nebo jakýmkoliv funkčním, estetickým či jiným spojením s Dílem.
119. Vlastnické právo k jakékoli dokumentaci vztahující se k Dílu, která není autorským dílem, nabývá Objednatel okamžikem jejího vyhotovení.
120. Je-li vlastníkem Díla nebo jeho části v souladu s §1083 a §1084 Občanského zákoníku vlastník pozemku, užijí se ustanovení odstavců 117 a 118 přiměřeně.
121. Nebezpečí škody na Díle nese Zhotovitel, na Objednatele přechází okamžikem oboustranného podpisu Předávacího protokolu. Pokud nebyly s Předmětem díla předány zároveň též všechny Doklady, nese Zhotovitel nebezpečí škody na dosud nepředaných Dokladech až do jejich převzetí Objednatelem.
122. Náklady nutné k odstranění škody na Díle vzniklé v době, kdy nebezpečí škody nese Zhotovitele, hradí Zhotovitel v plném rozsahu a tyto náklady nemají vliv na Cenu díla.
123. Škody na Díle vzniklé v době, kdy nebezpečí škody nese Zhotovitele, je povinen Zhotovitel odstranit v součinnosti s Objednatelem jako vlastníkem poškozené věci a dle jeho pokynů.
124. Ustanovení §2599 Občanského zákoníku se neužijí.

ČÁST 15 - VADY PLNĚNÍ A ZÁRUKA

125. Zhotovitel se zavazuje, že Dílo bude v okamžiku jeho převzetí Objednatelem vyhovovat všem požadavkům na dílo stanoveným Smlouvou o dílo, Obchodními podmínkami, Veřejnoprávními podklady, právními předpisy a příslušnými ČSN.
126. Zhotovitel se zavazuje, že Dílo bude vyhovovat též plnění nabídnutému Zhotovitelem v Nabídce.
127. Dílo musí být prosté všech faktických a právních vad. Plnění má právní vadu, pokud k němu uplatňuje právo třetí osoba.

128. Zhotovitel se zavazuje (poskytuje Objednateli záruku), že Dílo a veškeré jeho části si po celou dobu od okamžiku jeho převzetí Objednatelem, až do uplynutí Záruční doby zachová vlastnosti stanovené v odstavcích 125 - 127 Obchodních podmínek.
129. Záruční doba začíná běžet dnem převzetí Díla Objednatelem, nebo jeho poslední části, je-li Dílo dodáváno po částech, nebo ode dne úspěšného ukončení zkušebního provozu, je-li dle Smlouvy o dílo vyžadován a nastane-li okamžik úspěšného ukončení zkušebního provozu později než okamžik převzetí Díla, resp. jeho poslední části.
130. Dílo má vady (Zhotovitel plnil vadně), jestliže při převzetí Objednatelem nebo kdykoliv od převzetí Objednatelem do konce Záruční doby nebude mít vlastnosti stanovené v odstavcích 125 - 127 Obchodních podmínek.
131. Objednatel má práva z vadného plnění i v případě, jedná-li se o vadu, kterou musel s vynaložením obvyklé pozornosti poznat již při uzavření Smlouvy o dílo.
132. Objednatel nemá práva z vadného plnění, způsobila-li vadu po přechodu nebezpečí škody na věci na Objednatele vnější událost. To neplatí, způsobil-li vadu Zhotovitel nebo jakákoliv třetí osoba, jejímž prostřednictvím plnil své povinnosti vyplývající ze Smlouvy o dílo.
133. Zhotovitel neodpovídá za vady spočívající v opotřebení Předmětu díla, které je obvyklé u věcí stejného nebo obdobného druhu jako Předmět díla.
134. Zhotovitel odpovídá za vady spočívající v opotřebení Předmětu díla, ke kterému do konce Záruční doby vzhledem k požadavkům Smlouvy o dílo, Obchodních podmínek, Veřejnoprávních podkladů, právních předpisů a příslušných ČSN na jakost a provedení Předmětu díla nemělo dojít.
135. Zhotovitel nenese odpovědnost za vady způsobené Objednatelem nebo třetími osobami, ledaže Objednatel nebo takové osoby postupovaly v souladu s Doklady nebo pokyny, které obdrželi od Zhotovitele.

ČÁST 16 - UPLATNĚNÍ PRÁV Z VADNÉHO PLNĚNÍ

136. Odpovídá-li Zhotovitel za vady Díla, má Objednatel práva z vadného plnění.
137. Objednatel je oprávněn vady reklamovat u Zhotovitele jakýmkoliv způsobem, preferovaná je písemná forma. Zhotovitel je povinen přijetí reklamace bez zbytečného odkladu písemně potvrdit. V reklamaci Objednatel uvede popis vady nebo uvede, jak se vada projevuje.
138. Vada je uplatněna včas, je-li písemná forma reklamace odeslána Zhotoviteli nejpozději v poslední den Záruční doby. Připadne-li konec Záruční doby na sobotu, neděli nebo svátek, je vada včas uplatněna, je-li písemná forma reklamace odeslána Zhotoviteli nejblíže následující pracovní den.
139. Má-li Předmět díla vady, za které Zhotovitel odpovídá, má Objednatel právo
    139.1. na odstranění vady dodáním nového Předmětu díla nebo jeho části bez vady, pokud to není vzhledem k povaze vady zcela zřejmě nepřiměřené, nebo dodání chybějící části Předmětu díla,
    139.2. na odstranění vady opravou Předmětu díla nebo jeho části,
    139.3. na přiměřenou slevu z Ceny díla, nebo
    139.4. odstoupit od Smlouvy o dílo.
140. Objednatel je oprávněn požadovat odstranění vad dodáním nového Předmětu díla nebo jeho části bez vady, vyskytla-li se stejná vada po její opravě opětovně, nebo nemůže-li Objednatel řádně užívat Předmět díla nebo jeho část pro větší počet vad.
141. Objednatel je oprávněn nároky dle odstavce 139 kombinovat, je-li to vzhledem k okolnostem možné. Objednatel není oprávněn kombinovat nároky, které si navzájem odporují (např. dodání nové části Předmětu díla a zároveň slevy z Ceny díla na tutéž část Předmětu díla).
142. Objednatel sdělí Zhotoviteli volbu nároku z vady v reklamaci, nebo bez zbytečného odkladu po reklamaci. Provedenou volbu nemůže Objednatel změnit bez souhlasu Zhotovitele; to neplatí, žádal-li Objednatel opravu vady, která se ukáže jako neopravitelná.

143. Nesdělí-li Objednatel Zhotoviteli, jaké právo si zvolil ani bez zbytečného odkladu poté, co jej k tomu Zhotovitel vyzval, může Zhotovitel odstranit vady podle své volby opravou nebo dodáním nového Předmětu díla nebo jeho části; volba nesmí Objednateli způsobit nepřiměřené náklady.
144. Objednatel má nárok na náhradu nákladů účelně vynaložených v souvislosti s oznámením vad Zhotoviteli.

ČÁST 17 - PODMÍNKY ODSTRANĚNÍ VAD

145. Pokud Objednatel požaduje v reklamaci odstranění vady, je Zhotovitel povinen neprodleně po obdržení reklamace zahájit činnosti vedoucí k odstranění reklamované vady. Pokud Objednatel v reklamaci uvede, že se jedná o havárii, je Zhotovitel povinen zahájit odstraňování vady nejpozději do 48 hodin po obdržení reklamace.
146. Zhotovitel je povinen odstranit Objednatelem reklamovanou vadu nejpozději do 30 dnů ode dne oznámení vady Zhotoviteli. Jde-li o vadu označenou Objednatelem v reklamaci jako havarijní, je Zhotovitel povinen odstranit vadu nejpozději do 5 dnů.
147. Nezahájí-li Zhotovitel činnosti vedoucí k odstranění vady do 10 dnů od oznámení vady Zhotoviteli, nebo nebude-li vada odstraněna ve lhůtě dle předcházejícího odstavce, je Objednatel oprávněn
    147.1. zajistit odstranění vady jinou odborně způsobilou právnickou nebo fyzickou osobou na účet Zhotovitele,
    147.2. požadovat slevu z Ceny díla, nebo
    147.3. od Smlouvy o dílo odstoupit.
148. Veškeré náklady vzniklé Objednateli v souvislosti s odstranění vady způsobem dle předchozího odstavce je Zhotovitel povinen Objednateli uhradit.
149. Zhotovitel je povinen odstranit vadu bez ohledu na to, zda je uplatnění vady oprávněné či nikoli. Prokáže-li se však kdykoli později, že uplatnění vady Objednatelem nebylo oprávněné, tj. že Zhotovitel za vadu neodpovídal, je Objednatel povinen uhradit Zhotoviteli veškeré jím účelně vynaložené náklady v souvislosti s odstraněním vady.
150. Objednatel je povinen poskytnout Zhotoviteli součinnost nezbytnou k odstranění vady.
151. Do odstranění vady nemusí Objednatel platit dosud nezaplacenou část Ceny díla a případnou příslušnou DPH odhadem přiměřeně odpovídající jeho právu na slevu.
152. Při dodání nového Předmětu díla nebo jeho části vrátí Objednatel Zhotoviteli na náklady Zhotovitele Předmět díla nebo jeho část původně dodanou.
153. Týká-li se vada Dokladů nebo jiného plnění poskytnutého Zhotovitelem dle Smlouvy o dílo než Předmětu díla, užijí se ustanovení odstavců 136 – 152 obdobně.
154. Ustanovení §1917–1924, §2099–2101, §2103 – 2117, §2165 – 2172, §2618 a §2629 Občanského zákoníku se neužijí.

ČÁST 18 - POJIŠTĚNÍ

155. Ustanovení této části se užijí v případě, že ze Smlouvy o dílo vyplývá, že Zhotovitel je povinen být pojištěn pro případ odpovědnosti za škodu způsobenou při výkonu činnosti.
156. Zhotovitel je povinen mít ode dne zahájení provádění Díla, nejpozději však do 15 dnů od uzavření Smlouvy o dílo, až do uplynutí Záruční doby uzavřenou pojistnou smlouvu o pojištění odpovědnosti za škodu způsobenou Zhotovitelem při výkonu činnosti třetím osobám s limitem pojistného plnění pro 1 pojistnou událost ve výši odpovídající Ceně díla.
157. Zhotovitel je povinen předložit Objednateli uzavřenou pojistnou smlouvu dle této části nebo odpovídající pojistku nejpozději do 15 dnů ode dne uzavření Smlouvy o dílo a dále kdykoli v průběhu provádění Díla nebo trvání Záruční doby do 10 dnů ode dne, kdy k tomu byl Objednatelem vyzván. V případě změn v pojištění je Zhotovitel povinen bezodkladně tyto změny oznámit Objednateli a předložit dokumenty dokládající tyto změny.
158. Zhotovitel se zavazuje, že všichni poddodavatelé, kteří se budou podílet na provedení Díla, budou nejméně po dobu provádění poddodávky pojištěni pro případ škody

způsobené poddodavatelem při výkonu činnosti třetím osobám s limitem pojistného plnění pro 1 pojistnou událost minimálně ve výši odpovídající ceně poddodávky.

159. Porušení jakékoli povinnosti Zhotovitele dle této části je podstatným porušením Smlouvy o dílo.
160. Náklady na pojištění nese Zhotovitel, jsou zahrnuty v Ceně díla.

ČÁST 19 - DUŠEVNÍ VLASTNICTVÍ

161. Zhotovitel je povinen při provádění Díla postupovat tak, aby při provádění Díla ani následným užíváním Díla Objednatelem nedošlo k porušení práv duševního vlastnictví. Bude-li v souvislosti s Dílem, jakkoliv dotčeno právo k duševnímu vlastnictví, je Zhotovitel povinen upravit veškeré právní vztahy s osobami, kterým taková práva náležejí nebo jež jsou oprávněny je vykonávat, tak, aby zamezil vznášení jakýchkoli oprávněných nároků těchto osob ve vztahu k Objednateli.
162. Zhotovitel tímto poskytuje Objednateli oprávnění k výkonu práva duševního vlastnictví (licenci nebo podlicenci) ke všem plněním poskytnutým Objednateli při provádění Díla, které jsou nebo budou předmětem duševního vlastnictví a ke kterým je oprávněn takové oprávnění poskytnout. Oprávnění Zhotovitel poskytuje
    162.1. bezúplatně,
    162.2. jako nevýhradní,
    162.3. z hlediska časového a územního v rozsahu neomezeném,
    162.4. z hlediska věcného rozsahu (způsobu užití) tak, že opravňuje Objednatele ke všem známým způsobům užití,
    162.5. bez množstevního omezení.
163. Objednatel není povinen oprávnění využít.
164. Objednatel je oprávněn oprávnění tvořící součást licence nebo podlicence poskytnout nebo též postoupit třetí osobě zcela nebo zčásti.
165. Zhotovitel se zavazuje, že na žádost Objednatele autor nebo autoři autorského díla, jež je součástí nebo příslušenstvím Díla, udělí Objednateli bez zbytečného odkladu bezúplatně právo
    165.1. upravit či jinak změnit označení autora,
    165.2. autorské dílo nebo jeho název upravit či jinak měnit,
    165.3. autorské dílo s jakýmkoliv jiným autorským dílem spojit či zařadit do díla souborného.
166. Žádný výsledek činnosti provedené na základě Smlouvy o dílo nebo v souvislosti s ní, který je předmětem duševního vlastnictví, není Zhotovitel oprávněn bez předchozího písemného svolení Objednatele užít k jiným účelům, než je provedení Díla, zejména je nesmí poskytnout třetím osobám.

ČÁST 20 - SANKCE

167. Poruší-li Zhotovitel povinnost provést Dílo ve sjednané době, je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 0,5 % z Ceny díla za každý den prodlení.
168. Poruší-li Objednatel povinnost zaplatit Cenu díla ve sjednané době, je povinen uhradit Zhotoviteli zákonný úrok z prodlení ve výši dle právních předpisů.
169. Poruší-li Zhotovitel povinnost odstranit vadu Díla ve sjednané době, je povinen uhradit Objednateli smluvní pokutu ve výši 0,5 % z Ceny díla za každý 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.
170. 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.

171. Poruší-li Zhotovitel jakékoliv jiné povinnosti vyplývající ze Smlouvy o dílo, Obchodních podmínek nebo Veřejnoprávních podkladů než povinnosti, na které se vztahuje smluvní pokuta dle této části, je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 5% z Ceny díla za každý jednotlivý případ porušení povinnosti.
172. Poruší-li Zhotovitel nebo osoba, kterou Zhotovitel používá při provádění díla jakoukoliv povinnost stanovenou Směrnicí SŽDC č. 120 Dodržování zákazu kouření, požívání alkoholických nápojů a užívání jiných návykových látek, č.j. 36503/2017-SŽDC-GŘ-O10 ze dne 3.11.2017, účinnou od 7.1.1.2017 v rámci Objednatelem prováděné kontroly na základě výše uvedené směrnice je Objednatel oprávněn na základě posouzení souvisejících okolností, uplatnit vůči Zhotoviteli sankci ve výši 5 000,- Kč za každý jednotlivý případ.
173. Zaplacení smluvní pokuty nezbavuje Zhotovitele povinnosti splnit dluh smluvní pokutou utvrzený.
174. Objednatel je oprávněn požadovat náhradu škody a nemajetkové újmy způsobené porušením povinnosti, na kterou se vztahuje smluvní pokuta, v plné výši.

ČÁST 21 - OBECNÁ ODPOVĚDNOST ZHOTOVITELE

175. 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.
176. 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.
177. 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.
178. Zhotovitel odpovídá za jakékoli porušení svých povinností stanovených Smlouvou o dílo, Obchodními podmínkami, Veřejnoprávními podklady, právními předpisy a příslušnými ČSN a je povinen uhradit veškeré pokuty udělené mu příslušnými orgány státní správy v souvislosti s prováděním Díla ze svého, ledaže mu byla pokuta udělena v souvislosti s respektováním příkazu Objednatele, proti kterému uplatnil písemnou výhradu a na jehož splnění Objednatel trval anebo v souvislosti s užitím Objednatelem opatřené věci, na jejíž nevhodnost Objednatele písemně upozornil a Objednatel na jejím užití trval.
179. Povinnosti k náhradě újmy způsobené porušením svých povinností ze Smlouvy o dílo, Obchodních podmínek, Veřejnoprávních podkladů, právních předpisů a příslušných ČSN se Zhotovitel vůči Objednateli zprostí, prokáže-li, že mu ve splnění povinnosti zabránila mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na jeho vůli. Překážka vzniklá z osobních poměrů Zhotovitele nebo vzniklá až v době, kdy byl Zhotovitel s plněním povinnosti v prodlení, ani překážka, kterou byl Zhotovitel povinen překonat, jej však povinnosti k náhradě nezprostí.

ČÁST 22 - ODSTOUPENÍ OD SMLOUVY O DÍLO

180. Poruší-li Smluvní strana Smlouvu o dílo podstatným způsobem, může druhá Smluvní strana písemnou formou od Smlouvy o dílo odstoupit.
181. Podstatné je takové porušení povinnosti, o němž Smluvní strana porušující Smlouvu o dílo již při uzavření Smlouvy o dílo věděla nebo musela vědět, že by druhá Smluvní strana Smlouvu o dílo neuzavřela, pokud by toto porušení předvídala, nebo je-li porušení povinnosti ve Smlouvě o dílo nebo v Obchodních podmínkách jako podstatné označeno; v ostatních případech se má za to, že porušení podstatné není.

182. 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.
183. Objednatel je oprávněn od Smlouvy o dílo odstoupit též
    183.1. z důvodů uvedených v části Předání a převzetí Díla (viz ČÁST 13 - Obchodních podmínek),
    183.2. nabylo-li právní moci rozhodnutí o nařízení exekuce vůči Zhotoviteli jako povinnému,
    183.3. ocitne-li se Zhotovitel ve stavu úpadku nebo hrozícího úpadku,
    183.4. 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,
    183.5. uvedl-li Zhotovitel v Nabídce informace nebo doklady, které neodpovídají skutečnosti a měly nebo mohly mít vliv na výsledek řízení,
    183.6. stanoví-li tak Smlouvy o dílo.
184. Smluvní strana může od Smlouvy o dílo odstoupit, pokud z chování druhé Smluvní strany nepochybně vyplyne, že poruší Smlouvu o dílo podstatným způsobem, a nedá-li na výzvu oprávněné Smluvní strany přiměřenou jistotu.
185. 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.
186. Zakládá-li prodlení Smluvní strany nepodstatné porušení její povinnosti ze Smlouvy o dílo, může druhá Smluvní strana od Smlouvy o dílo odstoupit poté, co prodlévající Smluvní strana svoji povinnost nesplní ani v dodatečné přiměřené lhůtě, kterou jí druhá Smluvní strana poskytla výslovně nebo mlčky.
187. 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.
188. 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.
189. Plnil-li Zhotovitel zčásti, může Smluvní strana od Smlouvy o dílo odstoupit jen ohledně nesplněného zbytku plnění. Nemá-li však částečné plnění pro Objednatele význam, může Objednatel od Smlouvy o dílo odstoupit ohledně celého plnění. Odstoupil-li od nesplněného zbytku plnění Zhotovitel, je Objednatel oprávněn odstoupit od splněné části Smlouvy o dílo, nemá-li částečně plnění pro Objednatele význam.
190. 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.
191. Smluvní strany se dohodly, že dojde-li k odstoupení od Smlouvy o dílo jen ohledně nesplněného zbytku plnění, užijí se na splněnou část plnění obdobně všechna ustanovení Smlouvy o dílo a Obchodních podmínek týkající se předání a převzetí Díla, přičemž přejímací řízení Smluvní strany zahájí nejpozději do 3 pracovních dnů ode dne odstoupení od Smlouvy o dílo, a dále všechna ustanovení Smlouvy o dílo a Obchodních podmínek o právech a povinnostech Smluvních stran, které jsou Smluvní stany povinny plnit v době ode dne převzetí Díla Objednatelem, tedy zejm. ustanovení o vadách Díla.
192. Ustanovení §1977, §2002–2003 Občanského zákoníku se neužijí.

ČÁST 23 - OSTATNÍ UJEDNÁNÍ

Částečné plnění

193. 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

194. Zhotovitel není oprávněn postoupit žádnou svou pohledávku za Objednatelem vyplývající ze Smlouvy o dílo nebo vzniklou v souvislosti se Smlouvou o dílo.
195. K pohledávce za Objednatelem vyplývající se Smlouvy o dílo nebo vzniklé v souvislosti se Smlouvou o dílo nesmí být zřízeno zástavní právo.
196. 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.
197. 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

198. 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

199. 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

200. 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.
201. Je-li Dílo z jakékoliv části financováno z prostředků Evropské unie, je Zhotovitel povinen
    201.1. strpět veškeré kontroly vyplývající z režimu financování Díla z prostředků Evropské unie,
    201.2. poskytnout při takových kontrolách veškerou nezbytnou součinnost,
    201.3. archivovat veškerou dokumentaci týkající se Smlouvy o dílo po dobu stanovenou pravidly, jimiž se řídí financování Díla z prostředků Evropské unie.

Jazyk

202. Ve všech záležitostech souvisejících se Smlouvou o dílo budou zástupci Smluvních stran komunikovat v českém jazyce. Všichni zástupci musí plynně český jazyk ovládat. Jestliže český jazyk plynně neovládají, jsou povinni na náklady své Smluvní strany zajistit, aby byl po celou dobu vzájemné osobní komunikace k dispozici kvalifikovaný tlumočník.

Forma, označení času

203. Písemnou formou (podobou) se rozumí listina podepsaná oprávněnou osobou Smluvní strany nebo email podepsaný zaručeným elektronickým podpisem oprávněné osoby Smluvní strany.
204. 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

205. Zhotovitel je oprávněn uvádět Dílo a jméno Objednatele jako referenci na svou činnost pouze s předchozím písemným souhlasem Objednatele.

Salvatorní klauzule

206. 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. 4 Výzvy

SPRÁVA ŽELEZNIC

Harmonogram plnění

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

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

SPRÁVA ŽELEZNIC

HARMONOGRAM PLNĚNÍ

Fáze	Popis	Zahájení	Ukončení
F0	Mobilizační fáze.	od účinnosti smlouvy	do 3 týdnů
F1	Před-implementační analýza – Identifikace, a ve spolupráci se SŽ, klasifikace a identifikace přenášených dokumentů pro vytvoření základní knihovny pravidel a signatur. Identifikace šablon dokumentů.	od ukončení F0	do 16 týdnů
	Před-implementační analýza – Analýza zmapování datových toků z a do jednotlivých systémů.	od ukončení F0	do 16 týdnů
	Před-implementační analýza – Analýza aktuálně nasazeného systému Microsoft Purview, nasazovaných štítků a pravidel za účelem odhalení možných kolizí a případně spolupráce mezi systémy.	od ukončení F0	do 16 týdnů
	Před-implementační analýza – Vytvoření knihovny pravidel, pro nasazení na oba typy provozovaných FW, včetně popisu jednotlivých pravidel.	od ukončení F0	do 16 týdnů
	Před-implementační analýza – Návrh architektury DLP řešení.	od ukončení F0	do 16 týdnů
F2	Dodávka licencí – Dodávka veškerých licencí potřebných k provozu navrhovaného DLP řešení.	od ukončení F1	do 1 týdne
F3	Implementace DLP řešení - nasazení celého navrhovaného DLP řešení a jeho napojení na požadované zdroje dat, případně další nezbytnou infrastrukturu (pokud bude využita ze strany Dodavatele).	od ukončení F2	do 2 týdnů

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

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

Fáze	Popis	Zahájení	Ukončení
F4	Konfigurace DLP řešení - Další konfigurace SSL dekrypce aj.	od ukončení F3 (pokud bude F3 využita, jinak od ukončení F2)	do 3 týdnů
	Konfigurace DLP řešení – Nasazení základní databáze pravidel na základě provedené analýzy.	od ukončení F3 (pokud bude F3 využita, jinak od ukončení F2)	do 3 týdnů
F5	Testování DLP řešení – Zátěžové testy nové konfigurace (řeší Zadavatel).	od ukončení F4	do 4 týdnů
	Testování DLP řešení – Otestování detekčních schopností jednotlivých pravidel (řeší Zadavatel).	od ukončení F4	do 4 týdnů
F6	Testovací provoz – Ověření účinnosti nasazených pravidel v rámci testovacího běhu v produkčním prostředí systému (min 12 týdnů) a případné doladění (řeší Dodavatel ve spolupráci se Zadavatelem). Úspěšně provedené testy výpadku DLP řešení (řeší Zadavatel).	od ukončení F5	do 13 týdnů
F7	Adopce DLP řešení a školení administrátorů – Předání podkladů pro adopční kampaň (poster a video).	od započetí F4	do 19 týdnů
	Adopce DLP řešení a školení administrátorů – Provedení školení administrátorů.	od započetí F4	do 19 týdnů
F8	Post-implementační podpora nově nasazených komponent do infrastruktury SŽ.	od ukončení F6	po dobu 5 let
	Služby na vyžádání.	od ukončení F6 – dle Objednávky	dle Objednávky

Příloha č. 5 Výzvy

SPRÁVA ŽELEZNIC

Návrh dodávky (šablona)

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

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

1 Úvod

Cílem tohoto dokumentu je, aby účastník představil svůj návrh, jak hodlá dodávku realizovat. Účastník v této kapitole popíše své chápaní problematiky a situace Zadavatele, a základní premisy návrhu dodávky.

2 Představení nabídky

2.1 Před-implementační analýza

Účastník v této kapitole popíše svou metodiku, kterou navrhuje využít při realizaci plnění, a to s přihlédnutím k požadovaným oblastem, uvedeným v kapitole 4.2 Technické specifikace (Příloha č. 2 Výzvy k podání nabídky na veřejnou zakázku s názvem „Zavedení komplexního síťového řešení prevence úniku dat (DLP) pro non-Microsoft systémy v prostředí Správy železnic"):

- Provedení analýzy dat v rámci jednotlivých vybraných systémů a ve spolupráci se Zadavatelem jejich klasifikace. Identifikace šablon dokumentů.
- Provedení analýzy toku dat z a/nebo do jednotlivých vybraných systémů a identifikace možných cest úniku dat, které nelze pokrýt stávajícími technologiemi SŽ.
- Vytvoření knihovny signatur pro detekci dat v rámci DLP klasifikovaných jinak než veřejná, včetně popisu jednotlivých signatur.
- Vytvoření knihovny pravidel, pro reakce na detekovaná data, nasaditelná do DLP řešení.
- Provedení analýzy aktuálně nasazeného systému Microsoft Purview, nasazovaných štítků a pravidel se zaměřením na možné kolize s nově navrhovaným řešením a návrhu jejich řešení.
- Předložení testovacích scénářů a jejich schválení ze strany Zadavatele.
- Předložení návrhu architektury.
- Dodávku všech licencí potřebných k provozu navrhovaného DLP řešení, minimálně po dobu 5 let od akceptace fáze F6 a F7 ze strany SŽ (viz Příloha č. 4 Výzvy k podání nabídky s názvem – Harmonogram plnění).

Součástí představené metodiky musí být návrh předpokládané součinnosti a předpokládaných informací, které dodavatel bude vyžadovat.

2.2 Implementace DLP řešení

Účastník v této kapitole popíše svou metodiku, kterou navrhuje využít při **případné** realizaci plnění, a to s přihlédnutím k požadovaným oblastem, uvedenýmv kapitole 4.4 Technické specifikace (Příloha č. 2 Výzvy k podání nabídky na veřejnou zakázku s názvem „Zavedení komplexního síťového řešení prevence úniku dat (DLP) pro non-Microsoft systémy v prostředí Správy železnic"):

- Kompletní nasazení DLP řešení do infrastruktury SŽ a jeho napojení na požadované zdroje dat, případně další nezbytnou infrastrukturu (NTP, identitní databáze aj.).

2.3 Konfigurace a testování DLP řešení

Účastník v této kapitole představí přístup k nasazení vyspecifikovaných pravidel a konfigurace DLP řešení, včetně představení přístupu k otestovaní detekčních schopností každého z nasazených pravidel v souladu s kapitolami 4.5, 4.6 a 4.7 Technické specifikace (Příloha č. 2 Výzvy k podání nabídky na veřejnou zakázku s názvem „Zavedení komplexního síťového řešení prevence úniku dat (DLP) pro non-Microsoft systémy v prostředí Správy železnic"):

- Nasazení základní databáze pravidel na základě provedené analýzy a identifikovaných požadavků.
- Ověření účinnosti nasazených pravidel v rámci testovacího běhu systému (minimálně 12 týdnů) a případné doladění.
- Provedení zátěžových testů k ověření celkové konfigurace.
- Úspěšně provedené testy výpadku DLP řešení.

2.4 Adopce DLP řešení a školení administrátorů

Účastník v této kapitole představí přístup pro realizaci adopční fáze - provedení adopční kampaně (informační emaily a videa), dále pak představí formu školení řešení DLP pro vybrané uživatele v SŽ, jež je popsáno v kapitole 4.8 Technické specifikace (Příloha č. 2 Výzvy k podání nabídky na veřejnou zakázku s názvem „Zavedení komplexního síťového řešení prevence úniku dat (DLP) pro non-Microsoft systémy v prostředí Správy železnic"):

- Provedení adopční kampaně v podobě informačních emailů a videa.
- Provedení školení pro administrátory.

Příloha č. 6 Výzvy

SPRÁVA ŽELEZNIC

Formulář pro vyplnění nabídkové ceny

Prevence úniku dat pro non-Microsoft prostředí

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

Identifikace účastníka:

Postup pro vyplnění souboru

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

Legenda zabarvených polí:

textové doplnění pole

Nabídková cena
Účastník vyplní jednotkovou cenu dle jednotlivých částí plnění pro předdefinovaný počet jednotek. Účastník je povinen dodržovat uvedená omezení na cenu.

Nabídková cena

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

Ve sloupci I ("Omezení ceny za platební milník") je uvedena forma omezení ceny pro celkovou částku za platební milník, jejíž cena je vypočítána ve sloupci H. Omezení je vztaženo k celkové nabízené ceně, a proto je nutné soulad s omezením revidovat až po doplnění jednotkové ceny za všechny položky.

V případě, že formulář obsahuje červeně zbarvenou celkovou nabídkovou cenu, nabídka pravděpodobně obsahuje nesprávně vyplněné údaje, které v důsledku mohou vést až k vyloučení účastníka.

Fáze	Část služby	Odkaz na kapitolu TS	Jednotková cena (v CZK)	Počet jednotek	Jedn.	Nabídková cena v Kč bez DPH	Omezení ceny za platební milník
	Před-implementační analýza (celkový součet)			-	-	0,00 CZK	Cena za fázi F1 může tvořit max. 30% z ceny za F1, F3, F4, F6, F7
F1	**Před-implementační analýza – Identifikace, a ve spolupráci se SŽ, klasifikace a identifikace přenášených dokumentů pro vytvoření základní knihovny pravidel a signatur. Identifikace šablon dokumentů.**	4.2		1		0,00 CZK	
	Před-implementační analýza – Analýza zmapování datových toků z a do jednotlivých systémů.	4.2		1		0,00 CZK	
	Před-implementační analýza – Analýza aktuálně nasazeného systému Microsoft Purview, nasazovaných štítků a pravidel za účelem odhalení možných kolizí a případně spolupráce mezi systémy.	4.2		1		0,00 CZK	
	Před-implementační analýza – Vytvoření knihovny pravidel, pro nasazení na oba typy provozovaných FW, včetně popisu jednotlivých pravidel.	4.2		1		0,00 CZK	
	Před-implementační analýza – Návrh architektury DLP řešení.	4.2		1		0,00 CZK	
F2	**Dodávka licencí – Dodávka veškerých licencí potřebných k provozu navrhovaného DLP řešení.**	4.3		1		0,00 CZK	
F3	**Implementace DLP řešení - nasazení celého navrhovaného DLP řešení a jeho napojení na požadované zdroje dat, případně další nezbytnou infrastrukturu (pokud bude využita ze strany Dodavatele).**	4.4		1		0,00 CZK	Součet cen za fáze F3, F4, F6 může tvořit max. 50% z ceny za F1, F3, F4, F6, F7
	Konfigurace DLP řešení (celkový součet)					0,00 CZK	Součet cen za fáze F3, F4, F6 může tvořit max. 50% z ceny za F1, F3, F4, F6, F7

F4	**Konfigurace DLP řešení - Další konfigurace SSL dekrypce aj.**	4.5		1		0,00 CZK	
	Konfigurace DLP řešení – Nasazení základní databáze pravidel na základě provedené analýzy.	4.5		1		0,00 CZK	
F5	**Testování DLP řešení – Zátěžové testy nové konfigurace (Provádí zadavatel).**	4.6		-	-		
	Testování DLP řešení – Otestování detekčních schopností jednotlivých pravidel (Provádí zadavatel).	4.6		-	-		
F6	**Testovací provoz – Ověření účinnosti nasazených pravidel v rámci testovacího běhu v produkčním prostředí systému (min 12 týdnů) a případné doladění. Úspěšně provedené testy výpadku DLP řešení.**	4.7		1		0,00 CZK	Součet cen za fáze F3, F4, F6 může tvořit max. 50% z ceny za F1, F3, F4, F6, F7
	Adopce DLP řešení a školení administrátorů (Celkový součet)			-	-	0,00 CZK	Cena za fázi F7 může tvořit max. 20% z ceny za F1, F3, F4, F6, F7
F7	**Adopce DLP řešení a školení administrátorů – Předání podkladů pro adopční kampaň (poster a video).**	4.8		1		0,00 CZK	
	Adopce DLP řešení a školení administrátorů – Provedení školení administrátorů	4.8		1		0,00 CZK	
F8	**Post-implementační podpora nově nasazených komponent do infrastruktury SŽ**	4.9		60	měsíc	0,00 CZK	
	Služby na vyžádání	4.9		30	MD*	0,00 CZK	Placeno na základě vyžádaných služeb za odpracované MD
	Nabídková cena za F1, F3, F4, F6, F7					**0,00 CZK**	
	Nabídková cena celkem					**0,00 CZK**	

*MD = člověkoden

Příloha č. 10 Výzvy k podání nabídky – **Účastník předloží pouze v případě postupu dle článku 12.2. a 12.3 Výzvy**.

