

Naše zn. : 65403/2025-SŽ-GR-O25

ZADÁVACÍ DOKUMENTACE

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

„Segmentace sítě“

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

Identifikační údaje Zadavatele a osoby zastupující Zadavatele:

Název: **Správa železnic, státní organizace**

Sídlo: Dlážděná 1003/7, Praha 1 – Nové Město, PSČ 110 00

IČO: 709 94 234

DIČ: CZ 70994234

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

Zastoupen: Bc. Jiřím Svobodou, MBA, generálním ředitelem

Profil Zadavatele: <https://zakazky.spravazeleznic.cz/>

1. Druh veřejné zakázky a zadávacího řízení

- 1.1. Hlavní předmět veřejné zakázky ve smyslu § 15 ZZVZ odpovídá veřejné zakázce na dodávku.
- 1.2. Zadavatel zadává veřejnou zakázku v souvislosti s výkonem své relevantní činnosti ve smyslu § 153 odst. 1. písm. f) ZZVZ. Jedná se proto o sektorovou veřejnou zakázku.
- 1.3. Veřejná zakázka je v souladu s § 56 a násl. ZZVZ zadávána jako nadlimitní sektorová veřejná zakázka na dodávky v **otevřeném řízení** ve smyslu § 3 písm. b) ZZVZ.

2. Osoby podílející se na vypracování Zadávací dokumentace

2.1. Na zpracování Zadávací dokumentace se podílely:

- 2.1.1. Zadávací dokumentace a přílohy č. 1, 3, 6, 9, 10, 11, 14, 15, 16, 18 a 19 této Zadávací dokumentace PORTOS s.r.o., advokátní kancelář, IČO: 481 18 753, se sídlem Hvězdova 1716/2b, 140 00 Praha 4.
- 2.1.2. Přílohy č. 2, 4, 5, 6, 7, 8, 12, 13 a 17 této Zadávací dokumentace – s-boost s.r.o., IČO: 046 41 574, se sídlem Na Pankráci 1683/127, Nusle (Praha 4), 140 00 Praha.

3. Výsledek předběžné tržní konzultace

3.1. Před zahájením tohoto zadávacího řízení organizoval Zadavatel ve smyslu § 33 ZZVZ jednokolovou předběžnou tržní konzultaci (dále jen „PTK“) s dodavateli, a to písemnou formou (informace o konání PTK byla uveřejněna na profilu zadavatele – viz [Veřejné zakázky - E-ZAK Správa železnic](#)). 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 Segmentace sítě (dále jen „**Pozvánka**“) a zároveň zaslal Pozvánku 12 vybraným dodavatelům přímo prostřednictvím e-mailu. Dodavatelé, kteří projeví zájem účastnit se PTK, měli Zadavateli v rámci dotazovacího kola PTK zaslat odpovědi na otázky uvedené v Příloze č. 3 Pozvánky – Otázky pro dodavatele, a informace ohledně naplnění požadavků NGFW v Příloze č. 2 Pozvánky – Požadovaná specifikace segmentačních Next Generation Firewall, a to na e-mailovou adresu: cnitptk@spravazeleznic.cz.

3.2. Dotazovacího kola PTK se zúčastnili následující dodavatelé:

3.2.1. **Altepro solutions a.s.**, IČO: 036 654 96, se sídlem Na Maninách 1092/20, 170 00 Praha 7;

3.2.2. **Clarystone s.r.o.**, IČO: 277 45 422, se sídlem Na Větrově 889, 142 00 Praha 4;

3.2.3. **ICZ.INFRA a.s.**, IČO: 618 59 117, se sídlem Na hřebenech II 1718/10, Nusle, 140 00 Praha 4;

3.2.4. **IXPERTA s.r.o.**, IČO: 275 99 523, se sídlem Lihovarská 1060/12 190 00 Praha 9;

3.2.5. **Seyfor a.s.**, IČO: 015 72 377, Drobného 555/49, Ponava, 602 00 Brno;

3.2.6. **TTC Marconi s.r.o.**, IČO: 485 91 254, Třebostická 987/5, 100 00 Praha 10 – Strašnice.

3.3. Zadavatel prostřednictvím dokumentů, které byly uveřejněny na profilu Zadavatele, seznámil dodavatele se svým záměrem realizovat veřejnou zakázku a cílem, jehož má být prostřednictvím veřejné zakázky dosaženo.

3.4. V rámci dotazovacího kola PTK Zadavatel ověřoval:

3.4.1. srozumitelnost a pochopitelnost záměru a cíle aktivity segmentace sítě,

3.4.2. technologické požadavky vycházející ze specifikace NGFW,

3.4.3. jaké jsou požadované vstupy dat od SŽ. pro návrh koncepce segmentace,

3.4.4. z jakých rolí a v jakém počtu může SŽ předpokládat složení realizačního týmu,

3.4.5. jaké další nástroje, které by mohly pomoci realizovat prvotní analýzu, zmapování síťového prostředí a v následné evidenci jejího stavu či monitoringu průběžných změn,

3.4.6. jaká SLA může nabídnout výrobce při konfiguraci klastru o dvou nodech,

3.4.7. specifikace funkcionalit IDS/IPS, které mohou být nabízeny v rámci řešení,

3.4.8. informace, zdali navržený firewall podporuje integraci s externími DLP systémy,

3.4.9. zda je podporováno řešení pro OT protokoly,

3.4.10. podpora orchestrace firewallových pravidel platformy Tufin,

3.4.11. realizovatelnost navrženého harmonogramu,

3.4.12. standardy logování, které dané zařízení splňuje, konkrétní požadavky formátu logů, podporované protokoly (např. Syslog, JSON, CEF), možnosti integrace se SIEM systémy a soulad s regulačními standardy (např. GDPR, ISO 27001, PCI-DSS),

- 3.4.13. zdali existují možnosti integrace na systémy reportingu jako například PowerBI, Grafana, či obdobné,
- 3.4.14. výši předpokládané hodnoty pro jednotlivé části plnění,
- 3.4.15. možnosti poskytnout jako součást nabízeného řešení školení pro administrátory a uživatele systému,
- 3.4.16. významná rizika při implementaci segmentace v rozsahu a způsobem dle uvedené specifikace, bodů a dotazů,
- 3.4.17. počet zakázek na téma implementace segmentačních firewallů v uplynulých 5 letech.
- 3.5. Shrnutí výsledků PTK tvoří Příloha č. 17 této Zadávací dokumentace.

4. Účel a předmět veřejné zakázky

- 4.1. Předmětem plnění této veřejné zakázky je realizace zákonné povinnosti Zadavatele (dle § 18 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, ve znění pozdějších předpisů (dále jen „**VoKB**“), posílením odolnosti síťové infrastruktury proti kybernetickým hrozbám dodávkou technologie Next-Generation Firewall (dále také jen „**NGFW**“) v návaznosti na segmentaci uživatelské sítě Zadavatele pro jednotlivá oblastní ředitelství, implementace a konfigurace dodané technologie, odborné školení správy a údržby dodané technologie pro vybrané odborné pracovníky Zadavatele. Nedílnou součástí plnění jsou také vedle technické podpory dodaných technologií, pravidelné aktualizace bezpečnostních funkcionalit a post-implementační podpora Zadavatele i realizační a analytické práce při stanovování celkové koncepce „Segmentace sítě“.
- 4.2. Bližší specifikace předmětu plnění veřejné zakázky je uvedena v technické specifikaci, která tvoří Přílohu č. 2 této Zadávací dokumentace (dále jen „**technická specifikace**“), a v závazném vzoru smlouvy, který tvoří Přílohu č. 1 této Zadávací dokumentace (dále jen „**závazný vzor smlouvy**“).
- 4.3. 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 zvládnutí, kterým je nepřipustění použití těchto prostředků v rámci plnění veřejné zakázky.

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).

Zadavatel tak na základě varování NÚKIB, navazující metodiky a provedené analýzy rizik, ve spojení s § 4 odst. 4 ZoKB, nepřípouští 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.

Pokud by některý z dodavatelů ve své nabídce nerespektoval zákaz, resp. zadávací podmínku uvedenou v tomto čl. 4.3 Zadávací dokumentace, tzn. že by pro plnění veřejné zakázky navrhl použití technických nebo programových prostředků výše uvedených společností (výrobců), Zadavatel bude postupovat podle § 48 odst. 2 písm. a) ZZVZ ve spojení s § 48 odst. 8 ZZVZ a přistoupí k vyloučení takového dodavatele ze zadávacího řízení.

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 – Zabezpečení datových sítí SŽ“. Registrační číslo projektu: CZ.06.01.01/00/22_005/0000112.

4.4. Klasifikace předmětu veřejné zakázky:

- Kód CPV: 32415000-5 - Ethernetové sítě
- Kód CPV: 72511000-0 - Programové vybavení pro správu sítě
- Kód CPV: 50312310-1 - Údržba zařízení datové sítě
- Kód CPV: 50324100-3 - Údržba systémů
- Kód CPV: 72000000-5 - Informační technologie: poradenství, vývoj programového vybavení, internet a podpora
- Kód CPV: 72263000-6 - Implementace programového vybavení
- Kód CPV: 72261000-2 - Podpora programového vybavení

4.5. Předmět plnění veřejné zakázky bude spolufinancován z Evropských strukturálních a investičních fondů prostřednictvím Integrovaného regionálního operačního programu 2021 – 2027, v rámci projektu „Zabezpečení datových sítí SŽ“, reg. č. CZ.06.01.01/00/22_005/0000112.

5. Předpokládaná hodnota

5.1. Předpokládaná hodnota předmětu veřejné zakázky stanovená Zadavatelem se **nezveřejňuje**.

6. Doba plnění a místo plnění veřejné zakázky

6.1. Doba plnění veřejné zakázky

Termín zahájení plnění: Od okamžiku účinnosti smlouvy.

Termín ukončení plnění: Fáze F5 (Post-implementační a technická podpora) a F6 (Konzultační služby na vyžádání) nebudou ukončeny dříve než za 5 let od skončení všech přechozích fází – tj. fází F1.1 až F4.3.

Harmonogram plnění předmětu veřejné zakázky tvoří Přílohu č. 7 této Zadávací dokumentace.

6.2. Místo plnění veřejné zakázky

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.

7. Sociálně a environmentálně odpovědné zadávání, inovace

- 7.1. Zadavatel při vytváření zadávacích podmínek, včetně pravidel pro hodnocení nabídek, a výběru dodavatele, postupoval tak, aby v co nejvyšší možné míře naplnil zásady sociálně odpovědného zadávání, environmentálně odpovědného zadávání a inovací tak jak jsou definovány v § 28 odst. 1 písm. p) až r) ZZVZ (dále jen „**odpovědné zadávání**“). Vzhledem k tomu, že jednotlivé postupy odpovědného zadávání nebyly v ZZVZ ani v jiném zákoně taxativně vymezeny a současně je odpovědné zadávání stále se velmi dynamicky vyvíjejícím institutem veřejného zadávání, Zadavatel při vytváření podmínek zvažoval použití zejména těch prvků odpovědného zadávání, které byly v době vytváření zadávacích podmínek jednoznačně vymezitelné a vymahatelné, a současně byla u nich vysoká míra jistoty, že Zadavatel jejich aplikací neporuší ostatní zásady uvedené v § 6 ZZVZ a také principy 3E vyplývající ze zákona č. 320/2011 Sb. o finanční kontrole ve veřejné správě, ve znění pozdějších předpisů.
- 7.2. Zadavatel aplikuje v zadávacím řízení prvky odpovědného zadávání podle čl. 7.3 a 7.4 této Zadávací dokumentace. Použití jiných prvků odpovědného zadávání, které byly Zadavateli známy při vytváření této Zadávací dokumentace, není vzhledem k povaze a smyslu zakázky možné z těchto důvodů:
- 7.2.1. V oblasti environmentálního odpovědného zadávání Zadavatel neshledal potřebu použití dílčích aspektů odpovědného zadávání, neboť činnosti, které jsou předmětem této veřejné zakázky, nezatěžují životní prostředí nad rámec běžného života a spotřeba energií, vody, surovin a produkce znečišťujících látek je minimální či žádná.
- 7.2.2. V oblasti inovací Zadavatel nestanovil dílčí kritéria odpovědného zadávání s ohledem na skutečnost, že v rámci předmětu plnění veřejné zakázky neidentifikoval žádná možná inovativní řešení. Z těchto důvodů jsou inovace u daného předmětu plnění fakticky vyloučeny.
- 7.2.3. V oblasti sociálně odpovědného zadávání Zadavatel neshledal potřebu použití dalších dílčích aspektů odpovědného zadávání, kromě těch, které jsou uvedeny v čl. 7.3 a 7.4 této Zadávací dokumentace, s ohledem na specifčnost těchto služeb, kdy předmětem služeb je specializované plnění. Vzhledem k těmto důvodům je nutné, aby se na plnění veřejné zakázky podílely osoby s vysokou kvalifikací. Nejedná se tedy o vhodnou příležitost k zaměstnání osob znevýhodněných na trhu práce.
- 7.3. Rovnocenné platební podmínky v rámci dodavatelského řetězce:
- 7.3.1. Zadavatel realizuje zakázku s ohledem na ochranu malých a středních podniků v případném postavení poddodavatelů, a to formou:
- 7.3.2. umožnění přímých plateb případným poddodavatelům a
- 7.3.3. zajištění stejné doby splatnosti faktur pro poddodavatele jako pro vybraného dodavatele.
- 7.4. Dodržování pracovněprávních předpisů:
- 7.4.1. Zadavatel stanovuje, že vybraný dodavatel je při plnění veřejné zakázky povinen dodržovat pracovněprávní předpisy, a to zejména, nikoliv však výlučně, předpisy upravující mzdy zaměstnanců, pracovní dobu, dobu odpočinku mezi směnami, placené přesčasy, bezpečnost práce apod. Zadavatel dále vyžaduje zajistit férové pracovní podmínky a odpovídající úroveň bezpečnosti práce pro všechny osoby podílející se na plnění veřejné zakázky. Vybraný dodavatel je povinen zajistit splnění tohoto požadavku Zadavatele i u svých poddodavatelů.

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

8. Prohlídka místa plnění:

- 8.1. Zadavatel neumožňuje provedení prohlídky místa plnění ve smyslu ustanovení § 97 ZZVZ.

9. Požadavky Zadavatele na kvalifikaci dodavatelů

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

9.2. Kritéria kvalifikace

Zadavatel požaduje, aby dodavatelé prokázali:

- a) základní způsobilost dle § 74 a § 75 ZZVZ;
- b) profesní způsobilost dle § 77 ZZVZ;
- c) technickou kvalifikaci dle § 79 ZZVZ;

9.3. Forma prokazování splnění kvalifikace

- 9.3.1. Dodavatel prokáže splnění kvalifikace ve všech případech příslušnými doklady.
- 9.3.2. Za účelem prokázání kvalifikace Zadavatel přednostně vyžaduje doklady evidované v systému, který identifikuje doklady k prokázání splnění kvalifikace (systém e-Certis).
- 9.3.3. Zadavatel vylučuje možnost, aby dodavatelé pro účely podání nabídky požadované doklady o kvalifikaci dle čl. 9 této Zadávací dokumentace nahradili písemným čestným prohlášením dle § 86 ZZVZ. Tím není dotčen bod 9.3.10 této Zadávací dokumentace.
- 9.3.4. Dodavatel může nahradit požadované doklady jednotným evropským osvědčením pro veřejné zakázky ve smyslu § 87 ZZVZ. Vzor jednotného evropského osvědčení je stanoven prováděcím nařízením Komise (EU) 2016/7 ze dne 5. ledna 2016, kterým se zavádí standardní formulář jednotného evropského osvědčení pro veřejné zakázky (dostupný např. na internetové adrese: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0007&from=cs>).
- 9.3.5. Dodavatel není povinen předložit Zadavateli doklady osvědčující skutečnosti obsažené v jednotném evropském osvědčení pro veřejné zakázky, pokud Zadavateli sdělí, ve kterém jiném zadávacím řízení mu je již předložil.
- 9.3.6. Povinnost předložit doklad může dodavatel splnit odkazem na odpovídající informace vedené v informačním systému veřejné správy ve smyslu zákona č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů, nebo v obdobném systému vedeném v jiném členském státu, který umožňuje neomezený dálkový přístup. Takový odkaz musí obsahovat internetovou adresu a údaje pro přihlášení a vyhledání požadované informace, jsou-li takové údaje nezbytné. V ČR jde zejména o výpis z obchodního rejstříku, výpis z veřejné části živnostenského rejstříku nebo výpis ze seznamu kvalifikovaných dodavatelů.
- 9.3.7. Dodavatel předkládá doklady prokazující splnění kvalifikace ve formě prosté kopie. Tímto není dotčeno oprávnění Zadavatele dle bodu 23.2.1 této Zadávací dokumentace a právo požadovat předložení originálu nebo úředně ověřené kopie dokladu postupem dle § 46 odst. 1 ZZVZ.

- 9.3.8. Doklady prokazující základní způsobilost podle § 74 ZZVZ musí prokazovat splnění požadovaného kritéria způsobilosti nejpozději v době 3 měsíců přede dnem zahájení zadávacího řízení.
- 9.3.9. V případech, kdy Zadavatel v rámci prokázání splnění kvalifikace požaduje předložení čestného prohlášení dodavatele, musí takové čestné prohlášení obsahovat Zadavatelem požadované údaje.
- 9.3.10. Pokud ZZVZ nebo Zadavatel požaduje předložení dokladu podle právního řádu České republiky, může dodavatel předložit obdobný doklad podle právního řádu státu, ve kterém se tento doklad vydává. Doklad, který je vyhotoven v jiném jazyce, než který Zadavatel určil pro podání nabídky, se předkládá s překladem do jazyka určeného Zadavatelem pro podání nabídky. Není-li v zadávacích podmínkách výslovně stanoveno jinak, platí, že Zadavatel určil pro podání nabídky český jazyk. Bude-li mít Zadavatel pochybnosti o správnosti předkladu, je oprávněn si vyžádat předložení úředně ověřeného překladu dokladu tlumočnickem zapsaným do seznamu znalců a tlumočnicků podle zákona č. 36/1997 Sb., o znalcích a tlumočnících, ve znění pozdějších předpisů. Doklad v českém nebo slovenském jazyce a doklad o vzdělání v latinském jazyce se předkládají bez překladu; Zadavatel může povinnost předložit překlad prominout i u jiných dokladů. Pokud se podle příslušného právního řádu požadovaný doklad nevydává, může být nahrazen písemným čestným prohlášením.

9.4. Prokázání kvalifikace prostřednictvím jiných osob dle § 83 ZZVZ

- 9.4.1. Dodavatel může určitou část technické kvalifikace nebo profesní způsobilosti s výjimkou kritéria podle § 77 odst. 1 ZZVZ požadované Zadavatelem prokázat prostřednictvím jiných osob. Dodavatel je v takovém případě povinen Zadavateli předložit:
- a) doklady prokazující splnění profesní způsobilosti podle § 77 odst. 1 ZZVZ jinou osobou,
 - b) doklady prokazující splnění chybějící části kvalifikace prostřednictvím jiné osoby,
 - c) doklady o splnění základní způsobilosti podle § 74 ZZVZ jinou osobou a
 - d) smlouvu nebo jinou osobou podepsané potvrzení o její existenci, jejímž obsahem je závazek jiné osoby k poskytnutí plnění určeného k plnění veřejné zakázky nebo k poskytnutí věcí nebo práv, s nimiž bude dodavatel oprávněn disponovat při plnění veřejné zakázky, a to alespoň v rozsahu, v jakém jiná osoba prokázala kvalifikaci za dodavatele.
- 9.4.2. Nejedná-li se o situaci dle bodu 9.4.3 ZD, má se za to, že požadavek podle bodu 9.4.1. písm. d) je splněn, pokud z obsahu smlouvy nebo potvrzení o její existenci podle bodu 9.4.1. písm. d) vyplývá závazek jiné osoby plnit veřejnou zakázku společně a nerozdílně s dodavatelem.
- 9.4.3. Prokazuje-li dodavatel prostřednictvím jiné osoby kvalifikaci a předkládá doklady podle § 79 odst. 2 písm. a), b) nebo d) ZZVZ vztahující se k takové osobě, musí ze smlouvy nebo potvrzení o její existenci podle písm. d) vyplývat závazek, že jiná osoba bude vykonávat služby, ke kterým se prokazované kritérium kvalifikace vztahuje.
- 9.4.4. Dodavatelé a jiné osoby prokazují (mohou prokázat) kvalifikaci společně.
- 9.4.5. Dodavatel a jiná osoba, jejímž prostřednictvím dodavatel prokazuje ekonomickou kvalifikaci podle § 78 ZZVZ nesou společnou a nerozdílnou odpovědnost za plnění veřejné zakázky.

- 9.4.6. Zadavatel upozorňuje, že povinnost doložit veškeré doklady uvedené výše v tomto článku platí i v případě, kdy je část kvalifikace prokazována poddodavatelem poddodavatele (pod-poddodavatelem).
- 9.5. Prokazování kvalifikace v případě společné účasti dodavatelů dle § 82 ZZVZ
- 9.5.1. V případě společné účasti dodavatelů prokazuje základní způsobilost dle § 74 a § 75 ZZVZ a profesní způsobilost podle § 77 odst. 1 ZZVZ každý dodavatel samostatně.
- 9.6. Prokazování kvalifikace získané v zahraničí dle § 81 ZZVZ
- 9.6.1. V případě, že byla kvalifikace získána v zahraničí, prokazuje se doklady vydanými podle právního řádu země, ve které byla získána, a to v rozsahu požadovaném Zadavatelem.
- 9.6.2. Potvrzení pro daňové nedoplatky zahraničních dodavatelů v ČR vydává Finanční úřad pro Prahu 1 a potvrzení pro nedoplatky zahraničních dodavatelů v ČR na pojistném a na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti vydává Pražská správa sociálního zabezpečení.
- 9.7. Změny kvalifikace účastníka zadávacího řízení dle § 88 ZZVZ
- 9.7.1. Pokud po předložení dokladů nebo prohlášení o kvalifikaci dojde v průběhu zadávacího řízení ke změně kvalifikace účastníka zadávacího řízení, je účastník zadávacího řízení povinen tuto změnu Zadavateli do 5 pracovních dnů oznámit a do 10 pracovních dnů od oznámení této změny předložit nové doklady nebo prohlášení ke kvalifikaci. Zadavatel může tyto lhůty prodloužit nebo prominout jejich zmeškání. Povinnost podle věty první účastníku zadávacího řízení nevzniká, pokud je kvalifikace změněna takovým způsobem, že:
- a) podmínky kvalifikace jsou nadále splněny,
 - b) nedošlo k ovlivnění kritérií hodnocení nabídek.
- 9.7.2. Zadavatel může vyloučit účastníka zadávacího řízení, pokud prokáže, že účastník nesplnil shora uvedenou povinnost.
- 9.8. Výpis ze seznamu kvalifikovaných dodavatelů dle § 228 ZZVZ
- 9.8.1. Předložení dokladu o zapsání dodavatele do seznamu kvalifikovaných dodavatelů vedeného Ministerstvem pro místní rozvoj dle § 226 až § 232 ZZVZ nahrazuje v souladu s § 228 ZZVZ doklad prokazující profesní způsobilost podle § 77 ZZVZ v tom rozsahu, v jakém údaje ve výpisu ze seznamu kvalifikovaných dodavatelů prokazují splnění kritérií profesní způsobilosti, a základní způsobilost podle § 74 ZZVZ v plném rozsahu. Výpis ze seznamu kvalifikovaných dodavatelů nesmí být k poslednímu dni, ke kterému má být prokázána základní způsobilost nebo profesní způsobilost, starší než tři měsíce.
- 9.9. Předložení certifikátu dle § 234 ZZVZ
- 9.9.1. Platným certifikátem vydaným v rámci schváleného systému certifikovaných dodavatelů lze podle § 234 ZZVZ prokázat kvalifikaci v zadávacím řízení. Má se za to, že dodavatel je kvalifikovaný v rozsahu uvedeném na certifikátu.
- 9.10. Důsledek nesplnění kvalifikace
- 9.10.1. Dodavatel, který nesplní kvalifikaci v rozsahu požadovaném ZZVZ a touto zadávací dokumentací, může být Zadavatelem z účasti v zadávacím řízení vyloučen. Vybraný dodavatel, který nesplní kvalifikaci v rozsahu požadovaném ZZVZ a touto zadávací dokumentací, bude Zadavatelem z účasti v zadávacím řízení vyloučen.