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	.....
Sídlo/místo podnikání	.....
IČO	.....
Zastoupen	.....

který podává nabídku na podlimitní sektorovou veřejnou zakázku s názvem **„Zavedení komplexního síťového řešení prevence úniku dat (DLP) pro non-Microsoft systémy v prostředí Správy železnic"**, č.j. 80219/2025-SŽ-GŘ-O25, tímto čestně prohlašuje, že dále uvedené údaje a další skutečnosti uvedené či jinak řádné označené ve smlouvě na plnění předmětu veřejné zakázky, jež je součástí jeho nabídky (dále jen ***„smlouva"***), považuje účastník za obchodní tajemství ve smyslu ustanovení § 504 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen ***„obchodní tajemství"*** a ***„občanský zákoník"***), nebo se jedná o jiné informace, které nemohou být v registru smluv uveřejněny na základě ustanovení § 3 odst. 1 ZRS:

Obchodní tajemství či jiné informace dle § 3 odst. 1 ZRS	**Umístění ve smlouvě či jejích přílohách**
Zvolte položku.	Klikněte sem a zadejte text, např. „**Čl. 6 odst. 6.1 smlouvy.**"
	Klikněte sem a zadejte text.
	Klikněte sem a zadejte text.

Účastník tímto čestně prohlašuje, že údaje a skutečnosti uvedené ve smlouvě, která je nedílnou součástí nabídky, označené jako obchodní tajemství, naplňují současně všechny definiční znaky obchodního tajemství, tak jak je vymezeno v ustanovení § 504 občanského zákoníku, tj. obchodní tajemství tvoří konkurenčně významné, určitelné, ocenitelné a v příslušných obchodních kruzích běžně nedostupné skutečnosti, které souvisejí se závodem a jejichž vlastník zajišťuje ve svém zájmu odpovídajícím způsobem jejich utajení. Účastník dále čestně prohlašuje, že nese veškerou odpovědnost v případě, že část obsahu smlouvy, která se týká obchodního

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

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

tajemství účastníka a která v důsledku toho bude pro účely uveřejnění smlouvy v registru smluv znečitelněna, pokud by smlouva v důsledku takového označení byla uveřejněna způsobem odporujícím ZRS, a to bez ohledu na to, zda byla smlouva uveřejněna prostřednictvím registru smluv ze strany zadavatele nebo účastníka.

Účastník tímto čestně prohlašuje, že neprodleně písemně sdělí zadavateli skutečnost, že takto označené informace přestaly naplňovat znaky obchodního tajemství.

Účastník tímto čestně prohlašuje, že údaje a skutečnosti uvedené ve smlouvě, která je nedílnou součástí nabídky, jsou údaji nebo skutečnostmi (s výjimkou obchodního tajemství, uvedeného výše), které nemohou být v registru smluv uveřejněny na základě ustanovení § 3 odst. 1 ZRS. Účastník dále čestně prohlašuje, že nese veškerou odpovědnost v případě, že část obsahu smlouvy, která obsahuje informace označené účastníkem jako informace ve smyslu § 3 odst. 1 ZRS a která v důsledku toho bude pro účely uveřejnění smlouvy v registru smluv znečitelněna, pokud by smlouva v důsledku takového označení byla uveřejněna způsobem odporujícím ZRS, a to bez ohledu na to, zda byla smlouva uveřejněna prostřednictvím registru smluv ze strany zadavatele nebo účastníka.

V …….…. dne ……

Do 1. kola PTK je celkem přihlášeno 7 registrovaných účastníků (pod NDA), z toho:

- 4 účastníci reagovali na PTK:
  - 1 účastník odpověděl plnohodnotně,
  - 1 účastník odpověděl plnohodnotně, nikoliv však k požadovanému řešení (agentless DLP)
  - 2 účastníci odpověděli, že se PTK z kapacitních/jiných důvodů nezúčastní
- 3 účastníci nereagovali vůbec

Příloha č. 11 Výzvy

Předběžná tržní konzultace - Zavedení komplexního síťového řešení prevence úniku dat (DLP) pro non-Microsoft systémy v prostředí Správy železnic

Obsah / data

Odpovědi účastníků 1. kola PTK

Dotazy na účastníky PTK	Účastník 1 (odpovědi nejsou plně relevantní s ohledem na navrhované Agent-based řešení DLP, které není požadováno)		Účastník 2	
	ANO/NE/Částečně	Komentář	ANO/NE/Částečně	Komentář
Prosím o vyjádření k příloze č. 1 – Specifikace předmětu plnění: Je záměr a cíl Aktivity Implementace komplexního řešení prevence smyslu úniku v síti (DLP) pro jiné systémy než Microsoft v prostředí Správy železniční dopravní cesty srozumitelný a srozumitelný? Pokud ne, jaké další informace byste potřebovali, abyste mohli pohodlně odpovědět na otázky?	x	x	ČÁSTEČNĚ	Záměr je nesprávně pojmenovaný, protože reálným požadavkem je: „Zavedení komplexního síťového řešení prevence úniku dat (DLP) v prostředí Správy železnic“ doplňující dříve implementované řešení ochrany citlivých dat na koncových stanicích (DLP Endpoint). Z pohledu návrhu realizace chybí odpověď na otázky: - Transparentní Proxy DLP – existují jako stávající webové řešení? budou vytvořeny pro účely tohoto projektu? nebo mají být dodány v rámci projektu? Pokud už existují o jako se jedná technologií, verzi, sizing, konfigurace atd. - Existuje popis chráněných informací pro konfiguraci Network DLP, nebo má být jeho dodání součástí analytické fáze dodávky?
Jsou poskytnuty informace dostatečně podrobné (pokud ne, jaká úroveň podrobností by pro byla dostatečná)?	x	x	x	Dokument je dobře a přehledně zpracovaný až na zavádějící pojmenování PTK
Jaký je váš časový odhad pro trvání této etapy (v měsících)?	Cca 6 měsíců	x	x	Řádově se jedná a 14 dní na všechny přípravné práce pro vytvoření prostředí na straně SŽ a následnou instalaci řešení se základní konfigurací - Odladění nastavení 14 dní - Pilotní provoz 5 týdnů - Překlopení do produkčního provozu 4 týdny s pořadím – kontrola technického segmentu, následně celý webový provoz směrem z organizace - Implementace je tak řádově na 2 – 3 měsíce s kompletním odladěním Doba trvání implementace závisí na: - Poskytnutých součinnostech - Požadované doby testování a pilotního provozu - Jestli musí být zbudovány Transparentní DLP proxy, nebo lze využít existující řešení

Jaký je Váš odhad ceny následujících etap (v Kč bez DPH): · Návrh rozvrhu · Implementace vybraného DL řešení. · Detailní analýza pro nasaze vybraného DLP řešení. · Implementace a konfigurac vybraného DLP řešení (pravidla, politiky, proces řízení incidentů, role, školení administrátorů a dozorčích pracovníků (SOC)). · Příprava základní knihovn pravidel detekce a reakce. · Realizace adopční kampaně. · Implementace a konfigurac vybraného DLP systému. Uveďte také ceny licencí a dalších souvisejících služeb?	Indikativní cena 127.320.000,- Kč bez DPH	x	x	V rámci DLP projektů se obvykle naceňuje kompletní pracnost/cena za implementaci řešení, rozpad na jednotlivé fáze není relevantní z důvodu vysoké nepřesnosti způsobené obvykle neočekávanými okolnostmi a technologickými neznámými v jednotlivých fázích. ICZ garantuje cenu za nasazení v odsouhlaseném rozsahu prací. Odhady cen: - Implementace cca 750.000, - Kč bez DPH - Podpora na 5 let – cca 840.000, - Kč bez DPH Licence Forcepoint Network DLP (IP protection): - 17.000 uživatelů na 5 let – subsciprion licence s podporou od výrobce 79.708.750,- Kč bez DPH - Jedná se o ceníkové ceny – projektové budou vypracovány na základě upřesnění zadání ze strany SŽ
Uveďte také ceny licencí a dalších souvisejících služeb? • Zadejte celkovou cenu za licen pro 17 000 uživatelů (předkládáme doplňkové a neduplikované funkční pokrytí oproti MS Purview DLP). •Služby podpory výrobce (5 let). • Pravidelné škole administrátorů 1x (16 hodin) ročně. V doplňujících komentářích pak uveďte rozpis ceny včetně správy řešení na 5 let.	x	x	x	TOC náklady z ceníkových cen tak představují 81.298750,- Kč bez DPH pro 17.0000 uživatelů na 5 let včetně implementace a podpory
S ohledem na vybrané systémy uvedené v dokumentu „PTK – informace o systémech SŽ" a požadavky na zamezení úniku citlivých dat počítáte s nasazením dalších technologií kromě řešení DLP? Pokud ano, uveďte jaké a jejich cenu, vzor licence.	x	x	NE	za předpokladu, že má SŽ správně nasazené MDP, šifrování disků, správu přístupových oprávnění a optimálně klasifikaci dokumentů
Jsou poskytnuty podklady ceny dostatečné pro stanovení nabídky této etapy?	x	x	ČÁSTEČNĚ	Ze zadání není jasné jak a jestli má být realizována „Transparentní DLP Proxy" a dále jestli existují bezpečnostní politiky ohledně zabezpečení citlivých dat, nebo bude součástí implementace jejich návrh/odladění a pomoc s vybudováním kompletní bezpečnosti citlivých informací
Popis požadavku				
Architektura systému				
Jakou architekturu systému DLP navrhujete pro naši síťovou infrastrukturu?	x	Enterprise DLP je nejlepší volbou pro vaši infrastrukturu.	x	Topologie Network DLP bude odpovídat zapojení popsaném v popisu současného stavu, spolu s návrhem předpokládané architektury – Web DLP proxy v monitorovaných lokalitách a na odchozím/příchozím směru z celé organizace.
Je námi navrhované řešení pro integraci vašeho řešení kompatibilní s vámi doporučenou architekturou nebo navrhujete jiné řešení?	Ano		ANO	V popisu není definované, jestli lze využít integraci přes ICAP protokol na „Transparentní proxy DLP" nebo má být tato proxy zbudovaná také – obojí Forcepoint Network DLP umožňuje

Jak bude řešena redundance a vysoká dostupnost systému ve vámi navrhovaném řešení?	x	Platforma Sigma společnosti Proofpoint je cloudové řešení SaaS hostované v regionech AWS a zónách dostupnosti v USA, Německu, Japonsku a Austrálii. Všechna základní úložiště dat jsou distribuována, podporují nativní replikaci a mají automatické převzetí služeb při selhání. Webové koncové tělo jsou vystaveny prostřednictvím služeb Amazon ELB, která poskytuje záruky HA. Interně se náš systém spoléhá na asynchronní architekturu předávání zpráv, která omezuje účinky lokálních selhání běhového prostředí a poskytuje odolnost a kontinuitu. Všechna data, která procházejí platformou Propoint Sigma, jsou funkční archivována v geograficky replikovaném segmentu S3, který poskytuje bodové - v celém včasné obnově systému.	x	Komponenta Protector (network dlp), která bude analyzovat provoz posílaný z transparentních proxy nebývá budována v HA z důvodu, že se nejedná o kritický systém, narozdíl od „Transparentních Proxy DLP" které je doporučené budovat v režimu HA
Podporuje vámi navrhované řešení škálovatelnost pro budoucí rozšíření ochrany sítě?	ANO	Všechny runtime služby jsou nasazeny s více instancemi a schopnostmi samoopravy/škálování.	ANO	Analýza provozu probíhá na Protector serverech, kde se předpokládá využití virtualizovaných applaince s možností navyšování zdrojů a tím adekvátně reagovat na případné navýšení síťového provozu
Jaké jsou očekávané hardwarové a softwarové požadavky pro provoz navrhovaného řešení?	x	Platforma Sigma společnosti Proofpoint je cloudové řešení SaaS, které žádný hardware.	x	Systém se bude skládat ze 3 komponent: 1)Management server (Forcepoint Security Manager) – virtualizovaný server (8x vCPU, 16 GB RAM, 100GB systém, 400GB DATA) 2)DLP Protector – předpoklad 2x v prostředí, virtualizovaný server/appliance 8x vCPU, 16GB RAM, 100GB 3)Volitelně DLP Proxy 4x v prostředí dle požadavků na HA, virtualizovaný server/volitelně HW applaince od výrobce 20x vCPU, 36GB RAM Popis zde: https://help.forcepoint.com/docs/de ployctr/v85/dic_sys_req.aspx https://support.forcepoint.com/s/art icle/Forcepoint-V5K-and-V10K- Appliance-Resource-Equivalents-for- Virtual-Appliances
Jak systém zpracovává síťový provoz bez ztrát výkonu, případně jaké jsou očekávané výkonové ztráty v síťové komunikaci (např. zpoždění datových přenosů, latence sítě atd.)?	x	Všechny důležité databáze jsou denně zálohovány se zálohami uloženými v samostatném georeplikovaném kbelíku S3. V závislosti na závažnosti mohou být všechna data kdykoli obnovena do stejného datového centra, což poskytuje téměř nulové RPO. V případě katastrofy, která je natolik závažná, že vyžaduje přechod do jiného datového centra, je veškerá infrastruktura definována jako kód a lze ji spustit v novém datovém centru AWS prostřednictvím stávající automatizace.	x	Zpoždění vyhodnocení síťového provozu může vznikat hlavně na „Transparentní Proxy DLP" která by měla optimálně provádět SSL decryption a následně posílá provoz přes ICAP pro vyhodnocení. Při poruše vyhodnocení na DLP Protector-u lze nastavit čas, po kterém bude provoz puštěn dále.
Může systém DLP ovlivnit komunikační sítě na úrovni audio/video přenosů a jak byste řešili riziko ovlivnění?	NE	x	ČÁSTEČNĚ	Network DLP kontroluje webový/emailový provoz na základě integrace na proxy/email server s možnostmi provádět detekce v rámci obrazových formátů (OCR) audio/video přenosy nelze zabezpečit.
Vyžaduje navrhovaný systém pro svůj provoz připojení ke cloudu, nebo posílá nějaká data do cloudových služeb na internetu, případně je schopen fungovat zcela offline bez přímého přístupu k internetu?	ANO	Enterprise DLP Platform společnosti Proofpoint je cloudové řešení SaaS a jako takové vyžaduje připojení k internetu.	ANO	Navržené řešení lze provozovat plně v offline režimu, ale je doporučené zajistit plán aktualizací OS a samotných komponent.
Jaké jsou možnosti integrace vámi dodávaného řešení se stávajícími technologiemi Cisco FirePower a PaloAlto NGFW?	x	Vzhledem k povaze jakéhokoli řešení DLP nedojde k žádným integracím. Integrujeme a sdílíme informace o hrozbách s PaloAlto Wildfire v našem e-mailovém řešení a sandboxingu.	x	Lze využít pouze integrace na „Transparentní Proxy DLP" pomocí ICAP protokolu, nebo SPAN/Mirror Port mode napojení na Protector. Cisco FirePower – pokud umí SSL Decryption a ICAP je vhodný PaloAlto NGFW – pokud umí SSL Decryption a ICAP je vhodný
Jste schopni v rámci dodávky vašeho DLP systému dodat potřebnou doplňkovou konfiguraci pro všechny provozované technologie, pokud jsou součástí řešení?	ANO	Profesionální služby nastavují řešení společně s IT týmy našich zákazníků.	ANO	Konfiguraci lze dodat pro podporované verze systémů o kterých je dodavatel dopředu informován a jsou relevantní k nasazovanému řešení.

Funkční možnosti				
Jaké typy dat a informací může systém DLP detekovat a chránit?	x	Systém Enterprise Data Loss Prevention (DLP) společnosti Proofpoint dokáže detekovat a chránit různé typy dat a informací, včetně: •Citlivá nebo regulovaná data •Kontext aktivity uživatele, záměru a přístupu •Prolomené účty a phishing uživatelé •Přenosy exfiltrace dat prostřednictvím e-mailu •Citlivá data v nestrukturovaném obsahu •Citlivé dokumenty s otisky prstů s možností úplné i částečné přesné shody dat •Data v pohybu a v klidu v podporovaných cloudových službách (např. O365, Google Workspace, Box) •Ztráta dat prostřednictvím cloudové synchronizace, USB, nahrávání, tisku, webové pošty a dalších běžných kanálů pro ztrátu dat Systém také podporuje vynucování klasifikačních schémat organizačních informací (např. Vyhrazené, Důvěrné, Přísně tajné) a může blokovat exfiltraci důvěrných informací prostřednictvím e-mailu.	x	Dle definic vše podle: formátu, typu souborů, označení, počtu příloh, typu příloh, obsahové analýzy – slovníky, fráze, regulární výrazy, klasifikační značky,.. exaktní schody souboru (hash - fingerprint) částečná shoda, definice výjimek a hlavně vztahů mezi jednotlivými pravidly např. (1 OR 2) AND NOT 3 Pro Network DLP je dostupné OCR na obsahovou analýzu
Jsou v systému šablony pro odhalování úniku citlivých informací?	x	Email DLP sdílí více než 80 šablon zásad dostupných s Email Protection a dokáže detekovat citlivé informace ve více než 400 typech. E-mailové zásady DLP jsou plně přizpůsobitelné a lze je klonovat a upravovat za vytvoření dalších zásad. Pravidla můžete nakonfigurovat tak, aby se aplikovala na jednotlivé výskyty NPI nebo když je stejný počet slovníkových a inteligentních identifikátorů. Do zásad lze mapovat více pravidel (například zásady HIPAA, GLBA a AB 1950). Zásady lze nastavit na globální úrovni nebo lze nastavit jedinečné zásady pro jednotlivé skupiny/oddělení.	ANO	Forcepoint obsahuje od výrobce předpřipravené politiky, pravidla, slovníky dle zvoleného regionu (EU – Czechia) nebo oblasti činnosti (IT / Banking / Financial /…)
Jaké síťové protokoly podporují navrhované řešení pro monitorování a ochranu dat (např. HTTP, HTTPS, FTP, FTPS, SMB, TELNET, SSH atd.) a umožňuje přizpůsobení portů, na kterých tyto protokoly běží? Dokáže systém analyzovat a chránit provoz, jako je DNS přes HTTPS nebo SSH přes HTTPS a podobně?	x	Enterprise DLP spojuje výstupní kanály e-mailu, koncového bodu a cloudového zabezpečení do jediného skleněného panelu pro nápravu incidentů. Incidenty lze spravovat buď v samotné aplikaci, nebo v řešeních SIEM/SOAR, vlastních aplikací nebo prostřednictvím integrace s nástroji pro správu IT služeb, jako je ServiceNow. Zásady oznamování založené na http webhoocích nebo rozsáhlých veřejných rozhraní API usnadňují nastavení a správu podnikových dat DLP v externích nástrojích. Exportujte data o incidentu netechnickým týmům mimo tým Incident Response nebo SOC, který spravuje výstrahy, nebyl nikdy snazší, pomocí našich funkcí exportu do csv, json nebo pdf, včetně volitelného snímku obrazovky pro další nevyvratitelný kontext, který snadno interpretují i pracovníci mimo TO. . má kontextové menu.	x	Network DLP Protector analyzuje provoz směřovaný/dešifrovaný pomocí předřazené proxy a nativně tak vyhodnocuje http, HTTPS, FTP, SFTP provoz s možností definovat custom porty a služby pro kontrolu.
Podporuje systém klasifikace dat podle citlivosti a na základě jakých pravidel?	x	Proofpoint DLP podporuje 37 jazyků slovníků, dokáže detekovat citlivé informace ve více než 100 typech souborů a také podporuje čtení metadat štítků, které lze použít v pravidlech a zásadách DLP. Zásady jsou plně přizpůsobitelné a lze je klonovat a upravovat za účelem vytvoření dalších zásad. Zásady lze nastavit na globální úrovni nebo lze nastavit jedinečné zásady pro jednotlivé skupiny/oddělení. Společnost Proof neustále vydává nové předdefinované slovníky a inteligentní identifikátory, které poskytují pokrytí identifikace dat ve všech regionech USA, APJ a EMEA. Většinu čísel občanských průkazů, pasů a řidičských průkazů máme dobře pokrytou. Nové slovníky mohou být přidány nebo definovány pro podporu dalších předpisů, jako jsou NASD, PIPEDA nebo kódy specifické pro vaše regulační prostředí. Slovníkové termíny být vážené, aby mohly být použity nebo několikrát síla shody v nejbližším termínu nebo aby byly povoleny výjimky. Dynamické aktualizace zajišťující, že nainstalované slovníky jsou vždy aktuální s nejnovějšími kódy.	ANO	Lze integrovat s produkty třetích stran (MS, Titus, ..) nebo jen reagovat na klasifikační značku v dokumentu/vlastnostech dokumentu dle definovaných politik/pravidel

Podporuje systém integrace se stávajícími systémy označování a klasifikace dat, jako je Microsoft Purview Information Protection?	x	Proofpoint integrovat s Microsoft MIP Služba Cloud DLP podporuje čtení, zápis a mazání citlivosti štítků MIP pro kompatibilní typy souborů, když jsou upraveny na základě posouzení souboru podle identifikátorů DLP. Agent koncového bodu podporuje události čtení pro štítky citlivosti MIP, ale dnes již nezapisuje ani nemaže E-mailový DLP server podporuje čtení událostí pro štítky citlivosti MIP, ale dnes již nezapisuje ani nemaže má kontextové menu	ANO	Nativní integrace na Microsoft Purview Information Protection
Jaké metody používá systém k detekci úniku (např. pravidla, regulární výrazy, kontrola obsahu dokumentu, šablony dokumentů, strojové učení, analýza chování) v rámci řešení bez agentů?	x	Systém Enterprise DLP společnosti Proofpoint používá řadu metod k detekci úniku dat v rámci řešení bez agentů, včetně: •Pokročilý regulární výraz •Klíčová slova a datové slovníky •Částečná shoda dokumentů •Dokument otisky prstů •Bayesovská analýza •Shoda metadat •Optické rozpoznávání znaků (OCR) •Analýza jazykového obsahu pomocí strojového učení •Behaviorální analýza Tyto metody umožňují komplexní kontrolu obsahu a detekci citlivých nebo regulovaných dat, aktivity uživatele, záměru a kontextu přístupu, stejně jako kompromitovaných účtů a phishingových uživatelů.	x	Na síťové úrovni jsou dostupné všechny požadované metody detekce úniků citlivých dat včetně OCR
Jaké možnosti nabízí systém pro řízení přístupu uživatelů k citlivým informacím a je schopen se integrovat se systémy Active Directory, LDAP nebo IdM?		Enterprise DLP společnosti Proofpoint nabízí podrobné zásady přístupu na úrovni, které lze plně přizpůsobit pro řízení přístupu uživatelů k citlivým informacím. Tyto ovládací prvky umožňují řadu přístupů, od úplného administrativního přístupu až po kontrolu konkrétních incidentů v definovaném časovém rozsahu. Řešení lze integrovat se stávajícími řešeními IDP (založené na SAML 2.0), aby poskytovalo bezproblémové jednotné přihlašování a využívá skupiny zabezpečení Active Directory k udělení přístupu na základě rolí. Kromě toho se může integrovat s řešeními IAM, aby umožnil přístup do konzole Proofpoint Admin Console a může přijímat zdroje JSON pro příjem dat z platformy Enterprise DLP a provádění akcí pracovního postupu odezvy.	x	AD, LDAP, IdM dle typu, případně dvoufaktorové ověření
Podporuje systém kontroly šifrovaného provozu (dešifrování SSL/TLS) a v jaké verzi TLS?		Řešení Enterprise DLP společnosti Proofpoint podporuje kontrolu šifrovaného provozu prostřednictvím dešifrování SSL/TLS. Řešení využívá standardní zabezpečení transportní vrstvy (HTTPS v rámci TLS) a podporuje verze TLS až do TLS 1.2. Všechna data v pohybu pro připojení API, integrace komponent platformy, komunikace koncových agentů, přenos protokolů a přístup k uživatelskému rozhraní jsou zabezpečeny pomocí 256bitového šifrování AES.	ANO	Network DLP bude využívat: A)Transparentní Proxy DLP třetí strany Nebo B)Forcepoint Web Gateway
Vyžaduje navrhované řešení pro plnou funkčnost implementaci SSL offloadingu (dešifrování SSL/TLS provozu), nasazení webové proxy nebo jiných systémů? Jaké další součásti jsou nutné k zajištění plné funkčnosti systému?	Žádný	Řešení Enterprise DLP společnosti Proofpoint podporuje kontrolu šifrovaného provozu prostřednictvím dešifrování SSL/TLS a využívá zabezpečení standardní transportní vrstvy (HTTPS v rámci TLS) až do TLS 1.2. Řešení pro plnou funkčnost nevyžaduje snížení zátěže SSL. Podnikové řešení DLP společnosti Proofpoint má ve výchozím nastavení podporu proxy a může pracovat za proxy, aniž by vyžadovalo výjimky z infrastruktury proxy. Další komponenty potřebné pro plnou funkčnost systému zahrnují agenty koncových bodů DLP nasazené na koncové body zákazníků, volitelné on-premise komponenty, jako je naše zařízení pro zabezpečení e-mailu, a cloudová služba Proofpoint pro Endpoint DLP a Data Discover. Síťový proxy server Proofpoint je navíc plně cloudový a řešení lze integrovat se stávajícími řešeními IDP (založenými na SAML 2.0) a skupinami zabezpečení Active Directory pro řízení přístupu.	ANO	Pro plnou funkcionalitu je SSL offloading doporučený, pokud ho není možné provádět na infrastruktuře SŽ, lze plně zprovoznit v rámci dodávky DLP řešení Forcepoint.
Jaké kryptografické algoritmy systém podporuje v SSL Offloading?	x	Nepožadujeme SSL Offloading	x	Závisí plně na implementované „Transparentní Proxy DLP“ Alternativně Forcepoint DLP proxy podporuje většinu šifrovacím algoritmů

Pokud systém vyžaduje použití proxy pro snížení zátěže SSL, jaký protokol lze použít k připojení k tomuto proxy?	x	Nepožadujeme SSL Offloading	x	ICAP/ICAPS
Jak systém zpracování řeší data v archivních souborech, které se přenášejí bez hesla jako heslem? Dokáže analyzovat obsah nešifrovaných a šifrovaných archivů a odhalit možné úniky citlivých informačních skrytých v těchto souborech?	x	Naše podnikové DLP řešení dokáže analyzovat obsah nešifrovaných archivních souborů a zjistit možné úniky citlivých informací. Neposkytuje však konkrétní podrobnosti o zpracování šifrovaných archivů nebo možnosti analyzovat jejich obsah, pokud jsou chráněny heslem.	x	DLP řešení monitoruje/chrání citlivá data v archívech které nejsou chráněny heslem. V případě potřeby monitorovat obsah v šifrovaných souborech je nutné mít nastavené příslušné pravidlo v DLP pro koncové stanice (Endpoint DLP)
Dokáže systém detekovat citlivé informace v multimediálních, jako jsou obrázky, videa nebo zvukové soubory, a má funkci OCR (Optical Character Recognition) k identifikaci citlivých dat obsažených v obrazových formátech?	ANO	Ano, naše podniková DLP dokáže detekovat citlivé informace v multimediálních souborech, jako jsou obrázky. Podporuje funkci OCR (Optical Character Recognition) pro identifikaci citlivých dat obsažených v obrazových formátech. Modul OCR detekuje text vložený do obrázků, jako jsou naskenované formuláře, dokumenty, snímky obrazovky, obrázky a soubory PDF, extrahováním textu a jeho vyhodnocením proti povoleným detektorům.	ANO	Network DLP využívá OCR
Vyžaduje systém integraci do lokální infrastruktury Microsoft PKI a podporuje možnost použití HSM boxů?		Není potřeba integrace s šifrováním, pokud není řízena Microsoft MIP prostřednictvím Email DLP V koncovém bodě můžeme označit osobně zašifrovaný obsah jako neschopný skenování a podle toho jednat (blokovat atd.) Veškeré šifrování v rámci služby SaaS zajišťuje Proofpoint	NE	Není potřebné
Můžete váš systém přijímat data pro úpravy pomocí jiného protokolu než ICAP?	ANO	Ano, naše podnikové DLP může přijímat data pro úpravy pomocí jiných protokolů než ICAP. Proofpoint se může integrovat s jinými řešeními DLP přes port 25, kam obvykle Proofpoint nebo jiné řešení vloží hlavičky zpráv, které může alternativní řešení detekovat a dále analyzovat nebo provést vhodnou akci (tj. blokovat, šifrovat).	ANO	ICAP/ICAPS/MTA/SPAN/Mirror Port mode
Metody ochrany informací				
Jak systém detekuje a krádeži dat pomocí steganografie? Dokáže identifikovat skryté informace v obrazových a multimediálních souborech nebo jiných formátech, které lze použít ke skrytým exfiltracím citlivých dat?	x	Naše podnikové DLP detekuje, zda uživatel používá některé z předdefinovaných steganografických nástrojů, které lze použít ke skrytí textových informací v obrázcích, a zablokuje tyto nástroje, aby došlo k úniku dat. Neposkytuje však odchozí steganografickou detekci.	x	Žádné DLP steganografii neřeší, lze řešit produktem Forcepoint CRD
Umožňuje systém blokování, karanténu, dynamickou změnu dat nebo při zjištění úniku dat a jak upozornění upozornění na SD Jira nebo SIEM?	ANO	Naše podniková DLP umožňuje blokování, karanténu, dynamickou změnu dat a upozornění, když je zjištěn únik dat. Oznámení lze odeslat do SD Jira nebo SIEM prostřednictvím integrace s nástroji pro správu IT služeb, jako je ServiceNow, zásady oznamování založené na webhoocích HTTP nebo rozsáhlá veřejná rozhraní API. Díky tomu je spotřebování podnikových dat DLP v externích nástrojích jednoduché na nastavení a vlastní správu.	ANO/ANO	Systém umožňuje akce: Allow, Block, Quarantine, pro některé kanály Encrypt, Confirm Napojení je formou posílaní Syslog/Email notifikací, nebo vyčítáním událostí přímo z SQL DB
Jak systém zpracovává a minimalizuje falešné poplachy?	x	Naše podnikové řešení DLP obsahuje několik funkcí pro minimalizaci falešných poplachů. Tyto funkce zahrnují inteligentní identifikátory, které hledají správný počet číslic a počítají kontrolní součet, aby potvrdily, že číselné řetězce jsou skutečně chráněné informace. Proximity Matching najde slovníkové výrazy v těsné blízkosti inteligentních identifikátorů a slovníků pro vylučující velká písmena eliminují falešné poplachy tím, že ignorují shody s položkami ze slovníku s negativními písmeny. Zákaznická technická podpora společnosti Proofpoint navíc poskytuje průvodce zařazením na seznam bezpečných adres pro identifikaci IP adresy a domény, které lze zařadit do seznamu bezpečných přes různé filtry, aby se minimalizovaly falešné poplachy. Správci mohou také označit falešně pozitivní výstrahy jako „Není problém" a přidat výjimku do spouštěcího pravidla pro vyloučení podle uživatele, skupiny, geografické polohy atd. To pomáhá využít pracovní tok incidentu pro tuto výstrahu bez dynamických aktualizací pravidel.	x	Detekují se v rámci pilotního provozu a dále na základě pravidelných statusů po celou dobu běhu projektu. Upravují se definice na důvěryhodné zdroje, cíle, detekční meze, výjimky pro zvolené