10. Základní způsobilost dle § 74 a § 75 ZZVZ

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

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

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

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

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

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

*Dodavatel prokazuje splnění podmínek základní způsobilosti v tomto kritériu ve vztahu k České republice a k zemi svého sídla předložením **písemného čestného prohlášení**. Vzor čestného prohlášení ke splnění základní způsobilosti je zpracován jako Příloha č. 10 této Zadávací dokumentace.*

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

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

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

*Dodavatel prokazuje splnění podmínek základní způsobilosti v tomto kritériu ve vztahu k České republice předložením **výpisu z obchodního rejstříku, nebo předložením písemného čestného prohlášení v případě, že není v obchodním rejstříku zapsán**. V případě, že dodavatel není zapsán v obchodním rejstříku, je k prokázání uvedeného kritéria oprávněn využít vzor čestného prohlášení uvedeného jako Příloha č. 10 této Zadávací dokumentace.*

10.2. Je-li dodavatelem právnická osoba, musí podmínku uvedenou v odstavci 10.1 písm. a) splňovat tato právnická osoba a zároveň každý člen statutárního orgánu. Je-li členem statutárního orgánu dodavatele právnická osoba, musí podmínku uvedenou shora pod písm. a) splňovat:

- a. tato právnická osoba,
- b. každý člen statutárního orgánu této právnické osoby a
- c. osoba zastupující tuto právnickou osobu v statutárním orgánu dodavatele.

10.3. Účastní-li se zadávacího řízení pobočka závodu:

- 10.3.1. zahraniční právnické osoby, musí podmínku uvedenou v odstavci 10.1 písm. a) splňovat tato právnická osoba a vedoucí pobočky závodu

10.3.2. české právnické osoby, musí podmínku uvedenou v odstavci 10.1 písm. a) splňovat:

- a. tato právnická osoba,
- b. každý člen statutárního orgánu této právnické osoby,
- c. osoba zastupující tuto právnickou osobu v statutárním orgánu dodavatele, a
- d. vedoucí pobočky závodu.

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

- a. by vyloučení účastníka znemožnilo zadání veřejné zakázky v tomto zadávacím řízení a
- b. naléhavý veřejný zájem, zejména veřejné zdraví nebo ochrana životního prostředí, vyžaduje plnění veřejné zakázky.

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

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

11. Profesní způsobilost dle § 77 ZZVZ

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

- a) Dodavatel prokazuje splnění profesní způsobilosti ve vztahu k České republice předložením výpisu z obchodního rejstříku nebo jiné obdobné evidence, pokud jiný právní předpis zápis do takové evidence vyžaduje.

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

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

12. Technická kvalifikace dle § 79 ZZVZ

12.1. Dodavatel předloží **seznam obsahující významné služby**, jehož vzor je upraven jako Příloha č. 19 této Zadávací dokumentace, s předmětem plnění a technickými parametry tohoto plnění dle čl. 12.1.1 této Zadávací dokumentace, včetně uvedení:

- ceny
- doby jejich poskytnutí,
- identifikace objednatele a
- telefonní a e-mailový kontakt na kontaktní osobu každého objednatele pro ověření poskytnutí významné služby.

12.1.1. Dodavatel prokáže splnění tohoto kvalifikačního kritéria předložením seznamu významných služeb poskytnutých dodavatelem **za posledních 5 let** před zahájením zadávacího řízení, ze kterého bude vyplývat splnění níže uvedených požadavků. Ze seznamu významných služeb musí vyplývat, že dodavatel v uvedeném období realizoval:

- a) **alespoň 1 významnou službu**, jejímž předmětem byla implementační analýza segmentace a následná podpora segmentace pro správce nebo provozovatele informačního systému kritické informační infrastruktury nebo pro správce nebo provozovatele významného informačního systému nebo informační systém základní služby základní služby ve smyslu ZoKB, v minimálním finančním objemu (rozsahu) 5 000 000 Kč bez DPH,
- b) **alespoň 1 významnou službu**, jejímž předmětem byla realizace segmentace a dodávky, konfigurace NGFW (nástroj konfigurace), v minimálním finančním objemu (rozsahu) 10 000 000 Kč bez DPH.

12.1.2. Zadavatel upozorňuje, že doba 5 let před zahájením zadávacího řízení se považuje za splněnou, pokud byla služba uvedená v seznamu v průběhu této doby úspěšně dokončena. Pokud bude dodavatel prokazovat splnění podmínky technické kvalifikace dle čl. 12.1.1 písm. a) a b) významnou službou, považuje se doba 5 let před zahájením zadávacího řízení za splněnou, pokud již byla dokončena implementační analýza segmentace ze strany dodavatele již dochází pouze k následné podpoře segmentace v případě významné služby dle čl. 12.1.1 písm. a), stejně tak v případě významné služby dle čl. 12.1.1 písm. b), pokud již došlo k realizaci segmentace a dodávky, konfigurace NGFW (nástroj konfigurace) a nyní již probíhá pouze podpora segmentace NGFW (tzn. že služba jako celek ještě není dokončena).

12.1.3. Zadavatel umožňuje, aby dodavatel jednou významnou službou prokázal splnění technické kvalifikace dle obou písmen a) až b) zároveň. Pro vyloučení všech pochybností Zadavatel výslovně uvádí, že pokud jedna významná služba splňuje zároveň podmínky dle výše uvedených písmen a) i b), může jejím prostřednictvím dodavatel prokázat splnění technické kvalifikace dle obou těchto písmen.

12.2. Osvědčení o vzdělání a odborné kvalifikaci člena realizačního týmu

12.2.1. Dodavatel dále předloží seznam členů realizačního týmu, jehož vzor je upraven jako Příloha č. 11 této Zadávací dokumentace, a kteří budou splňovat požadavky dle tohoto článku 12.2 této Zadávací dokumentace.

12.2.2. Členové realizačního týmu budou odpovědní za činnosti, které bude dodavatel provádět v průběhu realizace veřejné zakázky. Každá osoba v realizačním týmu může zastávat právě jednu pozici.

12.2.3. Dodavatel prokáže splnění tohoto kvalifikačního požadavku, pokud doloží, že disponuje minimálně 4 osobami, jež splňují minimální požadavky uvedené v tabulce níže:

Pracovní pozice	Popis role a minimální požadavky na kvalifikaci člena realizačního týmu
Vedoucí realizačního týmu a garant řešení segmentace (PM) (minimálně 1 osoba)	Popis role: Vedoucí realizačního týmu a garant řešení segmentace (PM) bude zodpovědný za celkové řízení projektu, včetně plánování, koordinace činností a dodržení harmonogramu. Zajišťuje komunikaci mezi zadavatelem a dodavatelem, pravidelný reporting a řízení rizik. Koordinuje činnosti všech zapojených odborných rolí a dohlíží na plnění jednotlivých milníků. Podílí se na vedení workshopů a připomínkových jednání.

	<p>Zodpovídá za přehledné vedení projektové dokumentace a řízení změn.</p> <p>Popis minimálních požadavků na kvalifikaci člena realizačního týmu:</p> <ul style="list-style-type: none"> • Minimálně 7 let praxe v uvedené roli, přičemž obsahem této role bylo: <ul style="list-style-type: none"> ◦ vedení realizačního týmu a implementací obdobně rozsáhlých aplikačních ICT řešení. • Zkušenost s: <ul style="list-style-type: none"> ◦ Účastí na projektu realizace segmentace a dodávky, konfigurace NGFW (nástroj konfigurace) za posledních 5 let před zahájením zadávacího řízení, v minimálním finančním objemu (rozsahu) 5 000 000 Kč bez DPH. ◦ Tyto reference (zkušenosti) nemusí být vázány k nabízenému produktu.¹ • Certifikace: <ul style="list-style-type: none"> ◦ platná certifikace Prince2 (practitioner), nebo PMI6 nebo jiná obdobná či vyšší certifikace.
<p>Seniorní systémový produktový inženýr, specialista NGFW a nástroje pro jeho správu</p> <p>(minimálně 1 osoba)</p>	<p>Popis role:</p> <p>Seniorní systémový produktový inženýr, specialista NGFW a nástroje pro jeho správu bude zodpovědný za návrh a parametrizaci pravidel na NGFW prvcích. Podílí se na tvorbě bezpečnostních politik, vytváří šablony pravidel a scénářů filtrování včetně pravidel pro aplikace, služby a identity. Odpovídá za spolupráci s kybernetickým analytikem při definování detekčních a preventivních mechanismů. Účastní se pilotního nasazení a následné optimalizace řešení. Přípravuje technické výstupy potřebné pro budoucí správu a rozvoj NGFW řešení.</p> <p>Popis minimálních požadavků na kvalifikaci člena realizačního týmu:</p> <ul style="list-style-type: none"> • Minimálně 7 let praxe v uvedené roli, přičemž obsahem této role byla: <ul style="list-style-type: none"> ◦ Implementace nabízeného NGFW řešení spolu s implementací nástroje pro jejich správu. • Zkušenost s: <ul style="list-style-type: none"> ◦ Účastí na projektu realizace segmentace a dodávky, konfigurace NGFW (nástroj konfigurace) za posledních 5 let před zahájením zadávacího řízení, v minimálním finančním objemu (rozsahu) 5 000 000 Kč bez DPH,

¹ Vázanost na nabízený produkt se rozumí totožnost produktu, který dodavatel nabízí Zadavateli s produktem použitým v rámci získané zkušenosti.

	<ul style="list-style-type: none"> ○ Účastí na projektu, jehož předmětem byla implementační analýza segmentace a následná podpora segmentace pro správce nebo provozovatele informačního nebo komunikačního systému kritické informační infrastruktury, nebo pro správce nebo provozovatele významného informačního systému nebo informačního systému základní služby ve smyslu ZoKB, v minimálním finančním objemu (rozsahu) 5 000 000 Kč bez DPH na pozici produktového specialisty nebo síťového architekta. <ul style="list-style-type: none"> • Certifikace: <ul style="list-style-type: none"> ○ Platná oborová certifikace vázaná na produkt pokrývající design architektury a implementaci řešení.
Systémový analytik provádějící analýzu sítě SŽ a návrh řešení (minimálně 1 osoba)	<p>Popis role:</p> <p>Systémový analytik provádějící analýzu sítě SŽ a návrh řešení bude zodpovědný za verifikaci segmentační architektury sítě Zadavatele, včetně analýzy stávající infrastruktury a technologické řešení vlastní segmentace sítě. Na základě dostupných dat (např. IP Fabric, ETS) verifikuje logické členění sítě pomocí VRF a souvisejících směrovacích a bezpečnostních pravidel. Podílí se na tvorbě pilotního řešení a přípravě migračního postupu, kde bude rovněž zajišťovat konzultace, dokumentaci návrhu a podporu při validaci výstupů.</p> <p>Popis minimálních požadavků na kvalifikaci člena realizačního týmu:</p> <ul style="list-style-type: none"> • Minimálně 7 let praxe v uvedené roli, přičemž obsahem této role bylo: <ul style="list-style-type: none"> ○ Konzultant síťových řešení se znalostí architektury sítě provádějící analýzu sítě. • Zkušenost s: <ul style="list-style-type: none"> ○ Účastí na projektu realizace segmentace a dodávky, konfigurace NGFW (nástroj konfigurace) za posledních 5 let před zahájením zadávacího řízení, v minimálním finančním objemu (rozsahu) 5 000 000 Kč bez DPH, ○ návrhem a realizací (správy) segmentace sítě zákazníka, ve které bylo min. 20 zařízení ve funkci MPLS PE (Provider Edge) routeru s plnou podporou protokolu BGP, ○ návrhem a realizací (správy) segmentace sítě zákazníka, ve které bylo min. 5 FW v HA řešení min. z pohledu L2 až L4 OSI modelu,

	<ul style="list-style-type: none"> ○ účastí na projektu, jehož předmětem byla implementační analýza, segmentace a následná podpora segmentace pro správce nebo provozovatele informačního systému kritické informační infrastruktury, nebo pro správce nebo provozovatele významného informačního systému, nebo správce nebo provozovatele informačního systému základní služby základní služby ve smyslu ZoKB v minimálním finančním objemu (rozsahu) 5 000 000 Kč bez DPH na pozici systémového analytika. • Certifikace: <ul style="list-style-type: none"> ○ Platná certifikace CCNP „Routing and Switching“ zaměřená na síťovou architekturu (např. CCA) či jiná srovnatelná certifikace.
<p>Systémový analytik provádějící analýzu sítě SŽ a návrh řešení s přihlédnutím k otázce kybernetické bezpečnosti</p> <p>(minimálně 1 osoba)</p>	<p>Popis role:</p> <p>Systémový analytik provádějící analýzu sítě Zadavatele a návrh řešení s přihlédnutím k otázce kybernetické bezpečnosti posuzuje návrh síťové segmentace z hlediska souladu s právními předpisy (ZoKB, NIS2, GDPR) a bezpečnostních standardů. Spolupracuje na tvorbě bezpečnostních pravidel a posuzuje rizika spojená s komunikací mezi nimi. Poskytuje doporučení ke změnám návrhu z pohledu bezpečnosti a zajišťuje odbornou konzultaci k vybraným částem řešení. Podílí se na tvorbě dokumentace potřebné k bezpečnostnímu auditu. Zajišťuje metodický dohled nad bezpečnostními aspekty v průběhu projektu.</p> <p>Popis minimálních požadavků na kvalifikaci člena realizačního týmu:</p> <ul style="list-style-type: none"> • Minimálně 7 let praxe v uvedené roli, přičemž obsahem této role bylo: <ul style="list-style-type: none"> - Konzultant síťových řešení se znalostí síťových řešení provádějícím analýzu sítě, se znalostí kybernetické bezpečnosti. • Zkušenost s: <ul style="list-style-type: none"> - Účastí na projektu realizace segmentace a dodávku, konfigurace NGFW (nástroj konfigurace) za posledních 5 let před zahájením zadávacího řízení, v minimálním finančním objemu (rozsahu) 5 000 000 Kč bez DPH, - Návrhem a realizací (správy) segmentace sítě zákazníka v které bylo minimálně 20 zařízení ve funkci MPLS PE (Provider edge) routeru s plnou podporou protokolu BGP, - Návrhem a realizací (správy) segmentace sítě zákazníka v které bylo min 5 FW v HA řešení min z pohledu L2 až L4 OSI modelu,

	<ul style="list-style-type: none"> - účasti na projektu, jehož předmětem byla implementační analýza, segmentace a následná podpora segmentace pro správce nebo provozovatele informačního systému kritické informační infrastruktury, nebo pro správce nebo provozovatele významného informačního systému, nebo správce nebo provozovatele informačního systému základní služby základní služby ve smyslu ZoKB, v minimálním finančním objemu (rozsahu) 5 000 000 Kč bez DPH na pozici systémového analytika. • Další požadavky: Osoba způsobilá dle ZoKB, resp. příslušných vyhlášek, která je způsobilá vykonávat funkci architekta kybernetické bezpečnosti, tzn. musí se jednat o osobu, která je pro tuto činnost vyškolená a prokáže odbornou způsobilost praxí s navrhováním implementace bezpečnostních opatření a zajišťováním architektury bezpečnosti a) po dobu nejméně tří let, nebo b) po dobu jednoho roku, pokud absolvovala studium na vysoké škole.
--	---

12.2.4. Dodavatel prokáže splnění tohoto kvalifikačního požadavku předložením následujících dokumentů, z nichž bude vyplývat splnění výše uvedených požadavků:

- seznam členů realizačního týmu dle čl. 12.2.1 této Zadávací dokumentace,
- strukturovaný profesní životopis (lze využít vzor, který je Přílohou č. 18 Zadávací dokumentace), ze kterého bude vyplývat požadovaná praxe a zkušenosti člena realizačního týmu a jeho poměr k dodavateli (např. zaměstnanec apod.) a
- certifikát vyžadovaný dle tabulky výše (pozn. certifikáty je možné předložit v rámci nabídky v anglickém jazyce bez jejich překladu do českého jazyka).

12.2.5. V případě, že je u člena realizačního týmu vyžadována účast na projektu, považuje se podmínka účasti za splněnou pouze při naplnění následujících kumulativních podmínek:

- člen realizačního týmu se účastnil projektu v požadované roli, a
- účast na předloženém projektu trvala minimálně 12 měsíců či alespoň polovinu doby trvání projektu.

13. Požadavky Zadavatele na způsob zpracování nabídkové ceny:

13.1. Způsob zpracování nabídkové ceny

13.1.1. Zadavatel požaduje zpracovat nabídkovou cenu vyplněním formuláře, který tvoří Příloha č. 8 této Zadávací dokumentace (dále jen „**formulář pro vyplnění nabídkové ceny**“).

13.1.2. Celková nabídková cena za celou dobu trvání smlouvy, která bude předmětem hodnocení, bude při využití Přílohy č. 8 této Zadávací dokumentace vypočtena automaticky. Zadavatel však doporučuje dodavatelům, aby výpočet řádně zkontrolovali, neboť na tuto část se vztahuje pravidlo uvedené v čl. 13.1.4 této Zadávací dokumentace. Dodavatel je povinen ve formuláři pro vyplnění nabídkové ceny ocenit všechny položky.

13.1.3. Nabídková cena bude zahrnovat veškeré náklady nezbytné k řádnému, úplnému a kvalitnímu splnění předmětu této veřejné zakázky, včetně všech rizik a vlivů souvisejících s plněním předmětu této veřejné zakázky. Celková nabídková cena bude rovněž zahrnovat pojištění, garance, daně, cla, poplatky, inflační vlivy a jakékoli další výdaje nutné pro realizaci veřejné zakázky, jako je např. cena za odvoz a uskladnění veškerých zbytkových materiálů, obalů a dalšího odpadu souvisejícího s předmětem plnění veřejné zakázky, likvidaci vyřazených komponent a článků či dopravu.

13.1.4. Za správnost provedení výpočtu celkové nabídkové ceny odpovídá účastník zadávacího řízení.

13.2. Mimořádně nízká nabídková cena

13.2.1. V souladu s § 113 ZZVZ posoudí Zadavatel mimořádně nízké nabídkové ceny před odesláním oznámení o výběru dodavatele. Zadavatel požádá účastníka zadávacího řízení o písemné zdůvodnění způsobu stanovení mimořádně nízké nabídkové ceny, bude-li tato v jeho nabídce identifikována. Žádost o zdůvodnění mimořádně nízké nabídkové ceny se považuje za žádost podle § 46 ZZVZ, lze ji doplňovat a vznést opakovaně.

14. Jiné požadavky Zadavatele na plnění veřejné zakázky:

14.1. Využití poddodavatele

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

- a) určil části veřejné zakázky, které hodlá plnit prostřednictvím poddodavatelů, a
- b) předložil seznam poddodavatelů, pokud jsou dodavateli známi, a uvedl, kterou část veřejné zakázky bude každý z poddodavatelů plnit. Účastník zadávacího řízení může k tomuto účelu využít vzor seznamu poddodavatelů, který tvoří Příloha č. 6 této Zadávací dokumentace.

14.1.2. Vybraný dodavatel je povinen předložit zadavateli identifikační údaje poddodavatelů, a to nejpozději do 10 pracovních dnů od doručení oznámení o výběru dodavatele, pokud jsou známi. Poddodavatelé, kteří nebyli identifikováni podle věty první a kteří se následně zapojí do plnění veřejné zakázky, musí být identifikováni, a to před zahájením plnění veřejné zakázky.

14.1.3. Seznam poddodavatelů se v případě výběru daného účastníka stane přílohou smlouvy.

15. Varianty nabídky

15.1. Zadavatel nepřipouští varianty nabídky.

16. Závazný vzor smlouvy

16.1. Dodavatel je povinen využít závazný vzor smlouvy, který tvoří Příloha č. 1 této Zadávací dokumentace.

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

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

17. Způsob hodnocení nabídek:

17.1. Kritéria hodnocení

- 17.1.1. Hodnocení nabídek bude provedeno v souladu s § 114 a násl. ZZVZ podle jejich ekonomické výhodnosti dle níže uvedených dílčích hodnotících kritérií.
- 17.1.2. Hodnotícím kritériem pro výběr nejvýhodnější nabídky v rámci ekonomické výhodnosti nabídek je nejvýhodnější poměr ceny a zkušeností členů realizačního týmu, a to na základě následujících kritérií a vah, které představují podíl jednotlivých kritérií hodnocení na celkovém hodnocení:

Kritérium hodnocení	Váha
Nabídková cena	70 %
Zkušenosti členů realizačního týmu	30 %

17.2. Nabídková cena

- 17.2.1. V rámci dílčího kritéria hodnocení „Nabídková cena“ bude hodnocena celková nabídková cena stanovená způsobem dle čl. 13 této Zadávací dokumentace. Nabídková cena relevantní pro hodnocení nabídky bude v nabídce uvedena ve formuláři pro vyplnění nabídkové ceny na listu „Nabídková cena“.
- 17.2.2. Jako výhodnější bude v tomto kritériu hodnocena nabídka, která bude obsahovat nižší nabídkovou cenu za plnění v Kč bez DPH.
- 17.2.3. 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 vahou dílčího hodnotícího kritéria „Nabídková cena“ a následně matematicky zaokrouhlen na dvě desetinná místa.
- 17.2.4. Výpočet odpovídá následujícímu vzorci:

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

17.3. Zkušenosti členů realizačního týmu

- 17.3.1. Předmětem hodnocení nabídek v rámci dílčího hodnotícího kritéria „Zkušenosti členů realizačního týmu“ bude míra naplnění parametrů zkušeností relevantních pro plnění této zakázky u osob na klíčových pozicích týmu dodavatele uvedených v tabulce níže. Dodavatel je povinen zvolit právě jednu osobu zastávající níže uvedenou pozici jako osobu určenou k hodnocení, pokud by v rámci realizačního týmu na příslušné pozici nominoval více osob a neurčil by jednu osobu pro účely hodnocení, obdrží u takové pozice v rámci hodnocení 0 bodů. Dodavatel může toto rozlišení provést jednoduše prostřednictvím profesních životopisů uvedených v příloze, kde kapitolu s názvem: „Zkušenosti pro účely hodnocení v rámci dílčího hodnotícího kritéria „Zkušenosti členů realizačního týmu“ vyplní pouze u jedné osoby v rámci každé role.

- 17.3.2. Zadavatel s ohledem na ust. § 46 odst. 2 ZZVZ upozorňuje, na omezené možnosti údaje, které mají být předmětem hodnocení nabídek, po uplynutí lhůty pro podání nabídek měnit či doplňovat a v případě, kdy podaná nabídka nebude obsahovat všechny údaje, informace a doklady nezbytné pro hodnocení, může to vést k posouzení údaje jako nesplňujícího hodnotící kritéria stanovená Zadavatelem. Zadavatel tak upozorňuje Dodavatele, aby při uvádění těchto údajů postupovali se zvýšenou pečlivostí.
- 17.3.3. Hodnocení v rámci tohoto dílčího hodnotícího kritéria bude provedeno na základě posouzení údajů uvedených ve strukturovaných profesních životopisech jednotlivých členů realizačního týmu Dodavatele předložených v nabídce. **Zadavatel bude hodnotit výhradně ty parametry, které budou ve strukturovaných profesních životopisech uvedeny jako údaje uvedené za účelem hodnocení nad rámec požadované kvalifikace².** Zadavatel přidělí každé nabídce počet bodů v závislosti na prokázané zkušenosti u vybraných členů realizačního týmu Dodavatele. **Zadavatel požaduje, aby bodované zkušenosti byly realizovány v období za posledních 5 let před zahájením zadávacího řízení.** Jednotliví členové realizačního týmu dodavatele určení Dodavatelem k hodnocení budou v rámci tohoto hodnotícího kritéria získávat body dle následující tabulky:

Pozice člena realizačního týmu	Bodované zkušenosti (realizované v období za posledních 5 let před zahájení zadávacího řízení)	Hodnocení (počet bodů)	Maximální bodové ohodnocení
Vedoucí realizačního týmu a garant řešení segmentace (PM)	Projekt realizace segmentace a dodávky NGFW v rozsahu podnikové sítě, kde nejméně tři hlavní lokality (serverovny) jsou od sebe vždy vzdáleny minimálně 50 km vzdušnou čarou.	Účastník získá vždy 1 bod za doložení jedné zkušenosti (prostřednictvím uvedených významných zakázek). Pro zpřesnění Zadavatel uvádí, že jedna významná zakázka může prokázat plnění vždy pouze 1 zkušenosti. Zadavatel neupřesňuje, jaké bodované zkušenosti musí účastník prokazovat (tedy pro potřeby hodnocení může účastník doložit	5 bodů
	Návrh a realizace (či post-podpora) segmentace sítě zákazníka, v které bylo minimálně 20 zařízení ve funkci MPLS PE (Provider edge) routeru s plnou podporou protokolu BGP.		