Lze v systému nastavit zásady a pravidla pro různé typy dat a pro různé uživatele definované v Active Directory?	ANO	Zásady a pravidla v podnikové DLP lze nastavit pro různé typy dat a pro různé uživatele definované v Active Directory. Řešení DLP společnosti Proofpoint umožňuje granulární konfiguraci a kontrolu zásad a pravidel, což umožňuje identifikaci citlivých nebo regulovaných dat, chování uživatelů a povědomí o hrozbách. Zásady lze rozdělit na zeměpisné umístění, skupiny uživatelů, typy zařízení, sítě atd. a na základě těchto kritérií lze aplikovat akce řízené zásadami. Průzkumník Nexus People Risk Explorer společnosti Proofpoint navíc poskytuje přehled o rizicích uživatelů na základě jejich rolí, povinností a přístupu, což umožňuje výběr vhodných zásad a ovládacích prvků pro zabezpečení zranitelných uživatelů.	ANO	Všechny politiky lze přiřadit/výjimkovat na základě zadaných uživatelů, OU, custom computers, bussines units, atd.
Podporuje systém ochrany dat na úrovni aplikace a koncového bodu v režimu bez agenta, nebo má k dispozici agenta pro vybrané systémy, kde je vyžadována rozšířená ochrana?	x	Proofpoint Enterprise DLP podporuje ochranu dat na úrovni aplikací a koncových bodů v režimu bez agenta iv režimu založeném na agentech. Pro přístup z nespravovaných zařízení je k dispozici nasazení bez agentů, jako je použití proxy SAML v kombinaci s izolací pro poskytování DLP pro spravované aplikace. Navíc nabízíme agenta Endpoint DLP, který podporuje systémy Windows, Mac a VDI (Citrix, VMware atd.) pro rozšířenou ochranu v případě potřeby.	ANO	Forcepoint nabízí kromě Network DLP i Discover DLP a Endpoint DLP které poskytuje srovnatelné, nebo lepší výsledky než řešení od společnosti Microsoft. Nacenění a dodání klientského řešení proběhne na základě dodatečných požadavků.
Jaké jsou možnosti ochrany bez agenta (bez agenta na koncovém bodu) jako agenta na koncovém bodu?	x	Proofpoint Enterprise DLP nabízí možnosti ochrany bez agentů i na bázi agentů. Pro ochranu bez agentů využíváme proxy SAML v kombinaci s izolací k poskytování DLP pro spravované aplikace, zejména pro přístup z nespravovaných zařízení. Pro ochranu založenou na agentech nabízíme agenta Endpoint DLP, který podporuje systémy Windows, Mac a VDI (Citrix, VMware atd.), s podporou Linuxu plánovanou na H1 2025. Agent umožňuje komplexní ochranu dat, včetně kontroly DLP, sledování souborů a prevence/blokování nahrávání webových souborů do cloudových služeb a přenosů synchronizace cloudu do úložiště služeb.	x	Při využité Endpoint DLP je možné sledovat hlavně činnosti s daty před jejich zabalením/zašifrováním a také činnosti prováděné zaměstnanci nacházejícími se mimo organizaci.
Poskytuje systém ochrany pouze na aplikační vrstvu L7 modelu OSI, nebo může chránit i na vrstvách L4 a L5? Jaké konkrétní na těchto vrstvách nabízí, aby bezpečnostní funkce zajistila únik dat?	x	Proofpoint Enterprise DLP poskytuje ochranu na více vrstvách modelu OSI, včetně aplikačních vrstev L7. Nabízí také ochranu na transportní vrstvu L4 a vrstvu relace L5. Mezi specifické funkce zabezpečení v těchto vrstvách patří: •Aplikační vrstva L7: Kontrola DLP, sledování souborů, prevence/blokování nahrávání webových souborů do cloudových služeb a přenosy synchronizace cloudu do služeb úložiště. •Transportní vrstva L4: Šifrování TLS pro webový provoz a mezi a databází, zajišťující bezpečný přenos dat. •Vrstva relace L5: Správa a kontrola relací prostřednictvím serveru proxy SAML v kombinaci s izolací pro spravované aplikace, zejména pro přístup z nespravovaných zařízení. Tyto funkce společně pomáhají efektivně předcházet dat napříč různými vrstvami modelu OSI.	x	Network DLP toto neřeší.
Implementace procesu				

Jaký je navrhovaný postup implementace systému do naší síťové infrastruktury?	x	Navrhovaný postup pro implementaci Proofpoint Enterprise DLP ve vaší síťové infrastruktuře zahrnuje následující kroky: 1.Instalace a nastavení: Proofpoint Enterprise DLP, což je řešení SaaS, nabízí intuitivní a snadnou instalaci a nastavení. Cloudová platforma poskytuje viditelnost a správu napříč kanály a zvyšuje provozní efektivitu pro zákazníky. 2.Nasazení: Řešení je primárně zadáno jako cloudová služba s agenty koncových bodů DLP nasazenými na koncové body zákazníků. V cloudu lze také dodat volitelné místní komponenty, jako je naše zařízení pro zabezpečení e-mailu pro správu opuštění e-mailů. V případě potřeby může zákazník v AWS nasadit a provozovat virtuální stroje. 3.Politický lid: Platforma umožňuje populaci zásad a ochranu citlivých dat napříč zajišťuje-mailovými, cloudovými a koncovými kanály. Sjednocená konzole zjednodušuje třídění výstrah na e-mail, cloud a koncový bod. 4.Konfigurace: Pro pokrytí všech těchto případů použití a poskytnutí nejlepší možné ochrany proti úniku dat bude vyžadována podrobná diskuse o tom, jaké případy použití pokrýt a jak nastavit/konfigurovat podnikové DLP společnosti Proofpoint. 5.Průběžná podpora: Proofpoint poskytuje trvalou podporu, aby bylo zajištěno, že řešení bude i nadále splňovat vaše potřeby v oblasti ochrany dat. Produkt SaaS funguje agilním způsobem a umožňuje rychlé reakce na problémy zákazníků s minimálním dopadem.	x	Kick-off Analytické fáze (požadavky, infrastruktura, plán nasazení, bezpečnostní politiky,..) Příprava prostředí Instalace, počáteční konfigurace Napojení na infrastrukturu Pilotní provoz s laděním konfigurace a politik Podpora plošného nasazení Školení a dokumentace Akceptace Podpora po zvolenou dobu
Popište, jak jste realizovali jednotlivé fáze projektu od plánování až po plné nasazení?	x	Implementace Proofpoint Enterprise DLP od plánování až po úplné nasazení zahrnuje následující fázi: 1.Plánování: Tato fáze zahrnuje podrobnou diskusi o případech použití, které je třeba pokrýt, tedy, jak nastavit/konfigurovat Enterprise DLP společnosti Proofpoint. Tím je zajištěno, že jsou vyřešeny všechny případy použití a je zajištěna nejlepší možná ochrana proti úniku dat. 2.Instalace a nastavení: Proofpoint Enterprise DLP, což je řešení SaaS, nabízí intuitivní a snadnou instalaci a nastavení. Cloudová platforma poskytuje viditelnost a správu napříč kanály a zvyšuje provozní efektivitu pro zákazníky. 3.Nasazení: Řešení je primárně zadáno jako cloudová služba s agenty koncových bodů DLP nasazenými na koncové body zákazníků. V cloudu lze také dodat volitelné místní komponenty, jako je naše zařízení pro zabezpečení e-mailu pro správu opuštění e-mailů. V případě potřeby může zákazník v AWS nasadit a provozovat virtuální stroje. 4.Politický lid: Platforma umožňuje populaci zásad a ochranu citlivých dat napříč zajišťuje-mailovými, cloudovými a koncovými kanály. Sjednocená konzole zjednodušuje třídění výstrah na e-mail, cloud a koncový bod. 5.Konfigurace: Tato fáze zahrnuje konfiguraci řešení na základě podrobných plánovacích diskusí, aby byly pokryty všechny případy použití a poskytnuta optimální ochrana dat. 6.Průběžná podpora: Proofpoint poskytuje trvalou podporu, aby bylo zajištěno, že řešení bude i nadále splňovat vaše potřeby v oblasti ochrany dat. Produkt SaaS funguje agilním způsobem a umožňuje rychlé reakce na problémy zákazníků s minimálním dopadem.	x	Kick-off Analýza, detailní návrh a plán provedení Bezpečnostní procesy Workshopy – konfigurace, politiky, reakce, zapojení, atd. Vytvoření dokumentace Časová rezerva Etapa 2 - Pilotní nasazení Příprava prostředí (servery, SQL) Instalace řešení (centrální správa) Konfigurace a testovací napojení Network DLP - Proxy Školení I - práce s produktem Odladění konfigurace a bezpečnostních politik Časová rezerva Etapa 3 - Plošné nasazení Příprava plošného nasazení UAT testy Podpora plošného nasazení Podpora produktivního provozu 1 měsíc Časová rezerva Etapa 4 - Akceptace, podpora Finální konfigurace Školení II - vyhodnocení incidentů Finální dokumentace Akceptace Podpora, rozvoj
Jak je systém nakonfigurován a přizpůsobeným potřebám?	x	Podle výše uvedených kroků	x	Dle požadavků v zadávací dokumentaci a dále dle workshopů budou reflektovány požadavky relevantní k možnostem produktu

Jak probíhá testování a ověřování funkčnosti před spuštěním?	x	Testování a ověření funkčnosti Proofpoint Enterprise DLP před uvedením do provozu zahrnuje následující kroky: 1.Inscenace a příprava: To zahrnuje osvědčené postupy, migraci poskytovaných pravidel a předběžnou kontrolu stavu. 2.Pracovní sezení: Tato setkání zahrnují prověření osvědčených postupů, migraci sad pravidel, testování a ověřování a přenos znalostí. 3.Cutover: Tato fáze zahrnuje výřez „Herní plán", změny na poslední chvíli a závěrečné testování. 4.Přechod: Následné 'jemné ladění' a úvod do podpory jsou prováděny s cílem zajistit hladký přechod a ověření funkčnosti. Naše zákaznické služby jsou založeny na proaktivních programech, oslovení zákazníků a reaktivním reportu, který pomáhá s jakýmikoli problémy během tohoto procesu.	x	V rámci projektu je počítáno s pilotním provozem určeným k ověření všech integrací a ladění dokumentace a dále podporou při přechodu do ostrého provozu.
Používáte při zavádění DLP systémů nějaké metodiky a best practices nebo vlastníte vlastní zkušenosti z předchozích projektů podobného typu, pokud ano jakých?	x	Proofpoint Enterprise DLP využívá metodologie a osvědčené postupy při implementaci systémů DLP. Proces implementace zahrnuje podrobné plánování, instalaci a nastavení, nasazení, soubor politik, konfiguraci a průběžnou podporu. Tyto kroky zajistí, že budou vyřešeny všechny relevantní případy použití a bude poskytnuta nejlepší možná ochrana proti úniku dat. Naše zákaznické služby jsou navíc založeny na aktivních programech, dosahu zákazníků a reaktivním reportu, který pomáhá s jakýmikoli problémy během procesu implementace.	ANO	Best practices z projektů implementací DLP Endpoint/Netword/Discover/Cloud v rozsahu stovek a desítek tisíc zaměstnanců skrz všechny oblasti státní správy/soukromých společností.
Časově náročná realizace				
Jak dlouho trvá plná implementace systému po podpisu smlouvy?	x	Je těžké to odhadnout, protože každý zákazník má své vlastní požadavky. Nasazení archivu se obvykle provádí prostřednictvím malého počtu webových schůzek. Dalšími definujícími faktory by byly jakékoli časové osy příjmu dat (které mohou probíhat paralelně), složitost požadavků na supervizi, počet různých konektorů a dostupnost zdrojů zákazníků.	x	Záleží na poskytnutých součinnostech, samotná implementace je v řádu dnů, ladění do optimálního stavu nastavení detekcí týdny až měsíce
Jaký je odhadovaný časový rámec pro každou fázi projektu (analýza, návrh, pilotní provoz, živý provoz, školení a přijetí uživatele)?	x	Fáze 1 – Zahájení projektu: 1–2 týdny od uzavření obchodu Fáze 2 – Technický návrh: 2–3 týdny Fáze 3 – Implementace a návrh zařízení: 4 týdny Fáze 4 – Spuštění výroby: 2 týdny Fáze 5 – - Uzavření projektu: 1 týden Celková doba realizace projektu: 12 týdnů	x	Jednotlivé fáze se obvykle prolínají, takže trvání projektu není odpovídající prostému součtu trvání jednotlivých fází. Kick off – 1 den Analýza požadavků a prostředí – 10 dní Návrh zapojení a způsobu implementace –5 dní Příprava prostředí – 7 dní Instalace a počáteční konfigurace řešení – 2 dny Pilotní provoz – 5 týdnů Podpora plošného nasazení – 4 týdny Školení obsluhy – 2 dny Dodání dokumentace – 10 dní Akceptace – 1 den
Jaké faktory mohou ovlivnit časově osu implementace?	x	Časová osa implementace Proofpoint Enterprise DLP může být ovlivněna několika faktory, včetně: •Specifické požadavky každého zákazníka. •Složitost požadavků na dohled. •Potřebný počet různých konektorů. •Dostupnost zdrojů zákazníků. •Časové osy zpracování dat, ke kterému může docházet souběžně s jinými činnostmi.	x	Kapacity a součinnosti zadavatele a to hlavně s ohledem na: -Vytvoření prostředí -Schválení koncepce nasazení -Součinnost při nasazení řešení -Termín v rámci roku (například dovelené přes Vánoční svátky)
Je možné v případě naléhavé potřeby urychlit realizaci a jak?	x	Ano, v případě naléhavé potřeby je možné urychlit implementaci Proofpoint Enterprise DLP. Nasazení archivu se obecně provádí prostřednictvím malého počtu webových schůzek a časové osy příjmu dat mohou probíhat paralelně. Proofpoint navíc pracuje agilním způsobem a umožňuje rychlé reakce na problémy zákazníků s minimálním dopadem.	x	Ano obvykle lze upravit činnosti dle aktuální potřeby a priorit
Požadovaná součinnost ze strany zadavatele				

Jaké zdroje a informace od nás potřebujete pro úspěšnou implementaci?	x	Pro úspěšnou podnikovou implementaci DLP vyžaduje Proofpoint od zákazníka následující zdroje a informace: •Podrobná diskuse o případech použití, které je třeba pokrýt, případně také, jak nastavit/konfigurovat podnikové DLP společnosti Proofpoint, aby poskytovalo nejlepší možnou ochranu proti úniku dat. •Spolupráce s týmem zákazníka, aby bylo zajištěno, že jsou schopny replikovat kroky k vytvoření dalších případů použití v průběhu času. •Spolupráce s vedoucím prodejního účtu zákazníka, manažerem zákaznického úspěchu a týmem zákaznické technické podpory za účelem průběžné podpory a poradenství. •Přístup do prostředí zákazníka za účelem nasazení řešení a vybraných klíčových případů použití a zásad.	x	Popis prostředí, komentáře k navrženému zapojení DLP řešení, odsouhlasení dokumentace
Jaká je předpokládaná míra zapojení našeho IT týmu, garantů informačních aktiv a dalších při implementaci a přijetí systému?	x	Očekávaná úroveň zapojení vašeho IT týmu během implementace a přijetí Enterprise DLP zahrnuje dohled nad vytvářením pravidel DLP podle potřeb podniku a export uživatelských událostí DLP podle potřeby. Kromě toho se váš tým IT bude podílet na zajištění technické připravenosti, jako je propojení komunikace se školením s vaší podnikovou e-mailovou doménou, zařazení IP adresy na seznam bezpečných IP adres a provádění testů před spuštěním. Budou také muset upozornit interní týmy IT a helpdesk, když jsou naplánovány kampaně s cílem připravit se na dotazy a požadavky uživatelů. Garanti informačních aktiv a další zainteresované strany budou zapojeny do strategických cílů s cílem vytvořit komunikační plán a zajistit, aby byl program v souladu s kulturou a cílem vaší organizace. Budou se také účastnit pravidelných systémových auditů a zdravotních kontrol, aby byl zachován optimální výkon systému.	x	Bude detailně vypracováno s harmonogramem – vždy je uváděné: datum zahájení, datum ukončení, rozsah součinností zadavatele -Řádově se jedná o cca 4 pozice a 6 MD
Jaké školení budou naši zaměstnanci potřebovat a jste schopni je zajistit?		Naši zaměstnanci budou potřebovat školení o uživatelských upozorněních, možnostech zdůvodnění a organizačních zásadách, aby uživatelé pomohli vzdělávat uživatele o rizikovém chování. K dispozici je školení Proofpoint Security Awareness Training (PSAT), které zahrnuje obsahové moduly zaměřené na DLP/compliance/porušování soukromí. Toto školení je nezbytné pro zmírnění rizik, zejména pro nedbalé uživatele. Kromě toho může DLP v kombinaci s Nexus People Risk Explorer identifikovat rizikové uživatele a PSAT může poskytovat cílený obsah k nápravě případů nedbalého použití. Proofpoint nabízí vestavěné moduly na PSAT související se zpracováním citlivých dat, používáním schválených aplikací, ochranou soukromí a požadavky na dodržování předpisů, které lze uživatelům zasílat k řešení těchto problémů.	ANO	Školení provádíme pro: A) IT administrátory systému (provoz, aktualizace, vyhodnocení stavu, politiky a optimalizace) C) SOC tým – vyhodnocení událostí a požadavky na úpravu bezpečnostních politik
Jaké změny v naší současné infrastruktuře budou nutné pro provoz systému?	x	Pro provozování Proofpoint Enterprise DLP mohou být nutné následující změny vaší aktuální infrastruktury: 1.Nasazení DLP Endpoint Agents: Tyto agenty je třeba nainstalovat na koncové tělo zákazníka, aby mohli monitorovat a řídit činnosti související se ztrátou dat. 2.Integrace cloudových služeb: Řešení DLP společnosti Proofpoint je primárně založené na cloudu, takže bude nutná integrace s cloudovými službami společnosti Proofpoint. To zahrnuje konfiguraci nastavení přenosu a ukládání dat podle vašich regionálních požadavků. 3.Volitelné on-premise komponenty: Pokud se komponenty rozhodnete pro správu odchozích e-mailů používat místní, jako je zařízení pro zabezpečení e-mailu, bude nutné je odpovídajícím způsobem nasadit a nakonfigurovat. 4.Konfigurace síťového proxy: Síťový proxy server Proofpoint, který je plně cloudový, bude nutné integrovat do vaší síťové infrastruktury. 5.E-mailová implementace DLP: V závislosti na vašich preferencích lze Proofpoint Email DLP implementovat buď on-premise, nebo hostovat Proofpoint v cloudu. 6.Endpoint and Data Discover Agents: Tito agenti budou muset být nasazeni on-premise, aby mohli pracovat ve spojení s cloudovou službou Proofpoint.	x	Nutné bude napojení/zbudování „Transparentní Proxy DLP“ nebo využití SPAN/Mirror Port mode
Licence a náklady				

Jaké jsou celkové náklady na zařízení systému, pokud předpokládáme pokrytí na 2 místech v Internet-UAS (včetně DMZ) a na 8 místech v UAS-TDS za předpokladu poskytování služeb celkem pro 17000 uživatelů a propustnosti na linkách 2Gbps uplink/downlink?	x	Implementace	x	Forcepoint Network DLP je licencovaný per user bez ohledu na množství analyzovaného provozu/rychlost linek Licence je formou subscription s možností individuálně požádat o dodání perpetual varianty
Jaké jsou roční náklady na údržbu a podporu po dobu 5 let?	x	Dejte licence s vaší marží	x	Podpora je dle zkušeností v prvním roce zvýšená, následně klesne, proto obvykle dostávají zákazníci takto dělenou nabídku na podporu 1 rok – 16 MD 2 – 5 rok – 10MD/rok
Existují další náklady, které bychom měli považovat za skryté, pokud je požadována udržitelnost po dobu 5 let?	Žádný		x	Licenční náklady na podkladový OS (Windows Server 2016/2019/2022) a SQL Server 2016 a novější
Bude nutné v horizontu 5 let provést úplný upgrade systému, což by si vyžádalo další náklady spojené s další implementací, přepracováním zavedených pravidel apod.?	x	Kontrola zdravotního stavu je bezplatná a vystavujeme pouze dodatečnou fakturu, pokud uživatelé mají více než původní smlouvu	x	Ne pokud nedojde k zásadním změnám návazných v systémech SŽ
Pilotní provoz				
Je možné, že systém nejprve nasadí v pilotním režimu a je takový pilotní provoz jak?		Ano, je možné nasadit Proofpoint Enterprise DLP v pilotním režimu. Proofpoint poskytuje několik možností, jak simulovat dopad změny zásad. Při vytváření pravidel nebo podmínek zobrazuje rozhraní počet událostí, které podle pravidla spustilo za předchozí hodiny nebo dny, což správci poskytují okamžitý přehled o možném dopadu. Proofpoint Unified Alert Manager navíc obsahuje průzkumy, které umožňují analytikům filtrovat příchozí události na platformě Sigma a lokalizovat konkrétní události nebo skupiny událostí v rámci vyšetřování. Průzkumy se konfigurují podobně jako pravidlo, což umožňuje správci simulovat pravidlo nakonfigurováním Průzkumu na stejné parametry, což jim umožňuje zkoumat události, které by pravidlo vyvolalo nebo by mohlo spustit. Proofpoint také obsahuje funkci testeru v rozhraní DLP, kde lze nahrát dokumenty a ověřit jejich pozitivní nebo negativní shodu s zabudovaným detektorem DLP v aplikaci DLP.	ANO	Pilotní provoz je doporučený postup z důvodu otestování kompatibility se systémy zadavatele, reálné práce se systémem, ukázky odladění pravidel a konfigurace a v neposlední řadě vyhodnocení událostí po dobu pilotní
Jak dlouhá je pilotní fáze a co zahrnuje?	x	Pilotní fáze Proofpoint Enterprise DLP lze přizpůsobit na základě požadavků zákazníka. Zahrnuje možnosti pro simulaci dopadu změn, zobrazení počtu událostí, které by pravidlo vyvolalo, a použití Proofpoint Unified Alert Manager k filtrování a vyhledání konkrétních událostí. Správci mohou navíc použít funkci testeru v rozhraní DLP k nahrání a ověření dokumentů na pozitivní nebo negativní shodu do jakéhokoli detektoru DLP.	x	Dle požadavků zadavatele, obvykle 1 měsíc, ale není problém prodloužení až na 3 měsíce
Jaké metriky a KPI jsou během pilotního projektu sledovány?	x	Během pilotní fáze Proofpoint Enterprise DLP jsou monitorovány následující metriky a KPI: 1.Počet událostí spuštěných pravidel: Rozhraní zobrazuje počet událostí, které by pravidla vyvolala za předchozí hodiny nebo dny, a poskytuje okamžitý přehled o potenciálním dopadu. 2.Průzkumy v Unified Alert Manager: Analytici mohou filtrovat příchozí události, aby našli konkrétní události nebo skupiny událostí, a simulují pravidla pro zkoumání událostí, které mohly nebo mohly být spuštěny. 3.Výsledky funkce testeru: Správci mohou nahrát dokumenty k ověření pozitivních nebo negativních shody s jakýmkoli detektorem DLP zabudovaného do aplikace DLP. Tyto metriky pomáhají při hodnocení účinnosti a dopadu zásad DLP během pilotní fáze.	x	Kompatibilita se stávajícími systémy, stupeň odladění konfigurace (počet false positive událostí z celkového objemu detekcí např. pod 5%), zaškolení administrátorů v ladění konfigurace a vyhodnocování událostí
Jak se řeší případné problémy nebo úpravy během pilotní fáze?	x	Během pilotní fáze Proofpoint Enterprise DLP jsou problémy nebo úpravy prostřednictvím několika mechanismů. Správci mohou simulovat dopad změn zobrazením počtu událostí, které by pravidlo vyvolalo za předchozí hodiny nebo dny. Proofpoint Unified Alert Manager umožňuje analytikům filtrovat příchozí události a vyhledávat konkrétní události nebo skupiny událostí a simulovat pravidla pro zkoumání událostí, které mohly nebo mohly být spuštěny. Funkce testeru v rozhraní DLP navíc umožňuje správcům nahrávat a ověřovat dokumenty na pozitivní nebo negativní shodu do jakéhokoli detektoru DLP. Tyto nástroje poskytují okamžitou podporu a umožňují provádět úpravy v reálném čase, aby byla zajištěna účinnost zásad DLP.	x	Na základě zjištěných/nahlášených problémů dochází ke změně konfigurací/výjimkování zdrojů/cílů, změně detekčních metod a úrovní Na základě úrovní chyby se vše provádí bezodkladně, nebo dle domluveného časového schématu

Máte možnost řešit případné problémy s výrobcem daného DLP softwaru, jste partnerem daného výrobce?		Ano, partneři mají možnost řešit případné problémy s výrobcem softwaru Proofpoint Enterprise DLP. Společnost Proofpoint vytváří trvalé partnerství s nejlepšími bezpečnostními firmami v oboru, aby pomohla našim zákazníkům chránit jejich lidi, data a značku. Proofpoint má distribuční partneři, technologická a alianční partneři, partneři pro extrakci archivů, partneři pro ochranu sociálních médií a partneři Global System Integrator (GSI) a Managed Service Provider (MSP).	ANO	ICZ je partnerem společnosti Forcepoint a využívá mimo jiné i presales podpory lokálního zastoupení v možné roli quality assurence
Integrace a kompatibilita				
Je systém kompatibilní s našimi stávajícími síťovými zařízeními a bezpečnostními systémy? Přehled integrovaných systémů je uveden v dokumentu Informace o systémech Správy železniční dopravní cesty s tím, že další informace lze poskytnout na vyžádání.	ANO		ANO	Plně kompatibilní
Lze systém integrovat s dalšími bezpečnostními nástroji jako SIEM, IAM atd. a jaké bezpečnostní systémy podporuje?	x	Ano, Proofpoint Enterprise DLP lze integrovat s dalšími bezpečnostními nástroji, jako jsou SIEM a IAM. Proofpoint Enterprise DLP může posílat veškeré protokolování a upozornění na jakoukoli SIEM, která podporuje RESTful API jako zdroj dat, včetně Splunk. Platforma ochrany informací společnosti Proofpoint se navíc může integrovat s řešeními IAM, aby mohl být dostupný do konzole pro správu Proofpoint a obecně podporuje jakéhokoli poskytovatele federovaných identit založených na Oauth 2.0 nebo SAML 2.0. Proofpoint lze také integrovat s poskytovateli IAM, kteří mohou přijímat zdroje JSON pro příjem dat z platformy Enterprise DLP a provádět jakékoli akce pracovního postupu odezvy.	ANO	Integraci lze provést přes SysLog, nebo napojením na SQL DB
Podporuje systém standardních protokolů a API pro obousměrnou integraci (ovládání přes API, kontrola změn přes API, detekce zatížení přes API atd.)?	ANO	Ano, Proofpoint Enterprise DLP podporuje standardní protokoly a API pro obousměrnou integraci. Nabízím integraci DLP na bázi API pro rozšíření možností a přizpůsobení. Navíc podporuje integraci API (webhooky nebo Rest API) s předními cloudovými aplikacemi na trhu a umožňuje zásady oznamování tam, kde jsou aktuální řešení třetích stran. To umožňuje ovládání přes API, kontrolu změn přes API a načítání detekcí přes API.	ANO	Dostupný popis Forcepoint Management API
Jaké jsou požadavky na kompatibilitu s operačními systémy a aplikacemi v naší síti?	x	Pro koncové body DLP budeme muset nasadit lehké agenty na koncových bodech, ale není potřeba nic jiného.	x	Management OS – Microsoft Windows Server 2016 – 2022 SQL Server 2016 - 2024
Je systém schopen přímé integrace do různých aplikací pomocí speciálních konektorů pro připojení systémů? Pokud ano, aplikace a systémy podporují hlubší analýzu a ochranu dat na aplikační úrovni a jak probíhá integrace?	x	Proofpoint Enterprise DLP je schopen přímé integrace do různých pomocí speciálních konektorů pro připojení systémů. Proofpoint podporuje integraci s aplikacemi a systémy, jako jsou ServiceNow, Splunk, Microsoft 365, Google Workspace, Box a další cloudové služby. Integrace je dosaženo pomocí rozhraní API, webhooků a SAML pro jemné ovládací prvky zásad. Řešení CASB společnosti Proofpoint poskytuje detekci a odezvu DLP téměř v reálném čase pro podporované schválené cloudové aplikace prostřednictvím příslušných rozhraní API dodavatele. Proofpoint se navíc integruje s řešeními IAM, aby mohl být dostupný do administrátorské konzole Proofpoint a mohl zpracovávat zdroje JSON pro provádění akcí pracovního postupu odezvy.	NE	x
Podpora a údržba				
Jaký typ podpory poskytujete po implementaci systému (např. 24/7, SLA)?	x	Proofpoint poskytuje komplexní podporu po implementaci systému, včetně nepřetržité podpory pro všechny typy problémů P1 (kritické). Proofpoint nabízí různé úrovně podpory, včetně Platinové podpory, která poskytuje nepřetržitou podporu pro problémy s prioritou 1 a telefonickou podporu pro všechny problémy během pracovní doby. Proofpoint navíc nabízí doplněk Global Time Zone Add-On pro nepřetržitou podporu pro všechny problémy v libovolném časovém pásmu. Podrobné smlouvy SLA zahrnují definici priority a doby odezvy, jako je počáteční odpověď do 1 hodiny u problémů s prioritou 1 a nepřetržité úsilí až do vyřešení. Další podrobnosti naleznete v níže uvedených citacích. Úrovně podpory a smlouvy SLA, které Proofpoint zahrnovaly původní MSA, naleznete zde: •Podpora:https://www.proofpoint.com/sites/default/files/misc/pfpt-en-support-services-program.pdf •SLA:https://www.proofpoint.com/sites/default/files/general_terms_hosted_services_sla_-_mar_2016.pdf	x	Podpora jde požadavků zákazníka, SLA, pracovní doba 8:00 – 17:00

Jak se řeší aktualizace a upgrade systému?	x	Aktualizace a upgrady Enterprise DLP společnosti Proofpoint jsou spravovány společnostmi Proofpoint. Samotná platforma SaaS je pravidelně aktualizována společnostmi Proofpoint a zahrnuje nové vylepšení funkcí napříč každou z komponent platformy. Aktualizace agentů Endpoint DLP a vydávání oprav se obvykle řídí měsíční kadencí vydávání. Zákazníci mohou spravovat upgrady agentů sami nebo využít profesionální služby společnosti Proofpoint. Komponentu Auto Updater lze použít k automatické instalaci a aktualizaci koncových bodů, přičemž každých 10 minut kontroluje aktualizace a podle potřeby je použit.	x	Zákazník je informovaný o dostupnosti nových aktualizací verzí s informací jestli jsou nutné, doporučené, vhodné nejprve k otestování. Obvykle dochází k nasazení po otestování a schválení
Nabízíte pravidelné systémové audity a optimalizace po dobu podpory zavedeného systému?	ANO	Ano, Proofpoint nabízí pravidelné systémové audity a optimalizace. Zajišťujeme pravidelné kontroly stavu řešení, aby bylo zajištěno, že vše funguje podle plánu, který si může zákazník vyžádat. Kromě toho Proofpoint provozuje několik relací zpětné vazby od zákazníků a nabízí služby, které doplňují potřeby organizace, pokud nemají interní odborné znalosti nezbytné pro spuštění programu. Proofpoint také umožňuje provádět audity, buď sami, nebo prostřednictvím nezávislé třetí strany, s přiměřeným předchozím upozorněním a během běžné pracovní doby.	ANO	Záleží na zakoupené formě podpory: -Rozšířený support s pravidelnými optimalizace a statusy -Konzultační činnosti na vyžádání v doporučeném intervalu alespoň 1x ročně, doporučeno 2x ročně
Jak rychle reagujete na incidenty nebo systémové problémy? Popište prosím jak SLA pro reakci, tak čas pro zahájení řešení stavu incidentu pro dopady (stanovit kategorii dopadů)?	x	Následující smlouva SLA se vztahuje na dostupnost systému platformy Proofpoint E.1 Společnost Proofpoint zaručuje zákazníkovi alespoň 99% dostupnost systému platformy pro přístup k platformě během každého kalendářního měsíce. Dostupnost systému znamená celkovou dobu, po kterou je platforma k dispozici zákazníkovi, s výjimkou okna plánované údržby a nouzové údržby (dále jen „dostupnost systému"). E.2 Náprava: Pokud je dostupnost systému platformy nižší než 99 % a pokud zákazník splnil všechny povinnosti podle smlouvy a této smlouvy SLA, společnost Proofpoint zákazníkovi poskytne kredit na službu za měsíc, ve kterém došlo k nesplnění této dostupnosti systému platformy. došlo. Servisní kredit bude vypočítán podle níže uvedené tabulky. % dostupnosti systému platformy za kalendářní měsíc servisního kreditu	x	ICZ využívá Service desk řešení pro možnost zadávat požadavky včetně priority a sledování SLA dle servisní podpory. Service desk je dostupný 24/7 pro zadání požadavků, alternativně telefonní/e-mailové hlášení. Doba reakce je dle stupně SLA do 1 hodiny, doba zahájení řešení do 8 hodin, vyřešení pokud není potřeba součinnosti výrobce/zadavatele/třetí strany do 24 hodin s výjimkou objednaných konzultačních činností
Jsou hlavní verze systému součástí zakoupené podpory, a pokud nejsou, jaká aktualizace je zajištěna koncem podpory pro vámi dodávané řešení?	ANO	Ano, hlavní aktualizace verzí systému jsou součástí zakoupené podpory pro Proofpoint Enterprise DLP. Platformu SaaS spravuje Proofpoint a pravidelně provádějí aktualizace, které zahrnují nové vylepšení funkcí napříč každou z komponent. Poznámky k verzi jsou uvedeny v online dokumentaci společnosti Proofpoint. Plánovaný konec podpory řešení není v dodaném kontextu specifikován.	ANO	Dostupnost aktualizací je garantovaná výrobcem v rámci zakoupené licence/podpory, u výrobce existuje více úrovní podpory lišící se dle počtu uživatelů a požadovaných časů odezvy. Podpora ICZ je zakoupená na dobu projektu s tím, že dle požadavků zadavatel je možné pokračování v provozování systému nebo pomoc s vypnutím/migrací.
Reportování analytika				
Jaké reporty a analytické nástroje systém poskytuje jako nedílnou součást implementovaného řešení?	x	Platforma Proofpoint Information Protection Platform poskytuje vlastní a podrobné zprávy týkající se incidentů DLP prostřednictvím Unified Alert Manager (UAM). Analytici mohou vytvářet průzkumy, aby prozkoumali data, použili filtry a zobrazili konkrétní informace, které chtějí sledovat. Tyto průzkumy lze použít v řídicích panelech, sdílet je s dalšími analytiky a použít pro opakovatelné hlášení. Výstup průzkumu lze exportovat do souboru CSV, JSON nebo PDF. Platforma navíc podporuje centralizované nasazení, administraci, správu a reporting pro DLP, čímž zajišťuje efektivní správu a reporting systému.	x	Management poskytuje předpřipravené reporty dle volitelných parametrů (TOP, source, destiantion, policies, rules, trends, actions, ..) a jejich vzájemné kombinace. Reporty je možné plně custimozovat, nebo vytvářet vlastní včetně možnosti naplánovat automatické posílání reportu ve zvoleném čase na zvolenou skupiny příjemců.
Existují nějaké možnosti prémiových přehledů a jak se tyto služby liší od základních přehledů?		Enterprise DLP společnosti Proofpoint poskytuje robustní možnosti vytváření sestav prostřednictvím rozhraní Reporting and Dashboard, které zahrnuje základní i pokročilé možnosti. Základní sestavy pokrývají různé činnosti, jako je sdílení v cloudu, exfiltrace dat a podezřelé chování, a lze je přizpůsobit až 7 různými atributy pro podrobné filtrování a třídění. Prémiové možnosti sestav zahrnují možnost vytvářet víceúrovňové souhrnné sestavy, vytvářet vlastní průzkumy a integrovat se s externími systémy sestav, jako jsou PowerBI a Grafana. Tyto prémiové služby nabízejí podrobnější ovládání, pokročilé filtrování a možnost exportovat data v různých formátech (CSV, JSON, PDF) pro další analýzu a integraci s dalšími nástroji.	NE	Všechny reporty jsou dostupné v základní licenci včetně možností použít rozšířenou analytickou funkcionalitu.
Existují možnosti integrace s reportovacími systémy, jako je PowerBI, Grafana nebo podobné?	ANO	Ano, řešení Enterprise DLP společnosti Proofpoint podporuje integraci s externími systémy hlášení. Platforma poskytuje různé možnosti exportu, jako jsou soubory CSV, JSON a PDF, které lze využít k integraci s reportovacími systémy, jako je PowerBI, Grafana nebo podobné nástroje. Rozsáhlá veřejná rozhraní API platformy a zásady oznamování založené na webhoocích navíc usnadňují využívání dat DLP v externích nástrojích, což usnadňuje nastavení a vlastní správu těchto integrací.	ANO	Forcepoint DLP poskytuje popis pro integraci na SQL DB, API volání, Syslog události, SIEM

Umožňuje systém přizpůsobení reportů našim potřebám a kolik času průměrně zabere přizpůsobení reportu (prosím odhadněte na základě vašich zkušeností s podobnými projekty)?	x	Enterprise DLP společnosti Proofpoint umožňuje přizpůsobení sestav na základě požadavků zákazníků. Vlastní sestavy lze vytvářet pomocí robustního rozhraní Reporting and Dashboard platformy, které podporuje možnosti filtrování a řazení až se 7 různými atributy. Čas potřebný k přizpůsobení sestavy se může lišit v závislosti na složitosti a konkrétních požadavcích, ale na základě našich zkušeností s podobnými projekty obvykle trvá dokončení procesu přizpůsobení několik hodin až několik dní.	ANO	Viz popis v dotazu 65 reporty jsou plně customizovatelné. Obvykle se vytvářejí přehledy pro IT, Audit Log činností, přehledy pro SOC/Security na bázi 1x týdně a 1x měsíčně. Čas potřebný pro nastavení a otestování nepřekračuje 30 minut
Jak jsou údaje zpracovávány a nemocny pro zdravotní problémy a auditu (například pro potřeby GDPR, NIS2/ZoKB/ISO27001)?	x	Pro účely shody a auditu jsou data zpracovávána a léta prostřednictvím komplexního programu zabezpečení informací v souladu s požadavky NIST 800-53 a ISO 27001. Společnost Proofpoint zavedla bezpečnostní kontroly týkající se fyzického a logického přístupu, fyzické a personální bezpečnosti, řízení změn, softwaru Školení o vývoji, šifrování, nepřetržitém monitorování, zabezpečení, ochraně soukromí a hodnocení třetích stran. Tyto kontroly jsou každoročně auditovány jako součást našeho auditu SOC 2 Typ II pro zásady důvěryhodných služeb dostupnosti, důvěrnosti a zabezpečení. Kromě toho je Proofpoint certifikován podle rámce EU-US Data Privacy Framework a dodržuje zásady DPF. Společnost Proofpoint zdokumentovala svůj soulad s GDPR prostřednictvím smlouvy o zpracování dat (DPA) a standardních smluvních závazků specifických pro daný produkt.	x	Produkt umí kontrolovat činnosti s citlivými daty dle GDPR atd. s možností upozorňovat/chránit jejich porušení
Je možné nastavit upozornění a upozornění na základě konkrétních událostí?	ANO	Ano, v Proofpoint Enterprise DLP je možné nastavit výstrahy a upozornění na základě konkrétních událostí. Řešení DLP společnosti Proofpoint může posílat upozornění operačnímu týmu prostřednictvím různých metod, včetně e-mailu a webhooků. Předdefinované zásady webhooku zahrnují Splunk, Microsoft Teams a Slack, s vlastními nastaveními webhooku. Upozornění v systémech Proofpoint lze nakonfigurovat tak, aby spouštěly e-maily za určitých podmínek události. Platforma Proofpoint navíc umožňuje vytvářet zásady, které mohou odeslat oznámení o webhooku a/nebo e-mailové upozornění na spouštění zásad nebo naplánovanou zprávu, která ukáže, jaké zásady se spouštějí v daném časovém období. Oznámení lze také zasílat konkrétním uživatelům nebo správcům, když je překročena rychlost přijímání složek v karanténě nebo když je spuštěno narušení DLP nebo hrozby. Kromě toho může Endpoint DLP společnosti Proofpoint zobrazovat uživatelům v reálném čase upozornění na porušení zásad a řešení CASB e-mailová upozornění pro správce i koncové uživatele.	ANO	Řešení umožňuje nastavit uživatelských/administrátorských notifikací dle požadavků
Školení a dokumentace				
Poskytujete v rámci nabízeného řešení školení pro systémové administrátory a uživatele?	ANO	Ano, Proofpoint poskytuje několik školicích speciálně navržených pro administrátory, programy, aby měli potřebné dovednosti pro správu a odstraňování problémů se systémem Data Loss Prevention (DLP). Tyto školicí programy zahrnují kurzy o různých aspektech DLP, jako je navigace, konfigurace, pracovní postup, detektory dat a reakce na incidenty. Proofpoint navíc nabízí online průvodce, dokumentaci a školení uživatelů o konkrétních řešeních ze všech řešení DLP. Technická školení na webu mohou také poskytovat techniku společnosti Proofpoint jako součást placené služby pro hlubší školení.	ANO	Školení se dělí na školení pro: A) Administrátora systému B)SOC/bezpečnostní experty a analytiky C) Školení uživatelů se obvykle neprovádí – dostávají návod, že můžou nastat nové situace a jak v nich postupovat
Je k dispozici podrobná dokumentace a uživatelské příručky? V jakém jazyce jsou poskytovány?	ANO	Ano, k dispozici je podrobná dokumentace a uživatelské příručky pro Proofpoint Enterprise DLP. Tým podpory společnosti Proofpoint může poskytovat podpůrnou dokumentaci pro příslušné licencované produkty. Podporujeme více jazyků včetně angličtiny, němčiny, francouzštiny atd.	ANO	Kompletní dokumentace výrobce je volně ke stažení v angličtině. V rámci projektu ICZ standardně dodává následující dokumentaci v češtině: Administrátorská příručka Popis implementace/prostředí Popis aktuálních politik/akcí/výjimek UAT testy (návrh, popis, vyhodnocení) Návod pro uživatele s adekvátním popisem (cílem není upozorňovat na veškeré technické a bezpečnostní aspekty implementovaného řešení)
Nabízíte v rámci dodaného řešení e-learningové platformy nebo dílenská školení?	ANO	Ano, Proofpoint poskytuje několik školicích speciálně navržených pro administrátory, programy, aby měli potřebné dovednosti pro správu a odstraňování problémů se systémem Data Loss Prevention (DLP). Tyto školicí programy zahrnují kurzy o různých aspektech DLP, jako je navigace, konfigurace, pracovní postup, detektory dat a reakce na incidenty. Proofpoint navíc nabízí online průvodce, dokumentaci a školení uživatelů o konkrétních řešeních ze všech řešení DLP. Technická školení na webu mohou také poskytovat techniku společnosti Proofpoint jako součást placené služby pro hlubší školení.	ČÁSTEČNĚ	Kdyby bylo požadováno lze nabídnout, ale u tohoto produktu a rozsahu implementace není potřebné.

Jsou součástí školení osvědčené postupy pro provoz systému DLP?	ANO		ANO	Implementační tým má dlouhodobé zkušenosti a díky podpoře u velkého počtu zákazníků dochází k přenosu aktuálních změn na všechny.
Jak bude v rámci projektu řešena adopce dané technologie?	x	Přijetí technologie Enterprise Data Loss Prevention (DLP) společnosti Proofpoint v rámci podnikového projektu DLP bude řešeno prostřednictvím komplexního přístupu, který zahrnuje následující komponenty: 1.Integrace a nasazení: Enterprise DLP společnosti Proofpoint pokrývá kanály Endpoint, Cloud a Email s ovládacími prvky DLP. Může být integrován do stávajících systémů a nasazen napříč různými kanály, aby byla zajištěna komplexní ochrana dat. 2.Školicí programy: Proofpoint nabízí několik školicích speciálně navržených pro administrátory, programy abyi, že budou mít potřebné dovednosti pro správu a odstraňování problémů se systémem DLP. Tyto programy pokrývají základní a pokročilé znalosti, včetně navigace, konfigurace, pracovního postupu, detektorů dat a reakce na incidenty. 3.Dokumentace a uživatelské příručky: Pro podporu implementace a průběžné správy systému DLP je k dispozici podrobná dokumentace a uživatelské příručky. Tým společnosti Proofpoint může poskytovat zákaznickou podporu nezbytnou dokumentaci k jejím licencovaným produktům. 4.Nejlepší postupy: Školicí programy zahrnují osvědčené postupy pro provoz systému DLP, které zajišťují, že správci jsou dobře vybaveni pro efektivní správu a optimalizaci systému. 5.Podpora a služby: Proofpoint poskytuje online průvodce, dokumentace a školení uživatelů o konkrétních řešeních ze všech řešení DLP. Technická školení na webu mohou také poskytovat techniku společnosti Proofpoint jako součást placené služby pro hlubší školení.	x	Otestování kompatibility v rámci POC, plán integrace Proxy – DLP – odladění konfigurace a bezpečnostních pravidel.
Bezpečnost a dodržování předpisů				
Jak váš systém podporuje soulad s příslušnou legislativou a standardy (např. GDPR, ISO27001 atd.) a zákony NIS2/ZoKB?	x	Proofpoint Enterprise DLP podporuje soulad s příslušnými právními předpisy a standardy, včetně GDPR, poskytnutím smlouvy o zpracování dat (DPA), která dokumentuje náš soulad s GDPR. DPA je k dispozici zde:https://www.proofpoint.com/legal/trust/dpa. Kromě toho je řešení Enterprise DLP společnosti Proofpoint plně spravováno a podporováno společnostmi Proofpoint se specifickými funkcemi platformy a infrastruktury uvedené ve zprávě SOC 2 Report, která je v souladu s normami ISO27001.	x	Plně podporuje - DLP řešení je kontrolní/restriktivní nástroj, který umožňuje kontrolovat/vymáhat dodržování pravidel pro práci s citlivými daty na základě předdefinovaných politik/definovaných politik, kontrola uložení dat uložených na discích, úložištích atd.
Jak je zabezpečené zabezpečení samotného DLP systému proti útokům?	x	Zabezpečení systému Proofpoint Enterprise DLP je zajištěno několika opatřeními. Platforma je kompletní nabídka SaaS, která zahrnuje zabezpečenou infrastrukturu, operace na světové úrovni a prvotřídní podporu. Všechna základní úložiště dat jsou distribuována, podporují nativní replikaci a mají automatické převzetí služeb při selhání. Běhové služby jsou nasazeny s více instancemi a schopnostmi samoopravy/škálování. Webové koncové tělo jsou vystaveny prostřednictvím služeb Amazon ELB, která poskytuje záruky vysoké dostupnosti. Systém se spoléhá na asynchronní architekturu předávání zpráv, která omezuje účinky lokálních selhání běhu a poskytuje odolnost a kontinuitu. Všechna data pro stávající systém jsou aktuálně archivována v geograficky replikovaném segmentu S3, který poskytuje možnosti obnovení v určitém okamžiku. Důležité databáze jsou denně zálohovány, přičemž zálohy jsou uloženy v samostatném georeplikovaném kbelíku S3. V případě katastrofy je veškerá infrastruktura definována jako kód a může být spuštěna v novém datovém centru AWS prostřednictvím stávající automatizace.	x	Hardening podkladového prostředí a využívaného programového vybavení s možností využít bezpečné ověření pro přístup, audit všech činností atd. Veškerá zpracovávaná data jsou šifrována pomocí AES256.
Jak jsou data v systému zabezpečena proti neoprávněnému přístupu?	x	Kontrola zdravotního stavu je bezplatná a vystavujeme pouze dodatečnou fakturu, pokud uživatelé mají více než původní smlouvu	x	Veškeré činnosti jsou monitorované na úrovni managemntu řešení, lokálně uložené forézní data jsou šifrována, ostatní je řešeno na úrovni dvoufaktorového přístupových oprávnění, jednotlivé role je možné plně customizovat.
Má systém certifikace od renomovaných bezpečnostních organizací, případně od kterých?	x	Řešení Enterprise DLP společnosti Proofpoint má certifikace od renomovaných bezpečnostních organizací. Další podrobnosti naleznete v níže uvedených citacích. Certifikace produktu Proofpoint:https://www.proofpoint.com/us/legal/trust/product-certifications	ANO	ISO/IEC 27001: Information security management. -SOC 2 Type II: Data security and confidentiality. -Common Criteria Certification: International security standard. -FIPS 140-2: Cryptographic module security.
Výkon a škálovatelnost				

Jaký je vliv systému na latenci a propustnost sítě při provádění kontroly?	x	Agent Endpoint DLP/ITM společnosti Proofpoint má minimální dopad na výkon koncového bodu. Rozsáhlé testování zjistilo, že režie Endpoint Agent na koncovém bodu má minimální dopad na uživatele, s více než 2-4% využití CPU a 75 MB RAM využitých v průměru při monitorování. Při aktivované kontrole obsahu lze pozorovat mírné zvýšení. Řešení efektivně spravuje a zpracovává data při různé zátěži, aniž by došlo ke snížení výkonu, včetně faktorů, jako je schopnost zvládat rostoucí objemy dat, podpora pro více uživatelů a zařízení a flexibilita přizpůsobení měnícím se požadavkům. Výkonnostní aspekty řešení DLP jsou plně spravovány společností Proofpoint, což zajišťuje, že systém dokáže účinně chránit citlivá data a zároveň vyhovět budoucímu růstu a zvyšujícím se požadavkům.	x	Na tuto otázku se nedá jednoznačně odpovědět, závisí na počtu prováděných DLP kontrol. Výchozí nastavení obsahuje limity pro propuštění komunikace při překročení časového limitu.
Jak systém zvládá vysoký objem datového provozu a kontrolu velkých souborů (soubory nad 100 MB)?	x	Řešení Enterprise DLP společnosti Proofpoint efektivně spravuje a zpracovává data při různé zátěži, aniž by došlo ke snížení výkonu. Platforma je navržena tak, aby zvládala rostoucí objemy dat, podporovala více uživatelů a zařízení a přizpůsobovala se měnícím se požadavkům. Výkonnostní aspekty řešení DLP jsou plně spravovány společností Proofpoint, což zajišťuje, že systém dokáže účinně chránit citlivá data a zároveň se přizpůsobí budoucímu růstu a zvyšujícím se požadavkům. Pro zpracování velkých souborů umožňuje architektura a možnosti škálovatelnosti řešení spravovat velké objemy datového provozu, včetně velkých souborů o velikosti přes 100 MB, bez snížení výkonu.	x	Lze konfigurovat dle jednotlivých kanálů pro ICAP platí: -ICAP Configuration Changes for Large File Support (up to 400MB)
Je možné škálovat systém horizontálně nebo vertikálně, když je potřeba splnit požadavky a požadavek na provozschopnosti systému?	ANO	Ano, Proofpoint Enterprise DLP lze škálovat jak horizontálně, tak vertikálně, aby vyhověl rostoucím obytným prostorám a rychlému provozu systému. Prostředky DLP se vertikálně používají navyšováním zdrojů cloudových mikroslužeb v rámci jednoho systému nebo zákaznického tenanta v rámci aplikace IPCS AWS. Platforma se navíc může horizontálně škálovat pro monitorování stovek tisíc agentů koncových bodů a napříč mnoha schválenými aplikacemi SaaS.	ANO	Navýšení kapacity systému se provádí zvýšením zdrojů v případě virtualizovaných komponent nebo navýšení počtu applicnací/protectrů pro vyhodnocování komunikace.
Jaké jsou nejlepší postupy pro optimalizaci výkonu systému?	x	Proofpoint Enterprise DLP optimalizuje výkon systému pomocí následujících osvědčených postupů: 1.Škálovatelnost: Řešení DLP efektivně spravuje a zpracovává data při různé zátěži bez snížení výkonu. Vertikálně se vyskytuje navyšování zdrojů pomocí cloudových mikroslužeb v rámci jednoho systému nebo zákaznického tenanta v rámci aplikace IPCS AWS. 2.Vyrovnávání zátěže: Řešení spravuje transparentní vyrovnávání zátěže, aby zvládlo rostoucí objemy dat, podporovalo více uživatelů a zařízení přizpůsobovalo měnícím se podmínkám. 3.Rychlé nasazení: Jako cloudová platforma se Proofpoint Enterprise DLP nasazuje rychle a poskytuje použitelné výsledky okamžitě nebo po krátkém základním období. Toto rychlé nasazení pomáhá udržovat optimální výkon. 4.Pravidelné aktualizace a upgrade: Proofpoint spravuje pravidelné aktualizace a upgrady platformy SaaS, zahrnuje nové vylepšení funkcí a zajišťuje, že systém zůstane optimalizovaný. Aktualizace agentů Endpoint DLP sledují měsíční kadenci vydávání. 5.Systémové audity a zdravotní kontroly: Provádí se pravidelné systémové audity a zdravotní kontroly, aby bylo zajištěno, že vše funguje podle plánu. Zákazníci mohou vyžadovat pravidelné kontroly stavu řešení a provádět audity pro udržení výkonu systému. 6.Jednotná platforma: Jednotná konzole pro e-mail, cloud a DLP koncových bodů zjednodušuje třídění výstrah a reakcí na incidenty, které zkracuje čas a zdroje potřebné ke správě systému.	x	Vyloučení bezpečného provozu z analýzy, vyloučení důvěryhodných zdrojů/cílů z analýzy, optimalizace politik na počet false positive atd.
Zkušenosti a reference dodavatele				
Jaké jsou vaše předchozí zkušenosti s implementací DLP systémů v podobných prostředích?	x	V regionu EMEA máme řadu zákazníků	x	Network DLP byl implementován u zákazníků s 500 – 7.500 uživateli, web security u zákazníků s 200 – 5.000 uživateli, Endpoint DLP 100 – 25.000 uživatelů v prostředí státní správy i jednotlivých technologických/finančních/telekom unikačních oborů
Můžete poskytnout reference od jiných klientů (uveďte velikost organizace a segmentu, ve které organizace působí)?	x	Reference na vyžádání	ANO	Reference budou poskytnuty při představení řešení/dodání nabídky.

Jak dlouho působí na trhu řešení DLP?	x	Společnost Proofpoint poskytuje funkce DLP již více než 15 let. V září 2020 společnost Proofpoint integrovala tyto kanály DLP do uceleného podnikového řešení.	x	15 let certifikovaný partner pro technologie: Broadcom (dříve Symantec), Trellix (dříve McAfee), Forcepoint (dříve Websense), Safetica
Jaké jsou vaše konkurenční výhody oproti jiným dodavatelům?	x	Mezi konkurenční výhody společnosti Proofpoint pro řešení prevence ztráty dat (DLP) patří: 1.Komplexní pokrytí: Proofpoint Enterprise DLP chrání data přes e-mail, cloud, web a koncové kanály a řeší celé spektrum scénářů ztráty dat zahrnujících neopatrné, kompromitované a zlomyslné uživatele. 2.Jednotné řízení: Řešení nabízí jednotnou konzolu pro třídění a správu výstrah napříč všemi kanály, což zlepšuje provozní efektivitu. 3.Škálovatelnost: Řešení DLP společnosti Proofpoint je postaveno na škálovatelné cloudové nativní platformě, která zvládne rostoucí objemy dat a podporuje stovky tisíc uživatelů na jednoho tenanta. 4.Pokročilé ovládací prvky vynucení: Řešení poskytuje aktivní vynucení kontroly odchozího obsahu s přizpůsobitelnými zásadami a automatickými kontrolami vynucení, jako je karanténa, šifrování a přesměrování. 5.Integrace AI/ML: Společnost Proofpoint významně investovala do technologií AI/ML, aby se zlepšila detekci hrozeb a identifikovala včasný záměr exfiltrace dat, čímž poskytuje pokročilou ochranu proti hrozbám zevnitř. 6.Osvědčená zkušenost: Společnost Proofpoint má rozsáhlé zkušenosti s implementací systémů DLP v různých prostředích, což zajišťuje spolehlivost a škálovatelnost. 7.Neustálá inovace: Společnost Proofpoint soustavně investuje do výzkumu a vývoje, aby si udržela očekávání před potřebami trhu a přicházela s poptávkou inovativní řešení.	x	Realizační tým je tvořen interními zaměstnanci, reference a zkušenosti v regionu CZ/SK pro zakázky v rozsahu stovek až desítek tisíc implementaci
Testování a ověřování				
Nabízíte možnost provedení PoC (Proof of Concept) před konečným rozhodnutím a za jakých podmínek?	ANO	Ano, Proofpoint nabízí možnost provedení Proof of Concept (PoC) pro podnikové DLP. Podmínky pro PoC zahrnují vyhodnocení schopností řešení, jako je integrace se stávajícími systémy, informace o hrozbách a celkový výkon. PoC je navržen tak, aby demonstrovalo efektivitu řešení DLP společnosti Proofpoint v reálném prostředí a poskytovatelů, že plní specifické potřeby a požadavky podniku před přijetím konečného rozhodnutí.	ANO	Dle požadovaného rozsahu se jedná o neplacené, nebo placené POC
Jak můžeme ověřit účinnost systému v našem prostředí?	x	Zákazník si může ověřit efektivitu podnikového DLP společnosti Proofpoint ve svém prostředí provedení Proof of Concept (PoC). Proofpoint nabízí možnost PoC pro vyhodnocení schopností řešení, jako je integrace se stávajícími systémy, informace o hrozbách a celkový výkon. PoC je navržen tak, aby demonstrovalo efektivitu řešení DLP společnosti Proofpoint v reálném prostředí a poskytovatelů, že plní specifické potřeby a požadavky podniku před přijetím konečného rozhodnutí.	x	Pilotním nasazení, odladěním politik, pravidelným vyhodnocením a laděním po dobu například 6ti týdnů, závěrečným vyhodnocením počtu událostí, false positive, dopadů jednotlivých událostí, nezabezpečených kanálů atd.
Jak se řeší bezpečnostní testy a testování penetračního systému?	x	Proofpoint nemá neprodukční prostředí, ve kterém lze provádět penetrační testy. Kromě pravidelných týdenních interních a měsíčních externích skenů zranitelnosti na našich serverech provádíme každoroční penetrační testování služeb Proofpoint třetí stranou. Výsledky penetračních testů neposkytujeme jako součást žádosti o nabídku. Místo toho může být na požádání poskytnuto shrnutí.	x	Standardně se provádí UAT testy s cílem ověřit očekávané funkce a vlastnosti na všech kanálech, typech dat, typech citlivých dat, úrovních pro detekce, reakcí systému atd.
Povolit systém testování nových zásad a pravidel v sandboxu?		Podnikové DLP společnosti Proofpoint nepodporuje testování nových zásad a pravidel v sandboxu. Doporučujeme však nejprve nastavit pravidla pro povolení a upozornění, abyste mohli otestovat před povolením nápravy. Vzory DLP vyvinuté v konzole lze navíc otestovat nahráním souboru do systému, aby se porovnaly s detektorem před jeho aktivací.	ČÁSTEČNĚ	Lze vytvořit samostatné prostředí pro testování, nebo testovat jen pro vybranou skupinu uživatel/systémů.
Právní aspekty a podmínky				
Jaké jsou vaše standardní smluvní podmínky pro dodávku a implementaci systému?	x	Standardní smluvní podmínky společnosti Proofpoint pro dodávku systému a implementaci podnikového DLP lze nalézt ve smlouvě o předplatném mezi klientem a společnostmi Proofpoint. Smluvní podmínky jsou k dispozici zde:https://www.proofpoint.com/us/legal/trust/contracts	x	Řeší Všeobecné obchodní podmínky, přikládáme v příloze.

Jak se řeší odpovědnost za případné selhání systému?	x	Platforma Enterprise DLP společnosti Proofpoint implementuje odolnost proti chybám prostřednictvím různých mechanismů, aby byl zajištěn nepřetržitý provoz během selhání systému. Platforma je hostována v regionech AWS v USA, Německu, Japonsku a Austrálii s distribuovanými datovými úložišti, která podporují nativní replikace a automatické převzetí služeb při selhání. Všechny runtime služby jsou nasazeny s více instancemi a schopnostmi samoopravy. Webové koncové tělo jsou vystaveny prostřednictvím služeb Amazon ELB, aby byla zajištěna vysoká dostupnost. Interně se systém spoléhá na asynchronní architekturu předávání zpráv, aby se omezil dopad lokálních selhání běhu a zajišťuje se odolnost a kontinuita. Data procházející platformou jsou průběžně archivována v geograficky replikovaných segmentech S3, což umožňuje obnovení v určitém okamžiku. Důležité databáze jsou denně zálohovány v samostatných geografických replikovaných segmentech S3, což umožňuje téměř nulové cíle bodů obnovy (RPO). V případě havárie, která si vyžádá přechod do jiného datového centra, je veškerá infrastruktura definována jako kód a může být spuštěna v novém datovém centru AWS prostřednictvím stávající automatizace. Společnost Proofpoint navíc každoročně provádí testy služeb převzetí při selhání datových center, aby ověřila účinnost svých mechanismů převzetí služeb při selhání a nepřetržitého provozu. Řešení Endpoint DLP společnosti Proofpoint je plně spravováno společností Proofpoint, včetně všech možností zálohování a obnovy. Společnost Proofpoint nakládání s důvěrnými informacemi poskytuje kopie svých postupů pro a řízení obnovy po havárii a kontinuitě podnikání, s nimiž bude podle těchto zásad platit jako s těmito informacemi. Pokud Proofpoint zaznamená přerušení podnikání v jedné ze svých služeb, Proofpoint zavede svůj plán obnovy po havárii a zpřístupnění našim zákazníkům situační aktualizační zprávy s vhodnou frekvencí stanovenou Proofpointem, včetně souhrnného popisu události, dopadu na naše zákazníky, a odhad, kdy se služby vrátí do normálního provozu.	x	Odpovědnost za případné selhání systému je řešena s ohledem na rozsah dodávky, charakter poskytovaných služeb, požadavky vyplývající ze zákona o kybernetické bezpečnosti a GDPR a jiná specifika dané systému. Nelze obecně paušalizovat, ale využívají se klasické smluvní instituty jako stanovení SLA, smluvní pokuty za porušení SLA a obecná odpovědnost za škodu.
Jaké jsou podmínky pro ukončení smlouvy a případné kompenzace související s omezením funkčnosti našeho provozu?	x	ustanovení o ukončení jsou v Zákaznické smlouvě/MSA v části 7 7. Doba platnosti, ukončení a vypršení platnosti 7.1. Pokud není v příslušných Produktových podmínkách nebo Objednávce stanoveno jinak, Počáteční období platné pro každou Objednávku (včetně následných objednávek) začíná později z: (i) data, kdy společnost Proofpoint odešle výrobní zařízení zákazníkovi, (ii) datum, kdy společnost Proofpoint zpracuje příslušnou objednávku na produkt Proofpoint hodnocený zákazníkem, nebo (iii) pro všechny ostatní objednávky produktu Proofpoint, datum, kdy společnost Proofpoint odešle zákazníkovi e-mail s uvedením, že společnost Proofpoint Produkty jsou k dispozici k použití (v rozsahu, v jakém se každé z výše uvedených vztahuje na zákaznickou zakázku). Po vypršení Počátečního období a jakéhokoli Období prodloužení v rámci každé Nákupní objednávky se Období předplatného vztahující se na takovou Nákupní objednávku automaticky obnoví pro následující Podmínky prodloužení, pokud se strany nedohodnou jinak nebo pokud jedna ze stran neoznámí druhé straně neprodloužení. nejméně devadesát (90) dnů před koncem příslušného období předplatného. 7.2. Kterákoli strana může ukončit smlouvu nebo jakoukoli nákupní objednávku (i) okamžitě po písemném oznámení, pokud se druhá strana dopustí neodstranitelného závažného porušení; nebo (ii) pokud druhá strana nenapraví jakékoli napravitelné závažné porušení do třiceti (30) dnů od písemného oznámení o takovém porušení, pokud k takovému porušení nedošlo z důvodu nezaplacení, a poté do pěti (5) dnů od takového upozornění. 7.3. Kterákoli strana může zákaznickou smlouvu okamžitě ukončit písemným oznámením, pokud není v platnosti žádná Objednávka. 7.4. Při ukončení nebo vypršení platnosti smlouvy budou všechny licence na software, přístup ke službám, přístup ke spravovaným službám a/nebo plnění profesionálních služeb udělené na základě smlouvy automaticky ukončeny s okamžitou platností. V případě ukončení nebo vypršení Smlouvy zůstávají v platnosti ustanovení Smlouvy, která svou povahou přesahují dobu platnosti nebo ukončení Smlouvy, včetně, ale nikoli výhradně, části 2 („Odpovědnosti zákazníka"); oddíl 3 („Důvěrnost"); Oddíl 5 („Finanční podmínky"); Oddíl 7 („Doba platnosti, ukončení a vypršení platnosti"); oddíl 9 („Práva, licence a oprávnění k duševnímu vlastnictví"); § 10 („Omezení odpovědnosti"); oddíl 11 („Obecné"); a oddíl 12 („Definice"); a jakákoli nabytá práva na platbu zůstávají v platnosti i po ukončení nebo vypršení platnosti, dokud nebudou splněny.	x	Při stanovení podmínek ukončení smlouvy záleží na tom, zda je smlouva uzavřena na dobu určitou či neurčitou. V případě doby určité jsou možnosti předčasného ukončení smlouvy omezené, pouze s ohledem na podstatné porušení smlouvy. V případě smluv na dobu neurčitou je standardně stanovena možnost výpovědi s výpovědní dobou, jejíž délka se určuje dle charakteru poskytovaných služeb, klasicky v rozmezí 2 měsíců až klidně 1 roku. Kromě výše uvedeného využíváme klasických smluvních ustanovení vztahujících se k podstatnému či nepodstatnému porušení smlouvy a s tím související možností smlouvu ukončit. Pro vyloučení následných sporů preferujeme ustanovení ve smlouvě, které uvádí, že v případě předčasného ukončení smlouvy se nevrací již dodaná plnění. S ohledem na náhrady související s omezením provozu se odkazujeme na náhradu škody.
Další komentáře k předmětu PTK	x	x	x	Pro úspěšnou implementaci Network DLP v komplexním prostředí je nejdůležitější otestování vhodných technologií v reálném prostředí a důkladné vyhodnocení všech nároků a nákladů na integraci i v rámci snadnosti práce s produktem a provádění pravidelných optimalizací a vyhodnocení.