² Pro vyloučení pochybností, Zadavatel určuje pro danou část hodnocení následující pravidla:

- A) Pokud Dodavatel uvede totožnou zkušenost u identického člena realizačního týmu pro účely kvalifikace a hodnocení, Dodavatel za takovou zkušenost obdrží 0 bodů, tato zkušenost bude započítána jako zkušenost kvalifikační.
- B) Totožnými zkušenostmi se rozumí zkušenosti, které se, byť z části překrývají.
- C) Dodavatel může u jednotlivých členů týmu využít zkušenost, kterou prokazuje splnění kvalifikace dle čl. 12.1 této Zadávací dokumentace.
- D) Dodavatel může v rámci hodnocení u člena realizačního týmu využít totožnou zkušenost, kterou použil pro kvalifikaci či hodnocení u jiného člena realizačního týmu.

	Návrh a realizace (post- implementační podpora) segmentace sítě zákazníka, v které bylo min. 5 NGFW v HA řešení min. z pohledu L2 až L4 OSI modelu.	5 referenčních zakázek pro jednu z bodovaných zkušeností a pro ostatní bodované zkušenosti nemusí doložit žádnou zakázku). Maximální počet dodatečně získaných bodů je 5.	
Seniorní systémový produktový inženýr, specialista NGFW a nástroje pro jeho správu	Projekt realizace segmentace a dodávky NGFW v rozsahu podnikové sítě, kde nejméně tři hlavní lokality (serverovny) jsou od sebe vždy vzdáleny minimálně 50 km vzdušnou čarou.	Účastník získá vždy 1 bod za doložení jedné zkušenosti (prostřednictvím uvedených významných zakázek). Pro zpřesnění Zadavatel uvádí, že jedna významná zakázka může prokázat plnění vždy pouze 1 zkušenosti. Zadavatel neupřesňuje, jaké bodované zkušenosti musí účastník prokazovat (tedy pro potřeby hodnocení může účastník doložit 5 referenčních zakázek pro jednu z bodovaných zkušeností a pro ostatní bodované zkušenosti nemusí doložit žádnou zakázku). Maximální počet dodatečně získaných bodů je 5.	5 bodů
	Návrh a realizace (správy) segmentace sítě zákazníka, v které bylo minimálně 20 zařízení ve funkci MPLS PE (Provider edge) routeru s plnou podporou protokolu BGP.		
	Návrh a realizace (správy) segmentace sítě zákazníka, v které bylo min 5 NGFW v HA řešení min. z pohledu L2 až L4 OSI modelu.		
Systémový analytik provádějící analýzu sítě SŽ a návrh řešení	Projekt realizace segmentace a dodávky NGFW v rozsahu podnikové sítě, kde nejméně tři hlavní lokality (serverovny) jsou od sebe vždy vzdáleny minimálně 50 km vzdušnou čarou.	Účastník získá vždy 1 bod za doložení jedné zkušenosti (prostřednictvím uvedených významných zakázek). Pro zpřesnění Zadavatel uvádí, že jedna významná zakázka může prokázat plnění vždy pouze 1 zkušenosti. Zadavatel neupřesňuje, jaké bodované zkušenosti musí účastník prokazovat (tedy pro potřeby hodnocení může účastník doložit 5 referenčních	5 bodů
	Návrh a realizace (správy) segmentace sítě zákazníka, v které bylo minimálně 20 zařízení ve funkci MPLS PE (Provider edge) routeru s plnou podporou protokolu BGP.		
	Návrh a realizace (správy) segmentace sítě zákazníka, v které bylo min 5 NGFW v HA řešení		

	min. z pohledu L2 až L4 OSI modelu.	zakázek pro jednu z bodovaných zkušeností a pro ostatní bodované zkušenosti nemusí doložit žádnou zakázku). Maximální počet dodatečně získaných bodů je 5.	
Systémový analytik provádějící analýzu sítě SŽ a návrh řešení s přihlédnutím k otázce kybernetické bezpečnosti	Projekt realizace segmentace a dodávky NGFW v rozsahu podnikové sítě, kde nejméně tři hlavní lokality (serverovny) jsou od sebe vždy vzdáleny minimálně 50 km vzdušnou čarou.	Účastník získá vždy 1 bod za doložení jedné zkušenosti (prostřednictvím uvedených významných zakázek). Pro zpřesnění Zadavatel uvádí, že jedna významná zakázka může prokázat plnění vždy pouze 1 zkušenosti. Zadavatel neupřesňuje, jaké bodované zkušenosti musí účastník prokazovat (tedy pro potřeby hodnocení může účastník doložit 5 referenčních zakázek pro jednu z bodovaných zkušeností a pro ostatní bodované zkušenosti nemusí doložit žádnou zakázku). Maximální počet dodatečně získaných bodů je 5.	5 bodů
	Návrh a realizace (správy) segmentace sítě zákazníka, v které bylo min 20 zařízení ve funkci MPLS PE (Provider edge) routeru s plnou podporou protokolu BGP.		
	Návrh a realizace (správy) segmentace sítě zákazníka, v které bylo min 5 NGFW v HA řešení min. z pohledu L2 až L4 OSI modelu.		

- 17.3.4. Doba realizace bodovaných zkušeností v posledních pěti (5) letech se považuje za splněnou, pokud byly činnosti naplňující definici výše v průběhu této doby dokončeny.
- 17.3.5. Pokud bude Dodavatel prokazovat splnění bodovaných zkušeností významnou zakázkou, jejímž předmětem plnění je realizace a následná podpora segmentace, považuje se doba pěti (5) let před zahájením zadávacího řízení za splněnou, pokud již byla dokončena realizace segmentace ze strany Dodavatele a již dochází pouze k následné podpoře systému.
- 17.3.6. Přidělování bodů v rámci dílčího hodnotícího kritéria „Zkušenosti členů realizačního týmu“ bude probíhat tak, že Zadavatel přidělí body dle výše uvedené tabulky. Počet bodů bude dán součtem bodů za počet zkušeností 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 (20) 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. Výpočet odpovídá následujícímu vzorci:

17.4. Celkové hodnocení nabídek

17.4.1. Celkové hodnocení nabídek provede Zadavatel tak, že číselné hodnocení nabídek dle jednotlivých dílčích hodnotících kritérií sečte pro každou nabídku a stanoví pořadí úspěšnosti dodavatelů, přičemž jako nejvhodnější bude vyhodnocena nabídka, která dosáhla nejvyšší celkové bodové hodnoty. Pro vyloučení pochybností Zadavatel uvádí, že jednotlivé hodnoty budou při výpočtech hodnocení zaokrouhlovány vždy na 2 desetinná místa.

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

18. Zadávací dokumentace

18.1. Uveřejnění Zadávací dokumentace

18.1.1. Zadávací dokumentací se rozumí veškeré písemné dokumenty obsahující zadávací podmínky, sdělované nebo zpřístupňované účastníkům zadávacího řízení při zahájení zadávacího řízení, včetně změn či doplnění Zadávací dokumentace podle § 99 ZZVZ, včetně formulářů podle § 212 ZZVZ a výzev uvedených v příloze č. 6 ZZVZ.

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

18.2. Neveřejná část Zadávací dokumentace

18.2.1. Neveřejná část Zadávací dokumentace obsahuje následující dokumenty – Příloha č. 12 – Popis prostředí (dále jen „**neveřejná část Zadávací dokumentace**“), které jsou pro plnění předmětu veřejné zakázky závazné, a které nejsou bez znalosti příslušného hesla dodavatelům zpřístupněny na profilu Zadavatele, toto heslo je možné si pro přípravu nabídky písemně vyžádat u Zadavatele. Zadavatel uveřejnil tyto části Zadávací dokumentace na profilu Zadavatele jako složku s názvem „Neveřejná část ZD“ a tuto složku zahesloval. Části Zadávací dokumentace 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. 3 této Zadávací dokumentace. Po doručení žádosti včetně podepsaného návrhu NDA umožní Zadavatel dodavateli přístup k částem Zadávací dokumentace obsahující důvěrné informace způsobem podrobně popsáním v NDA. Za písemnou žádost dodavatele ve smyslu § 96 odst. 2 ZZVZ je považována žádost dodavatele, jejíž součástí je rovněž podepsaný návrh NDA.

18.3. Vysvětlení Zadávací dokumentace

18.3.1. Zadavatel může Zadávací dokumentaci vysvětlit, pokud takové vysvětlení, případně související dokumenty, uveřejní na profilu Zadavatele, a **to nejméně 5 pracovních dnů před uplynutím lhůty pro podání nabídek.**

18.3.2. Pokud žádost o vysvětlení Zadávací dokumentace doručí dodavatel ve stanové lhůtě písemnou formou, a to elektronicky, Zadavatel vysvětlení uveřejní prostřednictvím elektronického nástroje E-ZAK, včetně přesného znění žádosti bez identifikace tohoto dodavatele, na profilu Zadavatele. Zadavatel není povinen vysvětlení poskytnout, pokud není žádost o vysvětlení doručena včas, a to alespoň 3 pracovní dny před uplynutím shora uvedené lhůty 5 pracovních dnů. Písemná žádost tedy musí být Zadavateli doručena nejpozději 8 pracovních dnů před uplynutím lhůty pro podání nabídek. Pokud Zadavatel na žádost o vysvětlení, která není doručena včas, vysvětlení poskytne, nemusí uvedené lhůty dodržet. Žádost o vysvětlení Zadávací dokumentace musí být podána v českém jazyce, na žádost podanou v jiném, než v českém jazyce se hledí jako by nebyla podána včas.

18.3.3. Zadavatel je oprávněn uveřejnit na profilu Zadavatele za podmínek § 99 ZZVZ rovněž změnu nebo doplnění Zadávací dokumentace.

18.3.4. Pokud dodavatel požádá o vysvětlení ve vztahu k neveřejné části Zadávací dokumentace (viz čl. 18.2 této Zadávací dokumentace), Zadavatel takové vysvětlení zpřístupní všem dodavatelům, kteří splnili podmínky pro obdržení neveřejné části Zadávací dokumentace, obdobným způsobem jako zpřístupňuje neveřejné části Zadávací dokumentace.

18.3.5. Zadavatel i v tomto případě není povinen vysvětlení poskytnout, pokud není žádost o vysvětlení doručena včas, a to alespoň 3 pracovní dny před uplynutím shora uvedené lhůty 5 pracovních dnů. Písemná žádost tedy musí být Zadavateli doručena nejpozději 8 pracovních dnů před uplynutím lhůty pro podání nabídek. Pokud Zadavatel na žádost o vysvětlení neveřejné části Zadávací dokumentace, která není doručena včas, vysvětlení poskytne, nemusí uvedené lhůty dodržet, i tato žádost musí být podána v českém jazyce.

18.4. Námitky proti zadávacím podmínkám

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

19. Závaznost pokynů Zadavatele

19.1. Informace a údaje uvedené v této Zadávací dokumentaci vymezují závazné požadavky Zadavatele na plnění veřejné zakázky. Tyto požadavky je dodavatel povinen plně a bezvýhradně respektovat při zpracování své nabídky. Neakceptování požadavků Zadavatele uvedených v této Zadávací dokumentaci může být považováno za nesplnění zadávacích podmínek s následkem vyloučení dodavatele ze zadávacího řízení.

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

19.3. Pokud jsou v Zadávací dokumentaci uvedeny odkazy na normy či technické dokumenty podle § 90 odst. 1 a 2 ZZVZ, je tak učiněno v zájmu přesnosti a srozumitelnosti zadávacích podmínek. Zadavatel u každého takového odkazu v souladu s § 90 odst. 3 ZZVZ připouští nabídnout rovnocenné řešení.

20. Komunikace mezi Zadavatelem a dodavatelem

- 20.1. Veškerá komunikace mezi Zadavatelem a dodavatelem musí být v souladu s § 211 ZZVZ vedena pouze písemnou formou, a to elektronicky, s výjimkou případů vymezených v ustanovení § 211 odst. 3 ZZVZ. Doručování písemností a komunikace mezi Zadavatelem a dodavatelem bude ze strany Zadavatele probíhat prostřednictvím elektronického nástroje E-ZAK (na adrese: <https://zakazky.spravazeleznic.cz/>), který splňuje podmínky vyhlášky č. 260/2016 Sb., o stanovení podrobnějších podmínek týkajících se elektronických nástrojů, elektronických úkonů při zadávání veřejných zakázek a certifikátu shody. Na komunikaci ze strany dodavatelů učiněnou elektronicky, avšak nikoliv prostřednictvím elektronického nástroje E-ZAK, bude tedy Zadavatel vždy odpovídat prostřednictvím elektronického nástroje.
- 20.2. Zpracování osobních údajů včetně jejich zvláštních kategorií případně poskytnutých v průběhu zadávacího řízení je Zadavatelem prováděno pouze za účelem zadání veřejné zakázky, přičemž Zadavatel v celém procesu ochrany osobních údajů postupuje v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES, obecně závaznými právními předpisy a vnitřními předpisy zadavatele, které agendu ochrany osobních údajů upravují.
- 20.3. Za řádné a včasné seznamování se s písemnostmi zasílanými Zadavatelem prostřednictvím elektronického nástroje, jakož i za správnost kontaktních údajů uvedených u účastníka zadávacího řízení zodpovídá účastník zadávacího řízení.
- 20.4. Komunikace mezi Zadavatelem a dodavatelem v průběhu zadávacího řízení bude probíhat v českém jazyce.

21. Požadavky Zadavatele na zpracování nabídky, způsob podání nabídek a otevírání nabídek

- 21.1. 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/>.
- 21.2. Pro tyto účely a v souladu se ZZVZ systém vyžaduje registraci účastníků a elektronický podpis založený na kvalifikovaném certifikátu. Podáním nabídky účastník se stanovenou formou komunikace a doručování souhlasí a zavazuje se poskytnout veškerou nezbytnou součinnost, zejména provést registraci v elektronickém nástroji E-ZAK a pravidelně kontrolovat doručené zprávy.
- 21.3. Účastník je povinen přiložit ke své nabídce čestné prohlášení o tom, že v souvislosti se zadávacím řízením na předmětnou veřejnou zakázku neuzavřel a neuzavře s jinými osobami zakázanou dohodu ve smyslu zákona č. 143/2001 Sb., o ochraně hospodářské soutěže a o změně některých zákonů (zákon o ochraně hospodářské soutěže), ve znění pozdějších předpisů. Vzor čestného prohlášení ve vztahu k zakázaným dohodám je upraven jako č. 9 této Zadávací dokumentace.
- 21.4. Pro zpracování nabídky Zadavatel doporučuje níže uvedené řazení dokladů a dokumentů:
- a) Obsah nabídky;
 - b) Doklady prokazující splnění základní způsobilosti;
 - c) Doklady prokazující splnění profesní způsobilosti;
 - d) Doklady prokazující splnění technické kvalifikace a doklady pro hodnocení zkušeností členů realizačního týmu;

- e) Vyplněný formulář pro vyplnění nabídkové ceny v souladu s čl. 13.1 této Zadávací dokumentace;
- f) Vyplněný závazný vzor smlouvy v souladu s čl. 16 této Zadávací dokumentace;
- g) Čestné prohlášení ve vztahu k zakázaným dohodám dle čl. 21.3 této Zadávací dokumentace;
- h) Čestné prohlášení podle čl. 24.3 této Zadávací dokumentace v případě, že účastník v souladu s čl. 24.2 této Zadávací dokumentace vyznačí ve smlouvě 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;
- i) Čestné prohlášení ke střetu zájmů v souladu s čl. 25.2 této Zadávací dokumentace;
- j) Čestné prohlášení o splnění podmínek v souvislosti se situací na Ukrajině dle čl. 26.5 této Zadávací dokumentace;
- k) V případě využití poddodavatelů seznam poddodavatelů v souladu s čl. 14.1 této Zadávací dokumentace.

21.5. Nabídka musí být podána elektronickými prostředky prostřednictvím elektronického nástroje E-ZAK, který je profilem Zadavatele, a to v českém jazyce nebo v souladu s ustanovením § 45 odst. 3 ZZVZ. Zadavatel nepřipouští podání nabídky v listinné podobě ani v jiné elektronické formě mimo elektronický nástroj E-ZAK.

21.6. Nabídky podávané v elektronické podobě účastník doručí do konce níže uvedené lhůty pro podání nabídek, a to prostřednictvím elektronického nástroje E-ZAK na níže uvedenou elektronickou adresu <https://zakazky.spravazeleznice.cz/>.

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

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

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

22.2. Otevírání nabídek je v souladu s § 109 ZZVZ neveřejné, bude probíhat bez přítomnosti účastníků a bude zahájeno bez zbytečného odkladu po uplynutí lhůty pro podání nabídek.

23. Informace pro dodavatele a podmínky pro uzavření smlouvy

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

23.2. Požadavky Zadavatele pro uzavření smlouvy

23.2.1. Vybraný dodavatel je povinen Zadavateli na písemnou výzvu učiněnou dle § 122 odst. 3 písm. a) ZZVZ předložit doklady prokazující kvalifikaci dle této Zadávací dokumentace (tj. předložení originálů nebo ověřených kopií dokladů o kvalifikaci).

23.2.2. U vybraného dodavatele, je-li českou právnickou osobou, zadavatel zjistí údaje o jeho skutečném majiteli podle zákona upravujícího evidenci skutečných majitelů (dále jen „**skutečný majitel**“) z evidence skutečných majitelů podle téhož zákona (dále jen „**evidence skutečných majitelů**“).

23.2.3. Vybraného dodavatele, je-li zahraniční právnickou osobou, zadavatel vyzve k předložení výpisu ze zahraniční evidence obdobné evidenci skutečných majitelů nebo, není-li takové evidence,

- a) ke sdělení identifikačních údajů všech osob, které jsou jeho skutečným majitelem, a
- b) k předložení dokladů, z nichž vyplývá vztah všech osob podle předchozího písmene a) k dodavateli; těmito doklady jsou zejména:
 - výpis ze zahraniční evidence obdobné veřejnému rejstříku,
 - seznam akcionářů,
 - rozhodnutí statutárního orgánu o vyplacení podílu na zisku,
 - společenská smlouva, zakladatelská listina nebo stanovy.

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

23.2.5. Zadavatel vyloučí vybraného dodavatele, je-li zahraniční právnickou osobou, pokud nepředložil údaje.

23.2.6. Zadavatel upozorňuje, že preferuje uzavírání smluv v elektronické podobě prostřednictvím některého druhu zaručených elektronických podpisů. V případě, že dodavatel není schopen k takovému postupu zajistit Zadavateli součinnost, žádáme, aby Zadavatele o této skutečnosti informoval ve své nabídce, a to v průvodní zprávě k nabídce.

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

23.3.1. Vybraný dodavatel je povinen Zadavateli na písemnou výzvu učiněnou dle § 122 odst. 3 písm. b) ZZVZ předložit doklady a informace dle čl. 26.6 této Zadávací dokumentace.

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

24. Registr smluv

24.1. 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 (zákon o registru smluv), ve znění pozdějších předpisů (dále jen „**ZRS**“).

24.2. 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.

- 24.3. Pokud účastník ve smlouvě, která bude nedílnou součástí nabídky, označí její části nebo určité informace dle čl. 24.2 této Zadávací dokumentace, je účastník povinen o tomto předložit Čestné prohlášení. Vzor čestného prohlášení je zpracován jako č. 14 této Zadávací dokumentace. Tímto čestným prohlášením účastník prohlašuje, že jím uvedené údaje a skutečnosti kumulativně naplňují všechny definiční znaky obchodního tajemství tak, jak je vymezeno v ustanovení § 504 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**obchodní tajemství**“), a pro případ, že by takto označené údaje a skutečnosti nenaplněly znaky obchodního tajemství a takto znečitelněná smlouva by byla v důsledku toho uveřejněna způsobem odporujícím ZRS, nese účastník veškerou odpovědnost.
- 24.4. Výše uvedené čestné prohlášení dle čl. 24.3 této Zadávací dokumentace účastník nedokládá v případě, že neoznačí ve smlouvě, která bude nedílnou součástí nabídky, žádné takové části nebo informace ve smyslu čl. 24.2 této Zadávací dokumentace.
- 24.5. Účastník odpovídá za správnost a pravdivost veškerých údajů a skutečností, které jím budou uvedeny ve výše uvedeném čestném prohlášení. Zadavatel nebude přezkoumávat jejich pravdivost.
- 24.6. 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.

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

- 25.1. 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.
- 25.2. 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 v č. 15 této Zadávací dokumentace, ve své nabídce.
- 25.3. Vybraný dodavatel je povinen předložit k výzvě Zadavatele dle § 122 odst. 3 písm. b) ZZVZ doklady a informace, z nichž nepochybně vyplýne, že vybraný dodavatel i všichni poddodavatelé, jimiž vybraný dodavatel prokazuje kvalifikaci, splňují podmínku neexistence střetu zájmů ve smyslu § 4b Zákona o střetu zájmů a čl. 25 této Zadávací dokumentace. V případě vybraného dodavatele nebo jeho poddodavatele, prostřednictvím kterého vybraný dodavatel prokazoval část kvalifikace, je-li zahraniční právnickou osobou, je vybraný dodavatel povinen předložit zejména doklady ve smyslu § 122 odst. 5 ZZVZ, a to i ve vztahu k příslušnému poddodavateli, prostřednictvím kterého vybraný dodavatel prokazoval část kvalifikace.
- 25.4. V případě postupu účastníka zadávacího řízení v rozporu s čl. 25 této Zadávací dokumentace bude účastník zadávacího řízení vyloučen ze zadávacího řízení.

26. Další zadávací podmínky v návaznosti na sankce proti Rusku a Bělorusku v souvislosti se situací na Ukrajině

26.1. 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 předpisů³ (dále jen „**Nařízení č. 833/2014**“) 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, čl. 7 písm. a) až d), článku 8, 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:

- a) jakémukoli ruskému státnímu příslušníkovi, fyzické osobě s bydlištěm v Rusku nebo právnické osobě, subjektu či orgánu usazenému v Rusku,
- b) právnické osobě, subjektu nebo orgánu, které jsou z více než 50 % přímo či nepřímo vlastněny některým ze subjektů uvedených v písmeni a) tohoto odstavce, nebo
- c) fyzické nebo právnické osobě, subjektu nebo orgánu, které jedná jménem nebo na pokyn některého ze subjektů uvedených v písmeni a) nebo b) tohoto odstavce,

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

26.2. Zadavatel požaduje, aby účastník zadávacího řízení sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti v zadávacím řízení, ani žádný z jeho poddodavatelů nebo jiných osob, jejichž způsobilost je využívána ve smyslu směrnic o zadávání veřejných zakázek, **nebyli** osobami dle čl. 26.1 této Zadávací dokumentace a Nařízení č. 833/2014.

26.3. 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 (**tzv. sankční seznamy**)⁴, 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 (dále jen „**Osoby vedené na sankčních seznamech**“).

³ 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, a Nařízení Rady (EU) 2023/427 ze dne 25. února 2023, kterým se mění nařízení (EU) č. 833/2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině.

⁴ 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, 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 a prováděcí nařízení Rady (EU) 2023/429 ze dne 25. února 2023, kterým se provádí nařízení (EU) č. 269/2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny.

- 26.4. Zadavatel dále požaduje, aby účastník zadávacího řízení sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti v zadávacím řízení, ani žádný z jeho poddodavatelů nebo jiných osob, jejichž způsobilost je využívána ve smyslu směrnic o zadávání veřejných zakázek, **nebyli** Osobami vedenými na sankčních seznamech.
- 26.5. Splnění zadávacích podmínek stanovených Zadavatelem dle tohoto článku ZD prokáže účastník zadávacího řízení předložením čestného prohlášení, jehož vzorové znění je č. 16 této Zadávací dokumentace, ve své nabídce.
- 26.6. Zadavatel je oprávněn ověřovat si splnění zadávacích podmínek dle tohoto článku. Vybraný dodavatel je povinen předložit k výzvě Zadavatele dle § 122 odst. 3 písm. b) ZZVZ doklady a informace, z nichž nepochybně vyplyne, že vybraný dodavatel i všichni poddodavatelé nebo jiné osoby, jejichž způsobilost je využívána ve smyslu směrnic o zadávání veřejných zakázek, splňují podmínky uvedené v tomto článku Zadávací dokumentace.
- 26.7. V případě postupu účastníka zadávacího řízení v rozporu s čl. 26 této Zadávací dokumentace bude účastník zadávacího řízení vyloučen ze zadávacího řízení.

Přílohy Zadávací dokumentace

- č. 1. Závazný vzor smlouvy
- č. 2. Bližší specifikace předmětu plnění veřejné zakázky (Technická specifikace)
- č. 3. Dohoda o ochraně důvěrných informací
- č. 4. Zvláštní obchodní podmínky pro Zakázky v oblasti ICT
- č. 5. Platforma SŽ
- č. 6. Seznam poddodavatelů
- č. 7. Harmonogram
- č. 8. Formulář pro vyplnění nabídkové ceny
- č. 9. Čestné prohlášení ve vztahu k zakázaným dohodám
- č. 10. Čestné prohlášení ke splnění základní způsobilosti
- č. 11. Vzor seznamu členů realizačního týmu
- č. 12. Popis prostředí
- č. 13. Koncepce cílového stavu
- č. 14. Čestné prohlášení ve vztahu k zákonu o registru smluv
- č. 15. Čestné prohlášení o střetu zájmů
- č. 16. Čestné prohlášení o splnění podmínek v souvislosti se situací na Ukrajině
- č. 17. Výstupy z PTK
- č. 18. Vzor profesního životopisu
- č. 19. Vzor seznamu významných služeb

Bc. Jiří Svoboda, MBA
generální ředitel

Příloha č. 1 zadávací dokumentace – Závazný vzor smlouvy

Smlouva o dílo – Segmentace sítě

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 zadávacího řízení veřejné zakázky s názvem „Segmentace sítě“, ev. č. veřejné zakázky ve Věstníku veřejných zakázek: (bude doplněno) (dále jen „Veřejná zakázka“ a „Zadávací řízení“) Objednatel jako zadavatelem ve smyslu zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“), neboť nabídka Dodavatele podaná na Veřejnou zakázku (dále jen „Nabídka“) byla Objednatel 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 – Zabezpečení datových sítí SŽ“. Registrační číslo projektu: CZ.06.01.01/00/22_005/0000112.

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

Pokud nevyplývá z této Smlouvy jinak, mají pojmy s velkými počátečními písmeny význam definovaný 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. Dle § 18 vyhlášky 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) jsou pak Objednateli uloženy povinnosti v oblasti segmentace sítě, konkrétně je Objednatel zejm. povinen zajistit, aby byl implementován systematický přístup k ochraně integrity svých sítí prostřednictvím segmentace a řízeného přístupu, čímž se minimalizuje riziko neoprávněného přístupu a šíření kybernetických hrozeb v rámci sítě.
- 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 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 dodávka technologie Next-Generation Firewall (dále také jen jako „**NGFW**“) v návaznosti na segmentaci uživatelské sítě Objednatele pro jednotlivá oblastní ředitelství, implementace a konfigurace dodané technologie, odborné školení správy a údržby dodané technologie pro vybrané odborné pracovníky Objednatele. Nedílnou

součástí plnění jsou také vedle technické podpory dodaných technologií, pravidelné aktualizace bezpečnostních funkcionalit a post-implementační podpora Objednatele i realizační a analytické práce při stanovování celkové koncepce „Segmentace sítě“.

- 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 Zhodnocení stávající síťové infrastruktury uživatelské sítě Správy železnic a návrh rozvoje sítě z pohledu její segmentace s pilotní realizací.
- Zhodnocení stávající síťové infrastruktury Správy železnic,
 - Specifikace změn architektury segmentované uživatelské sítě,
 - Analýza a návrh řešení pro specifikum geo-redundance,
 - Příprava implementačních kroků pro realizaci vlastní segmentace
 - Implementační plán pro celou uživatelskou síť
- 2.4.2 Dodávka celkem 12 kusů NGFW a souvisejících komponentů dle uvedené specifikace
- Dodávka a implementace NGFW,
 - Dodávka SFP+ modelů,
 - Dodávka licencí na provoz dodaných nástrojů,
 - Zajištění napojení nových NGFW do nástroje pro centrální správu NGFW.
- 2.4.3 Odborné školení správy a údržby dodaných technologií.
- 2.4.4 Post-implementační a technická podpora.
- 2.4.5 Konzultační 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 A5 vymezeného v části 12 ZOP. Nezvolí-li Objednatel výslovně v rámci požadavku jinou kategorii, jedná se o požadavek kategorie B.

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 Doba trvání této Smlouvy činí nejméně 5 let od skončení všech fází F1.1 až F4.3 (v této době budou plněny fáze F5 (Post-implementační a technická podpora) a F6 (Konzultační služby na vyžádání)) (dále jen „**doba trvání Smlouvy**“).
- 4.2 Doba trvání Smlouvy nemá vliv na existenci práv a povinností Stran, která mají vzhledem ke své povaze a okolnostem trvat i po konci doby trvání Smlouvy.
- 4.3 Pokud není stanoveno jinak, je Zhotovitel povinen provádět Dílo a jeho části v termínech uvedených v závazném harmonogramu realizace Díla obsaženém v příloze č. 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 nutné 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 (Platební milník A): Výzva k úhradě ve výši ceny za položky označené v Příloze č. 2 této Smlouvy takto: Fáze F1.1 (Zhodnocení stávající síťové infrastruktury), Fáze F1.2 (Základní školení (seznámení s produktem)), Fáze F2.2 (Specifikace změn architektury), Fáze F3.1 (Implementace Next Generation Firewall a případná Implementace nástroje centrální správy), Fáze F3.2 (Příprava implementačních kroků pro realizaci vlastní segmentace (konzultace)), Fáze F4.1 (Analýza a návrh řešení pro specifikum geo-redundance), Fáze F4.2 (Implementační plán pro celou uživatelskou síť), Fáze F4.3 (Školení (odborné školení)), které jsou tvořeny činnostmi uvedenými v části 3.1, 3.2.3, 3.2.4 a 3.3 Přílohy č. 1 této Smlouvy;

- 6.1.2 Druhý platební milník: Výzva k úhradě ve výši ceny za položky označené v Příloze č. 2 této Smlouvy takto: Fáze F2.1 (Dodávka firewallů dle specifikace A, Dodávka firewallů dle specifikace B, Licence k NGFW dle specifikace A a dodávaným částem, Licence k NGFW dle specifikace B a dodávaným částem, Dodávka SFP+ modulů dle specifikace, Dodávka nástroje pro centrální správu NGFW dle specifikace), která je tvořena činnostmi uvedenými v části 3.2.1.1, 3.2.1.2, 3.2.2 a 3.2.4 Přílohy č. 1 této Smlouvy;
- 6.2 Zhotovitel je dále oprávněn doručit Objednateli Výzvu k úhradě vždy za každý měsíc, v němž došlo k akceptaci (bez výhrad) plnění na základě Objednávky Konzultačních služeb na vyžádání dle čl. 10 této Smlouvy, a to ve výši součinu počtu MD dle Objednávky či Objednávek a ceny za jednu MD dle příslušné položky ceny *Konzultační služby na vyžádání* uvedené Příloze č. 2 této Smlouvy.
- 6.3 Zhotovitel je dále oprávněn doručit Objednateli Výzvu k úhradě za každý měsíc po akceptaci (bez výhrad) služeb Post-implementační a technické podpory, a to ve výši ceny za příslušný měsíc dle příslušné položky ceny *Post-implementační a technická podpora* uvedené Příloze č. 2 této Smlouvy.
- 6.4 Výzva k úhradě musí být fakturou nebo daňovým dokladem. Kromě náležitostí účetního či daňového dokladu musí být Výzva k úhradě označena registračním číslem projektu: CZ.06.01.01/00/22_005/0000112. Pokud je Výzva k úhradě hrazena z více zdrojů, budou na ní uvedena všechna čísla projektů. Objednatel je oprávněn čísla projektu aktualizovat v průběhu trvání této Smlouvy a Zhotovitel je povinen tuto skutečnost akceptovat a zohlednit v rámci prováděné fakturace.
- 6.5 Výzvu k úhradě doručí Zhotovitel Objednateli jedním z následujících způsobů:
- 6.5.1 V listinné podobě na adresu:
- Správa železnic, státní organizace
Centrální finanční účtárna Čechy
Náměstí Jana Pernera 217
530 02 Pardubice
- 6.5.2 V elektronické podobě na adresu:
- ePodatelnaCFU@spravazeleznic.cz
- 6.5.3 prostřednictvím datové schránky:
- uccchjm
- 6.6 Splatnost každé Výzvy k úhradě se sjednává na 60 kalendářních dnů od jejího doručení Objednateli. V případě, že Výzva k úhradě nebude mít odpovídající náležitosti, je Objednatel oprávněn ve lhůtě splatnosti ji vrátit Zhotoviteli s vytknutím nedostatků, aniž by se dostal do prodlení se splatností. Lhůta splatnosti počíná běžet znovu od okamžiku doručení opravené či doplněné Výzvy k úhradě Objednateli.
- 6.7 Zhotovitel, poskytovatel zdanitelného plnění, je povinen bezprostředně, nejpozději do 2 (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.
- 6.8 Zhotovitel se zavazuje, že bankovní účet jím určený pro zaplacení jakéhokoliv závazku Objednatele na základě této Smlouvy bude od data podpisu této Smlouvy do ukončení její platnosti zveřejněn způsobem umožňujícím dálkový přístup ve smyslu § 96 odst. 2 ZDPH, v opačném případě je Zhotovitel povinen sdělit Objednateli jiný bankovní účet řádně zveřejněný ve smyslu § 96 ZDPH.

- 6.9 Strany se dohodly na tom, že Zhotovitel není oprávněn činit jednostranná započtení svých pohledávek vzniklých na základě této Smlouvy či v souvislosti s ní vůči jakýmkoliv pohledávkám Objednatele. Pohledávky a nároky Zhotovitele vzniklé na základě této Smlouvy či v souvislosti s ní nesmějí být Zhotovitelem postoupeny třetím osobám, zastaveny, nebo s nimi nesmí být jinak disponováno bez předchozího písemného souhlasu Objednatele (zahrnuje i zákaz Zhotovitele postoupit tuto Smlouvu). Jakýkoliv právní úkon učiněný Zhotovitelem v rozporu s tímto ustanovením bude považován za podstatné porušení této Smlouvy.
- 6.10 Zhotovitel se rovněž zavazuje zajistit řádné a včasné plnění finančních závazků vůči svým Poddodavatelům, prostřednictvím kterých bude realizovat Dílo, resp. jeho část dle této Smlouvy. Za řádné a včasné plnění dle předcházející věty se považuje plné uhrazení Poddodavatelem řádně vystavených faktur za předmět této Smlouvy, resp. jeho část, a to vždy do 60 kalendářních dnů od obdržení platby ze strany Objednatele za konkrétní plnění předmětu této Smlouvy, resp. jeho části.

7 Akceptační řízení

- 7.1 Akceptačnímu řízení dle části 8 ZOP a tohoto článku této Smlouvy podléhají všechny fáze dle Přílohy č. 2 této Smlouvy, přičemž každá z těchto fází je součástí některého z akceptačních milníků A až D, jak stanoví část 4 Přílohy č. 1 této Smlouvy.
- 7.2 Fáze plnění, podléhající Akceptačnímu řízení v rámci některého z akceptačních milníků A až D uvedených v části 4 Přílohy č. 1 této Smlouvy, se považují za ukončené akceptací (bez výhrad) posledního dílčího plnění uvedeného pro příslušné Fáze, resp. akceptační milník v Příloze 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 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.
- 7.4 Akceptačnímu řízení dle části 8 ZOP a tohoto článku této Smlouvy podléhají rovněž Konzultační služby na vyžádání dle čl. 10 této Smlouvy, které budou realizované na základě Objednávky. Akceptační kritéria budou v tomto případě vyplývat ze specifikace prací uvedených v Objednávce.
- 7.5 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 přiměřeně čl. 6.3. ZOP, a to včetně Dokumentace vztahující se k těmto výstupům.
- 8.2 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.

- 8.3 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 ze strany Zhotovitele. Podrobnosti stanoví Příloha č. 1 této Smlouvy.

10 Konzultační služby na vyžádání

- 10.1 Zhotovitel se zavazuje poskytovat Konzultační služby na vyžádání, které jsou blíže vymezeny v části 4.5 Přílohy č. 1 této Smlouvy.
- 10.2 Maximální souhrn Konzultačních služeb na vyžádání činí 35 MD za celou dobu trvání této Smlouvy. Objednatel není povinen Konzultační služby na vyžádání čerpat.
- 10.3 Objednatel v případě zájmu o provedení prací v rámci Konzultačních služeb na vyžádání doručí Zhotoviteli objednávku prostřednictvím e-mailu Kontaktních osob uvedených v čl. 12 této Smlouvy se specifikací požadovaných prací, termínem provedení těchto prací a předpokládanou časovou náročností vyjádřenou v MD (dále jen „**Objednávka**“).
- 10.4 Zhotovitel se zavazuje bez zbytečného odkladu projednat s Objednatelem své případné připomínky k Objednávce, přičemž je povinen postupovat v souladu s principy „best practice“ a s ohledem na účel této Smlouvy. Objednatel je povinen oprávněné připomínky Zhotovitele zohlednit v obsahu Objednávky.
- 10.5 V případě, že Zhotovitel (již) nemá žádné oprávněné připomínky k Objednávce, je povinen Objednávku nejpozději do 3 pracovních dnů písemně přijmout prostřednictvím e-mailu Kontaktních osob uvedených v čl. 12 této Smlouvy. Přijmutím Objednávky vzniká Zhotoviteli povinnost provést v Objednávce specifikované práce, a to při dodržení stanovených termínů a stanovené časové náročnosti vyjádřené v MD.
- 10.6 Na provedení prací dle Objednávky a s tím souvisejícího práva a povinnosti Stran se v rozsahu, v jakém je to možné, použijí ustanovení této Smlouvy. Zhotovitel je tak především, nikoliv však výlučně, povinen předložit provedené práce k Akceptačnímu řízení ve smyslu čl. 7 této Smlouvy a poskytnout ve vztahu k těmto pracím Objednateli licenci či jiná práva z duševního vlastnictví v rozsahu dle čl. 7.1 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 Seznam členů realizačního týmu je Přílohou 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 ve smyslu čl. 5.1 této Smlouvy, 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 změně 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 Dodavatel je povinen při ukončení Smlouvy poskytnout přiměřenou součinnost při převzetí provádění Plnění Objednatelem, nebo třetí osobou, přičemž tato součinnost při ukončení Smlouvy je již součástí Ceny díla.

15 Kybernetická bezpečnost

- 15.1 Zhotovitel se zavazuje k zachovávaní 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 on, ani žádný z jeho poddodavatelů nebo jiných osob, jejichž způsobilost byla využita ve smyslu evropských směrnic o zadávání veřejných zakázek, nejsou osobami:
- 18.2.1 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, čl. 7 písm. a) až d), článku 8, 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), 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,
- 18.2.2 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 (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 této 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, a dalších prováděcích předpisů k tomuto nařízení Rady (EU) č. 269/2014.

- 18.6 Zhotovitel se dále ve smyslu 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, 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 Ukáží-li se prohlášení Zhotovitele dle odstavce 18.1 a 18.2 této Smlouvy jako nepravdivá nebo poruší-li Zhotovitel svou oznamovací povinnost dle odstavce 18.4. nebo povinnosti dle odstavců 18.5 nebo 18.6 této 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 díla (Cena bez DPH) sjednané dle této Smlouvy. 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 kopií 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.

21 Závěrečná ujednání

- 21.1 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.
- 21.2 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.
- 21.3 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.
- 21.4 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 této 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.

- 21.5 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.
- 21.6 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.
- 21.7 Veškerá práva a povinnosti Stran vyplývající z této Smlouvy se řídí českým právním řádem.
- 21.8 Smluvní vztahy neupravené touto Smlouvou se řídí Občanským zákoníkem a dalšími právními předpisy.
- 21.9 Všechny spory vznikající z této Smlouvy a v souvislosti s ní budou dle vůle Stran rozhodovány soudy České republiky, jakožto soudy výlučně příslušnými.
- 21.10 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.
- 21.11 Tuto Smlouvu lze měnit pouze písemnými a řádně označenými dodatky.
- 21.12 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

- č. 1. Specifikace plnění této Smlouvy (*jedná se o přílohu č. 2 zadávací dokumentace k Veřejné zakázce – Technická specifikace, Přílohu č. 12 zadávací dokumentace k Veřejné zakázce – Popis prostředí, Přílohu č. 13 zadávací dokumentace k veřejné zakázce – Koncepce cílového stavu*)
- č. 2. Specifikace nabídkové ceny (bude doplněno v souladu s Nabídkou Dodavatele podle Dodavatelem vyplněného vzoru obsaženého v příloze č. 8 zadávací dokumentace k Veřejné zakázce – Formulář pro vyplnění nabídkové ceny)
- č. 3. Harmonogram plnění (jedná se o přílohu č. 7 zadávací dokumentace k Veřejné zakázce – Harmonogram plnění)
- č. 4. Seznam poddodavatelů (bude doplněno v souladu s Nabídkou Dodavatele podle Dodavatelem vyplněného vzoru obsaženého v příloze č. 6 zadávací dokumentace k Veřejné zakázce – Vzor seznamu poddodavatelů)
- č. 5. Zvláštní obchodní podmínky pro Zakázky v oblasti ICT
- č. 6. Obchodní podmínky ke Smlouvě o dílo
- č. 7. Platforma SŽ (jedná se o přílohu č. 5 zadávací dokumentace k Veřejné zakázce – Platforma SŽ)
- č. 8. Plná moc (pouze v případě zastoupení Dodavatele osobou na základě plné moci)

- č. 9. Realizační tým (bude doplněno v souladu s Nabídkou Dodavatele podle Dodavatelem vyplněného vzoru obsaženého v příloze č. 11 Zadávací dokumentace – Seznam členů realizačního týmu)

Za Objednatele:

V dne

Za Zhotovitele:

V dne

.....
Bc. Jiří Svoboda, MBA
generální ředitel

.....
[DOPLNÍ DODAVATEL]

Klasifikace: Veřejný dokument



Příloha č. 2 zadávací dokumentace

Technická specifikace

Obsah

1	Seznam zkratk	2
2	Úvod	6
2.1	Záměr SŽ v oblasti segmentace uživatelské sítě	6
2.2	Předmět plnění veřejné zakázky	6
3	Požadavky na plnění	7
3.1	Zhodnocení stávající síťové infrastruktury uživatelské sítě SŽ a návrh rozvoje sítě z pohledu její segmentace s pilotní realizací	8
3.1.1	Zhodnocení stávající síťové infrastruktury SŽ	8
3.1.2	Specifikace změn architektury	10
3.1.3	Analýza a návrh řešení pro specifikum geo-redundance	11
3.1.4	Příprava implementačních kroků pro realizaci vlastní segmentace v pilotní lokalitě	11
3.1.5	Implementační plán pro celou uživatelskou síť	13
3.2	Dodávka celkem 12 kusů NGFW a související komponentů dle uvedené specifikace	14
3.2.1	Technické požadavky na dodávku Next Generation Firewall	14
3.2.2	Dodávka SFP+ modulů	16
3.2.3	Implementace Next Generation Firewall	16
3.2.4	Nástroj centrální správy NGFW	17
3.3	Školení	19
3.4	Post-implementační a technická podpora	19
3.5	Konzultační služby na vyžádání	21
4	Fáze dodávky a akceptační milníky	22
5	Vyloučení technologií	24

1 Seznam zkratek

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

Přehled zkratek a pojmů:

Zkratka	Popis
Active Directory	(AD), adresářová služba společnosti Microsoft pro správu uživatelů, počítačů a síťových zdrojů v doménovém prostředí.
BGP	(Border Gateway Protocol) je protokol pro předávání informací mezi síťovými routery.
CE	(Customer Edge) je router na hranici zákaznické sítě v MPLS.
DMI	(Digital Monitoring Interface) je funkce diagnostiky SFP modulů.
DHCP	(Dynamic Host Configuration Protocol) je protokol pro automatické přidělování IP adres a síťových parametrů koncovým zařízením.
DHCP relay	Mechanismus pro přeposílání DHCP zpráv mezi klienty a DHCP serverem napříč různými sítěmi.
DNS	(Domain Name System) je distribuovaný hierarchický jmenný systém používaný v síti Internet. Překládá názvy domén na číselné IP adresy a zpět, obsahuje informace o tom, které stroje poskytují příslušnou službu.
EOS	(End of Sale) Datum ukončení prodeje.
EOL	(End of Life) Datum konce životnosti produktu.
ETC	(Evidence Technologických Systémů) Interní systém a konfigurační management (CMDB) zobrazují status sítě.
GDPR	(General Data Protection Regulation) nařízení EU o ochraně osobních údajů.
HA	(High Availability) je vysoká dostupnost služeb. Předpokladem řešení je použití dvou a více nezávislých zařízení s cílem zajistit funkčnost v případě výpadku.
HTTPS	(Hypertext Transfer Protocol Secure) je šifrovaný protokol pro zabezpečenou komunikaci na webu.
IDS	(Intrusion Detection System) Systém detekce průniku používaný v NGFW.
IPFabric	Nástroj pro automatizovanou analýzu a vizualizaci síťové infrastruktury, využívaný pro audit, návrh a správu sítí.

IPS	<i>(Intrusion Prevention System)</i> Systém prevence průniku používaný v NGFW.
IPv4	<i>(Internet Protocol version 4)</i> je starší verze protokolu IP.
IROP	Integrovaný regionální operační program.
L1 – L3	Vrstvy OSI modelu.
LC	<i>(Lucent Connector)</i> typ optického konektoru.
LDAP	<i>(Lightweight Directory Access Protocol)</i> je komunikační protokol adresářové služby. Je definován v rámci RFC 4511.
Least Privilege	Bezpečnostní princip, který poskytuje uživatelům a systémům pouze minimální práva nezbytná pro vykonání jejich úkolů.
LLD	<i>(Low level design)</i> , návrh a specifikace s vyšší mírou podrobnosti.
Malware	Software vytvořený k poškození nebo neoprávněnému přístupu.
MPLS	<i>(MultiProtocol Label Switching)</i> 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.
NBD	<i>(Next Business Day)</i> Režim poskytování servisu a podpory.
NGFW	<i>(Next-Generation Firewall)</i> Oproti běžným FW nabízí také doplňkové funkce jako AVC, AMP, IPS, IDS, DPI, DLP, TD, IdM a dešifrování a kontrolu TLS/SSL obsahu.
NIS2	<i>(Network and Information Security Directive 2)</i> je evropská směrnice o kybernetické bezpečnosti, rozšiřující povinnosti organizací v oblasti ochrany sítí a informačních systémů.
NTLMv2	<i>(NT LAN Manager version 2)</i> autentizační protokol společnosti Microsoft používaný pro ověřování uživatelů v prostředí Windows.
NTP	<i>(Network Time Protocol)</i> je protokol pro synchronizaci času v počítačových sítích.
OSI	<i>(Open Systems Interconnection)</i> Referenční sedmivrstvý ISO/OSI model slouží pro standardizaci řešení a popisu počítačových sítí podle normy ISO 7498.
OSPF	<i>(Open Shortest Path First)</i> je směrovací protokol pro vnitřní síť, který používá Dijkstrův algoritmus k nalezení nejkratší

	cesty. Podporuje hierarchické členění sítě do oblastí (areas) a rychle reaguje na změny topologie.
PE	(<i>Provider Edge</i>) Hraniční router MPLS sítě, na kterém jsou zakončeny VRF VPN nebo je prováděna manipulace s VRF VPN.
Radius	(<i>Remote Authentication Dial-In User Service</i>) protokol pro centrální ověřování a autorizaci uživatelů v síti.
Sandbox	Izolované testovací prostředí, kde lze bezpečně spouštět a analyzovat potenciálně nebezpečný kód nebo malware bez rizika ohrožení produkčních systémů.
SIEM	(<i>Security Information and Event Management</i>) Řešení zabezpečení, které organizacím pomáhá detekovat hrozby, analyzovat je a reagovat na ně dříve, než způsobí škody v provozu firmy/organizace.
SLA	(<i>Service Level Agreement</i>) je smluvně stanovená úroveň poskytovaných služeb mezi dodavatelem a odběratelem.
SFP	(<i>Small Form-factor Pluggable</i>) modulární síťové rozhraní.
SNMP	(<i>Simple Network Management Protocol</i>) protokol pro vzdálené monitorování a správu síťových zařízení.
SSO	(<i>Single Sign-On</i>) je metoda přihlašování umožňující přístup k více systémům po jediném ověření identity.
Syslog	Protokol pro sběr a přenos systémových a bezpečnostních logů ze zařízení do centrálního systému.
TLS	(<i>Transport Layer Security</i>) protokol pro šifrovanou komunikaci v počítačových sítích.
VLAN	(<i>Virtual Local Area Network</i>) je logické oddělení síťových segmentů na jedné fyzické infrastruktuře.
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	(<i>Virtual Private Network</i>) 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.
VRF	(<i>Virtual Routing and Forwarding</i>) Virtuální směrování a předávání je technologie, která v počítačových sítích založených na protokolu IP umožňuje souběžnou existenci

	více instancí směrovací tabulky v rámci sítě stejného směrovače ve stejnou dobu.
ZoKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.
ZTE	(ZTE Corporation) čínský výrobce technologií, uveden ve varování NÚKIB.