Do 2. kola PTK je celkem přihlášeno 14 registrovaných účastníků, z toho:

- **4 účastníci reagovali na PTK:**
  - **1 účastník odpověděl plnohodnotně (agentless DLP),**
  - **3 účastníci odpověděli plnohodnotně, nikoliv však k požadovanému řešení (agent-based DLP)**
- **10 účastníků nereagovalo vůbec**

Příloha č. 11 Výzvy

Předběžná tržní konzultace - Zavedení komplexního síťového řešení prevence úniku dat (DLP) pro non-Microsoft systémy v prostředí Správy železnic

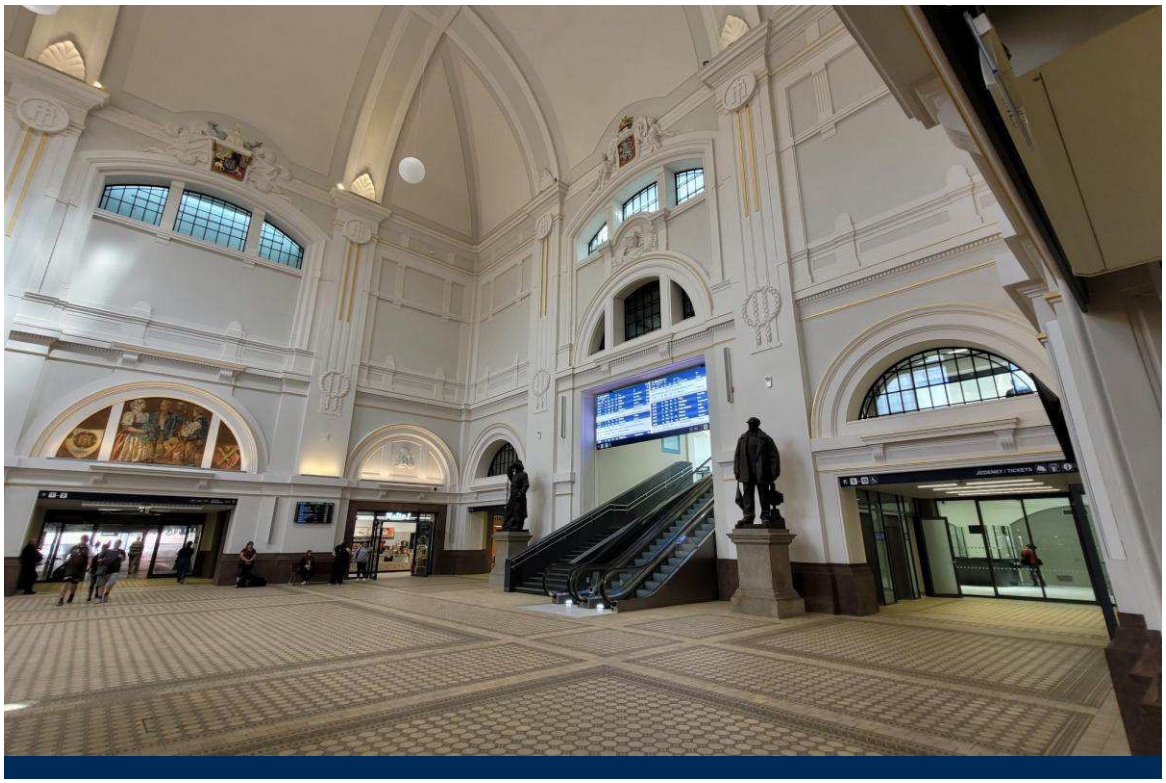
Obsah / data

	Odpovědi účastníků 2. kola PTK							
Dotazy na účastníky PTK	**Účastník 1 (odpovědi nejsou plně relevantní s ohledem na navrhované Agent-based řešení DLP, které není požadováno)**		**Účastník 2**		**Účastník 3 (odpovědi nejsou plně relevantní s ohledem na navrhované Agent-based řešení DLP, které není požadováno)**		**Účastník 4 (odpovědi týkající se cen licencí nejsou plně relevantní s ohledem na navrhované Agent-based řešení DLP, které není požadováno (ř. 10), ostatní odpovědi jsou považovány za relevantní)**	
	ANO/NE/Částečně	**Komentář**	**ANO/NE/Částečně**	**Komentář**	**ANO/NE/Částečně**	**Komentář**	**ANO/NE/Částečně**	**Komentář**
Jaký je Váš časový odhad délky trvání této etapy (v měsících)?	x	6 měsíců	x	Řádově se jedná a 14 dní na všechny přípravné práce pro vytvoření prostředí na straně SŽ a následnou instalaci řešení se základní konfigurací -Odladění nastavení 14 dní -Pilotní provoz 5 týdnů -Překlopení do produkčního provozu 4 týdny s pořadím: -kontrola technického segmentu, -následně celý webový provoz směrem z organizace -Implementace je tak řádově na 2–3 měsíce s kompletním odladěním	x	6 měsíců	x	Bude dodán po upřesnění architektury a záměru Zadavatele.
Doplňující komentář:	x	x	x	Doba trvání implementace závisí na: -Poskytnutých součinnostech -Požadované doby testování a pilotního provozu	x	Nutná součinnost Zákazníka	x	x
Jaký je Váš odhad ceny této etapy (v Kč bez DPH)? Etapa obsahuje: · Návrh harmonogramu implementace vybraného řešení DLP. · Detailní analýza pro nasazení vybraného řešení DLP. · Implementace a konfigurace vybraného řešení DLP (pravidla, politiky, procesy správy incidentů, role, proškolení správců a dohledových zaměstnanců (SOC)). · Příprava základní knihovny detekčních a reakčních pravidel. · Provedení adopční kampaně. · Implementace a konfigurace vybraného systému DLP. Cenu uveďte celkem za: · Licence pro 17 000 uživatelů (předpokládáme komplementární a neduplicitní funkční pokrytí vůči MS Purview DLP) nebo za průtok 5Gb/s. · Služby podpory výrobce (5 let). · Implementace (+ školení). Rozklad ceny včetně správy řešení na 5 let pak uveďte v doplňujícím komentáři.	x	119,891,800.00 Kč bez DPH	x	V rámci DLP projektů se obvykle naceňuje pouze kompletní pracnost/cena za implementaci řešení, rozpad na jednotlivé fáze není relevantní z důvodu vysokénepřesnostizpůsobenéobvykle neočekávanými okolnostmi a technologickými neznámými v jednotlivých fázích. Garantujeme cenu za nasazení v odsouhlaseném rozsahu prací. Cena za implementaci a podporu: Implementace 750.000,- Kč bez DPH Podpora na 5 let – 840.000,- Kč bez DPH Cena licence Forcepoint Network DLP (IP protection) pro: 17.000 uživatelů na 5 let – subscription licence s podporou od výrobce 41.860.430, - Kč bez DPH Celkové náklady na pořízení, nasazení a podporu řešení (TOC náklady) představují: 43.450.430,- Kč bez DPH pro 17.0000 uživatelů na 5 let včetně implementace, školení a podpory řešení. Poznámka: Jedná se o projektové ceny vypracované na základě upřesnění zadání ze strany SŽ	x	10.000.000,- Kč bez DPH Celková cena: 117.320.000,- Kč bez DPH	x	• Implementace a následné kroky: Bude dodáno po upřesnění architektury a záměru Zadavatele. • Licence (Forcepoint DLP Endpoint) 3.400.000,- EUR bez DPH/5 let • Podpora výrobce (Forcepoint DLP Endpoint) 283.000,- EUR bez DPH/5 let
Doplňující komentář:	x	Cena licencí na 5 let 116,705,000.00 Kč bez DPH Cena Gold support na 5 let 2,107,400.00 Kč bez DPH Cena Implementace 1,179,400.00 Kč bez DPH	x	Rozpad ceny: -Implementace 750.000,- Kč bez DPH -Podpora na 1. rok – 168.000,- Kč bez DPH -Podpora na 2. rok – 168.000,- Kč bez DPH -Podpora na 3. rok – 168.000,- Kč bez DPH Podpora na 4. rok – 168.000,- Kč bez DPH -Podpora na 5. rok – 168.000,- Kč bez DPH -Pořízení licence Forcepoint Network DLP (IP protection) na 5 let včetně podpory výrobce 41.860.430,-Kč bez DPH Poznámka: Do ceny řešení nejsou započítané náklady na podkladovýOS(1xWindowsServer 2016/2019/2022) a SQL Server 2016 a novější kde se předpokládá využití multi-licencí SŽ.	x	Licence: 90.000.000 Kč bez DPH Služby podpory výrobce: 23.000.000 Kč bez DPH Realizace, včetně školení: 4.320.000 Kč bez DPH	x	Správa řešení NENÍ součástí výše uvedené ceny za licence a podpory výrobce. Bude naceněna po vyjasnění architektury, požadovaného rozsahu prací a SLA.
Předpokládáte s ohledem na vybrané systémy uvedené v dokumentu „PTK – informace k systémům SŽ" a požadavky na prevenci úniku citlivých dat nasazení dalších technologií kromě DLP řešení? V případě, že ano, uveďte, které a jejich cenovou indikaci, licenční model.	x	NE	x	NE	x	ANO / NE / ČÁSTEČNĚ	x	ANO / NE / ČÁSTEČNĚ Řešení On prem vyžaduje licenci MS SQL pro databázi protokolů a licenci Windows Server pro server pro správu a servery OCR.
Doplňující komentář:	x	x	x	x	x	x	x	x
Jsou poskytnuté podklady dostatečné pro stanovení nabídkové ceny této etapy?	x	ANO	x	ANO	x	ANO / NE / ČÁSTEČNĚ	x	NE
Doplňující komentář: *(např. upřesnění jaké další podklady a informace budete potřebovat, abyste mohli stanovit nabídkovou cenu).*	x	x	x	x	x	x	x	Bude třeba: - Vyjasnit architekturu - Požadavky na správu řešení - SLA
Popis požadavku								
Architektura systému								
Vyžaduje navrhovaný systém pro svůj provoz připojení do cloudu, případně odesílá nějaká data do cloudových služeb v internetu, nebo je schopen fungovat zcela offline bez přímého přístupu k internetu?	Částečně	Safetica nabízí hostování jak v prostředí Cloud, tak On Premises. Safetica On Premises nevyžaduje připojení k internetu (s výjimkou updatu produktu). Ochrana stanic rovněž funguje i v režimu offline, ale systém a jakékoliv úpravy v nastavení (politiky, klasifikace atd.) se aktualizují na koncových zařízení až po připojení k serveru. Odkaz k porovnání Cloud a On-premises: Feature comparison between cloud-hosted Safetica and Safetica hosted on-premises	ČÁSTEČNĚ	Web security se opírá o aktuální definice hrozeb (viry, kategorie, IP rozsahy, atd) které stahuje z prostředí výrobce. Plně ostrovní režim je možný, ale provozně komplikovaný. Cloud není využíván v případě volby čistě on-prem varianty	ANO	x	ANO	V závislosti na potřebách zákazníka a zakoupené licenci může systém fungovat zcela odpojen od internetu v cloudu nebo v hybridním režimu.
Jaké jsou možnosti integrace vámi dodávaného řešení na stávající provozované technologie Cisco FirePower 3110 a PaloAlto 3400 NGFW?	x	Přímá integrace není možná, ale ani potřebná, protože Safetica řešení není založeno na síťovém provozu, ale chrání data pomocí klienta koncové stanice. Je k dispozici možnost použít bezpečnostní certifikáty použité na síti pro podpis Safetica síťové komunikace, která probíhá na koncových zařízeních.	x	Lze využít pouze integrace na „Transparentní Proxy DLP" pomocí ICAP protokolu, nebo SPAN/Mirror Port mode napojení na Protector. Cisco FirePower – pokud umí SSL Decryption a ICAP je vhodný. PaloAlto NGFW – pokud umí SSL Decryption a ICAP je vhodný.	ANO	Proofpoint Enterprise DLP lze integrovat se stávajícími technologiemi Cisco FirePower a Palo Alto Networks. Konkrétně podporuje platforma Threat Response společnosti Proofpointintegrace s Cisco FirePOWER NGIPS (SourceFire) a Palo Alto Networks pro vyměňání a sdílení informací o hrozbách. Tato integrace umožňuje automatizovanou nápravu nebo blokování na základě informací o hrozbách sdílených mezi e-maily a kanály sociálních médií, využívající technologie sandboxingu Proofpoint a WildFire od Palo Alto pro současnou kontrolu adres URL a příloh.	x	Stávající proxy servery lze integrovat prostřednictvím protokolu ICAP. Pro http(s) a ftp(s) lze použít další předávací proxy server. Pro smtp lze použít e-mailovou bránu.

Jaké jsou možnosti zdrojů dat na vámi dodané řešení (např ICAP, REST přes HTTPS, SPAN port)?	x	Řešení Safetica se zaměřuje na ochranu dat uložených nebo používaných na koncových zařízeních a jiné zdroje dat nejsou potřebné. I síťová komunikace je chráněna ze strany koncové stanice, její operačního systému nebo aplikací.	x	ICAP/ICAPS/MTA/SPAN/Mirror Port mode	x	Proofpoint Enterprise DLP podporuje následující možnosti zdroje dat: • ICAP: Možnosti SMTP DLP společnosti Proofpoint lze rozšířit na web (HTTP/S) DLP pomocí proxy serveru s povoleným ICAP. Proofpoint má integraci se Zscalerem • REST over HTTPS: Proofpoint Enterprise DLP může posílat protokolování všech aktivit a upozornění do libovolné SIEM, která podporuje RESTful API jako zdroj dat. • SMTP: Proofpoint se může integrovat s jinými řešeními DLP prostřednictvím portu 25, kam buď Proofpoint nebo jiné řešení vloží záhlaví zpráv pro alternativní řešení, aby bylo možné detekovat, dále analyzovat nebo podniknout příslušné kroky.	x	ICAP, HTTP, HTTPS, FTP, FTPS, SMTP
Funkční možnosti								
Jaké typy dat a informací dokáže DLP systém detekovat a chránit?	x	Safetica je schopna chránit veškerá data pomocí kontextuální obrany. Klasifikace dat probíhá na základě: obsahu souboru :(např. Klíčová slova, zašifrovaný, obsah a další), Typu souboru, původ souboru (např. Sdílené síťové úložiště) klasifikace třetích stran (např. Microsoft Information Protection). Odkaz: How to create a data classification Safetica je schopná ochránit jakákoli data, která např. odchází přes email, upload na web, externí zařízení apod. Odkaz na destinace, které jsme schopni ochránit: Destination types in policies: detailed info	x	Dle definic vše podle: formátu, typu souborů, označení, počtu příloh, typu příloh, obsahové analýzy – slovníky, fráze, regulární výrazy, klasifikační značky, exaktní schody souboru (hash – fingerprint) částečná shoda, definice výjimek, a hlavně vztahů mezi jednotlivými pravidly např. (1 OR 2) AND NOT 3 Pro Network DLP je dostupné OCR na obsahovou analýzu	x	Systém DLP společnosti Proofpoint dokáže detekovat a chránit různé typy dat a informací, včetně: • Citlivá data v nestrukturovaném obsahu • Ztráta dat prostřednictvím cloudové synchronizace, USB, nahrávání, tisku, webové pošty a dalších běžných kanálů pro ztrátu dat • Citlivá data ve více než 300 typech souborů, včetně Microsoft Office a příloh PDF 4/10 SŽ: Interní • Citlivé dokumenty s otisky prstů s možností úplné i částečné přesné shody dat • Data v pohybu a v klidu v podporovaných cloudových službách (např. O365, Google Workspace, Box) • Přenosy exfiltrace dat prostřednictvím e-mailu • Data založená na schématech klasifikace informací organizace (např. Vyhrazené, Důvěrné, Přísně tajné) • Vzory indikující citlivá data prostřednictvím statistické analýzy	x	Textová data v dokumentech nebo obrázcích
Existují v systému připravené šablony pro detekci úniku citlivých informací?	ANO	Safetica obsahuje následující šablony pro snadné použití produktu: šablony pro datové klasifikace, politiky a destinace. Lze je upravovat dle potřeb, případně vytvořit nové. Odkaz: Predefined data classifications, policies, and destinations groups in Safetica	ANO	Forcepoint obsahuje od výrobce předpřipravené politiky, pravidla, slovníky dle zvoleného regionu (EU – Czechia) nebo oblasti činnosti (IT / Banking / Financial /...)	ANO	Společnost Proofpoint pravidelně aktualizuje a vydává nové validátory obsahu DLP ve formě proprietárních inteligentních identifikátorů, aby se zvýšilo pokrytí identifikace dat ve všech regionech USA, APJ a EMEA. Proofpoint DLP také zahrnuje široký výběr předdefinovaných slovníků, které lze použít pro detekci obsahu běžně chráněných typů informací. Slovníky pro zdravotnictví zahrnují sady informačních kódů, jako jsou standardní nemoci, léky, léčba a diagnostika, a kódy ICD používané zdravotnickým průmyslem ke zjednodušení dodržování HIPAA nebo zjišťování citlivých zdravotnických informací. Slovníky finančního soukromí pokrývají podmínky SEC, obchodování zasvěcených osob a potvrzení obchodu používané v odvětví finančních služeb, aby napomohly dodržování souladu s GLBA, PCI-DSS a Sarbanes-Oxley. Osobní údaje, jako jsou čísla sociálního pojištění, čísla pasů a formáty řidičských průkazů lze také detekovat pomocí zahrnutých vzorů. Lze přidat nebo definovat nové slovníky pro podporu dalších předpisů, jako je GDPR, NASD, PIPEDA, nebo vzory specifické pro vaše regulační prostředí. Slovníkové výrazy mohou být individuálně váženy, aby se zvýšila nebo snížila síla shody jakéhokoli výrazu, a použity v seznamech vyloučení, aby se povolily výjimky. Dynamické aktualizace zajišťují, že nainstalované slovníky jsou vždy aktuální s nejnovějšími změnami. Zákazníci mohou pomocí detektorů vytvářet a rozšiřovat předdefinované zásady na data v pohybu i v klidu v cloudu, koncových bodech a e-mailových kanálech a lze je plně integrovat s Proofpoint Intelligent Data Classification. Slovníky a také proprietární inteligentní identifikátory, které mohou zahrnovat další algoritmické kontroly (jako je Luhnův algoritmus), lze snadno přidat pro podporu typů dat specifických pro zákazníka, jako jsou čísla účtů, čísla pacientů, čísla lékařských záznamů, fakturační kódy a místní formuláře. ID. Vlastní slovníky pro detekci obsahu mohou podporovat seznamy termínů i shody vzorů založené na regulárních výrazech.	ANO	x
Jaké síťové protokoly navrhované řešení podporuje pro monitorování a ochranu dat (např. HTTP, HTTPS, FTP, FTPS, SMB, TELNET, SSH, SMTP, SNMP atd.) a umožňuje přizpůsobení portů, na kterých tyto protokoly běží? Dokáže systém analyzovat a chránit i provoz typu DNS over HTTPS nebo SSH over HTTPS a podobný?	x	Safetica řešení se zaměřuje na uživatelské operace a přenosy dat detekuje např. jako uploady souborů prostřednictvím webového prohlížeče (HTTP, HTTPS), detekuje FTP přenosy pomocí podporovaných FTP klientů, sleduje emailovou komunikaci přes desktopové emailové klienty (SMTP), nebo synchronizace repozitářů (Git). Další typy přenosů dat je možné ošetřit z pohledu blokování nebo monitoringu aplikací, která využívají alternativní protokoly. Přizpůsobení portů je v případě tohoto přístupu irelevantní a ochrana je zajištěna nezávisle na jejich nastavení.	x	Network DLP Protector analyzuje provoz směřovaný/dešifrovaný pomocí předřazené proxy a nativně tak vyhodnocuje HTTP, HTTPS, FTP, SFTP provoz s možností definovat custom porty a služby pro kontrolu.	x	Enterprise DLP spojuje výstupní kanály e-mailu, koncového bodu a cloudového zabezpečení do jediného skleněného panelu pro nápravu incidentů. Incidenty lze spravovat buď v samotné aplikaci, nebo v řešeních SIEM/SOAR, vlastních aplikacích nebo prostřednictvím integrace s nástroji pro správu IT služeb, jako je ServiceNow. Zásady oznamování založené na http webhoocích nebo rozsáhlých veřejných rozhraních API usnadňují nastavení a správu podnikových dat DLP v externích nástrojích. Export relevantních dat o incidentu netechnickým týmům mimo tým Incident Response nebo SOC, který spravuje výstrahy, nebyl nikdy snazší, pomocí našich funkcí exportu do csv, json nebo pdf, včetně volitelného snímku obrazovky pro další nevyvratitelný kontext, který snadno interpretují i pracovníci mimo IT. . má kontextové menu.	x	Pro data v pohybu HTTP, HTTPS, FTP, FTPS, SMTP. Pro data v klidu a SMB. Porty lze nakonfigurovat. V případě připojení k existujícímu proxy serveru prostřednictvím ICAP záleží na tom, jaké protokoly proxy server podporuje. V případě relay proxy serveru lze blokovat tunelování neznámých protokolů přes https.
Podporuje systém integraci s existujícími systémy pro označování a klasifikaci dat, jako je Microsoft Purview Information Protection?	ANO	Synchronizace Microsoft Purview Information Protection (MIP) a Safetica je možná a lze ji realizovat prostřednictvím několika metod	ANO	Forcepoint DLP podporuje nativní integrace na Microsoft Purview Information Protection.	ANO	Proofpoint integrovat s Microsoft MIP Služba Cloud DLP podporuje čtení, zápis a mazání štítků citlivosti MIP pro kompatibilní typy souborů, když jsou upraveny na základě posouzení souboru podle identifikátorů DLP. Agent koncového bodu podporuje události čtení pro štítky citlivosti MIP, ale dnes již nezapisuje ani nemaže E-mailový DLP server podporuje čtení událostí pro štítky citlivosti MIP, ale nepodporuje zápis/mazání.	ANO	x
Jaké metody používá systém pro detekci úniku dat (např. pravidla, regulární výrazy, kontrolu obsahu dokumentů, šablony dokumentů, machine learning, behaviorální analýza) v rámci agentless řešení?	x	Safetica řešení je primárně založeno na agent-based přístupu. V rámci agentless režimu je možné integrovat a chránit Microsoft 365 prostředí, kde lze detekovat a chránit odchozí emailovou komunikaci a sdílení cloudových souborů. V rámci této ochrany lze definovat bezpečnostní i klasifikační pravidla.	x	Na síťové úrovni jsou dostupné všechny požadované metody detekce úniků citlivých dat včetně OCR.	x	Systém Enterprise DLP společnosti Proofpoint používá řadu metod k detekci úniku dat v rámci řešení bez agentů, včetně: • Pokročilý regulární výraz • Klíčová slova a datové slovníky • Částečná shoda dokumentů • Dokument otisky prstů • Bayesovská analýza • Shoda metadat • Optické rozpoznávání znaků (OCR) • Analýza jazykového obsahu pomocí strojového učení • Behaviorální analýza Tyto metody umožňují komplexní kontrolu obsahu a detekci citlivých nebo regulovaných dat, aktivity uživatele, záměru a kontextu přístupu, stejně jako kompromitovaných účtů a phishingových uživatelů.	x	Klíčová slova, slovníky, regulární výrazy, předdefinované skripty, názvy souborů, typy souborů, vlastnosti souborů, otisky dokumentů (kontrola částečných shod) otisky databází (například výskyt jména a s ním spojeného rodného čísla v dokumentu), strojové učení.

Vyžaduje navrhované řešení pro plnou funkčnost implementaci SSL offloadingu (dešifrování SSL/TLS provozu), nasazení webové proxy nebo jiné systémy? Jaké další komponenty jsou nutné k zajištění plné funkčnosti systému?	NE	Řešení k některým okrajovým scénářům vyžaduje dešifrování SSL provozu, ale obecně není vyžadováno. Základní funkcionalita vyžaduje klienta koncové stanice, pro ochranu cloudových služeb je potřeba API integrace do Microsoft 365. Proxy, ani jiné komponenty nejsou potřeba.	ANO	Pro plnou funkcionalitu je SSL offloading doporučený, pokud ho není možné provádět na infrastruktuře SŽ, lze plně zprovoznit v rámci dodávky DLP řešení Forcepoint.	NE	Řešení Enterprise DLP společnosti Proofpoint nevyžaduje nasazení žádné architektury kromě e-mailové brány Proofpoint (pro e-mailové DLP) a agenta koncového bodu.	x	Pro SMTP je vyžadována e- mailová brána. Pro HTTP(S) a FTP(S) je vyžadován proxy server nebo integrace se stávajícím proxy serverem prostřednictvím ICAP.
Pokud jsou do systému napojena data pomocí SPAN portů, jak je omezena jeho funkčnost?	NE	Řešení je nezávislé na síťové konfiguraci.	x	Není žádné omezení pro monitoring provozu.	x	Proofpoint enterprise nepoužívá SPAN porty a má modernější přístup k DLP se zaměřením na moderní kanály, jako je cloud, endpoint a e-mail	x	Nelze kontrolovat zašifrovaná data.
Jak systém řeší zpracování dat v archivních souborech, které jsou přenášeny bez hesla i s heslem? Dokáže analyzovat obsah nešifrovaných i šifrovaných archivů a detekovat případné úniky citlivých informací skrytých v těchto souborech?	x	Safetica dokáže klasifikovat archiv při jeho vytvoření, pokud na stanici běží Klient. Navíc, dokáže klasifikovat citlivý šifrovaný soubor na základě Microsoft Purview Information Protection labelu, pokud byl tímto způsobem označený. Pokud archivní soubor nelze klasifikovat (např. kvůli použitému šifrování nebo heslu), odesílání takových souborů lze zamezit pomocí DLP politik.	x	Network DLP řešení monitoruje/chrání citlivá data v archivech, které nejsou chráněny heslem. V případě potřeby monitorovat obsah v šifrovaných souborech je nutné mít nastavené příslušné pravidlo v DLP pro koncové stanice (Endpoint DLP) a například je označovat klasifikační značkou na kterou reaguje síťové DLP.	x	Naše podnikové DLP řešení dokáže analyzovat obsah nešifrovaných archivních souborů a detekovat možné úniky citlivých informací. Neposkytuje však konkrétní podrobnosti o zpracování šifrovaných archivů nebo možnosti analyzovat jejich obsah, pokud jsou chráněny heslem.	x	Řešení bez agenta nevidí do již zašifrovaných souborů přenášených po síti. Přenos souborů detekuje samo. Akce závisí na nastavených zásadách.
Dokáže systém detekovat citlivé informace v multimediálních souborech, jako jsou obrázky, videa nebo audio soubory, a disponuje funkcionalitou OCR (Optical Character Recognition) pro identifikaci citlivých dat obsažených v obrazových formátech?	ANO	Ano, Safetica dokáže detekovat citlivé informace pomocí OCR (Optical Character Recognition) s podporou více jazyků. How OCR works Audio a video soubory je Safetica schopna ochránit na základě kontextu. (Přednastavené kategorie audio a video, je možné manuálně dodat požadovaný typ přípony)	ANO	Network DLP Forcepoint využívá OCR.	ANO	Enterprise DLP Proofpoint dokáže detekovat citlivé informace v multimediálních souborech, jako jsou obrázky. Podporuje funkci OCR (Optical Character Recognition) pro identifikaci citlivých dat obsažených v obrazových formátech. Modul OCR detekuje text vložený do obrázků, jako jsou naskenované formuláře, dokumenty, snímky obrazovky, obrázky a soubory PDF, extrahováním textu a jeho vyhodnocením proti povoleným detektorům.	ČÁSTEČNĚ	Textová data v obrázcích jsou analyzována pomocí OCR. Videa a zvuky nejsou podporovány.
Vyžaduje systém integraci na lokální Microsoft PKI infrastrukturu a podporuje možnost využití HSM boxů?	NE	Ne, nevyžaduje. HSM boxy nepodporuje.	NE	Není potřebné.	x	Není potřeba integrace s šifrováním, pokud není řízena Microsoft MIP prostřednictvím Email DLP V koncovém bodě můžeme označit osobně zašifrovaný obsah jako neschopný skenování a podle toho jednat (blokovat atd.) Veškeré šifrování v rámci služby SaaS zajišťuje Proofpoint	x	Je možná integrace prostřednictvím SAML
Způsob ochrany informací								
Jak systém detekuje a zabraňuje odcizení dat pomocí steganografie? Dokáže identifikovat skryté informace v obrazových a multimediálních souborech nebo jiných formátech, které mohou být využity k utajené exfiltraci citlivých dat?	x	Safetica stenografii nepodporuje, jelikož chrání data z úhlu pohledu aktivity uživatelů a bezpečné práce s daty. Pokud uživateli smí používat skripty nebo aplikace pro stenografii, Safetica může detekovat tyto aktivity jakož anomálii a reportovat je administrátorovi, ale neskenuje takové soubory pro případná schovaná data.	x	Žádné DLP steganografii neřeší, lze řešit produktem Forcepoint CRD	x	Enterprise DLP Proofpoint detekuje, zda uživatel používá některý z předdefinovaných steganografických nástrojů, které lze použít ke skrytí textových informací v obrázcích, a zablokuje tyto nástroje, aby se zabránilo úniku dat. Neposkytuje však odchozí steganografickou detekci. To by spadalo pod schopnost monitorování hrozeb zasvěcených osob jako proaktivní přístup	x	Detekce - ne. Lze tomu zabránit použitím modulu, který generuje stejně vypadající dokument. Tento dokument bude vypadat jako originál, ale nebude obsahovat viry ani steganografické informace z původního dokumentu.
Poskytuje systém ochranu pouze na aplikační vrstvě L7 OSI modelu, nebo dokáže chránit i na vrstvách L4 a L5? Jaké konkrétní bezpečnostní funkce nabízí na těchto vrstvách pro efektivní prevenci úniku dat?	NE	Chráněna je pouze vrstva L7.	NE	Network DLP Forcepoint toto neřeší.	ANO	Proofpoint Enterprise DLP poskytuje ochranu na více vrstvách modelu OSI, včetně aplikační vrstvy L7. Nabízí také ochranu na transportní vrstvě L4 a vrstvě relace L5. Mezi specifické funkce zabezpečení v těchto vrstvách patří: • Aplikační vrstva L7: Kontrola DLP, sledování souborů, prevence/blokování nahrávání webových souborů do cloudových služeb a přenosy synchronizace cloudu do služeb úložiště. • Transportní vrstva L4: Šifrování TLS pro webový provoz a mezi aplikací a databází, zajišťující bezpečný přenos dat. • Vrstva relace L5: Správa a kontrola relací prostřednictvím serveru proxy SAML v kombinaci s izolací pro spravované aplikace, zejména pro přístup z nespravovaných zařízení. Tyto funkce společně pomáhají účinně předcházet úniku dat napříč různými vrstvami modelu OSI.	x	Systém Forcepoint DLP je navržen tak, aby chránil data na různých úrovních, nikoli pouze na aplikační vrstvě (L7) OSI modelu. Forcepoint DLP nabízí ochranu napříč všemi vektory, včetně koncových bodů, webu, e-mailů a cloudových aplikací
Licencování a náklady								
Jaké jsou celkové náklady na pořízení systému, pokud předpokládáme pokrytí na 2 místech v Internet-UAS (včetně DMZ) a na 8 místech v UAS-TDS, při předpokladu poskytování služby pro 17000 uživatelů celkem a při propustnostech na linkách 2Gbps uplink/downlink?	x	119,891,800.00 Kč bez DPH	x	TOC náklady představují 43.450.430,- Kč bez DPH pro 17.000 uživatelů na 5 let včetně implementace, školení a podpory řešení.	x	x	x	Záleží na zakoupených modulech
Jak je vámi dodávaný systém licencován (subskripce/perpetual licence)?	x	subskripce	x	Licence je formou subscription s možností individuálně požádat o dodání perpetual varianty.	x	Licencováno na uživatele jako předplatné	x	Subskripce
Jaká je licencovaná jednotka (uživatel/objem zpracovaných dat/jiné)? Pokud jiné prosím uveďte licencovanou jednotku.	x	uživatel	x	Licencování je formou „per User" bez ohledu na množství chráněných zařízení, objem přenášených dat.	x	Licencováno na uživatele	x	Uživatel
Jak se systém zachová v případě překročení licencí?	x	Notifikací, že je limit překročen Odkaz: What happens when the number of users exceeds the number of purchased licenses	x	Notifikace v rámci managementu a upozornění výrobce na překročení zakoupených licencí. Z pohledu provozu není provoz nijak ovlivněn.	x	Systém bude nadále fungovat	x	Hlásí překročení licence
V případě, že je systém licencována na uživatele, jak je definován uživatel a na základě jakých indikátorů je určen počet potřebných licencí?	x	Uživatel je zaměstnanec, který má své přihlašovací údaje, takový uživatel se může logovat až na 3 různých zařízeních	x	Řešení je licencováno na uživatele. Uživatel je definovaný jako uživatel počítačových služeb.	x	Zaměstnanecké	x	Uživatel je osoba, která pracuje s chráněnými daty a je podřízena politikám DLP
Jaké jsou roční náklady na údržbu a podporu po dobu 5 let?	x	Roční náklad činí 23,978,360.00 Kč bez DPH	x	Roční náklady na údržbu a podporu řešení představují 168.000,-Kč bez DPH	x	x	x	56.600,- EUR bez DPH / 170000 uživatelů
Existují další skryté náklady, které bychom měli vzít v úvahu, pokud je vyžadována udržitelnost po dobu 5 let?	x	Ne, náklady jsou obsaženy v ceně licencí a přímý support je zajištěný formou Gold support	ČÁSTEČNĚ	Licenční náklady na podkladový OS (Windows Server 2016/2019/2022) a SQL Server 2016 a novější.	x	Žádný	x	Pravidelná školení zaměstnanců z pohledu uživatele pro práci s DLP
Bude nutné v období 5 let provést plný upgrade systému, který by vyžadoval další náklady spojené s další implementací, přepracováním zavedených pravidel atd..?	x	NE	NE	Ne pokud nedojde k zásadním změnám návazných v systémech SŽ.	x	Upgrady řešení A SaaS jsou řízeny proofpointem. Mohou být nutné upgrady agentů	x	V případě cloudové licence ne. Nová verze řešení on prem je obvykle vydávána dvakrát ročně a obvykle je podporována po dobu dvou let od vydání.
Integrace a kompatibilita								
Je možné systém integrovat s dalšími bezpečnostními nástroji, jako jsou SIEM, IAM, atd. a jaké bezpečnostní systémy podporuje?	ANO	Ano je možná integrace se SIEM. How to send Safetica alerts to SIEM Řešení lze propojit s Active Directory nebo Entra ID pro identifikaci identit i správu přístupů do řešení.	ANO	Integraci lze provést přes SysLog, nebo napojením přímo na SQL DB bezpečnostního řešení.	ANO	Proofpoint Enterprise DLP lze integrovat s dalšími bezpečnostními nástroji, jako jsou SIEM a IAM. Proofpoint Enterprise DLP může posílat veškeré protokolování a výstrahy jakékoli činnosti SIEM, která podporuje RESTful API jako zdroj dat, včetně Splunk. Platforma ochrany informací společnosti Proofpoint se navíc může integrovat s řešeními IAM, aby umožnila přístup do konzole pro správu Proofpoint a obecně podporuje jakéhokoli poskytovatele federovaných identit založených na Oauth 2.0 nebo SAML 2.0. Proofpoint lze také integrovat s poskytovateli IAM, kteří mohou přijímat zdroje JSON pro příjem dat z platformy Enterprise DLP a provádět jakékoli akce pracovního postupu odezvy.	ANO	SIEM pro odesílání protokolů, SMTP pro odesílání incidentů, IMAP/POP3 pro správu incidentů prostřednictvím e- mailové odpovědi, LDAP pro správu přístupu a oprávnění, REST API pro integraci správy incidentů a zásad do řešení zákazníka.