2 Úvod

Tento dokument je přílohou a nedílnou součástí zadávací dokumentace týkající se veřejné zakázky s názvem „Segmentace sítě“ (dále jen „veřejná zakázka“), pro organizaci Správa železnic, státní organizace (dále jen „SŽ“ nebo „Zadavatel“). Dokument popisuje technické a jiné požadavky na veřejnou zakázku.

2.1 Záměr SŽ v oblasti segmentace uživatelské sítě

SŽ, v roli správce kritické infrastruktury, ve věci požadavků opatření ve vazbě na vyhlášku o kybernetické bezpečnosti (VoKB), konkrétně § 18, je povinna zajistit, aby byl implementován systematický přístup k ochraně integrity svých sítí prostřednictvím segmentace a řízeného přístupu, čímž se minimalizuje riziko neoprávněného přístupu a šíření kybernetických hrozeb v rámci sítě.

Segmentace uživatelské sítě – stávající uživatelská síť, která je většinou založena na Cisco prvcích, není v současné době logicky segmentována a slouží pro účely všech zařízení, uživatelů, a to i pro aplikace třetích stran. Záměrem je vytvoření nových VRF sítí a provedení migrace menších logicky oddělených částí sítě do těchto VRF. Tento přístup posiluje kybernetickou bezpečnost organizace hned několika způsoby:

- **Izolace citlivých dat.** Segmentace umožňuje vytvořit bezpečnostní zóny podle důležitosti a citlivosti dat, která jsou v nich uložena. Takovéto rozdělení omezuje možnost neoprávněného nahlížení do citlivých informací a chrání před pokusy o jejich zneužití.
- **Prevence šíření útoků.** V případě úspěšného proniknutí do jednoho segmentu, zůstávají ostatní části sítě izolovány a chráněny díky předem definovaným přístupovým pravidlům mezi segmenty. To znamená, že útočník nemůže snadno přejít do dalších částí sítě a pokračovat v útoku. Segmentace tímto způsobem výrazně omezuje dopad bezpečnostního incidentu a zkracuje čas potřebný k reakci na útok.
- **Detailní správa přístupů a pravidel mezi jednotlivými segmenty sítě.** Segmentace umožňuje správci sítě vytvářet přesná pravidla řízení přístupu mezi jednotlivými částmi sítě podle role uživatelů a zařízení. Tím lze snadno uplatnit bezpečnostní princip minimálních oprávnění („least privilege“), který zajišťuje, že uživatelé mají přístup pouze k nezbytným částem sítě.

2.2 Předmět plnění veřejné zakázky

Předmětem plnění této veřejné zakázky je realizace zákonné povinnosti Zadavatele (dle § 18 VoKB), posílením odolnosti síťové infrastruktury proti kybernetickým hrozbám **dodávkou technologie Next-Generation Firewall** (dále jen NGFW) v návaznosti na segmentaci uživatelské sítě Zadavatele pro jednotlivá oblastní ředitelství, implementace a konfigurace dodané technologie,

odborné školení správy a údržby dodané technologie pro vybrané odborné pracovníky Zadavatele.

Nedílnou součástí plnění jsou také vedle technické podpory dodaných technologií, pravidelné aktualizace bezpečnostních funkcionalit a post-implementační podpora Zadavatele i realizační a analytické práce při stanovování celkové koncepce „Segmentace sítě“.

Očekávaným výstupem, kromě hardwarové dodávky požadovaného počtu firewallů a souvisejících komponent (viz. kapitola 3.2 tohoto dokumentu), je Dodavatelská participace na vytvoření koncepce segmentace uživatelské sítě, tj. kromě analytické části i zpracování detailního návrhu projektového implementačního postupu konfiguračních prací pro vybranou část sítě, která bude sloužit jako implementační vzor, který bude následně již Zadavatelem implementován do zbytku sítě vycházející ze specifikace uvedené v příloze č. 13.

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

Implementační postup vytvořený v rámci plnění této veřejné zakázky bude otestován na vybrané pilotní lokalitě v regionu Praha, technická specifikace pilotní lokality bude výstupem analytické části plnění této zakázky. Finální Implementační plán potom představuje souhrnný dokument, jehož cílem je definovat harmonogram a metodiku zavádění síťové segmentace do jednotlivých lokalit. Součástí Implementačního plánu je i podrobný implementační postup konfigurace síťových prvků, který popisuje konkrétní technické kroky nutné k dosažení cílového stavu, včetně návrhu síťových pravidel, topologie a přidělení adresních rozsahů.

3 Požadavky na plnění

Plnění veřejné zakázky se musí skládat z níže uvedených částí:

- Zhodnocení stávající síťové infrastruktury uživatelské sítě SŽ a návrh rozvoje sítě z pohledu její segmentace s pilotní realizací.
 - Zhodnocení stávající síťové infrastruktury SŽ.
 - Specifikace změn architektury segmentované uživatelské sítě (konfigurační práce při realizaci segmentace uživatelské sítě SŽ).
 - Analýza a návrh řešení pro specifikum geo-redundance.
 - Příprava implementačních kroků pro realizaci vlastní segmentace.
 - Implementační plán pro celou uživatelskou síť.
- Dodávka celkem 12 kusů NGFW a související komponentů dle uvedené specifikace.
 - Dodávka a implementace Next Generation Firewall.
 - Dodávka SFP+ modulů.
 - Dodávka licencí na provoz dodaných nástrojů.
 - Zajištění napojení nových NGFW do nástroje pro centrální správu NGFW.
- Odborné školení správy a údržby dodaných technologií.

- Post-implementační a technická podpora.
- Konzultační služby na vyžádání.

3.1 Zhodnocení stávající síťové infrastruktury uživatelské sítě SŽ a návrh rozvoje sítě z pohledu její segmentace s pilotní realizací

Cílem Zhodnocení stávající síťové infrastruktury uživatelské sítě SŽ, která je většinou založena na Cisco prvcích, je návrh rozvoje sítě z pohledu segmentace a vytvoření komplexního strategicko-funkčního dokumentu, který bude tvořen minimálně těmito částmi:

- Zhodnocení stávající síťové infrastruktury dle dodaných podkladů SŽ.
- Specifikace změn architektury segmentované uživatelské sítě.
- Návrh a verifikace zapojení NGFW se stávajícími routery.
- Analýza a návrh řešení pro specifikum geo-redundance.
- Příprava implementačních kroků pro realizaci vlastní segmentace v pilotní lokalitě v regionu Praha.
- Implementační plán pro celou uživatelskou síť.

Očekávaný informační rozsah jednotlivých oblastí, včetně definice odpovědností a činností Zadavatele a Dodavatele je uveden níže v jednotlivých podkapitolách.

Doplňující informace popisující technické prostředí Zadavatele a požadavky je blíže popsáno v příloze č. 12 a č. 13.

Zadavatel v rámci plnění této veřejné zakázky počítá s nastavením úzké spolupráce mezi týmy Zadavatele a Dodavatele, kdy Dodavatel bude vytvářet požadované výstupy definované tímto dokumentem a Zadavatel bude výstupy připomínkovat a na základě schválených výstupů realizovat konkrétní konfigurační kroky pro realizaci segmentace sítě.

3.1.1 Zhodnocení stávající síťové infrastruktury SŽ

Cílem první oblasti je zhodnotit stávající síťovou infrastrukturu uživatelské sítě Zadavatele. Pro potřeby tohoto zhodnocení poskytne Zadavatel Dodavateli níže uvedené podklady. Dodavatel na základě uvedených podkladů a případně dodatečně vyžádaných podkladů zpracuje finální výstup popisující současný stav a návrh budoucích kroků k realizaci požadované segmentace.

Vymezení rozsahu analýzy:

Cílem této fáze je zhodnocení stávající síťové infrastruktury uživatelské sítě Zadavatele a návrh budoucích kroků vedoucích k její segmentaci. S ohledem na povahu prostředí a dostupné kapacity je touto technickou specifikací upřesněn a vymezen rozsah analýzy.

Podklady dodané Zadavatelem budou sloužit jako primární vstup do analýzy. Je však třeba počítat s tím, že některé dokumenty budou vyžadovat doplnění v

průběhu analýzy. Poskytnutí všech informací nemusí být okamžité a některé detaily mohou být dostupné pouze v omezeném rozsahu.

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

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

Zadavatel neočekává detailní specifikace v následujících bodech:

- Podrobnou analýzu přístupové vrstvy sítě.
- Analýzu na úrovni L2, tedy jednotlivých přepínačů v lokalitách, fyzických rozhraní a jejich konfigurací (např. portových nastavení).
- Verifikaci všech síťových toků a závislostí mezi zařízeními na úrovni jednotlivých VLAN nebo portů.
- Komplexní analýzu konfigurací každého jednotlivého síťového prvku.

Současná kapacitní struktura uživatelské sítě jako je počet CE routerů je uvedena v příloze č.12 – Popis prostředí.

Účastník	Požadavek
Zadavatel	Dodané podklady Zadavatelem <ul style="list-style-type: none"> • Podklady síťové infrastruktury: <ul style="list-style-type: none"> ◦ Výstupy z ETS (CMDB). ◦ Výstupy z IP Fabric. ◦ Schémata topologie sítě. • Návrh koncepce segmentace uživatelské sítě SŽ. • Inventarizace síťových zařízení a jejich konfigurací. • Seznam současných síťových toků a závislostí. • Seznam aplikací a služeb třetích stran. • Návrh pilotní lokality v regionu Praha.
Dodavatel	Výstup Dodavatele <ul style="list-style-type: none"> • Zhodnocení návrhu koncepce segmentace uživatelské sítě SŽ (případné formování návrhů Dodavatele na modifikaci). • Zhodnocení zdrojů a kontrola souladu současného stavu s požadavky ZoKB a VoKB, případně NIS2 a dalšími platnými souvisejícími předpisy (dle platné legislativy), a GDPR a souvisejícími právními předpisy (identifikace konkrétních nesouladů).

- Analytický výstup popisující přístup řešení dále uvedených oblastí v prostředí SŽ (definování postupu kroků v rámci segmentace, specifikace postupu vlastní konfigurace, stanovení pořadí konfigurace jednotlivých prvků, přístup k migraci, definice rizik a jejich mitigace).
- Zhodnocení vstupů a konsolidace výkonnostních parametrů routerů, zdali jsou technologicky připraveny z hlediska nové VRF segmentace.
- Odsouhlasený návrh pilotu v požadované pilotní lokalitě.

3.1.2 Specifikace změn architektury

Předmětem této části je návrh změny architektury uživatelské sítě a definice pravidel segmentace ze strany Dodavatele, a to na základě podkladů od Zadavatele.

Výstupem bude návrhový dokument obsahující strukturu segmentace, bezpečnostní pravidla a technické detaily řešení dle níže uvedených požadavků.

Součástí dodávky bude vytvoření testovacích scénářů pro ověření funkčnosti nastavených pravidel. Verifikace bude provedena v rámci akceptace fáze Zadavatelem. Koncepce předpokládaného řešení je uvedena v příloze č. 13.

Oblast	Činnost
Základní specifikace změn architektury	Výstup Dodavatele <ul style="list-style-type: none"> • Schéma zapojení NGFW ve vrstvách L1 – L3 OSI modelu. • Definice segmentačních pravidel routování VRF • Popis komponent nové architektury. • Návrh změn propojení mezi PE a CE routery. Dokumentace bezpečnostních mechanismů pro NGFW.
Definice VRF instancí a jejich účelu	Výstup Dodavatele <p>Analytický výstup Dodavatele musí pokrývat níže uvedené oblasti:</p> <ul style="list-style-type: none"> • Seznam nových VRF instancí. • Popis účelu každé VRF instance. • Definice „routovacích“ politik mezi VRF. • Návrh bezpečnostních politik pro každou VRF. • Definice IPv4 adresních rozsahů pro každý segment. • Rezervace adresních rozsahů pro budoucí růst. • Dokumentace překryvných sítí pro VRF.

	<ul style="list-style-type: none"> • Plán pro migraci IP adres.
Definice postupu konfiguračních prací	Výstup Dodavatele Analytický výstup Dodavatele musí pokrývat níže uvedené oblasti: <ul style="list-style-type: none"> • Návrh nastavení konfiguračních pravidel. • Pořadí konfigurace jednotlivých prvků. • Plán migrace do nových segmentů sítě. • Návrh implementace Konceptu segmentace SŽ. do prostředí pilotní lokality. • Návrh nastavení implementačních postupů. • Návrh procesního zajištění konfigurace v rámci organizace SŽ.

3.1.3 Analýza a návrh řešení pro specifikum geo-redundance

SŽ aktuálně disponuje dvěma konektivitami do sítě Internet, v Praze a Plzni.

Na základě úvodní části 3.1.1 *Zhodnocení stávající síťové infrastruktury SŽ* a 3.1.2 *Specifikace změn architektury* segmentované sítě dojde k vytvoření analytického výstupu pro možnosti nastavení geo-redundance konektivity v těchto lokalitách.

Analytický výstup musí pokrývat minimálně tato témata:

- Zhodnocení stávajícího stavu.
- Návrh infrastrukturního nastavení obou lokalit v režimu Active – Passive, příp. Active – Active.

3.1.4 Příprava implementačních kroků pro realizaci vlastní segmentace v pilotní lokalitě

Příprava implementačních kroků pro realizaci vlastní segmentace v závislosti na inventuře stávající sítě ve spolupráci s provozními složkami Zadavatele v pilotní lokalitě. Cílem této implementační části je provést segmentaci v rámci pilotního provozu vydefinované a schválené lokality takovým způsobem, aby pověření pracovníci Zadavatele mohli provádět segmentaci sítě v budoucnu již bez asistence ze strany Dodavatele.

Role Dodavatele v této fázi je podpůrná, konzultační, poskytuje doporučení. Vlastní konfigurační práce budou vykonávány pracovníky Zadavatele.

Oblast	Činnost
Příprava prostředí	Zajistí Zadavatel <ul style="list-style-type: none"> • Fyzická instalace NGFW do prostředí SŽ. Zajistí Dodavatel

	<ul style="list-style-type: none"> Konfigurace NGFW v prostředí SŽ přes definované VPN připojení.
Nastavení VRF v prostředí SŽ	Zajistí Zadavatel <ul style="list-style-type: none"> Vytvoření testovacích VRF instancí. Konfigurační specifikace směrování mezi VRF. Specifikace implementace bezpečnostních politik.
Implementace směrovacích protokolů – routing	Zajistí Zadavatel <ul style="list-style-type: none"> Konfigurace BGP pro páteřní směrování. Nastavení OSPF pro interní směrování. Implementace redundantních cest. Optimalizace směrovacích metrik. Testování „failover“ scénářů. Vytvoření testovacích scénářů (podléhá odsouhlasením Zadavatele).
Testovací prostředí a zátěžové testy v síti SŽ, případně v testovacím prostředí Dodavatele	Zajistí Zadavatel <ul style="list-style-type: none"> Definice typu testování Testování maximální propustnosti. Validace latence a jitter. Stress testy bezpečnostních funkcí. Testování vysoké dostupnosti (trhací testy). Zajistí Dodavatel <ul style="list-style-type: none"> Příprava testovacích dat (konzultace). Testy izolace mezi VRF (konzultace). Poskytnutí testovacího prostředí (generátor provozu) pro testování NGFW pravidel definovaných během analýzy.
Bezpečnostní testování	Zajistí Zadavatel <ul style="list-style-type: none"> Validace segmentace. Testování bezpečnostních politik. Ověření logování a auditních záznamů. Návrh analýzy bezpečnostních rizik. Zajistí Dodavatel <ul style="list-style-type: none"> Plnou podporu při identifikaci a odstranění nálezů z testování a návrh nápravných opatření. Spolupráce na implementaci nápravných opatření.
Optimalizace konfigurace	Zajistí Zadavatel <ul style="list-style-type: none"> Dokumentace provedených změn.

- Na základě zjištění Dodavatel uvede návrh optimalizace konfigurace.

3.1.5 Implementační plán pro celou uživatelskou síť

Na základě části 3.1.1 *Zhodnocení stávající síťové infrastruktury SŽ* a 3.1.2 *Specifikace změn architektury* segmentované sítě a úspěšně otestovaném pilotním řešení pro definovanou pilotní lokalitu, dle článku 3.1.4, Dodavatel připraví detailní plán segmentace (jak postupovat) pro další lokality uživatelské sítě v prostředí SŽ.

Oblast	Činnost
Implementační plán	<p>Výstup Dodavatele</p> <p>Na základě úspěšně otestovaného pilotního řešení vytvoření dokumentu, popisujícího kroky pro provedení segmentace pro další lokality v následujícím časovém období. Je očekáváno, že primární výstupem Dodavatele bude zpracování detailního návrhu projektového implementačního postupu konfiguračních prací. Výstup musí být aplikovatelný pro každou lokalitu (šest oblastních ředitelství) a musí minimálně obsahovat:</p> <ul style="list-style-type: none"> • Časový harmonogram implementace. • Rozdělení úkolů a odpovědností mezi členy týmu SŽ. • Postup pro konfiguraci síťových zařízení (přepínače, směrovače, firewallly). • Plán migrace existujících systémů do nových segmentů.
Rozvojový plán	<p>Výstup Dodavatele</p> <p>Vytvoření dokumentu, který navrhne strategii s ohledem na budoucí další dílčí segmentaci v rámci pokračování projektu a budoucího rozvoje.</p> <ul style="list-style-type: none"> • Nastavení postupů pro izolaci napadené části sítě • Nastavení pravidel pro detekci hrozeb • Optimalizace bezpečnostních nastavení

3.2 Dodávka celkem 12 kusů NGFW a souvisejících komponentů dle uvedené specifikace

3.2.1 Technické požadavky na dodávku Next Generation Firewall

3.2.1.1 Technická specifikace položky A:

V oblasti dodávky **dvou (2)** kusů zařízení NGFW definuje Zadavatel následující požadavky pro každé z nich:

Oblast	Požadavek
Typ zařízení	Fyzické ve standardním provedení do rozvaděče o šířce 19 palců.
Minimální počet 25 Gbps rozhraní	4x SFP+
Minimální počet 10 Gbps rozhraní	4x SFP+
Dosažitelná reálná propustnost při zapnutých funkcionalitách Firewall, IPS a/nebo IDS, Aplikační kontrola	Minimálně 40 Gbps provozu označovaného jako „Enterprise Mix traffic“.
SSL/TLS inspekce až do propustnosti	Minimálně 20 Gbps
Celková minimální propustnost	60 Gbps
Minimální propustnost NGFW	60 Gbps

3.2.1.2 Technická specifikace položky B:

V oblasti dodávky **deseti (10)** kusů zařízení NGFW definuje Zadavatel následující požadavky pro každé z nich:

Oblast	Požadavek
Typ zařízení	Fyzické ve standardním provedení do rozvaděče o šířce 19 palců.
Minimální počet 25 Gbps rozhraní	4x SFP+
Minimální počet 10 Gbps rozhraní	4x SFP+

Dosažitelná reálná propustnost při zapnutých funkcionalitách Firewall, IPS a/nebo IDS, Aplikační kontrola	Minimálně 20 Gbps provozu označovaného jako „Enterprise Mix traffic“.
SSL/TLS inspekce	Minimálně 8 Gbps
Minimální propustnost IPS a/nebo IDS	30 Gbps
Minimální propustnost NGFW	30 Gbps

3.2.1.3 Obecné požadavky pro položky A i B:

Oblast	Požadavek
Propustnost SSL/TLS inspekce	Minimálně TLS 1.2 a TLS 1.3.
Interní virtualizace	Požadována možnost potencionální virtualizace (minimálně 2 samostatných administrativně nezávislých virtuálních zařízení bez nutnosti pořízení dodatečné licence).
Podpora pravidel na základě identit uživatelů	Firewallová pravidla umožňují řízení provozu na základě uživatelské identity a uživatelských skupin, ve kterých je uživatelská identita členem.
Způsoby ověřování uživatelů či napojení na autentizační systémy	Podpora proaktivního ověřování pomocí protokolu LDAP, NTLMv2, RADIUS a TACACS+. Dále je požadována SSO funkcionalita na základě proaktivního vyčítání událostí o přihlášení ze systému Active Directory.
Módy vysoké dostupnosti klastru	Podpora režimů Active-Passive.
Aplikační kontrola	Detekce a řízení síťových aplikací. minimálně 4000 rozpoznávaných aplikací.
Směrování provozu	Podpora statického, policy based a dynamického směrování provozu.
Velikost lokálního úložiště	Minimálně 100 GB.
Ochrana proti DoS a DDoS útokům	Ano.

Podpora pravidel na základě identit uživatelů	Ano.
Vzdálená správa	<ul style="list-style-type: none"> Vzdálená správa s dedikovaným vlastním portem 1Gbps. Možnost vzdálené aktualizace firmware. Podpora protokolu SNMP minimálně ve verzi 2c. Podpora protokolu Syslog a předávání logů na vzdálený systém
Další funkcionality	Antibot, Ochrana DNS.
Podpora IPS a/nebo IDS	Licence by měla pokrývat funkcionality IPS a/nebo IDS v rozsahu funkčně obdobném se Snort 3 (reference snort.org) nebo lepším (licence pro inspekci HTTPS není podmínkou).
Napájení	2x napájecí zdroj AC 230 V.

Zařízení NGFW musí být dodány včetně veškerých potřebných licencí k provozu požadovaných služeb, viz. detailnější obecné požadavky uvedené v předchozí kapitole, s dobou platnosti a veškerými systémovými update po dobu 60 měsíců od ukončení fáze F2.1.

3.2.2 Dodávka SFP+ modulů

Požadujeme dodání kompatibilních SFP+ modulů pro dodaná NGFW zařízení v následujících počtech:

SFP+ Modul (Rychlost)	Počet
10 Gbps/25 Gbps	48 kusů.

Specifikace SFP+ modulů:

- Typ: Multimode.
- Konektor: LC duplex.
- Kompatibilita: NGFW zařízení dle specifikace výrobce
- Podpora rychlostí 10 Gbps i 25 Gbps
- DMI diagnostika.

3.2.3 Implementace Next Generation Firewall

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

Oblast	Činnost
Dodávka zařízení	Zadavatel požaduje dodávku zařízení do jedné lokality organizace SŽ v Praze. Tato lokalita bude upřesněna před ukončením fáze F1.1. Následná distribuce všech těchto zařízení do finálních lokalit a fyzická instalace do racků bude v režii Zadavatele.
Základní konfigurace	<ul style="list-style-type: none"> • Ověření zařízení na absenci HW vad. • Registrace zařízení. • Instalace výrobcem doporučené verze operačního systému. <ul style="list-style-type: none"> ◦ Konfigurace základních parametrů (management rozhraní, hostname, DNS, NTP, administrátorské přístupy, napojení na centrální uživatelský systém (LDAP/RADIUS), odesílání událostí do externího zařízení).
Konfigurace vysoké dostupnosti (HA)	Nasazení v režimu Active – Passive.
Síťová konfigurace	<ul style="list-style-type: none"> • Linková agregace. • IP adresace a VLAN tagy. • Směrování. • DHCP relay.
Vytvoření objektů a bezpečnostní politiky	<ul style="list-style-type: none"> • Specifikace nových pravidel pro nové NGFW. • Návrh jmenné konvence pravidel a objektů dle akceptované metodiky.
Dodavatel definuje vzorové bezpečnostní politiky dle vzoru Zadavatele	<ul style="list-style-type: none"> • IPS a/nebo IDS. • Application Control.
SSO Autentizace	Napojení na Active Directory řízení přístupů na základě identit.

3.2.4 Nástroj centrální správy NGFW

Zadavatel požaduje plnou kompatibilitu dodávaných firewallů s jedním ze současných nástrojů centrální správy a managementu, které již provozuje (Panorama a FMC – Firewall Management Center).

Pokud nebude možné zajistit plnou kompatibilitu dodávaných NGFW Dodavatelem se současným centrálním managementem, je Dodavatel povinen v rámci své dodávky dodat a naimplementovat v prostředí Zadavatele nový nástroj centrální

správy NGFW včetně příslušných licencí s dobou platnosti a veškerými systémovými update po dobu 60 měsíců od doručení nástroje centrální správy, který bude splňovat následující požadavky:

3.2.4.1 Požadavky na nástroj centrální správy NGFW

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

Oblast	Požadavek
Typ nástroje	Nástroj může být realizován jako fyzický nebo virtualizovaný, optimálně s podporou pro virtualizační platformu VMware.
Počet spravovaných zařízení	Nástroj centrální správy musí umožnit správu minimálně 12 fyzických zařízení.
Práce s událostmi	Nástroj centrální správy umožňuje příjem a uložení událostí v minimálním množství 10 GB událostí za den s možností licenčního rozšíření minimálně na 50 GB událostí za den.
Pokročilá analýza událostí	Nástroj centrální správy umožňuje základní analýzu událostí za účelem včasné identifikace reálné či potencionální hrozby. Primárně bude pro vyhodnocování incidentů používán nástroj aktuálně využívaný v prostředí SŽ, log management a SIEM.

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

Oblast	Činnost
Dodávka nástroje	Dodávka nástroje do lokality Praha. V případě virtualizovaného zařízení poskytnutí instalačních dat skrze internetovou konektivitu.
Základní konfigurace	<ul style="list-style-type: none"> Ověření zařízení na absenci HW vad (pouze u fyzického zařízení). Registrace zařízení. Instalace výrobcem doporučené verze operačního systému. <ul style="list-style-type: none"> Konfigurace základních parametrů (management rozhraní, hostname, DNS, NTP, administrátorské přístupy, napojení na centrální uživatelský systém (LDAP/RADIUS), odesílání událostí do externího zařízení).

Připojení spravovaných zařízení	Integrace dodaných NGFW do centrální správy.
Součinnost při konfiguraci	Poskytnutí plné podpory Dodavatele při konfiguraci dodaného nástroje až po úplné spuštění nástroje pro centrální správu NGFW.

3.3 Školení

V oblasti odborného školení je požadováno následující plnění:

Typ školení	Popis
Základní školení	Úvodní seznámení s produktem pro 7 zástupců Zadavatele v rozsahu min. 1 MD a poskytnutí školících materiálů.
Odborné školení	<p>Dodavatel zajistí pro 7 zástupců Zadavatele odpovídající, výrobcem NGFW certifikované, školení dodávané technologie, včetně nástroje centrální správy, které odpovídá požadavkům na každodenní správu a údržbu zařízení, správu z pohledu kybernetické bezpečnosti a kybernetického monitoringu (například představení kybernetických funkcionalit, jejich napojení na dohledové nástroje typu SIEM a využití NGFW pro forenzní šetření).</p> <p>Obecné požadavky na školení</p> <ul style="list-style-type: none"> • Dodavatel poskytne Zadavateli kompletní školící materiály k dodávaným nástrojům. • Školení bude realizováno v rozsahu minimálně 3 MD. • Školení bude realizováno prezenční formou v lokalitě Praha. • Zadavatel bude moci pořídit z celého školení obrazový i zvukový záznam, který bude moci dále využívat pro potřeby školení vlastních pracovníků a externích partnerů. • Školení nemusí být zakončeno certifikační zkouškou.

3.4 Post-implementační a technická podpora

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

Oblast	Požadavky
--------	-----------

Technická podpora výrobce	<p>Zařízení nesmí mít oznámené EOS dříve než za 2 roky a oznámené EOL dříve než za 5 let. Dodavatel zajistí oficiální podporu výrobce po dobu 60 měsíců od dodávky technologií a licencí (fáze F2.1), která zahrnuje minimálně:</p> <ul style="list-style-type: none"> • Režim podpory 8x5 (8 hodin denně v rámci pracovních dní, reakční doba 4 hodiny). • Doručení vadného dílu v režimu NBD. • Podpora dostupná na webovém portálu výrobce, e-mailu a telefonu. • Přístup k novým verzím firmware či OS. • Aktualizace bezpečnostních definic pro funkcionality definované v kapitole 3.1.
Post-implemenční podpora Dodavatele	<p>Dodavatel zajistí post-implemenční podporu Zadavatele v rozsahu:</p> <p>(1) Poskytování expertních služeb, které budou využívány zejména pro podporu činností SŽ v případě řešení nestandardních stavů a pro profylaxi řešení, aby se předcházelo omezením jeho správné funkčnosti.</p> <p>(2) Konzultace při konfiguraci síťových komponentů a realizaci segmentační strategie definované výstupy této Veřejné zakázky.</p> <p>(3) Post-implemenční podpora bude poskytována po dobu 5 let od ukončení fáze 4.</p> <p>(4) Post-implemenční podpora bude poskytována v souladu s ustanoveními Zvláštních obchodních podmínek pro Zakázky v oblasti ICT (Příloha č. 5 Závazného vzoru smlouvy) podle servisního modelu A5). Plánované změny či významné změny (aktualizace, patch atd.) budou ze strany Dodavatele poskytnuty (uvolněny) SŽ vždy v pracovních dnech, a to konkrétně v pondělí a ve středu. V případě, že plánovaná změna či významná změna a její poskytnutí vychází na státní svátek, vyzve Dodavatel SŽ k upřesnění poskytnutí (uvolnění).</p> <p>(5) Poskytování služeb Helpdesku ze strany Dodavatele bude realizováno v souladu s ustanoveními Zvláštních obchodních podmínek pro Zakázky v oblasti ICT (Příloha č. 5 Závazného vzoru smlouvy) v Režimu 3 (5x8, tj. v pracovních dnech v době od 9:00 do 17:00 na telefonním čísle určeném Dodavatelem) a bude poskytovat podporu na třetí úrovni (L3) v souladu s ustanoveními Zvláštních obchodních podmínek pro</p>

Zakázky v oblasti ICT (Příloha č. 5 Závazného vzoru smlouvy).

(6) Měření SLA bude realizováno na straně Zadavatele.

(7) Součinnost při auditech řešení, opravu a zapracování identifikovaných nedostatků.

3.5 Konzultační služby na vyžádání

V oblasti konzultačních služeb jsou definovány následující požadavky:

Oblast	Požadavky
Konfigurační konzultace a práce	Dodavatel poskytne konfigurační a konzultační práce prostřednictvím rolí Seniorní systémový produktový inženýr, Specialista NGFW v oblasti dodané technologie, který Zadavateli umožní konzultovat konfigurační parametry dodaného řešení.
Analytická konzultace	Dodavatel poskytne analytické konzultační práce prostřednictvím role Systémový analytik v oblasti dodané technologie, který Zadavateli umožní konzultovat analytické parametry dodaného řešení.

Maximální počet k čerpání všech Konzultačních služeb na vyžádání je 35 MD. Tyto služby budou čerpány až po akceptaci výstupů F1 a dodávky a implementaci komponentů F2. SŽ není povinna Konzultační služby na vyžádání čerpat.

4 Fáze dodávky a akceptační milníky

Plnění musí být dodáno v níže uvedených fázích. Každá z níže uvedených fází (tj. každý řádek níže uvedené tabulky) je součástí jednoho z uvedených čtyř akceptačních milníků (A až D) a musí být Zadavatelem akceptována nejpozději v termínu uvedeném v Harmonogramu. Zadavatel akceptuje výstupy dané akceptační fází, jestliže je Dodavatel provedl v šíři a kvalitě požadované v zadávací dokumentaci této veřejné zakázky. V opačném případě je Dodavatel povinen napravit nedostatky plnění.

Akceptační milník	Fáze	Popis	Způsob akceptace fáze	Kapitola obsahující požadavky
A	F1.1	Zhodnocení stávající síťové infrastruktury	Akceptační protokol: <ul style="list-style-type: none"> • Zhodnocení návrhu koncepce segmentace uživatelské sítě SŽ • Zhodnocení souladu současného stavu s požadavky ZoKB, NIS2, GDPR, ISO IEC: 27033 v plném znění (identifikace konkrétních nesouladů) • Analytický výstup popisující přístup řešení v prostředí SŽ • Odsouhlasený návrh pilotu v požadované pilotní lokalitě 	3.1.1
	F1.2	Základní školení	<ul style="list-style-type: none"> • Realizace školení s parafovanou prezenční listinou 	3.3
B	F2.1	Dodávka NGFW a související komponentů dle uvedené specifikace	<ul style="list-style-type: none"> • Posouzení parametrů dodávaných komponent a Akceptační protokol: Dodávka NGFW dle specifikace ZD • Dodávka SFP+ modulů • Dodávka licencí dle funkční specifikace, viz. kapitola 3.2.1 • Dodávka nástroje centrální zprávy 	3.2
C	F2.2	Specifikace změn architektury	Akceptační protokol: Pokrytí témat definovaných v bodu 3.1.2	3.1.2
D	F3.1	Implementace NGFW a související komponentů dle uvedené specifikace	Akceptační protokol: <ul style="list-style-type: none"> • Konfigurace komponent 	3.2

Akceptační milník	Fáze	Popis	Způsob akceptace fáze	Kapitola obsahující požadavky
			<ul style="list-style-type: none"> Implementace NGFW do nástroje centrální správy 	
D	F3.2	Příprava implementačních kroků pro realizaci vlastní segmentace	Akceptační protokol: <ul style="list-style-type: none"> Pokrytí témat definovaných v bodu 3.1.4 Na základě výstupu testování akceptace finálního návrhu 	3.1.4
D	F4.1	Analýza a návrh řešení pro specifikum geo-redundance	Akceptační protokol potvrzující, že výstup obsahuje: <ul style="list-style-type: none"> Zhodnocení stávajícího stavu Návrh infrastrukturního nastavení obou lokalit v režimu Active - Active nebo Active - Passive 	3.1.3
D	F4.2	Implementační plán pro celou uživatelskou síť SŽ	Akceptační protokol: <ul style="list-style-type: none"> Zpracování detailního návrhu projektového implementačního postupu konfiguračních prací 	3.1.5
	F4.3	Odborné školení	<ul style="list-style-type: none"> Předání školících materiálů Realizace školení Realizace školení s parafovanou prezenční listinou 	3.3
	F5	Post-implementační a technická podpora:	Fáze F5 bude vykazována na základě pravidelných měsíčních výkazů	3.4
	F6	Konzultační služby na vyžádání	Fáze F6 bude realizována na základě objednaných služeb dle příslušných objednávek	3.5

5 Vyloučení technologií

Vyloučení technologií představujících kybernetickou hrozbu

Dne 17. prosince 2018 vydal Národní úřad pro kybernetickou a informační bezpečnost 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:

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

1.2. ZTE Corporation, Šen-čen, Čínská lidová republika“.

Dne 4. ledna 2019 vydal Národní úřad pro kybernetickou a informační bezpečnost 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 na dodávky, jak je jeho povinností podle § 5 a § 8 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, ve znění pozdějších předpisů. V návaznosti na to Zadavatel identifikoval rizika spojená s výše uvedenými technickými a programovými prostředky jako neakceptovatelná a současně opatření k jejich zvládnutí, kterým je nepřipouštění použití těchto prostředků v rámci plnění veřejné zakázky.

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.

Příloha č. 3 Zadávací dokumentace

DOHODA O OCHRANĚ DŮVĚRNÝCH INFORMACÍ

k veřejné zakázce:

„Segmentace sítě“

Zadavatel: **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

Dodavatel: **[DOPLNÍ DODAVATEL]**

společnost zapsaná v obchodním rejstříku vedeném **[DOPLNÍ DODAVATEL]**
soudem v **[DOPLNÍ DODAVATEL]**, oddíl **[DOPLNÍ DODAVATEL]**, vložka
[DOPLNÍ DODAVATEL]

se sídlem: **[DOPLNÍ DODAVATEL]**

IČO: **[DOPLNÍ DODAVATEL]**, DIČ: **[DOPLNÍ DODAVATEL]**

oddíl **[DOPLNÍ DODAVATEL]**, vložka **[DOPLNÍ DODAVATEL]**

zastoupená: **[DOPLNÍ DODAVATEL]**

(Zadavatel a Dodavatel společně také jako „**Strany**“)

dnešního 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**“)

1. ÚČEL DOHODY

1.1. Zadavatel zadává nadlimitní sektorovou veřejnou zakázku s názvem „**Segmentace sítě**“, (dále jen „**Veřejná zakázka**“) podle ustanovení zákona č. 134/2016 Sb., o zadávání veřejných zakázkách, ve znění pozdějších předpisů (dále jen „**ZZVZ**“). Dodavatel s úmyslem účastnit se zadávacího řízení na zadání Veřejné zakázky požaduje vydání částí zadávací dokumentace uvedených v Příloze č. 1 této Dohody, 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 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 v zadávacím 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 v zadávacím 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 4 této Dohody.
- 3.5. Po doručení této podepsané Dohody ze strany Dodavatele Zadavateli prostřednictvím elektronického nástroje E-ZAK, bude ve lhůtě dle § 96 odst. 2 ZZVZ předán Dodavateli přístupový údaj k Důvěrným informacím – heslo k neveřejné části zadávací dokumentace k Veřejné zakázce, a to formou SMS zprávy zasláné 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 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 (dále jen „**Poddodavatelé**“), zavazuje se sdílet s těmito osobami Důvěrné informace jen v souladu s tímto článkem 4 této Dohody.
- 4.2. Za Poddodavatele se považuje jakákoliv třetí osoba spolupracující s Dodavatelem dle odst. 4.1 této Dohody 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 zadávacího řízení na zadání Veřejné zakázky, nepodal-li nabídku před jejím uplynutím;
 - 5.1.2. skončení účasti Dodavatele v zadávacím řízení na zadání Veřejné zakázky nebo ukončení zadávacího 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 známy 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 nevyklučuje, na právní nástupce Stran.
- 7.4. 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.
- 7.5. Nedílnou součástí Dohody tvoří tyto přílohy:

Příloha č. 1: Specifikace Důvěrných informací

Strany prohlašují, že si tuto Dohodu přečetly, že s jejím obsahem souhlasí a na důkaz toho k ní připojují svoje podpisy.

Za Zadavatele

V Praze dne _____

Za Dodavatele

V [DOPLNÍ DODAVATEL], dne [DOPLNÍ
DODAVATEL]

.....
Správa železnic, státní organizace

Ing. Dalibor Fajkus

ředitel organizační jednotky

Správa železniční telematiky

.....
[DOPLNÍ DODAVATEL]

[DOPLNÍ DODAVATEL]

Příloha č. 1 Dohody o ochraně důvěrných informací**Specifikace Důvěrných informací**

Zadavatel poskytuje Dodavateli níže uvedené Důvěrné informace. Heslo k zpřístupnění těchto dokumentů bude po podpisu této Dohody předáno Dodavateli prostřednictvím SMS na telefonní číslo jím určené v Dohodě.

Seznam Důvěrných informací:

- a) Příloha č. 12 zadávací dokumentace na Veřejnou zakázku – Popis prostředí

Zvláštní obchodní podmínky pro Zakázky v oblasti ICT

OBSAH

1. VÝKLAD POJMŮ.....	2
2. DOBA A MÍSTO PLNĚNÍ.....	8
3. PRÁVA A POVINNOSTI OBOU STRAN	8
4. POVINNOSTI DODAVATELE.....	9
5. POVINNOSTI OBJEDNATELE	10
6. LICENČNÍ UJEDNÁNÍ	10
7. ZDROJOVÝ KÓD A DOKUMENTACE	14
8. AKCEPTAČNÍ ŘÍZENÍ	15
9. ŠKOLENÍ	17
10. HELPDESK.....	17
11. NAHLÁŠENÍ INCIDENTU	18
12. SERVISNÍ MODELY	19
13. ÚČAST PODDODAVATELŮ.....	21
14. REALIZAČNÍ TÝM	21
15. KOMUNIKACE STRAN	22
16. SMLUVNÍ POKUTY.....	22
17. ZÁRUKA ZA JAKOST A PRÁVA Z VADNÉHO PLNĚNÍ	24
18. UKONČENÍ SMLUVNÍHO VZTAHU	25
19. ZMĚNY SMLOUVY A ZMĚNOVÉ ŘÍZENÍ	26
20. KYBERNETICKÁ BEZPEČNOST	27
21. OCHRANA OSOBNÍCH ÚDAJŮ	31
22. OCHRANA DŮVĚRNÝCH INFORMACÍ.....	32

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 Objednatелеm. 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 částí Předmětu Smlouvy a limitu stanoveného v této Smlouvě jako maximální souhrnná hodnota bez DPH všech dílčích smluv uzavřených na základě této Smlouvy.
- 1.8. **Čas nahlášení Incidentu** představuje časový údaj, vyjadřující datum a čas, kdy byl Incident nahlášen Dodavateli způsobem stanoveným ve Smlouvě a ZOP, tj. vytvořením ticketu v Helpdesku, vytěžením e-mailu z e-mailového serveru Objednatele a jeho vložení 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/člověkodenní. 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 optimalizací funkce Softwaru nad rámec Aktualizace, zpravidla v IT označovaná jako „update“ (v rámci IT se také často označuje jako změna druhé číslice v čísle verze Softwaru, tedy např. 4.1. na 4.2.).
- 1.35. **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 ZZZV 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 trvajících či opakujících 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 Ohlašovatel.
- 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 nahlásování 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 takového Softwaru, neboť nebude nutné zasahovat do Zdrojových kódů takového Softwaru anebo proto, že případné nahrazení takového Softwaru nebude představovat výraznější komplikaci a náklad na straně Objednatele.
 - 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 zkompileovat 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 jejich 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 Poddodavatelem jako zaměstnanecké dílo ve smyslu § 58 odst. 1 a 7 Autorského zákona, a že je oprávněn k postoupení výkonu majetkových práv v souladu s tímto odst. 6.3 ZOP a má k takovému postoupení 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 jakékoli třetí osoby, jež budou vykonávat autorská majetková práva k tomuto Software.
- 6.3.5. Dodavatel dále prohlašuje, že vyloučil oprávnění autorů dle ustanovení § 58 odst. 3 Autorského zákona i vůči všem budoucím vykonavatelům autorských majetkových práv k Software.
- 6.3.6. Dodavatel dále převádí veškerá zvláštní práva pořizovatele k Databázím, jež tvoří součást Plnění. Nedojde-li z jakéhokoliv důvodu k převodu práva dle předchozí věty, uděluje Dodavatel Objednateli oprávnění k vytěžování a zužitkování celého obsahu takové Databáze nebo její kvalitativně nebo kvantitativně podstatné části a právo udělit jinému oprávnění k výkonu tohoto práva.
- 6.3.7. K ostatním majetkovým hodnotám, které spadají pod pojem Software a zároveň nespádají pod definici Autorského díla, uděluje Dodavatel Objednateli oprávnění v rozsahu dle odst. 6.3.8. ZOP. Ustanovení odst. 6.5 a 6.6 ZOP tímto nejsou dotčena.
- 6.3.8. Nevznikne-li Objednateli z jakéhokoliv důvodu ke kterékoliv části Softwaru oprávnění k výkonu autorských majetkových práv, uděluje Dodavatel Objednateli k dotčené části množstevně a územně neomezenou výhradní licenci ke všem známým způsobům užití, a to na dobu trvání autorských majetkových práv. Objednatel je oprávněn k dotčené části Softwaru udělovat licence, tyto dále postoupit a udělovat podlicence třetím osobám. Objednatel je dále oprávněn dotčené části upravovat a měnit (včetně Zdrojového a strojového kódu takové části Software), dokončovat, včetně práva takto upravené či dokončené části užívat, a dále tyto původní, upravené či dokončené

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

6.4. Nevýhradní licence k Software

- 6.4.1. Ve vztahu k Software Dodavatel tímto uděluje Objednateli okamžikem akceptace Plnění ve smyslu čl. 8 ZOP, nebo jinak vymezeným okamžikem akceptace Plnění Smlouvou a jejími přílohami nevýhradní oprávnění k výkonu práva 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 zužívat 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 povinen, po dohodě s Objednatelem, a v případě, že tato dohoda nebude možná, pak dle volby Dodavatele:
- a. na vlastní náklady dodat Objednateli Zdrojový kód předmětného Standardního Software a poskytnout Objednateli oprávnění užívat tento Standardní Software včetně Zdrojového kódu (včetně dalších způsobů nakládání) v rozsahu Licence dle odst. 6.4 ZOP; nebo
 - b. nahradit na vlastní náklady předmětný Standardní Software jiným Standardním Software, který bude mít alespoň srovnatelné funkcionality, kvalitu a technickou způsobilost jako nahrazovaný Standardní Software a zároveň splňovat podmínky stanovené v odst. 6.5.7 ZOP, a poskytnout k tomuto Standardnímu Software Objednateli Licenci k Standardnímu Software dle odst. 6.5 ZOP; nebo
 - c. nahradit na vlastní náklady předmětný Standardní Software vlastním Softwarem, tj. přeprogramovat část Díla představovanou předmětným Standardním Softwarem za využití vlastního Software vytvořeného na míru Objednateli, který bude mít alespoň srovnatelné funkcionality, kvalitu a technickou způsobilost jako nahrazovaný Standardní Software, a poskytnout k tomuto vlastnímu Softwaru Objednateli Licenci dle odst. 6.4 ZOP, a to včetně Zdrojového kódu.
- 6.5.9. Postupy dle odst. 6.5.8 písm. a) až c) ZOP podléhají samostatnému Akceptačnímu řízení. Vznikla-li Dodavateli povinnost dle odst. 6.5.8 ZOP, je Dodavatel povinen splnit povinnosti dle uvedeného odstavce i po ukončení Smlouvy. Ustanovení Smlouvy a ZOP relevantní pro splnění povinností dle předchozí věty se použijí i po ukončení Smlouvy.
- 6.5.10. Pokud v rámci Akceptačního řízení dle čl. 8 ZOP vyjde najevo, že Standardní Software nesplňuje podmínky odst. 6.5.7 ZOP, je Objednatel oprávněn Akceptační řízení přerušit, dokud Dodavatel nenapraví tento nedostatek předmětného Standardního Software jedním ze způsobů uvedených v odst. 6.5.8 ZOP. Objednatel není v takovém případě v prodlení.
- 6.5.11. Ustanovení odst. 6.3 a 6.6 ZOP se pro Standardní Software nepoužijí.

6.6. Software vztahující se k Hardware

- 6.6.1. V případech, kdy je k řádnému užívání dodaného Hardwaru potřebný určitý Software, je Dodavatel povinen poskytnout/zajistit Objednateli jako součást Plnění a za cenu zahrnutou v ceně Hardwaru, oprávnění užit tento Software v rozsahu, způsoby a za účelem obvyklým ve vztahu k Hardwaru, se kterým je spojen, nejméně však za podmínek dle Smlouvy a jejích příloh.
- 6.6.2. Ustanovení odst. 6.3 a 6.4 ZOP se pro Software vztahující se k Hardwaru nepoužijí.