Podporuje systém standardní protokoly a API pro obousměrnou integraci (ovládání pomocí API, kontroly změn pomocí API, načítání detekcí pomocí API, atd.)?	NE	Obousměrná integrace není podporována.	ANO	Dostupný popis Forcepoint Management API.	ANO	Proofpoint Enterprise DLP podporuje standardní protokoly a rozhraní API pro obousměrnou integraci. Nabízí integraci DLP na bázi API pro rozšíření možností a přizpůsobení. Navíc podporuje integraci API (webhooky nebo Rest API) s předními cloudovými aplikacemi na trhu a umožňuje zásady oznamování tam, kde jsou webhooky dodávány řešením třetích stran. To umožňuje ovládání přes API, kontrolu změn přes API a načítání detekcí přes API	ANO	x
Je systém schopen se přímo integrovat do různých aplikací prostřednictvím speciálních konektorů pro připojení systémů? Pokud ano, které aplikace a systémy podporujete pro hlubší analýzu a ochranu dat na úrovni aplikací a jakým způsobem se provádí integrace?	ČÁSTEČNĚ	Microsoft 365	NE		ANO	Proofpoint Enterprise DLP je schopen přímé integrace do různých aplikací pomocí speciálních konektorů pro připojení systémů. Proofpoint podporuje integraci s aplikacemi a systémy, jako jsou ServiceNow, Splunk, Microsoft 365, Google Workspace, Box a další cloudové služby. Integrace je dosaženo pomocí rozhraní API, webhooků a SAML pro jemné ovládací prvky zásad. Řešení CASB společnosti Proofpoint poskytuje detekci a odezvu DLP téměř v reálném čase pro podporované schválené cloudové aplikace prostřednictvím příslušných rozhraní API dodavatele. Proofpoint se navíc integruje s řešeními IAM, aby umožnil přístup do administrátorské konzole Proofpoint a mohl zpracovávat zdroje JSON pro provádění akcí pracovního postupu odezvy.	ANO	Lze integrovat prostřednictvím rozhraní REST API
Bezpečnost a compliance								
Jak je zajištěna bezpečnost samotného DLP systému proti útokům?	x	Šifrování dat na databázové úrovni, komunikace mezi klienty Role a přístupová práva RBAC, Autentizace Ochrana proti manipulaci, Integrity Checks Bezpečnostní aktualizace	x	Hardening podkladového prostředí a využívaného programového vybavení s možností využít bezpečné ověření pro přístup, audit všech činností atd. Veškerá zpracovávaná data jsou šifrována pomocí AES256.	x	Proofpoint udržuje zdokumentovaný program zabezpečení informací v souladu s požadavky NIST 800-53 a ISO 27001. Bezpečnostní kontroly zahrnují šifrování v klidu pomocí AES 256 nebo silnějších šifer, mechanismy řízení přístupu pro fyzický a logický přístup k zařízením a infrastruktuře a zásady a postupy pro identifikaci a nápravu slabých míst ve svých produktech a službách. Proofpoint využívá distribuovanou infrastrukturu pro monitorování zabezpečení k monitorování a varování před bezpečnostními incidenty. Program zabezpečení informací společnosti Proofpoint navíc prochází každoročním auditem SOC 2 typu II na principy důvěryhodných služeb dostupnosti, důvěrnosti a zabezpečení.	x	Oddělení rolí, protokoly auditu. Aktualizace v případě nalezené zranitelnosti.
Jakým způsobem jsou data v systému zabezpečena proti neoprávněnému přístupu?	x	Auditní záznamy a logování Monitorování a detekce hrozeb Omezení přenosu dat a kontrola zařízení Zálohování a obnova dat Soulad s legislativními požadavky GDPR a ISO27001	x	Veškeré činnosti jsou monitorované na úrovni managementu řešení, lokálně uložená forenzní data jsou šifrována, ostatní je řešeno na úrovni dvou-faktorového přístupových oprávnění, jednotlivé role je možné plně customizovat.	x	Pro přístup ke konzole pro správu se uživatelé obvykle ověřují prostřednictvím poskytovatelů identity (IdPs), které podporuje Proofpoint Information and Threat Management (ITM). Mezi podporované IdP patří široce používané platformy, jako je Google IdP a OneLogin. Komunikace konzole pro správu je zabezpečena pomocí komplexních protokolů a opatření navržených k ochraně integrity a důvěrnosti dat během přenosu. To zahrnuje použití robustních šifrovacích standardů, které zajišťují, že všechna data vyměňovaná mezi uživatelem a konzolou pro správu jsou šifrována, aby se zabránilo neoprávněnému přístupu. Proofpoint ITM navíc využívá zabezpečené kanály, jako je HTTPS, který integruje protokoly SSL/TLS pro další ochranu komunikace před potenciálními kybernetickými hrozbami. Tento vrstvený přístup zajišťuje, že přístup a komunikace s konzolou pro správu jsou vedeny bezpečným a důvěryhodným způsobem. má kontextové menu	x	Forenzní data o incidentech se přenášejí šifrovaně a ukládají se na serveru pro správu. Systém neobsahuje žádná další citlivá data.
Další komentáře dodavatele k plnění PTK								
Komentáře	x	x	x	x	x	x	x	x



Platforma SŽ
Základní dokument

Červen 2025

Obsah

Seznam zkratek

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

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

Seznam vysvětlivek

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

1 Úvod

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

2 Platforma Správy železnic

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

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

Platforma SŽ obsahuje:

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

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

3 Motivace Platformy SŽ

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

Cílem Správy železnic je zajistit:

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

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

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

Mezi hlavní přínosy Platformy SŽ patří:

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

4 Architektonické principy

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

4.1 Bezpečnost a soulad s vnitropodnikovými předpisy

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

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

4.2 Auditní záznamy

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

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

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

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

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

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

Pomocí aspoň jednoho z protokolů:

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

A musí obsahovat minimálně následující informace:

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

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

4.3 Provozovatelnost řešení

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

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

4.4 Znovupoužitelnost řešení

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

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

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

4.5 Nezávislost na dodavatelích

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

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

4.6 Nákup a vývoj

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

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

4.7 Business kontinuita

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

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

5 Služby Platformy SŽ

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

5.1 Infrastrukturní služby

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

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

5.2 Platformní služby

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

Detailní přehled o infrastrukturních službách je předmětem Příloh Platformy SŽ.

5.3 Podpůrné služby

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

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

5.3.1 Bezpečnostní služby

Přehled dostupných služeb bezpečnostních aplikací

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

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

5.3.2 Služby monitoringu

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

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

5.3.3 Služby patch managementu

Popis služeb patch managementu, aktualizací a distribuce aplikací

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

5.3.4 Služby zálohování

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

5.3.5 Síťové služby

Přehled síťových služby

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

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

6 Technologie Platformy SŽ

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

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

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

Použití takových zapouzdřených technologií je možné jen v následujících případech:

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

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

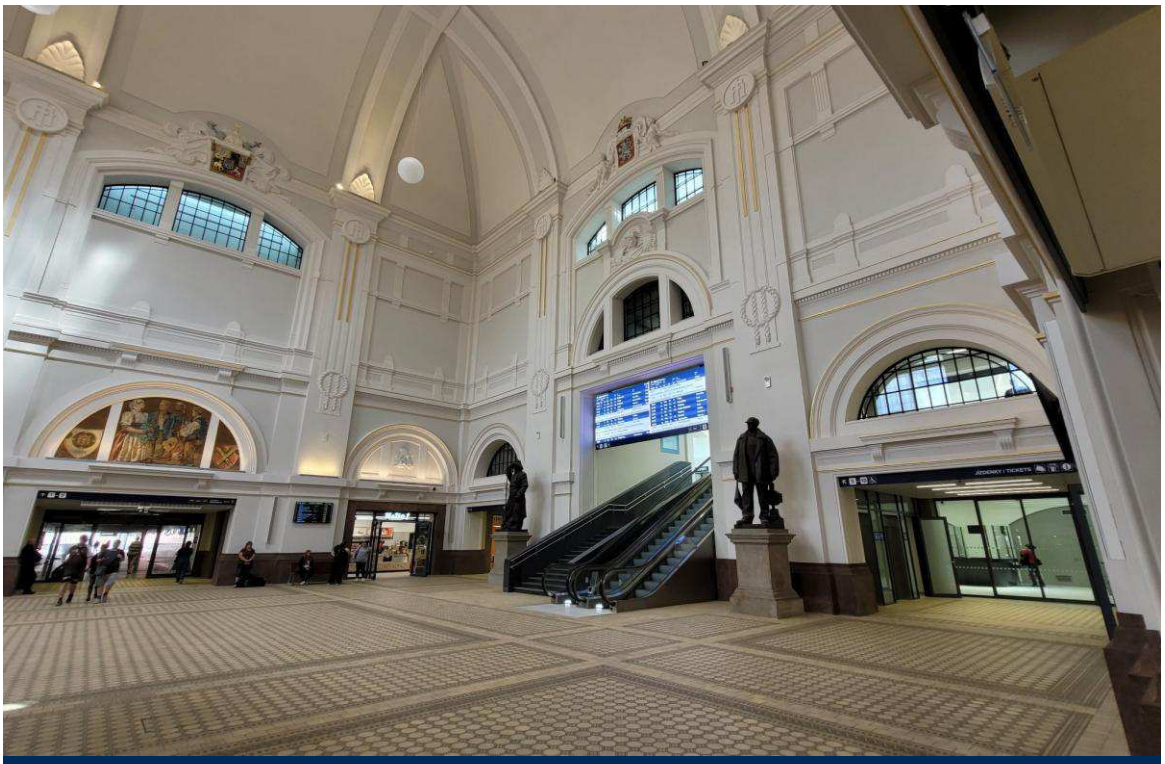
7 Přílohy Platformy SŽ

Jednotlivé oblasti jsou dále detailně zpracovány v těchto přílohách:

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

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

Datum tisku
2025-07-30



Platforma SŽ Standardy vývoje software

Červen 2025

Obsah

Seznam zkratek

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

Seznam vysvětlivek

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

1 Úvod

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

2 Standardy vývoje informačních systémů Správy železnic

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

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

2.1 Prostředí

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

2.1.1 Vývojové prostředí

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

2.1.2 Testovací prostředí

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

2.1.3 Produkční prostředí

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

2.2 Dvouvrstvá architektura

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

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

2.2.1 Datová vrstva

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

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

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

2.2.2 Aplikační vrstva

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

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

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

2.3 Třívrstvá a vícevrstvá architektura

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

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

2.3.1 Datová vrstva

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

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

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

2.3.2 Aplikační vrstva

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

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

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

2.3.3 Prezentační vrstva

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

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

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

2.3.4 Integrační vrstva

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

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

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

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

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

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

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

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

2.4 Požadavky na prezentační vrstvu

2.4.1 Uživatelské rozhraní

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

Pro návrh UI informačních systémů SŽ platí následující zásady:

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

2.4.2 Uživatelská zkušenost

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

UX informačních systémů SŽ musí splňovat následující vlastnosti:

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

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

2.5 Bezpečnost

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

Z pohledu požadavků na vyvíjený software je nutné zajistit oblasti:

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

2.5.1 Zabezpečení aplikací

Je požadováno, aby jednotlivé vrstvy splňovaly minimálně tyto požadavky:

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

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

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

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

2.5.2 Autentizace a autorizace

2.5.2.1 Autentizace

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

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

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

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

2.5.2.2 Autorizace

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

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

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

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

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

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

2.5.3 Zpracování osobních údajů

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

2.6 Dokumentace

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

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

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

2.6.1 Technická dokumentace jádra systému

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

2.6.2 E-R modely databáze

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

2.6.3 Objektový model pro aplikace

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

2.6.4 Procesní diagramy, schémata toků dat

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

2.6.5 Komunikační rozhraní

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

2.6.6 Drátové modely všech obrazovek uživatelského rozhraní aplikací

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

2.6.7 Popis konfigurace provozního prostředí

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

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

2.6.8 Uživatelská příručka

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

2.6.9 Příručka administrátora

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

2.6.10 Disaster Recovery postup (D/R Postup)

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

2.7 Modelování EA architektury

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

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

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

Hlavním schvalovatelem předkládaných modelů je Odbor IT architektury SŽT.

2.8 Předávání vývoje do provozu

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

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

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

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

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

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

Datum tisku
2025-07-30

Platforma SŽ Datová centra a serverovny

Červen 2025

Obsah

Seznam zkratek

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

Seznam vysvětlivek

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

1 Úvod

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

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

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

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

Tabulka 1. Rozdělení DC a serveroven dle velikosti a významu

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

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

2 Datová centra

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

2.1 Datové centrum CDP Praha

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

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

2.2 Datové centrum CDP Přerov

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

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

3 Serverovny

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

3.1 Významné serverovny

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

3.2 Serverovny dle geografických oblastí

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

3.3 Serverovny vybraných organizačních jednotek

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

3.4 Technologické serverovny

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

3.5 Technologické a sdělovací místnosti

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

4 Technologické vybavení

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

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

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

4.1 Stavební provedení

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

4.2 Napájení

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

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

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

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

4.3 Chlazení

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

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

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

4.4 Bezpečnost

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

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

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

4.5 Síťová infrastruktura

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

4.6 Ostatní vybavení

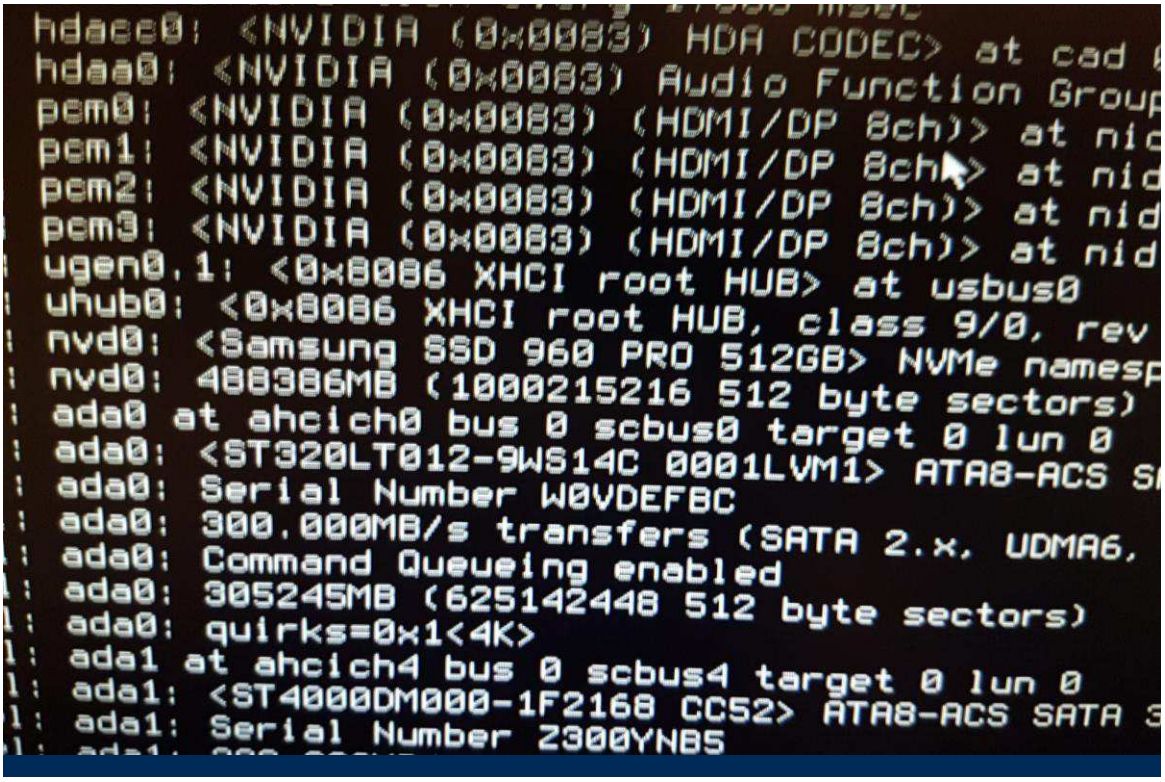
Monitorování prostředí v datových centrech je velmi důležité, protože kritické IT systémy jsou citlivé na změny teploty, vlhkosti a kvality vzduchu. Při narušení těchto parametrů může dojít ke vzniku problémů, jako jsou selhání systémů a ztráta dat. Proto se v datových centrech používají speciální senzory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

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

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

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

Datum tisku
2025-07-30



Platforma SŽ
Virtuální prostředí, serverové farmy, servery

Červen 2025

Obsah

Seznam zkratek

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

Seznam vysvětlivek

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

1 Úvod

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

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

2 Virtualizační prostředí

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

2.1 Virtualizace serverů

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

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

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

2.2 Virtualizace koncových počítačů

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

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

2.3 Kontejnerizace

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

3 Serverové farmy

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

3.1 Konvergovaná infrastruktura

V rámci konvergované infrastruktury provozuje SŽ tyto druhy farem:

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

3.2 Hyper-konvergovaná infrastruktura

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

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

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

4 Fyzické servery

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

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

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

5 Datová úložiště

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

5.1 Datová úložiště farem

Pro farmy klasické konvergované infrastruktury jsou provozovány datová úložiště:

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

5.2 Datová úložiště pro zálohy a archivaci

Pro ukládání záloh a archivaci jsou určena datová úložiště:

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

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

5.3 Datová úložiště pro off-line zálohy

Pro archivaci a offline ukládání záloh jsou určeny páskové knihovny:

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

5.4 Kancelářská datová úložiště

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

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

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

6 Virtuální servery

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

6.1 Služba virtuálních strojů

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

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

Služby virtuálních serverů

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

6.2 Služby diskových uložišť

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

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

Služby diskových úložišť

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

7 Databázové servery

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

Služby databázových prostředí

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

8 Webové servery

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

Služby webových serverů

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

9 Aplikační servery

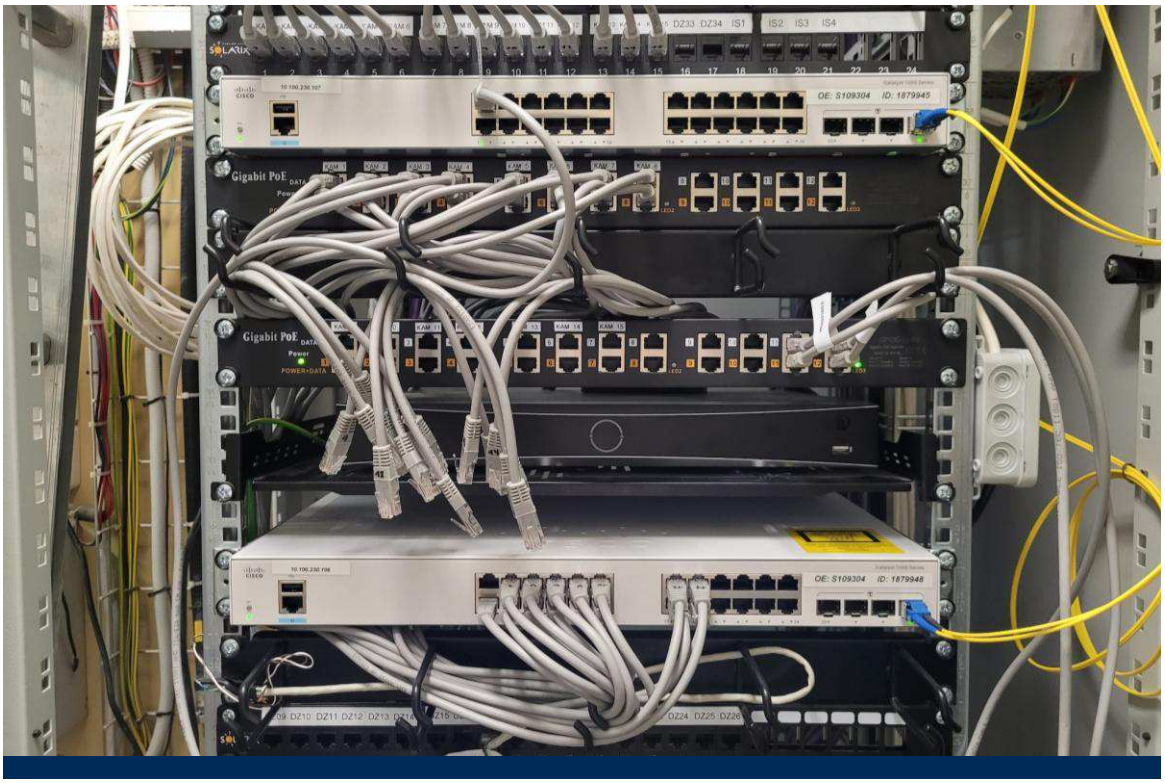
V prostředí Správy železnic je provozováno jedno portálové řešení, které je v rámci Platformy SŽ poskytováno jako platformní služba:

Služba zabezpečeného portálového řešení

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

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

Datum tisku
2025-07-30



Platforma SŽ Konektivita a síťové prostředí

Červen 2025

Obsah

Seznam zkratek

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

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

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

Seznam vysvětlivek

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

1 Úvod

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

2 Perimetr Správy železnic

2.1 Perimetr

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

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

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

2.2 Demilitarizovaná zóna

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

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

2.2.1 Demilitarizovaná zóna pro OT

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

2.3 Přístup přes VPN

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

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

2.3.1 Uživatelské VPN s MFA

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

Pro tyto VPN platí následující pravidla:

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

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

2.3.2 Site to Site VPN

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

2.4 Komunikační směry

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

Pravidla síťové komunikace na perimetru SŽ

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

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

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

3 Fyzické sítě Správy železnic

3.1 Uživatelsko-aplikační síť

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

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

3.2 Technologické datové sítě

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

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

3.2.1 Segmentace sítě

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

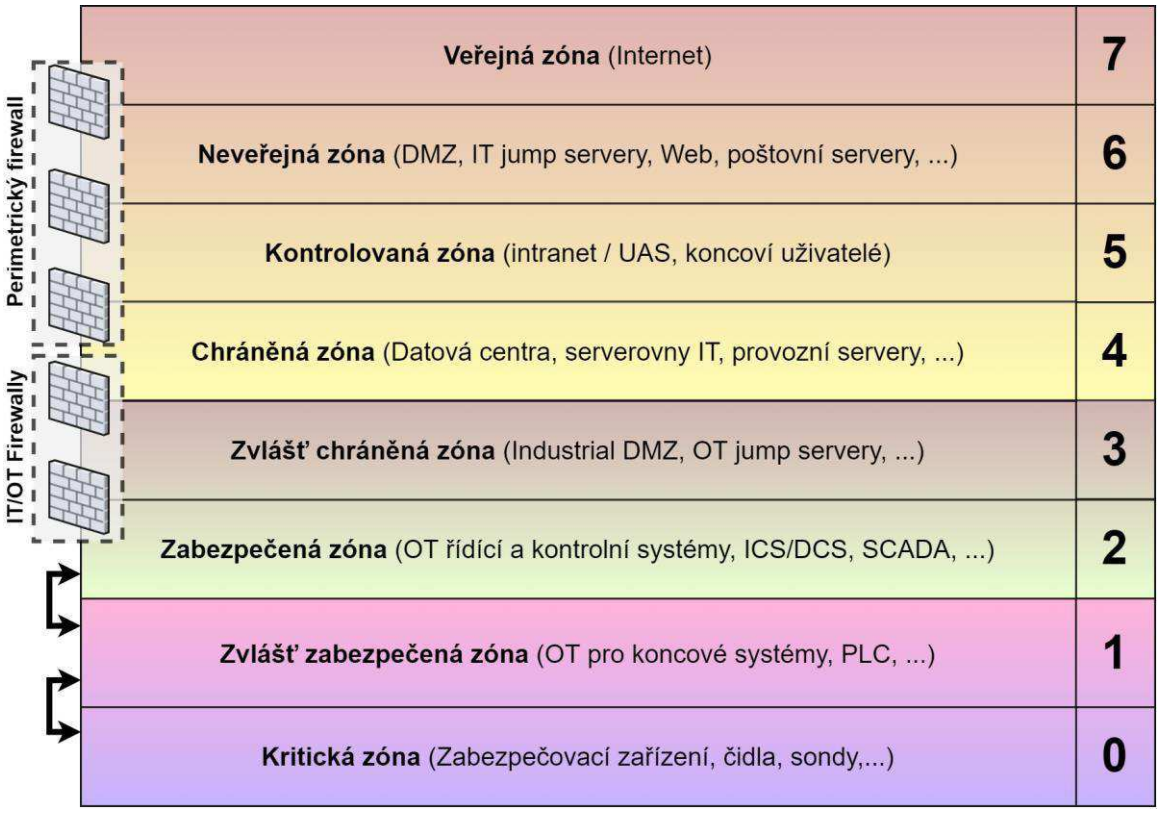
Segmentace UAS se v současné době aktivně připravuje, čili tato síť zatím není segmentována, rozdělena.

3.2.2 Ostrovní oddělené sítě

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

4 Logické síťové prostředí

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



Obrázek 1: Purdue ICS model

4.1 Komunikace mezi sítěmi

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

4.2 Georedundance

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

4.3 Řešení High Availability

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

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

5 Sítě APN

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

6 Síťová zařízení

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

6.1 Používané technologie

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

6.1.1 VLAN

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

6.1.2 VRF

Virtual Routing and Forwarding (VRF) je technologie používaná v sítích pro oddělení a izolaci síťového provozu na virtuální síťové segmenty. Každá VRF reprezentuje oddělenou síť, která má vlastní směrovací tabulky a rozhraní. Využívá se zejména v prostředí, kde se vyskytují různé typy síťového provozu, které se musí oddělit a izolovat, aby nedocházelo ke kolizím nebo únikům dat. VRF umožňuje vytvořit více logických sítí v jedné fyzické síti a zajistit tak bezpečné oddělení a izolaci síťového provozu.

Využití VRF VPN se obvykle pojí s technologií MPLS, která umožňuje efektivní směrování a přepínání datových toků mezi jednotlivými virtuálními sítěmi.

VRF Lite je technologie Virtual Routing and Forwarding (VRF) bez podpory MPLS. Oproti VRF VPN, která využívá MPLS pro směrování datových toků mezi různými virtuálními sítěmi, VRF Lite používá standardní směrování IP paketů v sítích založených na protokolu IP.

Správa železnic využívá VRF pro segmentaci MPLS sítí.

6.1.3 Technologie DWDM

U technologie DWDM jde o metodu vlnového multiplexování, díky tomu se optické vlákno využije pro více vlnových délek (více barev) pro oddělené datové přenosy.
V rámci celorepublikového řešení síťové infrastruktury Správy železnic jsou použity DWDM propoje mezi jednotlivými lokalitami jako nosná přenosová technologie pro MPLS sítě i pro přímé propoje datacenter, kde nejsou k dispozici přímá vlákna. DWDM síť obsahuje mnoho plnohodnotných přípojných bodů a více opakovačů pro zajištění spojů na velkou vzdálenost, zároveň poskytuje redundantní připojení jednotlivých DWDM bodů z více směrů.

Výčet používaných / preferovaných typů zařízení DWDM

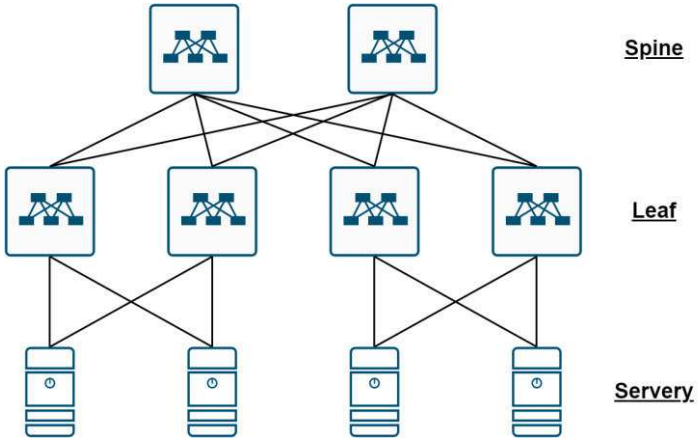
Typ zařízení	Popis	Konkrétní řady
DWDM	**Přípojný bod**	**NCS 1000** **NCS 2000**

6.1.4 Sítě MPLS

MPLS je technologie sítí, která umožňuje efektivní a spolehlivý přenos datových paketů vysokého objemu v rozsáhlých sítích. V prostředí Správy železnic jsou vybudovány dvě MPLS sítě. Stará MPLS síť pro uživatelsko-aplikační síť a některé technologické prvky a nová MPLS síť určená primárně pro technologické datové sítě. Záměrem SŽ je starou MPLS síť postupem času opustit.

6.1.5 Síťová spine-leaf topologie

Na rozdíl od klasické 3vrstvé topologie (Access-Distribution-Core) umožňuje Spine-Leaf díky dvouvrstvé topologii mimo jiné snížení latence mezi servery, snížení počtu fyzických switchů v datacentru, snížení počtu hopů při komunikaci mezi servery, zvyšuje propustnost a omezuje riziko vzniku úzkého hrdla.



Obrázek 2: Schéma Spine-Leaf topologie

Všechny nově instalované datacentrové switche v síťovém prostředí Správy železnic již plně podporují integraci do Spine-Leaf topologie, ať už přímým napojením, nebo jako Remote Leaf.

6.1.6 Technologie Cisco ACI

Cisco ACI (Application Centric Infrastructure) je softwarově definované síťové řešení, které zjednodušuje, automatizuje a zabezpečuje provoz sítě v datových centrech. V prostředí SŽ se používá výhradně v Network-Centric módu, který je síťově zaměřen na tradiční přístup k subnettingu a používání VLAN. Jedná se o poměrně nové řešení, v datových centrech se tato technologie postupně rozšiřuje, z toho důvodu všechny nově instalované switche v datových centrech již podporují integraci do Cisco ACI.

6.1.7 Sítě OOB

V datových centrech SŽ je vyžadováno, aby všechny servery a síťové prvky měly k dispozici dedikovaný síťový port pro dohled a konfiguraci těchto zařízení. Tyto porty se propojují do oddělené OOB (Out-of-band) sítě, která je síťově oddělena od hlavní datové sítě. Lokálně v datovém centru se jedná o fyzicky oddělenou síť, v rámci intranetu jsou odděleny virtuálně pomocí VLAN a VRF.

6.2 Firewally

Vzhledem k množství a různorodosti datových sítí jsou z pohledu kybernetické bezpečnosti firewally nejdůležitějšími síťovými prvky pro Správu železnic. Je kladen velký důraz na striktně oddělené provozy mezi uživatelskými a technologickými sítěmi, mezi uživatelskými sítěmi a datovými centry a samozřejmě mezi sítěmi SŽ a Internetem. Perimetrický firewall musí umožňovat testovací mód FW pravidel, který umožní odladit pravidla bez dopadu na probíhající provoz, dále musí podporovat HA zapojení a distribuovanou konfiguraci. Podle logického umístění firewallu je zvolen konkrétní model viz následující tabulka.