6.7. Společná ustanovení

- 6.7.1. Nestanoví-li Smlouva a její přílohy či jiné části Zadávací dokumentace jinak, je Dodavatel při plnění Smlouvy oprávněn využít programy s otevřeným kódem či jejich části distribuovanými pod FOSS licencemi. Dodavatel však není oprávněn využít programy s otevřeným kódem či jejich části, které jsou distribuovány pod FOSS licencemi, jejichž podmínky by Objednateli ukládaly povinnost sdělovat nebo jinak šířit Software či jeho části, včetně Zdrojových kódů, třetím osobám, nebo umožnit jim změny, úpravy či jiné zásahy do Softwaru nebo jeho části.
- 6.7.2. Dodavatel je povinen zajistit Objednateli udělení oprávnění k veškerým programům s otevřeným kódem poskytnutým Objednateli v rozsahu takových FOSS licencí, které se na konkrétní program s otevřeným kódem, který je součástí Plnění, vztahují, přičemž konkrétní rozsah licence lze určit odkazem na soubor předávaný v rámci výstupu z Plnění anebo odkazem ve Zdrojovém kódu či jiným označením takové licence ve formátu vyžadovaném takovou veřejnou licencí, včetně odkazu na kompletní znění aktuálních licenčních podmínek příslušné FOSS licence; Dodavatel je dále povinen zajistit poskytnutí podpory k veškerým programům s otevřeným kódem, které jsou součástí Plnění, tj. povinnost Dodavatele zajistit poskytování nejnovějších verzí programů s otevřeným kódem a dalších služeb v souladu se standardními licenčními podmínkami programů s otevřeným kódem, a to alespoň na dobu trvání této Smlouvy. Ustanovení čl. 7 ZOP se pro programy s otevřeným kódem či jejich části, které jsou distribuovány pod FOSS licencemi, použije obdobně.
- 6.7.3. Dodavatel prohlašuje, že je oprávněn udělit Objednateli veškerá oprávnění v souladu s tímto článkem ZOP, má k takovému udělení veškeré potřebné souhlasy a jejich udělením Objednateli ani užíváním Plnění Objednatelem či uživateli Objednatele nebudou porušena práva duševního vlastnictví třetí osoby. Dodavatel odpovídá Objednateli za zajištění všech nezbytných oprávnění a souhlasů autora či autorů Software či Standardního Software k oprávněním udělovaným Objednateli dle tohoto článku ZOP. Dodavatel se zavazuje 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 uveřejněné 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 Dodavatelem skutečně předán Objednateli a ten se s ním mohl seznámit. Objednatel na žádost Dodavatele bez zbytečného odkladu potvrdí převzetí Předmětu Smlouvy k Akceptačnímu řízení v 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 Akceptačního protokolu společně s vyznačením „**Akceptováno**“, nebo „**Akceptováno s výhradou**“ je Předmět Smlouvy proveden.
- 8.1.11. Podpis Akceptačního protokolu s vyznačením „**Akceptováno s výhradou**“ nezbujuje 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 řádně provedeno akceptací výstupu, který byl předmětem hands-on školení dle odst. 8.1 ZOP.

8.5. **Akceptace ve vztahu k Hardware**

8.5.1. Je-li Předmětem Smlouvy či dílčí části, jež je určena k akceptaci, pouze dodání Hardware, použije se pro akceptaci odstavce 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, Objednatel ověřuje v rámci akceptace Hardware:

- a. parametry, vlastnosti a funkcionality uvedené ve specifikaci plnění Objednatele, která je součástí Smlouvy, a dále vlastnosti a funkcionality uvedené ve specifikaci plnění Dodavatele (je-li taková), která je součástí Smlouvy;
- b. příslušenství a dokumentaci, jež mělo být dodáno spolu s Hardware.

9. **ŠKOLENÍ**

9.1. Vyplývá-li ze Smlouvy Dodavateli povinnost poskytnout školení, aniž jsou blíže určeny jeho podmínky, zavazuje se Dodavatel poskytnout školení osobám určeným Objednatelem pomocí metod výkladu (zejména popis jednotlivých prvků a funkcionalit Předmětu Smlouvy ve vztahu k jeho užívání), praktických ukázek obsluhy Předmětu Smlouvy a zodpovězení dotazů školených osob tak, aby tyto osoby byly na základě provedeného školení ve vztahu ke svým rolím nebo pracovnímu zařazení (dle sdělení Objednatele) schopné plně porozumět svým odpovědnostem při obsluze Předmětu Smlouvy, provádět obsluhu v souvislosti se svou rolí nebo pracovním zařazením samostatně, a přitom minimalizovat riziko chybné obsluhy nebo závad na Předmětu Smlouvy.

9.2. Dodavatel provede zaškolení příslušných osob určených Objednatelem v termínu dle Smlouvy, a pokud takový termín není, pak v termínu určeném Objednatelem po dohodě s Dodavatelem.

9.3. Dodavatel je dále povinen provést v přiměřeném rozsahu školení příslušných zaměstnanců Dodavatele a dalších osob podílejících se na poskytování Plnění dle Smlouvy za účelem splnění povinností dle čl. 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:**

5x8, tj. osm (8) hodin pět (5) dní v týdnu.

10.4. Nestanoví-li Smlouva jinak, počíná časový rozsah dle zvoleného režimu dle odst. 10.3 ZOP (s výjimkou režimu 1) vždy zároveň s časovým rozsahem dle zvoleného Servisního modelu dle odst. 12.2 ZOP (např. pokud doba Servisního modelu začíná každý pracovní den v 7:00, provoz 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 Helpdesku mít nejpozději k okamžiku nabytí účinnosti Smlouvy zřízenou elektronickou adresu a telefonní linku a tuto adresu a telefonní číslo linky sdělit Objednateli, 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 Objedatele 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 nahlášován prostřednictvím Helpdesku, pak se za Čas nahlášení Incidentu považuje čas vytvoření ticketu v Helpdesku. Je-li Incident nahlášován písemně na e-mailovou adresu, pak se za Čas nahlášení Incidentu považuje čas odeslání e-mailu z e-mailového serveru Ohlašovatele, nebo v případě hlášení Incidentu telefonicky čas ukončení telefonického hovoru. Dodavatel je povinen prokazatelným způsobem bezodkladně potvrdit přijetí nahlášení Incidentu, a to vždy prostřednictvím 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:

- dočasné vyřazení Softwaru z provozu na základě předchozí dohody Objednatele a Dodavatele (odstávka),
- pravidelná vyřazení Softwaru z provozu Dodavatelem v časech sjednaných ve Smlouvě nebo její příloze (servisní okna),
- smluvními stranami předem dohodnutý časový úsek za účelem instalace upgradu,
- výpadky Softwaru způsobené Objednatelem přímo v důsledku jím provedených zásahů do Softwaru, které nebyly Dodavatelem předem schváleny,
- skutečnosti ve vztahu k Hardware dle odst. 12.9 ZOP za podmínky, 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:

$$Doba\ výpadku = \sum_{i=1}^n T_i$$

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:

- dočasná vyřazení Hardware z provozu na základě předchozí dohody Objednatele a Dodavatele (odstávka),
- pravidelná vyřazení Hardware z provozu Dodavatelem v časech sjednaných ve Smlouvě nebo její příloze (servisní okna)
- 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 využit k Plnění dle Smlouvy Poddodavatele neuvedené ve Smlouvě jen v případě, že to Smlouva výslovně připouští, a to za podmínek v ní uvedených. Nestanoví-li Smlouva jinak, podléhají jednotliví Poddodavatelé Významného dodavatele předchozímu písemnému schválení ze strany Objednatele. Dodavatel může ke schválení navrhnout nebo do Plnění Smlouvy zapojit pouze takové Poddodavatele, kteří nejsou v rozporu s požadavky Objednatele na Významného dodavatele.

14. 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 peněžitě 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:
- provozováním Díla Objednatelem v rozporu s Dokumentací;
 - neoprávněným nebo neodborným zásahem či nesprávným užitím Díla Objednatelem;
 - 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 nezabývá Dodavatele povinností 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:

- 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.
- 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.
- 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:

- 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.
- Dodavatel je v prodlení s Plněním dle Smlouvy déle než 60 dnů, a to i bez nutnosti zaslání předchozího upozornění.
- 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:
 - Dodavatel je opakovaně v prodlení s prováděním Plnění dle Smlouvy;
 - prohlášení Dodavatele učiněné na základě Smlouvy se ukáže jako nepravdivé;
 - Dodavatel bez upozornění a relevantního odůvodnění nepoužil k Plnění člena Realizačního týmu, ač k tomu byl povinen; nebo
 - 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 vyplývajících 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 zapláceno.

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 započatím 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 bezpečnostní 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 Objednatel. 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 požadovat se toho, aby Dodavatel odstranil vady vzniklé vadným postupem Dodavatele, zdržel se provádění postupů, které jsou v rozporu s tímto článkem, nebo konal, jak je od něj vyžadováno tímto článkem, a dále 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

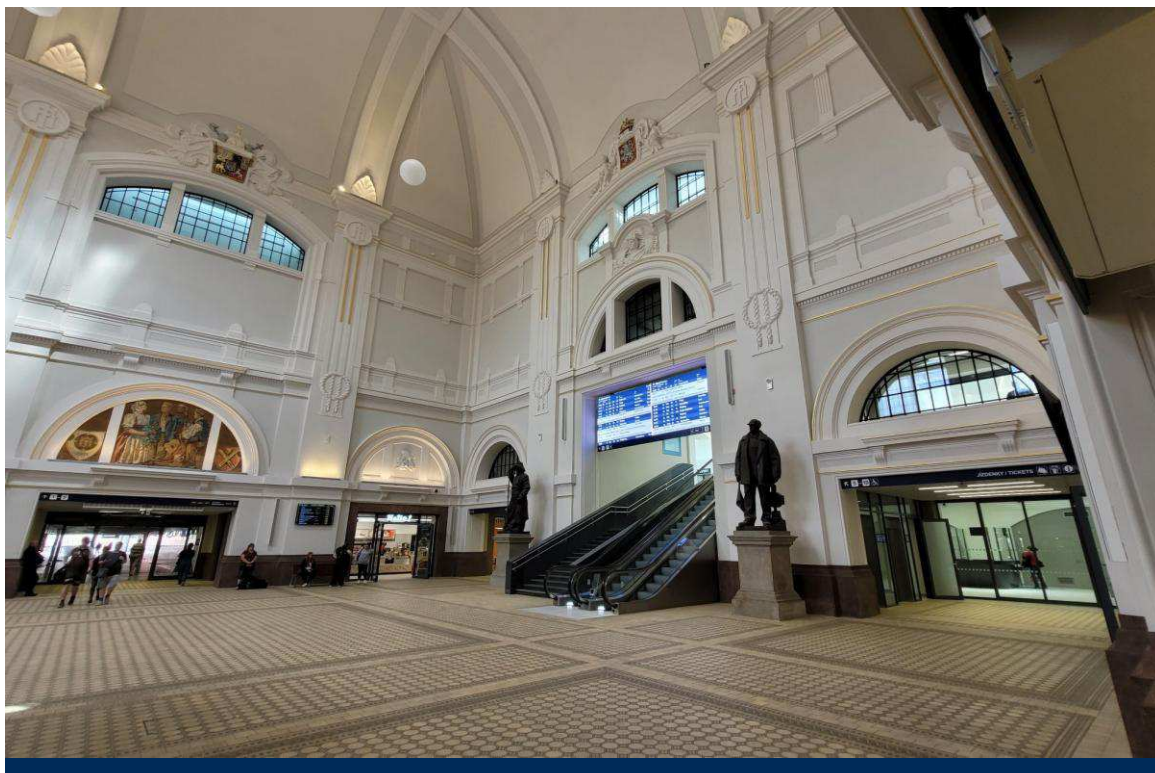
- 21.1. Budou-li údaje, ke kterým Dodavatel získá přístup v souvislosti s Plněním dle Smlouvy, mít povahu Osobních údajů, je Dodavatel povinen přijmout veškerá opatření k tomu, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k těmto Osobním údajům, jejich změně, zničení či ztrátě, neoprávněným 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 jakémkoliv 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.



Platforma SŽ Základní dokument

Červen 2025

Obsah

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

Seznam zkratek

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

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

Seznam vysvětlivek

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

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

4.2 Auditní záznamy

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

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

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

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

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

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

Pomocí aspoň jednoho z protokolů:

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

A musí obsahovat minimálně následující informace:

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

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

4.3 Provozovatelnost řešení

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

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

4.4 Znovupoužitelnost řešení

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

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

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

4.5 Nezávislost na dodavateli

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

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

4.6 Nákup a vývoj

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

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

4.7 Business kontinuita

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

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

5 Služby Platformy SŽ

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

5.1 Infrastrukturní služby

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

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

5.2 Platformní služby

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

Detailní přehled o infrastrukturních službách je předmětem Příloh Platformy SŽ.

5.3 Podpůrné služby

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

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

5.3.1 Bezpečnostní služby

Přehled dostupných služeb bezpečnostních aplikací

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

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

5.3.2 Služby monitoringu

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

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

5.3.3 Služby patch managementu

Popis služeb patch managementu, aktualizací a distribuce aplikací

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

5.3.4 Služby zálohování

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

5.3.5 Síťové služby

Přehled síťových služeb

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

6 Technologie Platformy SŽ

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

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

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

Použití takových zapouzdřených technologií je možné jen v následujících případech:

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

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

7 Přílohy Platformy SŽ

Jednotlivé oblasti jsou dále detailně zpracovány v těchto přílohách:

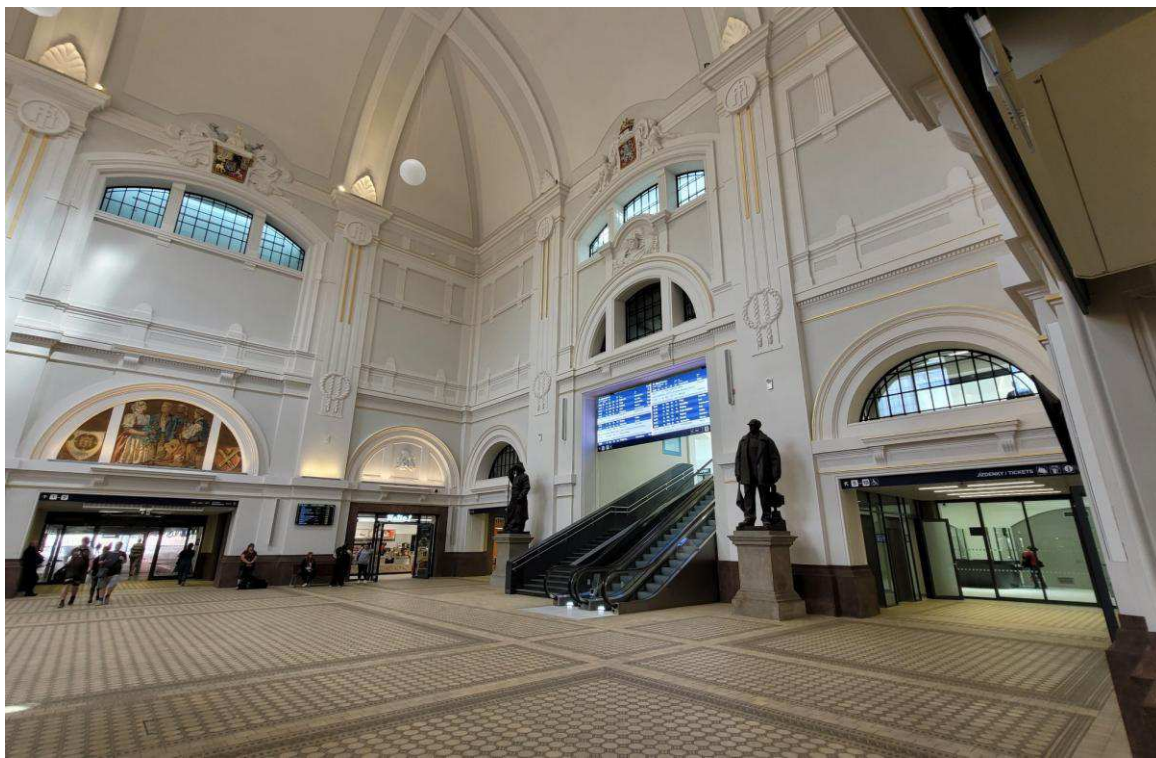
- Příloha 1 – Standardy softwarového vývoje
- Příloha 2 – Datová centra a serverovny
- Příloha 3 – Virtuální prostředí, serverové farmy a servery
- Příloha 4 – Konektivita a síťové prostředí
- Příloha 5 – Integrační standardy
- Příloha 6 – Komunikační standardy
- Příloha 7 – Standardy zálohování a disaster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

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

© 2025

Datum tisku
2025-07-30

spravazeleznic.cz



Platforma SŽ Standardy vývoje software

Červen 2025

Obsah

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

Seznam zkratek

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

Seznam vysvětlivek

E-R model

(Entity-Relationship model)

Platforma SŽ

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

1 Úvod

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

2 Standardy vývoje informačních systémů Správy železnic

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

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

2.1 Prostředí

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

2.1.1 Vývojové prostředí

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

2.1.2 Testovací prostředí

Testování probíhá v testovacím prostředí (TEST) v prostředí Správy železnic. Mimo prostředí Správy železnic probíhá testování jen v odůvodněných případech. Při testování se používají zcela oddělené instance databází a plně anonymizovaná data. Testovací prostředí musí co 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 takového software je plánováno pro menší desítky uživatelů, bez požadavku na vysokou dostupnost a možnosti škálování výkonu a rozložení zátěže prostřednictvím clusterování. U tohoto typu software nejsou definovány požadavky na vysokou odolnost proti chybám, rychlou reakci systému, nebo správu dat pro velké sítě.

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

2.2.1 Datová vrstva

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

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

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

2.2.2 Aplikační vrstva

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

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

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

2.3 Třívrstvá a vícevrstvá architektura

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

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

2.3.1 Datová vrstva

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

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

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

2.3.2 Aplikační vrstva

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

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

V rámci vývoje musí být ošetřena všechna bezpečnostní rizika 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 systém bude zabezpečovat konzistenci aplikační logiky, napříč všemi desktopovými klienty.

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

2.3.4 Integrační vrstva

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

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

V případě, že má být vyvíjená komponenta integrována se **spisovou službou SŽ**, musí splňovat požadavky na integraci prostřednictvím Národního standardu pro elektronické systémy spisové služby¹ a integrace musí být rozhraními definovanými v tomto standardu také realizována.

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

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

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

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

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

2.4 Požadavky na prezentační vrstvu

2.4.1 Uživatelské rozhraní

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

Pro návrh UI informačních systémů SŽ platí následující zásady:

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

2.4.2 Uživatelská zkušenost

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

UX informačních systémů SŽ musí splňovat následující vlastnosti:

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

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

2.5 Bezpečnost

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

Z pohledu požadavků na vyvíjený software je nutné zajistit oblasti:

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

2.5.1 Zabezpečení aplikací

Je požadováno, aby jednotlivé vrstvy splňovaly minimálně tyto požadavky:

- Ke komunikaci mezi jednotlivými vrstvami je používán systémový účet, který lze v případě ohrožení kybernetické bezpečnosti deaktivovat, nebo změnit.
- Systémový účet, který je využíván ke komunikaci mezi vrstvami není privilegovaným účtem.
- Všechny vrstvy jsou ošetřeny proti nejzávažnějším bezpečnostním rizikům jako jsou²:
 - Injection
 - Broken Authentication
 - Sensitive Data Exposure
 - XML External Entities (XXE)
 - Broken Access Control
 - Security Misconfiguration
 - Cross-Site Scripting (XSS)
 - Insecure Deserialization
 - Using Components with Known Vulnerabilities
 - Insufficient Logging&Monitoring
- Jednotlivé vrstvy uchovávají své konfigurační parametry v šifrované podobě.

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

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

Dodržování těchto standardů je potřeba průběžně ověřovat pomocí automatizovaných nástrojů, které dokáží odhalit porušení konvencí nebo potenciálně rizikové konstrukce již v rané fázi vývoje.

Neméně důležitou součástí procesu vývoje je pravidelná revize kódu prováděná druhým vývojářem před sloučením změn do hlavní vývojové větve. Uplatnění principu „čtyř očí“ pomáhá odhalit chyby a nedostatky ještě před nasazením do produkce a ověřit dodržování stanovených standardů i architektonických principů. Každý podstatný zásah do kódu proto musí projít nezávislou kontrolou, aby se do produkčního prostředí dostal pouze prověřený kód odpovídající požadované kvalitě.

Aplikace musí důsledně logovat všechny podstatné události v systému. Zejména veškeré administrátorské akce, změny konfigurací nebo zásadních oprávnění a přístupy k citlivým datům musí být zaznamenány v auditních záznamech s informací o tom, kdo a kdy danou operaci provedl.

Logy je doporučeno centralizovat pomocí nástroje typu SIEM, což umožní efektivní vyhledávání a detekci podezřelých aktivit a vytvoření ucelené auditní stopy pro potřeby bezpečnostních kontrol či vyšetřování incidentů. Je zároveň nezbytné zajistit integritu a důvěrnost těchto záznamů – přístup k nim smí mít pouze pověřené osoby a úložiště logů musí být chráněno proti neoprávněným zásahům.

2.5.2 Autentizace a autorizace

2.5.2.1 Autentizace

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

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

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

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

2.5.2.2 Autorizace

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

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

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

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

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

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

2.5.3 Zpracování osobních údajů

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

2.6 Dokumentace

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

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

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

2.6.1 Technická dokumentace jádra systému

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

2.6.2 E-R modely databáze

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

2.6.3 Objektový model pro aplikace

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

2.6.4 Procesní diagramy, schémata toků dat

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

2.6.5 Komunikační rozhraní

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

2.6.6 Drátové modely všech obrazovek uživatelského rozhraní aplikací

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

2.6.7 Popis konfigurace provozního prostředí

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

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

2.6.8 Uživatelská příručka

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

2.6.9 Příručka administrátora

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

2.6.10 Disaster Recovery postup (D/R Postup)

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

2.7 Modelování EA architektury

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

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

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

© 2025

Datum tisku
2025-07-30

spravazeleznic.cz



Platforma SŽ Datová centra a serverovny

Červen 2025

Obsah

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

Seznam zkratek

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

Seznam vysvětlivek

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

1 Úvod

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

Z pohledu ICT infrastruktury jde o lokality, kde jsou 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 umístovány technologie jak IT, tak OT. Tato datová centra jsou součástí technologických řídicích center, odkud je dálkově řízen železniční provoz.

2.1 Datové centrum CDP Praha

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

3.3 Serverovny vybraných organizačních jednotek

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

3.4 Technologické serverovny

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

3.5 Technologické a sdělovací místnosti

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

4 Technologické vybavení

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

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

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

4.1 Stavební provedení

Datová centra, serverovny a datové sály musí být projektovány v souladu se souborem norem ČSN EN 50600. Nepísaným 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

© 2025

Datum tisku
2025-07-30

spravazeleznic.cz

```
hdac0: <NVIDIA (0x0083) HDA CODEC> at cad 0
hdaa0: <NVIDIA (0x0083) Audio Function Group>
pcm0: <NVIDIA (0x0083) (HDMI/DP 8ch)> at nid
pcm1: <NVIDIA (0x0083) (HDMI/DP 8ch)> at nid
pcm2: <NVIDIA (0x0083) (HDMI/DP 8ch)> at nid
pcm3: <NVIDIA (0x0083) (HDMI/DP 8ch)> at nid
ugen0.1: <0x0086 XHCI root HUB> at usb0
uhub0: <0x0086 XHCI root HUB, class 9/0, rev
nvd0: <Samsung SSD 960 PRO 512GB> NVMe namesp
nvd0: 488386MB (1000215216 512 byte sectors)
ada0 at ahcich0 bus 0 scbus0 target 0 lun 0
ada0: <ST320LT012-9WS14C 0001LVM1> ATAB-ACS S
ada0: Serial Number W0VDEFBC
ada0: 300.000MB/s transfers (SATA 2.x, UDMA6,
ada0: Command Queueing enabled
ada0: 305245MB (625142448 512 byte sectors)
ada0: quirks=0x1<4K>
ada1 at ahcich4 bus 0 scbus4 target 0 lun 0
ada1: <ST4000DM000-1F2168 CC52> ATAB-ACS SATA 3
ada1: Serial Number Z300YNB5
```

Platforma SŽ

Virtuální prostředí, serverové farmy, servery

Červen 2025

Obsah

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

Seznam zkratek

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

Seznam vysvětlivek

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

1 Úvod

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

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

2 Virtualizační prostředí

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

2.1 Virtualizace serverů

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

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

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

2.2 Virtualizace koncových počítačů

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

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

2.3 Kontejnerizace

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

3 Serverové farmy

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

3.1 Konvergovaná infrastruktura

V rámci konvergované infrastruktury provozuje SŽ tyto druhy farem:

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

3.2 Hyper-konvergovaná infrastruktura

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

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

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

4 Fyzické servery

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

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

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

5 Datová úložiště

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

5.1 Datová úložiště farem

Pro farmy klasické konvergované infrastruktury jsou provozovány datová úložiště:

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

5.2 Datová úložiště pro zálohy a archivaci

Pro ukládání záloh a archivaci jsou určena datová úložiště:

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

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

5.3 Datová úložiště pro off-line zálohy

Pro archivaci a offline ukládání záloh jsou určeny páskové knihovny:

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

5.4 Kancelářská datová úložiště

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

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

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

6 Virtuální servery

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

6.1 Služba virtuálních strojů

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

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

Služby virtuálních serverů

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

6.2 Služby diskových úložišť

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

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

Služby diskových úložišť

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

7 Databázové servery

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

Služby databázových prostředí

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

8 Webové servery

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

Služby webových serverů

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

9 Aplikační servery

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

Služba zabezpečeného portálového řešení

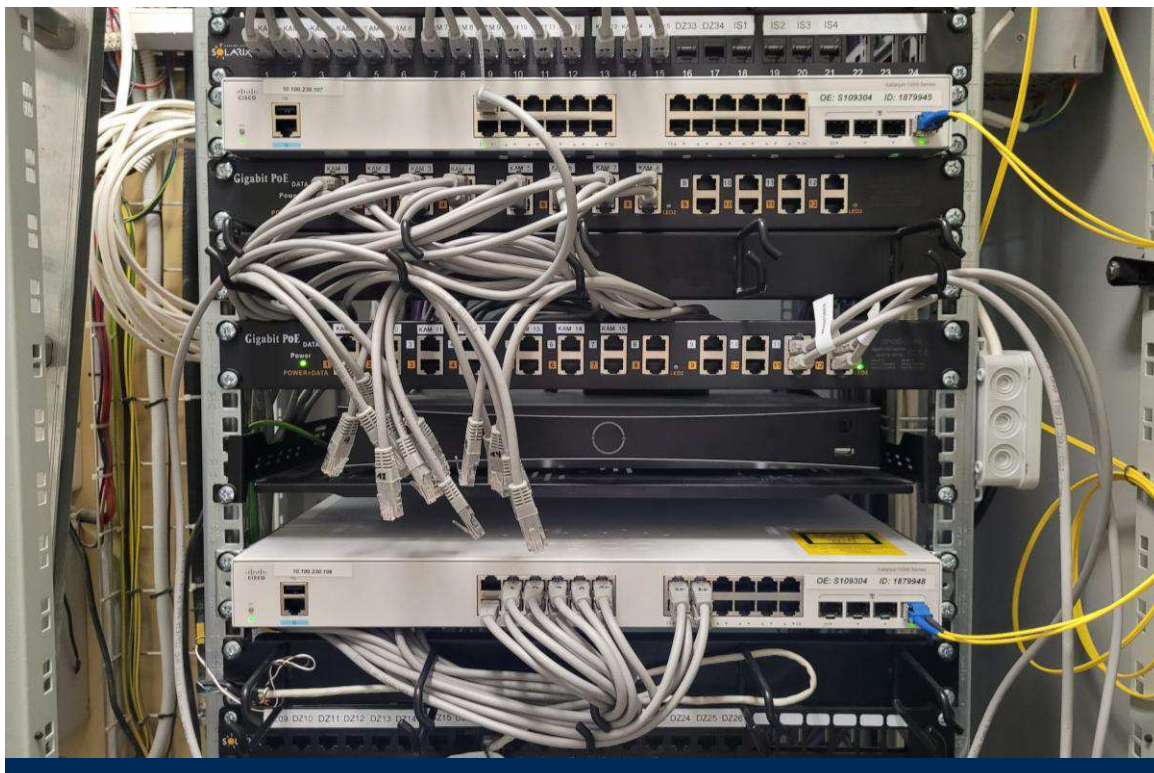
Služba	Popis
Liferay na Win.VMware.x86_64	Liferay je přední open-source podnikové portálové řešení založené na jazyce Java, které umožňuje správu dat, aplikací, procesů a integrace současných i nových aplikací z jednoho centrálního uživatelského rozhraní.