Výčet používaných / preferovaných typů firewallů

Typ routeru	Popis	Konkrétní řady
Perimetr	Hraniční firewall	Palo Alto vyšších řad
Pro segmentaci	Segmentační firewally pro IT sítě a IT/OT DMZ	Cisco Firepower 1xxx Cisco Firepower 31x0 Cisco Firepower 4xxx
Pro datová centra	Firewall pro aplikační farmy, clustery, single nody, NAS atd.	Cisco Firepower 31x0 Fortinet Fortigate 600F Fortinet Fortigate 1801F Fortinet Fortigate 2601F
Pro aplikace	Firewall na aplikační vrstvě OSI modelu (WAF)	F5 BIG-IP
Pro load balancing	Loadbalancer pro vyrovnání zátěže serverů	Kemp LoadMaster

6.3 Routery

Routery, nebo také směrovače, jsou zásadní aktivní síťové prvky pro segmentaci sítí. Podle způsobu použití jsou děleny na routery pro provoz v MPLS síti, routery v datových centrech a perimetru sítě, případně pro IT nebo OT sítě.

Jsou podporovány routery Cisco s požadovanými protokoly:

- **HSRP** – pro hraniční routery
- **VRF** – pro MPLS routery
- **VRF-Lite** – pro routery bez MPLS
- **BGP** – pro hraniční a MPLS routery
- **TACACS+**
- **RADIUS**

V následující tabulce jsou uváděny jednotlivé řady vždy pro konkrétní použití.

Výčet používaných / preferovaných typů routerů

Typ routeru	Popis	Konkrétní řady
MPLS	Routery typu P, PE a RR v MPLS síti	Cisco ASR Cisco NCS Cisco 8000
MPLS	Routery typu CE	Cisco C9400 Cisco C9300 Cisco C8000 Cisco ISR
IT	Routery pro datová centra a IT sítě	Cisco C9300 Cisco ISR
OT	Lokální routery pro OT sítě	Cisco IR

6.4 Switche

V prostředí SŽ jsou switche (přepínače) nejčastější síťová zařízení, proto existuje velké riziko možného nasazení nekompatibilních typů s následnou problematickou výměnou za kompatibilní. Obecně jsou preferované switche od renomovaného výrobce Cisco řady C9xxx a pro datacentra řada Nexus 9300, u nichž jsou do značné míry zaručené jednotné konfigurační prostředí (CLI), podpora VLAN bez omezení jejich počtu, kompatibilita používaných síťových protokolů, možnost stohování dedikovaným portem aj.

Jsou požadovány síťové a autorizační protokoly jako:

- **HSRP** – Hot Standby Router Protocol
- **PVST+** – Per-VLAN Spanning Tree Plus
- **TACACS+**
- **RADIUS**

Platí zákaz používání switchů bez managementu. V následujících podkapitolách jsou uváděny jednotlivé řady vždy pro konkrétní použití.

6.4.1 Switche pro datová centra

K již zmiňovaným požadavkům je u switchů pro datová centra vyžadováno redundantní napájení.

Výčet používaných / preferovaných typů

Typ switche	Popis	Konkrétní řady
Spine	Spine switch v topologii Spine-Leaf	Cisco Nexus 9332C Cisco Nexus 9364C
Leaf/ToR	Leaf switch v topologii Spine-Leaf nebo Top of Rack / Top of Row switch	Cisco Nexus 93180YC Cisco Nexus 93240YC Cisco Nexus 93360YC
Backend	Lokální propojení nodů farem (HCI)	Cisco Nexus 93180YC Cisco C9300X
Access	Jako access switch v malých serverovnách	Cisco C9300X Cisco C9300

6.4.2 Switche pro fibre channel

K již zmiňovaným požadavkům je u switchů pro datová centra vyžadováno redundantní napájení.

Výčet používaných / preferovaných typů

Typ switche	Popis	Konkrétní řady
Fibre Channel	Fibre Channel switche převážně pro připojení síťových úložišť typu SAN	Cisco MDS 9124T/V Cisco MDS 9132T/V Cisco MDS 9148T/V

6.4.3 Switche pro kamerové systémy

Pro kamerové systémy jsou požadovány switche s napájením PoE+ podle standardu 802.3at, případně PoE++ podle standardu 802.3bt.

Výčet používaných / preferovaných typů pro kamerové systémy

Typ switche	Popis	Konkrétní řady
Access	Běžný PoE switch pro připojení kamerových systémů	Cisco C9200, resp. C9200L Cisco C9300, resp. C9300L

6.4.4 Switche pro management zařízení

Pro OOB switche v datových centrech platí mimo jiné požadavek na redundantní napájení. V ostatních lokalitách, kde nejsou zajištěny dvě nezávislé napájecí větve, je tento požadavek bezpředmětný.

Výčet používaných / preferovaných typů pro management zařízení

Typ switche	Popis	Konkrétní řady
OOB	Běžný access switch s metalickými RJ45 porty pro připojení MGMT portů	Cisco C9200, resp. C9200L
OOB	Velká datacentra spine-leaf	Cisco Nexus 9348GC

6.4.5 Switche pro lokální sítě

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

Výčet používaných / preferovaných typů pro lokální sítě

Typ switche	Popis	Konkrétní řady
Access	Běžný access switch pro připojení pracovních stanic, tiskáren atp.	Cisco C9200 všech variant Cisco C9300 všech variant
OT	Lokální switche pro OT sítě	Cisco IE2xxx
End of Support	Dosluhující řada, postupně se nahrazují	Cisco C2960 více variant Cisco C2950

6.5 Bezdrátová zařízení

Tato zařízení pro obsluhu bezdrátových sítí (WLAN) jsou používána v prostředí Správy železnic.

Výčet používaných / preferovaných typů pro zařízení pro bezdrátová sítě

Typ zařízení	Popis	Konkrétní řady
Controller	Controller pro bezdrátové sítě WLAN	Cisco Catalyst 9800
Access Point	Bezdrátové přípojné body (AP)	Cisco Catalyst 91xx

6.6 Huby

Ethernetový hub neboli síťový rozbočovač se v prostředí SŽ nenachází a jeho použití je zakázané.

6.7 Modemy a datová zařízení

V prostředí rozlehlé sítě SŽ se používají různé typy modemů, tedy zařízení pro převod mezi digitálním a analogovým rozhraním. Jde např. o GSM modemy s protokolem LTE nebo GPRS, DSL modemy, 2-pair / dial-up.

Výčet používaných / preferovaných modemů a datových zařízení

Výrobce	Technologie	Popis	Konkrétní řady/modely
Patton	DSL		1088, 3200, 3088
Albis / Siemens	DSL		BSTU4 / ULAF+
RAD	DSL		ASMi50
Patton	2-pair		3202

CONEL	GPRS	GPRS modem, již ukončená výroba	ER75i
Siemens	GPRS		M35i
Teltonika	4G/LTE	Průmyslové LTE routery s rozhraním RS232, RS485, Ethernet, M-bus	TRBxxx
Advantech	4G/LTE	Průmyslové LTE routery s rozhraním RS232, RS485, Ethernet	ICR-xxxx

6.8 Centralizovaná správa síťových prvků

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

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

Datum tisku
2025-07-30

Platforma SŽ Integrační standardy

Červen 2025

Obsah

Seznam zkratek

API	Komplexně definované komunikační rozhraní aplikace *(Application Programming Inteface)*
CSV	Jednoduchý textový souborový formát (Comma-separated values)
ESB	Softwarová architektura a technologie používaná v oblasti podnikové integrace a správy služeb *(Enterprise Service Bus)*
IoT	Internet věcí je souborné označení pro síť fyzických zařízení, která vzájemně, centrálně nebo i s vnějším světem komunikují a mají možnost předávat data. Každé z těchto zařízení je jasně identifikovatelné díky implementovanému výpočetnímu systému, ale přesto je schopno pracovat samostatně v existující infrastruktuře sítě *(Internet of Things)*
IT	Informační technologie *(Information Technology)*
ITIL	*(Information Technology Infrastructure Library)*
JSON	Datový formát primárně určený pro přenos dat *(JavaScript Object Notation)*
KII	Kritická informační infrastruktura
REST/API	Webově založené klient-server API *(Representational State Transfer)*
SAP	Modulární ERP systém od německé firmy SAP AG
SFTP	Zabezpečený protokol pro přenos souborů. Pro zajištění šifrování využívá protokol SSH *(SSH File Transfer Protocol)*
SMTP	Základní síťový protokol pro přenos elektronické pošty *(Simple Mail Transfer Protocol)*
SOA	Architektura orientovaná na služby – jedná se o softwarovou architekturu, která se zaměřuje na organizaci a strukturu aplikací a systémů jako soubor nezávislých a dobře definovaných služeb *(Service-Oriented Architecture)*
SŽ	Správa železnic, státní organizace
XML	Standardizovaný jazyk používaný pro serializaci dat *(Extensible Markup Language)*

Seznam vysvětlivek

Platforma SŽ	Soubor dokumentů, rozdělený na veřejnou, interní a metodickou část, určený pro seznámení dodavatelů se standardy a technologiemi v ICT prostředí SŽ.
Platforma WSO2	Open-source platforma pro správu služeb (ESB) a integraci aplikací (API Management) vyvinutá společností WSO2 Inc. WSO2 poskytuje komplexní sadu nástrojů a produktů, které pomáhají organizacím implementovat a spravovat architekturu orientovanou na služby (SOA) a rozhraní pro programování aplikací (API) v jejich IT infrastruktuře.

1 Úvod

Tento dokument slouží jako příloha k základního dokumentu Platformy SŽ, který je součástí veřejných zakázek a podrobněji rozvádí integrační standardy naší organizace. Cílem je poskytnout jasný a konzistentní rámec pro všechny integrační aktivity. Naše cíle dále zahrnují modernizaci a konsolidaci současných integračních mechanismů za účelem zvýšení efektivity a snížení nákladů na údržbu. Dokument specifikuje požadavky a standardy, které musí být dodrženy při implementaci integračních scénářů, s důrazem na bezpečnost a využití hybridních řešení kombinujících on-premise a cloudovou infrastrukturu s ohledem na celkovou IT strategii. Všechny aktivity musí cílit na ITIL rámec pro řízení IT služeb, neboť tímto rámcem se naše organizace rozhodla řídit IT služby.

2 Moderní architektonické rámce

V rámci moderního IT prostředí naše organizace využívá pro nová řešení různé architektonické rámce a principy k zajištění flexibility, škálovatelnosti a efektivního poskytování služeb. Tato kapitola se zaměřuje na popis klíčových architektonických principů a jejich implementaci v naší organizaci. Použití současně moderní architektury nám umožňují efektivně reagovat na měnící se potřeby a technologické požadavky.

2.1 Flexibilita

Naše architektura umožňuje snadné přizpůsobení se měnícím se potřebám businessu. Tím, že kombinujeme lokální a cloudové infrastruktury, jsme schopni efektivně reagovat na dynamické požadavky a přizpůsobit naše služby v reálném čase. Hybridní řešení nám umožňují optimalizaci výkonu a nákladů tím, že strategicky využíváme výhody obou typů prostředí. Tato flexibilita nám dává možnost optimalizovat zdroje podle aktuálních potřeb a strategických cílů, ale hlavně dodržování bezpečnostních kritérií.

2.2 Škálovatelnost

Díky využití mikroslužeb a škálovatelné cloudové infrastruktury můžeme dynamicky přizpůsobovat kapacitu našich systémů podle aktuální požadavků. To zajišťuje, že naše služby jsou vždy dostupné a výkonné, i při náhlých změnách v zatížení. Implementujeme mechanismy automatického škálování, které umožňují plynulý růst a adaptaci bez potřeby manuálního zásahu, což přispívá k vyšší efektivitě a spolehlivosti.

2.3 Bezpečnost

Naše integrační architektura zahrnuje robustní bezpečnostní opatření na všech úrovních. Zajišťujeme ochranu dat a služeb pomocí pokročilých metod autentizace a autorizace, šifrování dat a pravidelného monitorování bezpečnostních hrozeb. Primárně z pohledu Compliance a regulace dbáme na dodržování všech relevantních bezpečnostních standardů a právních předpisů, což zajišťuje důvěryhodnost a právní jistotu pro business partnery.

2.4 Efektivita

Využití automatizace v rámci integračních procesů nám umožňuje snížit provozní náklady a zvýšit produktivitu. Automatizované workflow a orchestrace služeb minimalizují potřebu manuálních zásahů a zvyšují přesnost a rychlost procesů. Tohoto stavu jsme dosáhli díky centrálnímu řízení integrací prostřednictvím platformy ESB, ta nám umožňuje efektivně monitorovat a spravovat všechny integrační toky, což přispívá k vyšší přehlednosti a lepší koordinaci mezi jednotlivými systémy.

3 Architektura integrací

V rámci naší organizace se zaměřujeme na implementaci moderní architektury integrací, která podporuje jak on-premise, tak cloudové prostředí. Tato hybridní přístup zajišťuje flexibilitu, škálovatelnost a bezpečnost, což jsou klíčové faktory pro úspěšné řízení IT služeb podle ITIL principů. Cílový stav architektury je ESB.

Naše integrační architektura je postavena hlavně na následujících architekturních principech:

3.1 Microservices Architecture

Naše organizace implementuje architekturu mikroslužeb, což znamená decentralizaci a rozdělení monolitických aplikací na menší, nezávislé služby. Tento přístup zajišťuje vysokou flexibilitu a usnadňuje správu jednotlivých služeb. Díky mikroservisům můžeme rychleji reagovat na změny a inovace, což nám umožňuje poskytovat kvalitnější služby našim zákazníkům v podobě businessu.

3.2 Event-Driven Architecture

Pro lepší škálovatelnost a reaktivitu využíváme architekturu řízenou událostmi. Tento přístup umožňuje systémům komunikovat prostřednictvím událostí, což zvyšuje jejich schopnost rychle reagovat na provozní incidenty. Díky tomu můžeme dosahovat vyšší efektivity a pružnosti v našich provozních procesech.

3.3 API-First Approach

Při návrhu a vývoji systémů se naše organizace řídí principem API-First. API jsou navrhována a vyvíjena jako primární prostředek komunikace mezi systémy. Tento přístup je v souladu s ITIL principy, které se zaměřují na poskytování hodnoty zákazníkům prostřednictvím dobře definovaných služeb. API-First nám umožňuje dosahovat vyšší konzistence a standardizace v naší IT infrastruktuře.

3.4 Hybridní architektura

Pro zajištění flexibility a škálovatelnosti kombinujeme on-premise a cloudová řešení. Tento hybridní přístup nám umožňuje využívat výhod obou prostředí, což zajišťuje kontinuitu služeb a splnění compliance požadavků. Díky hybridní architektuře můžeme optimalizovat naše IT zdroje a lépe podporovat business v naší organizaci. Toto je obzvláště důležité z důvodu kritické infrastruktury informací (KII), která vyžaduje vysokou míru bezpečnosti a spolehlivosti. Hybridní přístup nám umožňuje zajistit, že klíčové systémy a data jsou chráněny a zároveň flexibilně škálovatelné dle aktuálních potřeb.

4 Typy integrací

Pro celkové pochopení integrací je nutné zmínit úrovně integrací. Existuje totiž několik pohledů, které následně definují oblasti soustředění a úroveň detailu. Je potřeba podotknout, že při komplexním řešení integrací dochází k jejich vzájemnému prolínání. Zde jsou vyjmenovány ty hlavní z nich:

- **Datová integrace** – Tento typ integrace se zabývá shromažďováním dat z různých zdrojů a jejich následným poskytnutím uživatelům v jednotné a konzistentní struktuře a formátu. Datová integrace umožňuje kombinaci dat umístěných v různých zdrojích a poskytuje uživateli sjednocený pohled na tyto data.
- **Procesní integrace** – Procesní integrace má za cíl propojit aplikace z hlediska podnikových procesů. Jakmile skončí jedna činnost, je vykonána činnost druhá. Při dokončení prvního procesu se spustí proces další, a tím že různé procesy mohou být realizovány odlišnými subsystémy je důležité zajistit, že tyto procesy jsou správně a efektivně koordinovány.

- **Aplikační integrace** – U aplikační integrace jde v zásadě o realizaci výměny informací (různého charakteru) mezi různými aplikacemi. Výměna přitom může probíhat s využitím široké škály transportních technologií – např. přes webové služby, databáze, sdílený soubor, messaging apod.
- **Systémová integrace** – Systémová integrace je proces spojování různých softwarových komponent, subsystémů, v jeden fungující celek. Cílem je, aby tento celek pracoval co možná nejefektivněji, tedy z pohledu jednotlivých subsystémů, aby komunikace mezi nimi probíhala podle definovaného schématu.

Každý z těchto typů integrace má své výhody a nevýhody a je důležité na základě analýz vybrat ten vhodný typ integrace, který bude respektovat konkrétní potřeby a požadavky jednotlivých projektů.

5 Softwarová architektura Enterprise Service Bus

ESB je softwarová architektura pro distribuované výpočty. ESB implementuje komunikační systém mezi vzájemně interagujícími softwarovými aplikacemi v rámci SOA. ESB je centralizovaný, standardizovaný hub, který přijímá, transformuje a poskytuje data, aby různé aplikace a služby napříč organizací mohly snadno komunikovat. ESB je cílový stav architektury, která je preferovaná v naší organizaci. Vzhledem ke složitosti prostředí však je doplňován i jinými způsoby integrací na základě výše popsaných architektur integrací.

ESB poskytuje hlavně tyto funkce:

- **Transformace dat** – provádí transformování zpráv do formátů, které jsou pro příjemce zpracovatelné a srozumitelné
- **Směrování zpráv** – dokáže rozhodovat, kam má zprávu odeslat na základě atributů obsažených v obsahu daných zpráv
- **Mediace služeb** – může poskytnout jednotné rozhraní pro více služeb
- **Orchestrace** – koordinuje interakce mezi službami

ESB je navržen tak, aby zjednodušil vazby a pomohl se oprostit od „Spaghetti" architektury, která v organizaci zatím dominuje. ESB je sada nástrojů, která posílá zprávu přímo do konkrétní destinace mezi buď aplikací a/nebo komponentami. Ať už je to klient nebo proces, cokoli, co je připojeno k ESB, nekomunikuje přímo mezi sebou, protože komunikují prostřednictvím samotného ESB platformy.

6 Primární integrační scénáře

6.1 Integrační platforma

Naše organizace plánuje rozvinout integrační platformu WSO2 do podoby ESB, který bude sloužit jako hlavní integrační páteř. WSO2 bude poskytovat následující funkcionality:

- **Service Orchestration** – Koordinace a řízení komunikace mezi různými službami, což podporuje efektivní řízení provozu služeb a incidentů.
- **Data Transformation** – Převod a mapování datových formátů mezi různými systémy, což umožňuje jednotné zpracování dat v rámci celé infrastruktury.
- **Security Enforcement –** Implementace bezpečnostních politik a autentizace, což je klíčové pro řízení rizik a zajištění integrity služeb.

6.1.1.1 Preferované Protokoly pro Integraci s WSO2

- **REST/HTTPS** – Pro aplikační a datové integrace díky své jednoduchosti a široké podpoře, což umožňuje snadnou správu a podporu služeb.
- **SOAP** – Pro integrace, kde je vyžadována robustní bezpečnost a transakční podpora, což je v souladu s potřebami řízení kritických služeb.
- **MQTT** – Pro event-driven integrace a IoT komunikace, které podporují rychlou reakci na změny a incidenty.
- **AMQP** – Pro spolehlivý a škálovatelný messaging mezi aplikacemi, což zajišťuje stabilní a efektivní komunikaci.

6.2 SAP Business Technology Platform

SAP BTP hraje klíčovou roli v naší integrační strategii. Specifické požadavky na integraci SAP BTP zahrnují:

- **Integration Suite** – Použití SAP Integration Suite pro propojení SAP a non-SAP systémů, což podporuje jednotnou správu a provoz služeb.
- **Event Mesh** – Využití SAP Event Mesh pro událostmi řízenou architekturu, což umožňuje rychlé a efektivní řízení změn a incidentů.
- **Business Process Management** – Automatizace a optimalizace obchodních procesů pomocí SAP Workflow Management, což zajišťuje efektivní poskytování služeb.

6.2.1.1 Preferované Protokoly pro Integraci s SAP BTP

- **OData** – Pro přístup k datům a jejich manipulaci přes standardizované API, což podporuje transparentní správu dat.
- **RFC/BAPI** – Pro volání vzdálených funkcí v SAP systémech, což zajišťuje spolehlivou integraci služeb.
- **IDoc** – Pro elektronickou výměnu dat mezi SAP a non-SAP systémy, což umožňuje efektivní řízení datových toků.
- **SOAP** – Pro služby vyžadující vysokou úroveň bezpečnosti a transakční podporu, což zajišťuje integritu a důvěryhodnost služeb.

6.3 Microsoft nástroje a Azure

Integrace s Microsoft technologiemi, včetně Azure, zahrnuje tyto základní komponenty:

- **Azure Logic Apps** – Automatizace a orchestraci pracovních toků, což podporuje efektivní správu a provoz služeb.
- **Azure API Management** – Správa a bezpečné publikování API, což zajišťuje jednotný přístup a kontrolu nad službami.
- **Azure Service Bus** – Spolehlivá messagingová platforma pro integraci aplikací, což podporuje stabilní a efektivní komunikaci.
- **Azure Arc** – Pro správu a orchestrace zdrojů v hybridním prostředí, což umožňuje jednotnou správu a kontrolu napříč on-premise a cloudovými systémy.

6.3.1.1 Preferované Protokoly pro Integraci s Azure

- **REST/HTTPS** – Pro širokou škálu aplikačních a datových integrací, což podporuje snadnou správu a podporu služeb.
- **gRPC** – Pro vysoce výkonné, nízko-latentní komunikace mezi mikroservisami, což zajišťuje rychlou a efektivní komunikaci.
- **Event Grid** – Pro event-driven architekturu a notifikace, což umožňuje rychlou reakci na změny a incidenty.
- **Service Bus** – Pro messaging a integraci podnikových aplikací, což zajišťuje spolehlivou komunikaci a řízení služeb.

6.4 Integrace stávajících aplikací

Mnoho aplikací, je stále ještě integrováno point-to-point, ty budou postupně převedeny do centralizovaného integračního prostředí. Hlavní kroky zahrnují:

- **Inventarizace a Analýza** – Zmapování současných integrací a identifikace klíčových závislostí, což podporuje efektivní správu a plánování změn.
- **Standardizace API** – Vytvoření standardních API pro všechny aplikace, což zajišťuje jednotný přístup a kontrolu nad službami.
- **Refaktoring a Modernizace** – Přepsání nebo refaktoring stávajících integrací podle moderních standardů, což podporuje efektivní a bezpečné poskytování služeb.

Tabulka protokolů

Protokol	Použití	Výhody	Nevýhody	Důvod Preference/Nepreference
REST/HTTPS	Aplikační, datové	Jednoduchost, široká podpora, škálovatelnost	Omezená bezpečnost ve srovnání s jinými protokoly	Preferovaný pro svou jednoduchost a širokou podporu
SOAP	Kritické služby	Vysoká úroveň bezpečnosti, transakční podpora	Složitost, větší režie	Preferovaný pro kritické a transakční služby
MQTT	Event-driven, IoT	Nízká režie, efektivní pro nízko-šířková pásma	Omezená podpora pro složitější operace	Preferovaný pro IoT a event-driven architekturu
AMQP	Messaging	Spolehlivost, škálovatelnost	Komplexita implementace	Preferovaný pro spolehlivý a škálovatelný messaging
OData	Data, API	Standardizace, jednoduchý přístup k datům	Omezená funkčnost ve srovnání s plně funkčními API	Preferovaný pro transparentní správu dat
RFC/BAPI	SAP integrace	Efektivní volání SAP funkcí	Specifické pro SAP	Preferovaný pro spolehlivou integraci SAP
IDoc	EDI, SAP integrace	Robustní, vhodné pro velké objemy dat	Specifické pro SAP, složitost	Preferovaný pro EDI a integraci SAP
WebSocket	Real-time komunikace	Obousměrná komunikace, nízká latence	Omezená bezpečnost	Preferovaný pro real-time aplikace
gRPC	Mikroservisy	Vysoký výkon, nízká latence	Menší podpora ve srovnání s HTTP	Preferovaný pro výkonné komunikace mikroservis
FTP/SFTP	Přenos souborů	Jednoduchost, široká podpora	Zastaralost (FTP), bezpečnostní rizika (FTP)	Preferovaný (SFTP) pro bezpečný přenos souborů, FTP je nepreferovaný kvůli bezpečnostním rizikům
JMS	Messaging	Spolehlivost, asynchronní komunikace	Komplexita, omezená podpora	Preferovaný pro robustní messagingové potřeby
SMTP	Email	Široká podpora, standardní pro email	Zastaralost, omezená bezpečnost	Nepreferovaný pro datové a aplikační integrace kvůli zastaralosti
CORBA	Distribuované aplikace	Jazyková nezávislost, robustnost	Komplexita, zastaralost, velká režie	Nepreferovaný kvůli zastaralosti a komplexitě
RMI	Java aplikace	Efektivní pro Java, jednoduchost	Omezené na Java, bezpečnostní rizika	Nepreferovaný kvůli omezené použitelnosti mimo Java a bezpečnostním rizikům
Telnet	Vzdálená správa	Široká podpora	Velmi slabá bezpečnost (nešifrované)	Nepreferovaný kvůli vážným bezpečnostním rizikům

XMPP	Real-time komunikace	Široká podpora, rozšiřitelnost	Omezená škálovatelnost, bezpečnostní problémy	Nepreferovaný kvůli omezené škálovatelnosti a bezpečnostním problémům

Tabulka poskytuje přehled preferovaných a nepreferovaných protokolů pro integrační architekturu naší organizace, zdůvodňuje jejich použití a vyzdvihuje klíčové výhody a nevýhody. Protokoly jako REST/HTTP, SOAP, MQTT, AMQP a další jsou preferovány pro svou robustnost, flexibilitu a bezpečnost. Naopak protokoly jako FTP (nešifrované), SMTP, CORBA, RMI, Telnet a XMPP jsou nepreferované kvůli jejich zastaralosti, bezpečnostním rizikům nebo omezené funkčnosti.

7 Datové formáty

V rámci organizace je klíčové zajistit efektivní, bezpečnou a interoperabilní výměnu dat mezi různými informačními systémy a platformami. Výběr vhodných datových formátů hraje zásadní roli při dosahování těchto cílů. Datový formát určuje způsob, jakým jsou informace strukturovány a jakým způsobem mohou být přenášeny a zpracovávány mezi různými systémy. V této části se zaměříme na nejčastěji používané datové formáty, jejich typické použití, výhody, nevýhody a důvody, proč jsou preferovány nebo nepreferovány v naší organizaci, se zvláštním důrazem na bezpečnostní aspekty. Kromě toho uvádíme níže v tabulce i formáty, které jsou z bezpečnostních nebo jiných důvodů nevhodné a v podstatě zakázané.

Tabulka datových formátů

Formát	Použití	Výhody	Nevýhody	Důvod Preference/Nepreference
REST/HTTPS	Aplikační, datové	Jednoduchost, široká podpora, škálovatelnost	Omezená bezpečnost ve srovnání s jinými protokoly	Preferovaný pro svou jednoduchost a širokou podporu
JSON (JavaScript Object Notation)	Webové API, konfigurace, mobilní aplikace	Jednoduchost, čitelnost, podpora v moderních programovacích jazycích	Není vhodný pro složité datové struktury, bez schématu	Preferován pro svou jednoduchost a širokou podporu, bezpečnostní riziko lze mitigovat validací a šifrováním
XML (eXtensible Markup Language)	Webové služby, dokumenty, datová výměna mezi systémy	Flexibilita, podporuje složité datové struktury, možnost validace pomocí XSD	Verbóznost, vyšší nároky na výkon	Preferován pro komplexní strukturovaná data, bezpečnost lze zlepšit pomocí šifrování a podpisů
CSV (Comma-Separated Values)	Export/import dat, tabulkové aplikace	Jednoduchost, široká podpora v aplikacích	Omezená strukturovanost, citlivost na formátování	Preferován pro jednoduchou tabulkovou data, nepreferován pro složité struktury, bezpečnostní riziko při přenosu nešifrovaných dat
YAML (YAML Ain't Markup Language)	Konfigurace, data pro DevOps nástroje	Čitelnost, jednoduchost, podpora komplexních datových struktur	Méně robustní než XML, obtížnější validace	Preferován pro konfigurace a čitelnost, nepreferován pro kritická data kvůli chybějícímu schématu a validaci
EDIFACT (Electronic Data Interchange for Administration, Commerce and Transport)	EDI v obchodních a státních systémech	Standardizace, spolehlivost, široká akceptace v EDI	Složitost, náročná implementace	Preferován pro standardizované obchodní procesy, bezpečnostní riziko lze řešit šifrováním EDI zpráv
Plain Text (neformátovaný text)	Základní komunikace, logy	Jednoduchost, univerzální čitelnost	Žádná strukturovanost, vysoké riziko chyb	Zakázán pro přenos citlivých dat, protože postrádá jakoukoliv formu zabezpečení a struktury

HTML (HyperText Markup Language)	Webové stránky, obsah dokumentů	Flexibilita, široká podpora v prohlížečích	Neefektivní pro strukturovaná data, riziko XSS útoků	Zakázán pro datovou výměnu kvůli bezpečnostním rizikům a nevhodnosti pro strukturovaná data
Proprietární Formáty (např. specifické formáty určitého softwaru)	Specifické aplikace	Optimalizace pro konkrétní software	Omezená interoperabilita, závislost na konkrétním dodavateli	Zakázány kvůli uzamčení na jednoho dodavatele a nízké interoperabilitě, což zvyšuje riziko vendor lock-in

Tabulka níže poskytuje přehled jednotlivých datových formátů, jejich specifické použití, výhody a nevýhody, a důvody preference či nepreference v kontextu naší organizace.

8 Metody

Metody integrací se liší v závislosti na povaze dat, četnosti výměny, úrovni transformace dat a typu architektury integrace dat. Metody primárně využívané naší organizací lze rozdělit na tyto čtyři základní:

- **ETL - extract, transform, load** – je běžnou metodou pro dávkové/hromadné zpracování velkých objemů strukturovaných nebo částečně strukturovaných dat
- **ELT extract, load, transform** – je podobná ETL, ale transformace se provádí až po načtení do cílového místa určení
- **CDC - change data capture** – zachycuje a přenáší pouze změny ve zdrojových datech a je užitečná pro integraci v reálném čase nebo téměř v reálném čase
- **Virtualizace dat** – vytváří virtuální vrstvu, která integruje data z různých zdrojů, aniž by je fyzicky přesouvala nebo ukládala, tato metoda poskytuje jednotný pohled na data a je vhodná pro komplexní a heterogenní datová prostředí

9 Dokumentace integračních scénářů

V naší organizaci je dokumentace integračních scénářů klíčovým nástrojem pro zajištění přehlednosti a konzistence v rámci všech integračních aktivit. Pro tento účel používáme standardizovaný dokument s názvem Integrační specifikace, který obsahuje veškeré potřebné informace k pochopení, implementaci a konfiguraci konkrétního integračního scénáře. Tento dokument slouží jako detailní blueprint pro všechny zúčastněné strany.

9.1.1.1 Integrační specifikace zahrnuje primárně:

- Stručný popis integračního scénáře, jeho účel a přínosy.
- Název integračního scénáře přidělený dle katalogu Integračních scénářů a zavedené jmenné konvence, což zajišťuje konzistenci a snadnou identifikaci.
- Popis technologií, protokolů a datových formátů použitých v integraci.
- Detailní popis procesních a datových toků, které jsou součástí integračního scénáře.
- Specifikace bezpečnostních opatření, jako je šifrování, autentizace a autorizace.

Kromě textového popisu využíváme modelovací jazyky, jako je Archimate v poslední platné verzi, pro vizualizaci integračních scénářů. Tyto modely poskytují grafický přehled o architektuře, komponentách a vztazích mezi nimi, což usnadňuje pochopení komplexních integrací.

9.1.1.2 Další používané modelovací jazyky zahrnují:

- UML (Unified Modeling Language) - Pro vytváření diagramů tříd, sekvencí a aktivit, které detailně popisují jednotlivé části integračního scénáře.

- BPMN (Business Process Model and Notation) - Pro modelování procesů organizace a jejich interakcí v rámci integračních scénářů.

Integrace jsou v naší organizaci také popsány v katalogu Integračních scénářů, který obsahuje všechny aktuální a historické integrační scénáře s příslušnými metadaty. Tento katalog je pravidelně aktualizován a slouží jako centrální zdroj informací pro všechny týmy zapojené do integračních projektů.

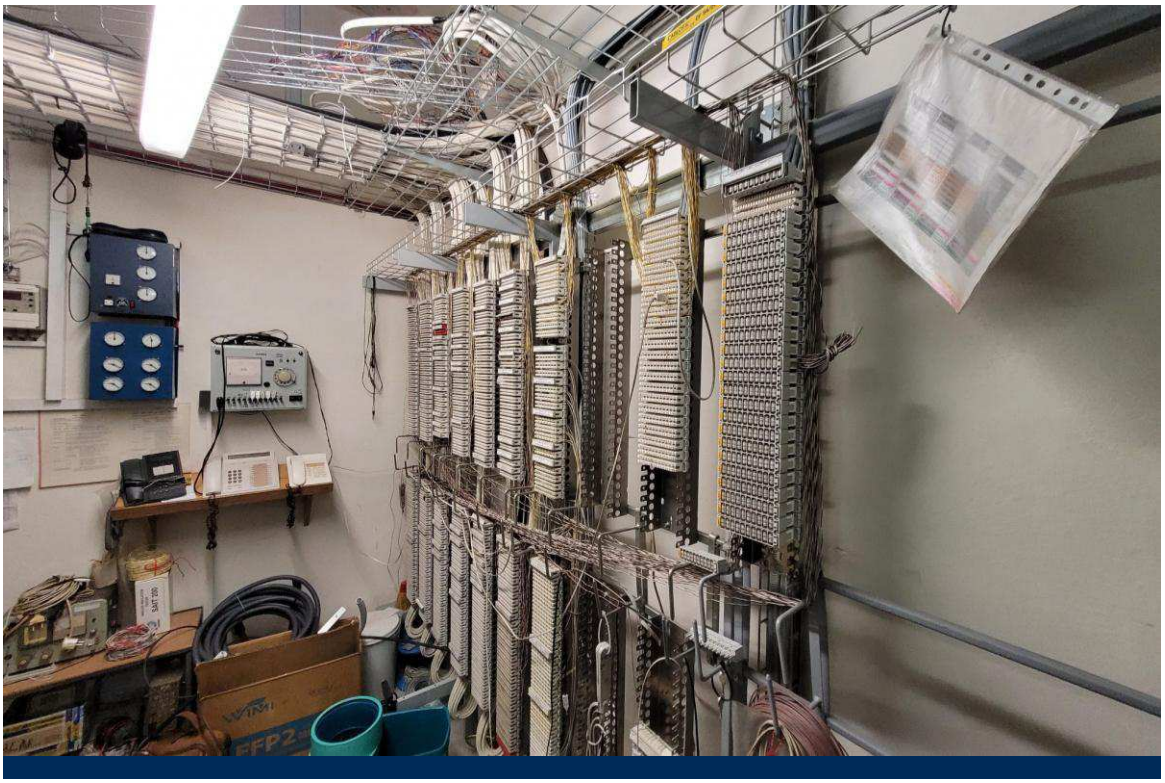
Dokumentace integračních scénářů je důkladně verifikována a validována, aby byla zajištěna její přesnost a úplnost. To zahrnuje revize od technických odborníků, bezpečnostních specialistů a dalších relevantních stakeholderů. Tento proces zajišťuje, že všechny integrační aktivity jsou prováděny konzistentně, efektivně a bezpečně.

10 Řízení integračních scénářů

Jakékoliv nové Integrační scénáře, či změny Integračních scénářů musí projít skrze Architecture Board nebo Change managment a být posouzeny v širším kontextu. Skrze jaký proces bude integrační scénář posuzován určí matice, která zahrnuje posouzení složitosti změny a její dopady. Integrační scénář následně bude nově zaevidován do katalogu Integračních scénářů nebo proběhne aktualizace u již existujícího.

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

Datum tisku
2025-07-30



Platforma SŽ Komunikační standardy

Červen 2025

Obsah

Seznam zkratek

API	Komplexně definované komunikační rozhraní aplikace *(Application Programming Inteface)*
APN	Virtuální vyhrazená část mobilní datové sítě. Nejedná se tak o mobilní připojení k Internetu, ale k lokální síti daného zákazníka mobilního operátora.
CPS	Centrální poštovní systém Správy železnic
ICT	Informační a komunikační technologie *(Information and Communication Technology)*
O27	Odbor komunikace GŘ SŽ
SAP	Modulární ERP systém od německé firmy SAP AG
SMS	Krátká textová zpráva *(Short Message Service)*
SMTP	Základní síťový protokol pro přenos elektronické pošty *(Simple Mail Transfer Protocol)*
SŽ	Správa železnic, státní organizace
SŽT	Správa železničních informačních technologií
UAS	Logická uživatelsko-aplikační síť SŽ, zahrnuje VRF v MPLS sítích a lokální VLAN, běžně se nazývá také „Intranet SŽ“
VPN	Virtuální privátní síť *(Virtual Private Network)*

Seznam vysvětlivek

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

1 Úvod

Cílem této přílohy Platformy SŽ je popsat podporovaných komunikačních služeb a technologií, které lze v rámci Platformy SŽ využít a současně definuje služby, zařízení a technologie, které není možné z důvodu duplicity v rámci navrhovaných řešení dodávat do ICT prostředí Správy železnic.

2 Komunikační služby

Platforma Správy železnic definuje základní komunikační služby, které lze v rámci aplikací a informačních systémů využívat primárně technické notifikace. Použití k jiným účelům (například pro marketingové účely nebo komunikaci s veřejností) je možná jen po předchozím schválení ze strany Správy železnic, a to minimálně ze strany SŽT a O27.

3 SMS brána

SMS je negarantovaná služba telekomunikačních operátorů. Garantován není čas doručení ani samotné doručení SMS zprávy vůbec. SMS brána je aplikace instalovaná v prostředí SŽ napojená přímo na telekomunikačního operátora. Nejedná se tedy o použití koncového zařízení přihlášeného do veřejné mobilní telefonní sítě.

SMS brána umožňuje obousměrnou komunikaci, to znamená odesílání SMS zpráv definovaným příjemcům a příjem odpovědí na odeslané zprávy. Stejně tak umožňuje evidenci (logování) doručenek zpráv. Komunikaci se SMS bránou zajišťuje jednoduché API rozhraní popsané v implementačním manuálu.

Službu SMS brány lze využít jen pro aplikace a informační systémy umístěné v ICT prostředí Správy železnic a to pouze v UAS.

4 Emailová komunikace

Pro navrhovaná řešení, pokud je součástí i emailová komunikace, poskytuje službu emailového serveru pro odchozí poštu. je pro aplikace odpůrné služby standardně poskytované k využití pro dodávaná ICT řešení.

4.1 Z uživatelsko-aplikační sítě

Z UAS je služba odesílání emailových zpráv zprostředkována takto:

- Nešifrovaně přes CPS a jeho Open-Relay SMTP servery umístěné ve vnitřní síti
- Šifrovaně přes služby MS Exchange

4.2 Z technologických datových sítí

Z technologických datových sítí není v současné době služba odesílání elektronické pošty podporováno.

4.3 Z externích sítí Správy železnic

Z externích sítí a připojení Správy železnic (VPN a APN) není služba odesílání emailových zpráv dostupná.

4.4 Mimo sítě Správy železnic

Odesílání emailové komunikace z vnějších sítí mimo perimetr Správy železnic (například SAP Cloud, MS Azure atp.) není v současné době možné.

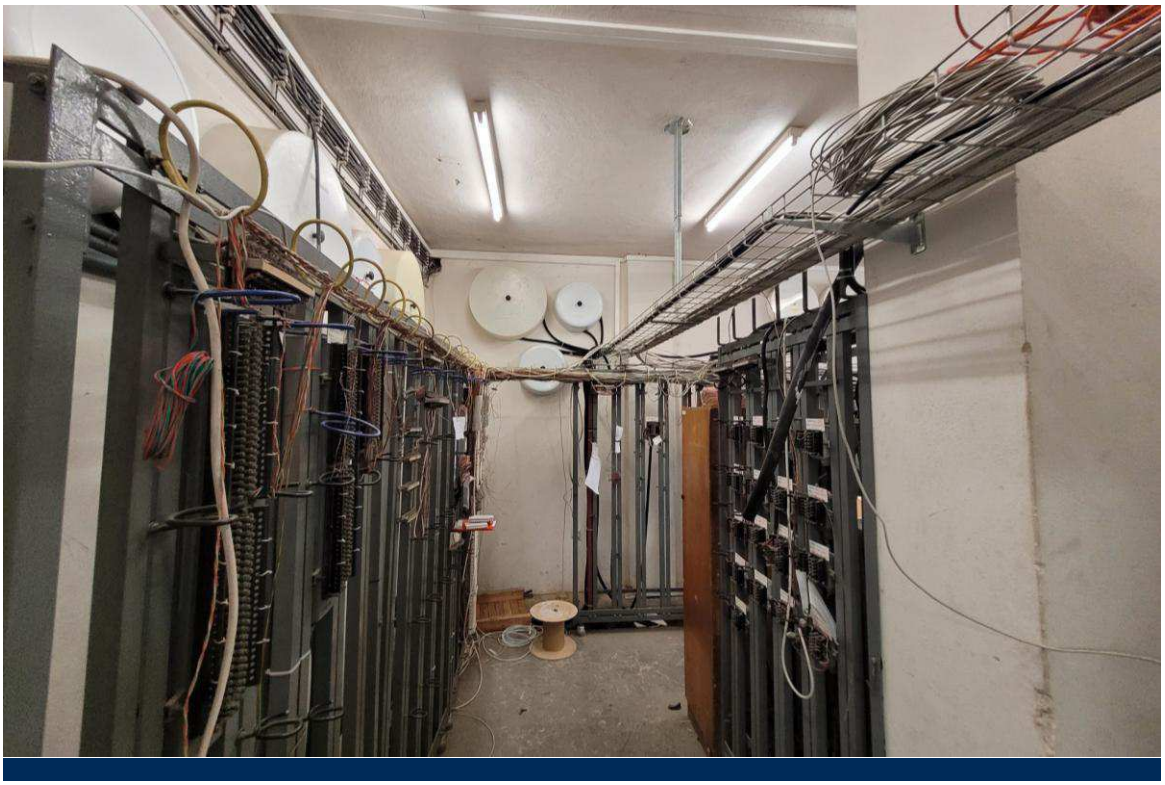
Pro tuto službu je nutné využít lokálních SMTP služeb s omezením, že z technických a bezpečnostních důvodů nelze takto odesílat emaily z domén Správy železnic.

5 Komunikační platforma dispečerských pracovišť

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

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

Datum tisku
2025-07-30



Platforma SŽ Standardy zálohování a disaster recovery

Červen 2025

Obsah

Seznam zkratek

DB	Databázová aplikace *(Database Engine)*
DR	Plán obnovy po havárii, součást kontinuity IT služeb *(Disaster Recovery)*
IBM	Americká technologická společnost *(International Business Machines)*
ICT	Informační a komunikační technologie *(Information and Communication Technology)*
LTO	Otevřený formát magnetické pásky určené pro záznam velkých objemů dat *(Linear Tape Open)*
MSSQL	Databázový server od firmy Microsoft *(Microsoft SQL Server)*
OS	Operační systém *(Operating System)*
SQL	Standardní jazyk pro manipulaci s relačními databázemi. SQL umožňuje ukládat, manipulovat a vyhledávat data v relačních databázích. SQL je založeno na dotazech (queries) na data v databázích. Dotazy lze pak definovat a modifikovat strukturu databází, vytvářet a upravovat tabulky, indexy a další prvky, vkládat a aktualizovat data, mazat data a další operace. SQL je nezávislý na platformě, což znamená, že může být použit na různých operačních systémech a s různými databázovými systémy, avšak každá databázová platforma může mít různé změny v syntaxi *(Structured Query Language)*
SŽ	Správa železnic, státní organizace
TSM	Nástroj pro zálohování, v současné době již nese název IBM Storage Protect *(Tivoli Storage Manager)*
UAS	Logická uživatelsko-aplikační síť SŽ, zahrnuje VRF v MPLS sítích a lokální VLAN, běžně se nazývá také „Intranet SŽ“

Seznam vysvětlivek

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

1 Úvod

Cílem této části Platformy SŽ je popis podporovaných služeb, technologií, a architektonických principů v oblasti zálohování a disaster recovery v ICT prostředí Správy železnic.

2 Služby zálohování

Služba zálohování ICT prostředí Správy železnic je zajištěna technologií IBM Storage Protect (dříve známý jako IBM Spectrum Protect nebo TSM). Jedná se o komplexní řešení pro fyzické fileservery, virtualizovaná prostředí a širokou škálu aplikací. IBM Storage Protect zálohuje data především s využitím technologie VMware Snapshot. Služba zálohování je dostupná v současné době jen v UAS.

Služba zálohování umožňuje 3 základní typy zálohování:

- Snapshot disku pro dosažení rychlé obnovy celého OS v Crash Consistent stavu včetně aplikační konfigurace. Zpravidla je takto zálohován pouze systémový oddíl virtualizovaného serveru. Záloha probíhá jednou denně a retence je nastavena na 30 posledních verzí.
- Záloha datových svazků připojených k jednotlivým serverům, pro dosažení maximální možné odolnosti proti náhodnému smazání či poškození apod. Záloha probíhá jednou denně, kdy se uchovává 90 posledních verzí souborů a poslední smazaná verze souboru je uchovávána 365 dní.
- Zálohy databází Oracle nebo MSSQL pomocí agentů. Záloha probíhá dvakrát denně. Přes den jsou zálohovány transakční logy databází, v noci pak vlastní databáze. Retence je nastavena na 60 posledních verzí.

Zálohy jsou řešeny lokálním backup serverem u každé virtualizační farmy, odkud jsou poté přenášeny do DR lokality a v rámci řešení offline záloh (pro další zvýšení odolnosti proti ztrátě dat) jsou zálohy dále ukládány na LTO pásky v páskové knihovně umístěné v DR lokalitě.

3 Řešení Disaster recovery

V rámci UAS byla jako DR lokalita určen objekt *Praha U2*, kam jsou pravidelně přenášeny zálohy ze všech lokálních backup serverů.

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

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

Datum tisku
2025-07-30

Platforma SŽ Cloudové prostředí

Červen 2025

Obsah

Seznam zkratek

AAD	Služba AD provozovaná v cloudovém prostředí MS Azure. Nový název služby je „MS EntraID“ *(Azure Active Directory)*
AD	Rozšiřitelná a škálovatelná adresářová služba, která umožňuje efektivně uspořádat síťové prostředky. Kromě informací o objektech v počítačové síti (uživatelské účty, počítače, tiskárny) umožňuje používat stromovou strukturu objektů, nastavovat globálně systémové politiky, instalovat programy na počítače nebo aplikovat kritické aktualizace v celé organizační struktuře. Má úzkou vazbu na DNS *(Active Directory)*
AWS	Cloudové prostředí firmy Amazon *(Amazon Web Services)*
DNS	Distribuovaný hierarchický jmenný systém používaný v síti Internet. Překládá názvy domén na číselné IP adresy a zpět, obsahuje informace o tom, které stroje poskytují příslušnou službu *(Domain Name System)*
ERP	Informační systém pro řízení podniku, který integruje různé oblasti podnikání, jako je například finanční řízení, řízení zásob, výroby, prodeje, nákupu a personálního řízení. Cílem je poskytovat podnikovým uživatelům přehled o celkových aktivitách a umožňovat efektivní a koordinované řízení všech procesů v rámci podniku *(Enterprise Resource Planning)*
IaaS	Typ cloudové služby, který poskytuje zákazníkům základní IT infrastrukturu jako službu, včetně serverů, úložiště, sítě a virtuálních počítačů. Tyto služby se často poskytují prostřednictvím Internetu a umožňují zákazníkům snadno a rychle využívat IT infrastrukturu bez nutnosti jejího nákupu, instalace a správy. Mezi nejznámější poskytovatele IaaS patří Amazon Web Services, Microsoft Azure a Google Cloud Platform *(Infrastructure as a Service)*
ICT	Informační a komunikační technologie *(Information and Communication Technology)*
IP	Jeden ze základních komunikačních protokolů používaných v počítačových sítích *(Internet Protocol)*
IT	Informační technologie *(Information Technology)*
M365	Globální označení služeb společnosti Microsoft, umožňující licencování jejich produktů a provoz aplikací, a to ať už jako on-premise řešení, či v cloudovém prostředí *(Microsoft 365)*
MS	Microsoft Corporation, americký výrobce především SW a provozovatel cloudového prostředí MS Azure
PaaS	Typ cloudové služby, která poskytuje vývojářům a IT týmům platformu pro vývoj, nasazení a správu aplikací bez nutnosti starat se o správu hardwaru a infrastruktury. Poskytovatelé PaaS nabízejí vývojové nástroje, databáze, síťové služby a další nástroje jako služby, což umožňuje vývojářům se soustředit pouze na vývoj aplikace *(Platform as a Service)*
SaaS	Model poskytování software, kdy je software hostován v cloudovém prostředí a poskytován uživatelům přes Internet. Tyto služby jsou poskytovány vývojáři software jako služby a účtovány jsou za používání (pay-as-you-go). To umožňuje uživatelům využívat software bez nutnosti investovat do hardware a IT infrastruktury *(Software as a Service)*
SAP	Modulární ERP systém od německé firmy SAP AG
SSO	Metoda jednotného přihlášení *(Single Sign-On)*
SW	Software je sada všech počítačových programů používaných v počítači, které provádějí nějakou činnost
SŽ	Správa železnic, státní organizace
SŽT	Správa železničních informačních technologií

Seznam vysvětlivek

MS Azure	Cloudové prostředí firmy Microsoft.
MS EntraID	Služba AD provozovaná v cloudovém prostředí MS Azure.
Platforma SŽ	Soubor dokumentů, rozdělený na veřejnou, interní a metodickou část, určený pro seznámení dodavatelů s ICT prostředím SŽ a současně s používanými standardy a technologiemi.
Tenant	Dedikovaný virtuální prostor v cloudovém prostředí MS Azure

1 Úvod

Cílem této části Platformy SŽ je popis podporovaných cloudových služeb, technologií, a architektonických principů v rámci tenantu provozovaného Správou železnic v cloudovém prostředí.

Důvodem je zajistit ve fázích přípravy poptávky, návrhu ICT řešení a realizace dodávky kompatibilitu se stávajícím cloudovým prostředím Správy železnic a umožnit využití pro aplikace, které splňují podmínky pro umístění v cloudovém prostředí.

2 Cloudové prostředí

U aplikací a informačních systémů, kde je to z technických a bezpečnostních důvodů možné, adoptuje Správa železnic moderní technologie včetně cloudového prostředí. S ohledem na vysoké zastoupení kritické informační infrastruktury v portfoliu Správy železnic je tento proces řízen přísnou metodikou.

V současnosti využívá Správa železnic cloudová prostředí na platformách Microsoft Azure, Amazon AWS, SAP HANA Cloud a Oracle Cloud Infrastructure, která podporují různé typy cloudových služeb:

- IaaS – infrastruktura jako služba
- PaaS – platforma jako služba
- SaaS – software jako služba

V rámci Platformy SŽ pak nabízí výhradně SaaS na platformě MS Azure, jelikož ostatní cloudová prostředí jsou v případě SŽ úzce svázána s konkrétními informačními systémy.

2.1 Microsoft Entra ID

Správa železnic provozuje ve svém ICT prostředí službu Active Directory a spolu s příchodem cloudového prostředí ho rozšířila i tam, dříve pod názvem Azure Active Directory, dnes Microsoft Entra ID.

2.2 Služby M365

Správa železnic využívá velkou část portfolia SaaS služeb poskytovaných na platformě MS Azure pod názvem M365.

3 Cloudové služby

V rámci svého v současnosti používaného cloudového prostředí na platformě Microsoft Azure jsou Platformou SŽ poskytovány následující služby.

3.1 Služba ověření proti Microsoft Entra ID

Zejména u aplikací jejichž uživatelé se pohybují mimo interní sítě Správy železnic je k dispozici služba Microsoft Entra ID. Ověřování proti Microsoft Entra ID přináší vyšší bezpečnost a pohodlí uživatelů i pomocí jednotného přihlašování (SSO).

3.2 Integrace s M365

Pokud u informačního systému či aplikace předpokládá Dodavatel jakoukoli integraci s aplikacemi z rodiny M365, je nutné využít tenant Správy železnic.

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

Datum tisku
2025-07-30

Příloha č. 13 Výzvy k podání nabídky

DOHODA O OCHRANĚ DŮVĚRNÝCH INFORMACÍ

k veřejné zakázce:

„Zavedení komplexního síťového řešení prevence úniku dat (DLP) pro non-Microsoft systémy v prostředí Správy železnic"

Smluvní strany:

Správa železnic, státní organizace

se sídlem: Dlážděná 1003/7, 110 00 Praha 1

IČO: 70994234, DIČ: CZ70994234

zastoupená: **Ing. Daliborem Fajkusem,** ředitelem organizační jednotky Správa železniční telematiky

(dále jen „**Zadavatel**")

a

[DOPLNÍ DODAVATEL]

se sídlem: [DOPLNÍ DODAVATEL]

IČO: [DOPLNÍ DODAVATEL], DIČ: [DOPLNÍ DODAVATEL]

společnost zapsaná v obchodním rejstříku vedeném [DOPLNÍ DODAVATEL] soudem v [DOPLNÍ DODAVATEL]

oddíl [DOPLNÍ DODAVATEL], vložka [DOPLNÍ DODAVATEL]

zastoupená: [DOPLNÍ DODAVATEL]

(dále jen „**Dodavatel**")

(společně také jako „**Strany**")

níže uvedeného dne uzavřely tuto dohodu v souladu s ustanovením § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku, v platném znění (dále jen „**Občanský zákoník**")

(dále jen „**Dohoda**")

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

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

1. ÚČEL DOHODY

1.1 Zadavatel zadává veřejnou zakázku jako podlimitní sektorovou veřejnou zakázku s názvem „Zavedení komplexního síťového řešení prevence úniku dat (DLP) pro non-Microsoft systémy v prostředí Správy železnic" č. j. 80219/2025-SŽ-GŘ-O25 (dále jen „**Veřejná zakázka**") mimo režim zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**"). Dodavatel s úmyslem účastnit se výběrového řízení na zadání Veřejné zakázky požaduje vydání části zadávací dokumentace, resp. Výzvy k podání nabídky, a to konkrétně Přílohy č. 7 Výzvy k podání nabídky s názvem „Popis prostředí", která tvoří Přílohu č. 1 této Dohody, Přílohy č. 8 Výzvy k podání nabídky s názvem „Informace k systémům SŽ", která tvoří Přílohu č. 2 této dohody, Přílohy č. 9 Výzvy k podání nabídky s názvem "Interní předpis Zadavatele – Politika klasifikace aktiv", která tvoří Přílohu č. 3 této dohody, a Přílohy č. 14 Výzvy k podání nabídky s názvem "Interní předpis Zadavatele - Provozní politika prvků v působnosti systému řízení bezpečnosti informací", která tvoří Přílohu č. 4 této dohody a které obsahují informace, jež Zadavatel považuje za důvěrné a vyžaduje jejich ochranu (dále jen „**Důvěrné informace**"). Z tohoto důvodu uzavírají Strany tuto Dohodu, která upravuje pravidla pro nakládání s Důvěrnými informacemi převzatými Dodavatelem.

2. PŘEDMĚT DOHODY

2.1 Veškeré informace uvedené v Příloze č. 1, č. 2, č. 3 a č. 4 této Dohody, jsou považovány za Důvěrné informace, jejichž použití podléhá této Dohodě.

2.2 Dodavatel se zavazuje, že Důvěrné informace dle této Dohody použije pouze způsobem a k účelu v této Dohodě stanoveným.

3. UŽITÍ DŮVĚRNÝCH INFORMACÍ

3.1 Dodavatel je oprávněn Důvěrné informace užít jen pro účely své účasti ve výběrovém řízení na zadání Veřejné zakázky a dále při jejím případném plnění.

3.2 Dodavatel se zavazuje zachovat důvěrnost Důvěrných informací a nezpřístupnit je žádné třetí osobě.

3.3 Svým zaměstnancům a orgánům je Dodavatel oprávněn Důvěrné informace zpřístupnit jen v rozsahu, v jakém je pro danou osobu nezbytně nutné se s Důvěrnými informacemi seznámit pro účely účasti Dodavatele ve výběrovém řízení na zadání Veřejné zakázky nebo případně jejího plnění. Tyto osoby musí být poučeny o důvěrném charakteru předávaných informací a v rozsahu odpovídajícím této Dohodě zavázány k mlčenlivosti.

3.4 Dodavatel je oprávněn zpřístupnit Důvěrné informace jiným třetím osobám jen s předchozím písemným souhlasem Zadavatele, anebo při splnění podmínek uvedených v článku 3.5 této Dohody.

3.5 Po doručení této podepsané Dohody ze strany Dodavatele Zadavateli prostřednictvím elektronického nástroje E-ZAK, bude ve lhůtě analogicky dle § 96 odst. 2 ZZVZ předán Dodavateli přístupový údaj k Důvěrným informacím – heslo k neveřejné části zadávací dokumentace, resp. Výzvy k podání nabídek k Veřejné zakázce, a to formou SMS zprávy zaslané na číslo určené Dodavatelem. Obdrží-li Dodavatel heslo, potvrdí tuto skutečnost odesláním takové zprávy zpět na číslo, z kterého heslo obdržel. Neobdrží-li Dodavatel předmětné heslo ve lhůtě 48 hodin

od odeslání podepsané Dohody Zadavateli, obrátí se na Zadavatele prostřednictvím elektronického nástroje E-ZAK s tím, že heslo neobdržel. Nebude-li z jakéhokoli důvodu technicky možné heslo předat předvídaným způsobem, mohou Smluvní strany dohodnout jiný způsob předání hesla, ten však jasně zdokumentují a provedou tak, aby nedošlo k narušení zásad zadávání Veřejné zakázky ve smyslu § 6 ZZVZ.

3.6 Dodavatel určuje jako osobu pro obdržení a správu hesla k neveřejné části zadávací dokumentace, resp. Výzvy k podání nabídek osobu: JMÉNO A PŘÍJMENÍ. Tato osoba je oprávněna jednat za Dodavatele. Telefonní číslo, na které má být heslo zasláno je: DOPLNÍ DODAVATEL. Dodavatel se zavazuje, že uvedené telefonní číslo je telefonním číslem osoby uvedené v tomto článku.

4. PODDODAVATELÉ

4.1 Pokud Dodavatel zvažuje spolupracovat při přípravě nabídky na realizaci Veřejné zakázky a/nebo při eventuálním plnění Veřejné zakázky Dodavatelem se třetími osobami, zavazuje se sdílet s těmito osobami (dále jen „**Poddodavatelé**“) Důvěrné informace jen v souladu s tímto článkem 3.5 této Dohody.

4.2 Za Poddodavatele se považuje jakákoliv třetí osoba spolupracující s Dodavatelem dle odst. 4.1 bez ohledu na to, zda:

4.2.1 spolupráce probíhá v rámci konsorcia Dodavatele a takovéto třetí osoby, jehož členové odpovídají Zadavateli společně a nerozdílně, nebo

4.2.2 spolupráce je založena na poddodavatelském vztahu takovéto třetí osoby vůči Dodavateli, nebo

4.2.3 spolupráce je založena na poddodavatelském vztahu Dodavatele vůči takovéto třetí osobě, nebo

4.2.4 Dodavatel a třetí osoba zvolili eventuální jinou formu spolupráce.

4.3 Za Poddodavatele se považují i zajišťovny a další pojistitelé poskytující Dodavateli zajištění pro účely plnění veřejné zakázky.

4.4 Dodavatel je oprávněn sdílet Důvěrné informace s Poddodavateli pouze za předpokladu, že jsou vázáni mlčenlivostí minimálně v rozsahu dle této Dohody.

5. SPLNĚNÍ ÚČELU DOHODY

5.1 Dodavatel se zavazuje, že Důvěrné informace, přístupové údaje k Důvěrným informacím a rovněž jakékoliv kopie Důvěrných informací, které v souvislosti s plněním předmětu a účelu této Dohody pořídil, znehodnotí tak, že informace nebudou dále zobrazitelné, použitelné ani obnovitelné, a to bezodkladně po:

5.1.1 uplynutí lhůty pro podání nabídek do výběrového řízení na zadání Veřejné zakázky, nepodal-li nabídku před jejím uplynutím;

5.1.2 skončení účasti Dodavatele ve výběrovém řízení na zadání Veřejné zakázky nebo ukončení výběrového řízení, pokud s ním nebyla uzavřena smlouvy na plnění Veřejné zakázky;

5.1.3 nebo po doručení písemné výzvy Zadavatele.

6. PORUŠENÍ POVINNOSTÍ

6.1 Poruší-li Poddodavatel dohodu uzavřenou s Dodavatelem nebo Zadavatelem na základě odst. 4.4 této Dohody a Zadavateli v důsledku toho vznikne škoda, Dodavatel za takto vzniklou škodu odpovídá.

6.2 Za každé jednotlivé porušení povinnosti Dodavatele uvedené v článku 3 této Dohody nebo povinnosti dle odst. 4.4 této Dohody, má Zadavatel právo požadovat zaplacení smluvní pokuty ze strany Dodavatele ve výši 500.000 Kč (slovy: pět set tisíc korun českých). Za porušení těchto povinností Dodavatele se nepovažuje nakládání s Důvěrnými informacemi, které jsou veřejně známé nebo se staly veřejně známými bez porušení této Dohody, a dále poskytnutí Důvěrných informací na základě právních předpisů či vykonatelného rozhodnutí soudu nebo jiného orgánu veřejné moci.

6.3 Povinnost Dodavatele zaplatit smluvní pokutu dle této Dohody se nedotýká nároku Zadavatele na náhradu škody způsobené porušením povinnosti, které ke vzniku nároku na smluvní pokutu vedlo, a to v plné výši.

7. ZÁVĚREČNÁ USTANOVENÍ

7.1 Povinnost chránit Důvěrné informace zavazuje Dodavatele bez ohledu na případné ukončení této Dohody po dobu pěti (5) let od uzavření této Dohody. Ustanovení o odpovědnosti a smluvních pokutách se uplatní také v případě porušení povinnosti chránit Důvěrné informace dle předchozí věty.

7.2 Tuto Dohodu je možné měnit pouze písemnou dohodou Stran ve formě číslovaných dodatků k této Dohodě, podepsaných za každou Stranu osobou nebo osobami oprávněnými zastupovat tuto Stranu.

7.3 Veškerá práva a povinnosti vyplývající z této Dohody přecházejí, pokud to povaha těchto práv a povinností nevylučuje, na právní nástupce Stran.

7.4 Nedílnou součást Dohody tvoří tyto přílohy:

Příloha č. 1: Dokument obsahující Důvěrné informace (tj. „Popis prostředí")

Příloha č. 2: Dokument obsahující Důvěrné informace (tj. „Informace k systémům SŽ")

Příloha č. 3: Dokument obsahující Důvěrné informace (tj. "Interní předpis Zadavatele – Politika klasifikace aktiv")

Příloha č. 4 Dokument obsahující Důvěrné informace (tj. "Interní předpis Zadavatele - Provozní politika prvků v působnosti systému řízení bezpečnosti informací")

7.5 Tato Dohoda je vyhotovena v elektronické podobě, přičemž obě Strany obdrží její elektronický originál opatřený elektronickými podpisy. V případě, že tato Dohoda z jakéhokoli důvodu nebude vyhotovena v elektronické podobě, bude sepsána ve třech (3) stejnopisech, z nichž Zadavatel obdrží dvě (2) vyhotovení a Dodavatel obdrží jedno (1) Vyhotovení.

Strany prohlašují, že si tuto Dohodu přečetly, že s jejím obsahem souhlasí a na důkaz toho k ní připojují svoje podpisy.

Za Zadavatele	**Za Dodavatele**
V Praze, dne _____	V [DOPLNÍ DODAVATEL], dne [DOPLNÍ DODAVATEL]
.....	.....
Správa železnic, státní organizace	**[DOPLNÍ DODAVATEL]**
Ing. Dalibor Fajkus, ředitel OJ SŽT	[DOPLNÍ DODAVATEL]

SPRÁVA ŽELEZNIC

Příloha č. 1 Dohody o ochraně důvěrných informací

Dokument obsahující Důvěrné informace

Zadavatel poskytuje Dodavateli dokument obsahující Důvěrné informace, tj. Přílohu č. 7 Výzvy k podání nabídek s názvem „Popis prostředí SŽ".

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

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

Příloha č. 2 Dohody o ochraně důvěrných informací

Dokument obsahující Důvěrné informace

Zadavatel poskytuje Dodavateli dokument obsahující Důvěrné informace, tj. Přílohu č. 8 Výzvy k podání nabídek s názvem „Informace k systémům SŽ".

Příloha č. 3 Dohody o ochraně důvěrných informací

Dokument obsahující Důvěrné informace

Zadavatel poskytuje Dodavateli dokument obsahující Důvěrné informace, tj. Přílohu č. 9 Výzvy k podání nabídek s názvem „Interní předpis Zadavatele – Politika klasifikace aktiv".

Příloha č. 4 Dohody o ochraně důvěrných informací

Dokument obsahující Důvěrné informace

Zadavatel poskytuje Dodavateli dokument obsahující Důvěrné informace, tj. Přílohu č. 14 Výzvy k podání nabídek s názvem „Interní předpis Zadavatele - Provozní politika prvků v působnosti systému řízení bezpečnosti informací".

Tabulka pro vyplnění údajů pro dílčí hodnotící kritérium „Kvalita“

Účastník vyplní žlutě označná pole. Pokud daný člen týmu nedisponuje žádnou relevantní certifikací, ponechá účastník příslušné pole prázdné.

	Počet požadovaných jader CPU*	Počet požadovaných GB paměti RAM**
Vstup		

Člen Týmu	Název certifikace	
Cert. Seniorní produktový specialista 1		Certifikace k produktům Cisco FirePower nebo Palo Alto na téma konfigurace, architektura, deployment.
Cert. Seniorní produktový specialista 2		
Cert. Specialista ochrany dat a řízení rizik		

* Jedná se o celkový počet jader pro všechny požadované virtuální stroje.

** Jedná se o celkový počet GB pro paměti RAM pro všechny požadované virtuální stroje.