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

© 2025

Datum tisku
2025-07-30

spravazeleznic.cz



Platforma SŽ Konektivita a síťové prostředí

Červen 2025

Obsah

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

Seznam zkratek

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

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

Seznam vysvětlivek

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

1 Úvod

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

2 Perimetr Správy železnic

2.1 Perimetr

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

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

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

2.2 Demilitarizovaná zóna

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

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

2.2.1 Demilitarizovaná zóna pro OT

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

2.3 Přístup přes VPN

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

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

2.3.1 Uživatelské VPN s MFA

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

Pro tyto VPN platí následující pravidla:

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

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

2.3.2 Site to Site VPN

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

2.4 Komunikační směry

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

Pravidla síťové komunikace na perimetru SŽ

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

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

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

3 Fyzické sítě Správy železnic

3.1 Uživatelsko-aplikační síť

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

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

3.2 Technologické datové sítě

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

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

3.2.1 Segmentace sítě

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

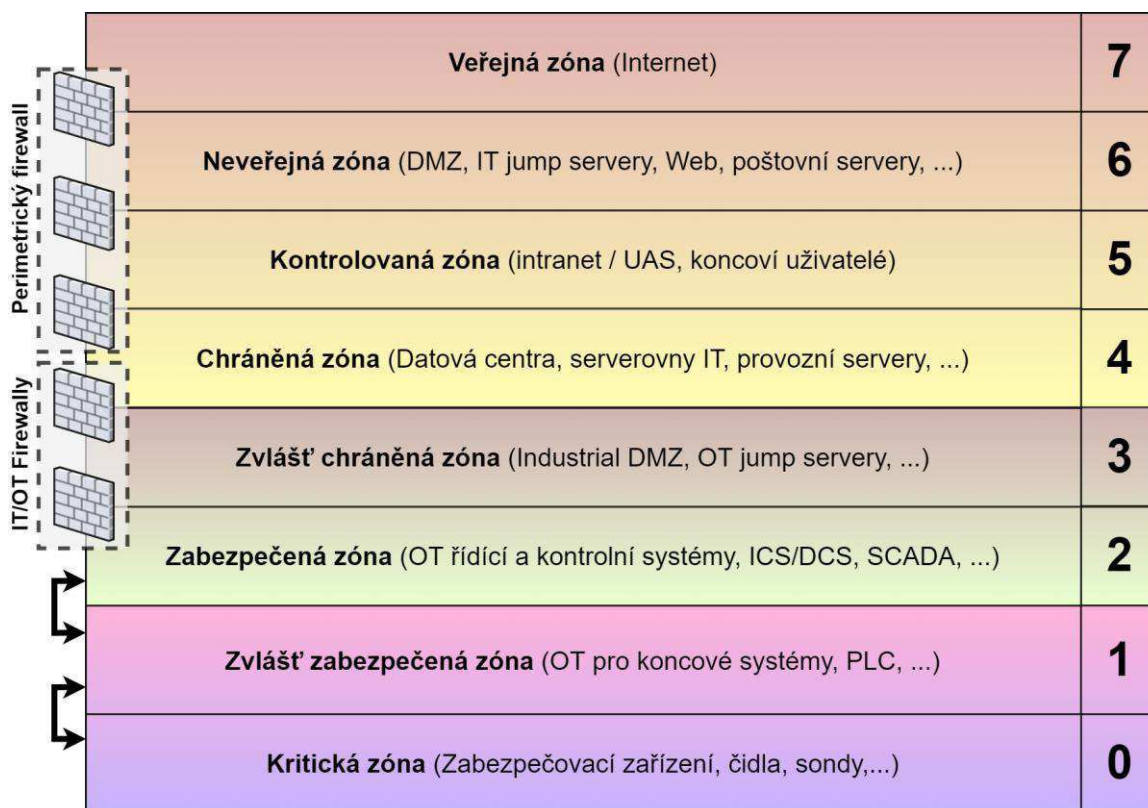
Segmentace UAS se v současné době aktivně připravuje, čili tato síť zatím není segmentována, rozdělena.

3.2.2 Ostrovní oddělené sítě

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

4 Logické síťové prostředí

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



Obrázek 1: Purdue ICS model

4.1 Komunikace mezi sítěmi

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

4.2 Georedundance

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

4.3 Řešení High Availability

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

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

5 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 síť i pro přímé propoje datacenter, kde nejsou k dispozici přímá vlákna. DWDM síť obsahuje mnoho plnohodnotných přípojných bodů a více opakovačů pro zajištění spojů na velkou vzdálenost, zároveň poskytuje redundantní připojení jednotlivých DWDM bodů z více směrů.

Výčet používaných / preferovaných typů zařízení DWDM

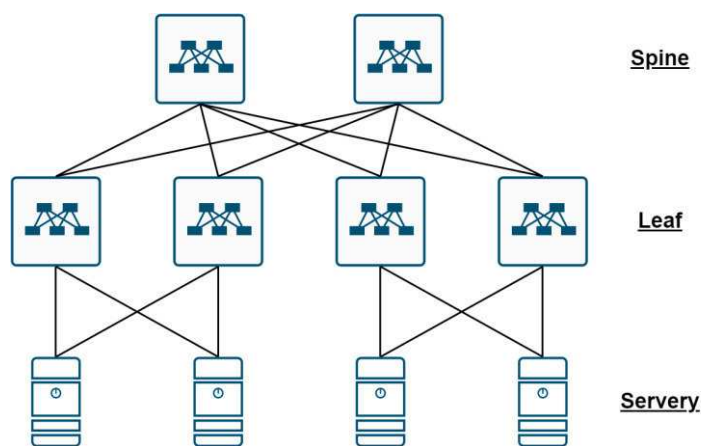
Typ zařízení	Popis	Konkrétní řady
DWDM	Přípojný bod	NCS 1000 NCS 2000

6.1.4 Síť MPLS

MPLS je technologie sítí, která umožňuje efektivní a spolehlivý přenos datových paketů vysokého objemu v rozsáhlých sítích. V prostředí Správy železnic jsou vybudovány dvě MPLS sítě. Stará MPLS síť pro uživatelsko-aplikační síť a některé technologické prvky a nová MPLS síť určená primárně pro technologické datové 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 switchy v síťovém prostředí Správy železnic již plně podporují integraci do Spine-Leaf topologie, ať už přímým napojením, nebo jako Remote Leaf.

6.1.6 Technologie Cisco ACI

Cisco ACI (Application Centric Infrastructure) je softwarově definované síťové řešení, které zjednodušuje, automatizuje a zabezpečuje provoz 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 switchy 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 síť a IT/OT DMZ	Cisco Firepower 1xxx Cisco Firepower 31x0 Cisco Firepower 4xxx
Pro datová centra	Firewall pro aplikační farmy, clustery, single nody, NAS atd.	Cisco Firepower 31x0 Fortinet Fortigate 600F Fortinet Fortigate 1801F Fortinet Fortigate 2601F
Pro aplikace	Firewall na aplikační vrstvě OSI modelu (WAF)	F5 BIG-IP
Pro load balancing	Loadbalancer pro vyrovnání zátěže serverů	Kemp LoadMaster

6.3 Routery

Routery, nebo také směrovače, jsou zásadní aktivní síťové prvky pro segmentaci sítí. Podle způsobu použití jsou děleny na routery pro provoz v MPLS síti, routery v datových centrech a perimetru sítě, případně pro IT nebo OT síť.

Jsou podporovány routery Cisco s požadovanými protokoly:

- **HSRP** – pro hraniční routery
- **VRF** – pro MPLS routery
- **VRF-Lite** – pro routery bez MPLS
- **BGP** – pro hraniční a MPLS routery
- **TACACS+**
- **RADIUS**

V následující tabulce jsou uváděny jednotlivé řady vždy pro konkrétní použití.

Výčet používaných / preferovaných typů routerů

Typ routeru	Popis	Konkrétní řady
MPLS	Routery typu P, PE a RR v MPLS síti	Cisco ASR Cisco NCS Cisco 8000
MPLS	Routery typu CE	Cisco C9400 Cisco C9300 Cisco C8000 Cisco ISR
IT	Routery pro datová centra a IT síť	Cisco C9300 Cisco ISR
OT	Lokální routery pro OT síť	Cisco IR

6.4 Switche

V prostředí SŽ jsou switche (přepínače) nejčastější síťová zařízení, proto existuje velké riziko možného nasazení nekompatibilních typů s následnou problematickou výměnou za kompatibilní. Obecně jsou preferované switche od renomovaného výrobce Cisco řady C9xxx a pro datacentra řada Nexus 9300, u nichž jsou do značné míry zaručené jednotné konfigurační prostředí (CLI), podpora VLAN bez omezení jejich počtu, kompatibilita používaných síťových protokolů, možnost stohování dedikovaným portem aj.

Jsou požadovány síťové a autorizační protokoly jako:

- **HSRP** – Hot Standby Router Protocol
- **PVST+** – Per-VLAN Spanning Tree Plus
- **TACACS+**
- **RADIUS**

Platí zákaz používání switchů bez managementu. V následujících podkapitolách jsou uváděny jednotlivé řady vždy pro konkrétní použití.

6.4.1 Switche pro datová centra

K již zmiňovaným požadavkům je u switchů pro datová centra vyžadováno redundantní napájení.

Výčet používaných / preferovaných typů

Typ switche	Popis	Konkrétní řady
Spine	Spine switch v topologii Spine-Leaf	Cisco Nexus 9332C Cisco Nexus 9364C
Leaf/ToR	Leaf switch v topologii Spine-Leaf nebo Top of Rack / Top of Row switch	Cisco Nexus 93180YC Cisco Nexus 93240YC Cisco Nexus 93360YC
Backend	Lokální propojení nodů farem (HCI)	Cisco Nexus 93180YC Cisco C9300X
Access	Jako access switch v malých serverovnách	Cisco C9300X Cisco C9300

6.4.2 Switche pro fibre channel

K již zmiňovaným požadavkům je u switchů pro datová centra vyžadováno redundantní napájení.

Výčet používaných / preferovaných typů

Typ switche	Popis	Konkrétní řady
Fibre Channel	Fibre Channel switche převážně pro připojení síťových úložišť typu SAN	Cisco MDS 9124T/V Cisco MDS 9132T/V Cisco MDS 9148T/V

6.4.3 Switche pro kamerové systémy

Pro kamerové systémy jsou požadovány switche s napájením PoE+ podle standardu 802.3at, případně PoE++ podle standardu 802.3bt.

Výčet používaných / preferovaných typů pro kamerové systémy

Typ switche	Popis	Konkrétní řady
Access	Běžný PoE switch pro připojení kamerových systémů	Cisco C9200, resp. C9200L Cisco C9300, resp. C9300L

6.4.4 Switche pro management zařízení

Pro OOB switche v datových centrech platí mimo jiné požadavek na redundantní napájení. V ostatních lokalitách, kde nejsou zajištěny dvě nezávislé napájecí větve, je tento požadavek bezpředmětný.

Výčet používaných / preferovaných typů pro management zařízení

Typ switchu	Popis	Konkrétní řady
OOB	Běžný access switch s metalickými RJ45 porty pro připojení MGMT portů	Cisco C9200, resp. C9200L
OOB	Velká datacentra spine-leaf	Cisco Nexus 9348GC

6.4.5 Switche pro lokální síť

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

Výčet používaných / preferovaných typů pro lokální síť

Typ switchu	Popis	Konkrétní řady
Access	Běžný access switch pro připojení pracovních stanic, tiskáren atp.	Cisco C9200 všech variant Cisco C9300 všech variant
OT	Lokální switche pro OT síť	Cisco IE2xxx
End of Support	Dosluhující řada, postupně se nahrazují	Cisco C2960 více variant Cisco C2950

6.5 Bezdrátová zařízení

Tato zařízení pro obsluhu bezdrátových sítí (WLAN) jsou používána v prostředí Správy železnic.

Výčet používaných / preferovaných typů pro zařízení pro bezdrátová síť

Typ zařízení	Popis	Konkrétní řady
Controller	Controller pro bezdrátové síť WLAN	Cisco Catalyst 9800
Access Point	Bezdrátové přípojné body (AP)	Cisco Catalyst 91xx

6.6 Huby

Ethernetový hub neboli síťový rozbočovač se v prostředí SŽ nenachází a jeho použití je zakázané.

6.7 Modemy a datová zařízení

V prostředí rozlehlé sítě SŽ se používají různé typy modemů, tedy zařízení pro převod mezi digitálním a analogovým rozhraním. Jde např. o GSM modemy s protokolem LTE nebo GPRS, DSL modemy, 2-pair / dial-up.

Výčet používaných / preferovaných modemů a datových zařízení

Výrobce	Technologie	Popis	Konkrétní řady/modely
Patton	DSL		1088, 3200, 3088
Albis / Siemens	DSL		BSTU4 / ULAF+
RAD	DSL		ASMi50
Patton	2-pair		3202

CONEL	GPRS	GPRS modem, již ukončená výroba	ER75i
Siemens	GPRS		M35i
Teltonika	4G/LTE	Průmyslové LTE routery s rozhraním RS232, RS485, Ethernet, M-bus	TRBxxx
Advantech	4G/LTE	Průmyslové LTE routery s rozhraním RS232, RS485, Ethernet	ICR-xxxx

6.8 Centralizovaná správa síťových prvků

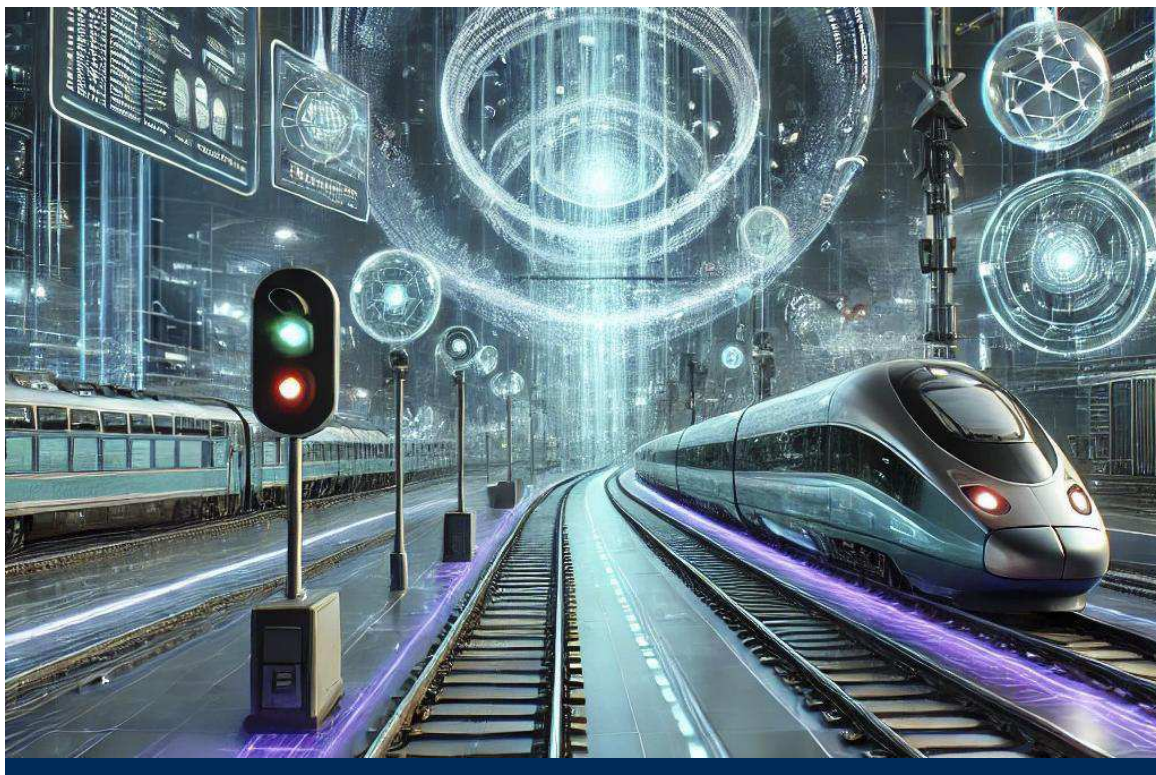
V prostředí Správy železnic se pro centralizovanou správu síťových prvků používají nástroje Cisco Catalyst Center (dříve Cisco DNA Center) a Cisco Nexus Dashboard Fabric Controller (dříve Cisco Data Center Network Manager). Tyto nástroje slouží pro správu, maintainance, aktualizace, zajištění jednotné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

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

© 2025

Datum tisku
2025-07-30

spravazeleznic.cz



Platforma SŽ Integrační standardy

Červen 2025

Obsah

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

Seznam zkratk

API	Komplexně definované komunikační rozhraní aplikace (<i>Application Programming Interface</i>)
CSV	Jednoduchý textový souborový formát (Comma-separated values)
ESB	Softwarová architektura a technologie používaná v oblasti podnikové integrace a správy služeb (<i>Enterprise Service Bus</i>)
IoT	Internet věcí je souborné označení pro síť fyzických zařízení, která vzájemně, centrálně nebo i s vnějším světem komunikují a mají možnost předávat data. Každé z těchto zařízení je jasně identifikovatelné díky implementovanému výpočetnímu systému, ale přesto je schopno pracovat samostatně v existující infrastruktuře sítě (<i>Internet of Things</i>)
IT	Informační technologie (<i>Information Technology</i>)
ITIL	(<i>Information Technology Infrastructure Library</i>)
JSON	Datový formát primárně určený pro přenos dat (<i>JavaScript Object Notation</i>)
KII	Kritická informační infrastruktura
REST/API	Webově založené klient-server API (<i>Representational State Transfer</i>)
SAP	Modulární ERP systém od německé firmy SAP AG
SFTP	Zabezpečený protokol pro přenos souborů. Pro zajištění šifrování využívá protokol SSH (<i>SSH File Transfer Protocol</i>)
SMTP	Základní síťový protokol pro přenos elektronické pošty (<i>Simple Mail Transfer Protocol</i>)
SOA	Architektura orientovaná na služby – jedná se o softwarovou architekturu, která se zaměřuje na organizaci a strukturu aplikací a systémů jako soubor nezávislých a dobře definovaných služeb (<i>Service-Oriented Architecture</i>)
SŽ	Správa železnic, státní organizace
XML	Standardizovaný jazyk používaný pro serializaci dat (<i>Extensible Markup Language</i>)

Seznam vysvětlivek

Platforma SŽ	Soubor dokumentů, rozdělený na veřejnou, interní a metodickou část, určený pro seznámení dodavatelů se standardy a technologiemi v ICT prostředí SŽ.
Platforma WSO2	Open-source platforma pro správu služeb (ESB) a integraci aplikací (API Management) vyvinutá společností WSO2 Inc. WSO2 poskytuje komplexní sadu nástrojů a produktů, které pomáhají organizacím implementovat a spravovat architekturu orientovanou na služby (SOA) a rozhraní pro programování aplikací (API) v jejich IT infrastruktuře.

1 Úvod

Tento dokument slouží jako příloha k základního dokumentu Platformy SŽ, který je součástí veřejných zakázek a podrobněji rozvádí integrační standardy naší organizace. Cílem je poskytnout jasný a konzistentní rámec pro všechny integrační aktivity. Naše cíle dále zahrnují modernizaci a konsolidaci současných integračních mechanismů za účelem zvýšení efektivity a snížení nákladů na údržbu. Dokument specifikuje požadavky a standardy, které musí být dodrženy při implementaci integračních scénářů, s důrazem na bezpečnost a využití hybridních řešení kombinujících on-premise a cloudovou infrastrukturu s ohledem na celkovou IT strategii. Všechny aktivity musí cílit na ITIL rámec pro řízení IT služeb, neboť tímto rámcem se naše organizace rozhodla řídit IT služby.

2 Moderní architektonické rámce

V rámci moderního IT prostředí naše organizace využívá pro nová řešení různé architektonické rámce a principy k zajištění flexibility, škálovatelnosti a efektivního poskytování služeb. Tato kapitola se zaměřuje na popis klíčových architektonických principů a jejich implementaci v naší organizaci. Použití současně moderní architektury nám umožňují efektivně reagovat na měnící se potřeby a technologické požadavky.

2.1 Flexibilita

Naše architektura umožňuje snadné přizpůsobení se měnícím se potřebám businessu. Tím, že kombinujeme lokální a cloudové infrastruktury, jsme schopni efektivně reagovat na dynamické požadavky a přizpůsobit naše služby v reálném čase. Hybridní řešení nám umožňují optimalizaci výkonu a nákladů tím, že strategicky využíváme výhody obou typů prostředí. Tato flexibilita nám dává možnost optimalizovat zdroje podle aktuálních potřeb a strategických cílů, ale hlavně dodržování bezpečnostních kritérií.

2.2 Škálovatelnost

Díky využití mikroslužeb a škálovatelné cloudové infrastruktury můžeme dynamicky přizpůsobovat kapacitu našich systémů podle aktuální požadavků. To zajišťuje, že naše služby jsou vždy dostupné a výkonné, i při náhlých změnách v zatížení. Implementujeme mechanismy automatického škálování, které umožňují plynulý růst a adaptaci bez potřeby manuálního zásahu, což přispívá k vyšší efektivitě a spolehlivosti.

2.3 Bezpečnost

Naše integrační architektura zahrnuje robustní bezpečnostní opatření na všech úrovních. Zajišťujeme ochranu dat a služeb pomocí pokročilých metod autentizace a autorizace, šifrování dat a pravidelného monitorování bezpečnostních hrozeb. Primárně z pohledu Compliance a regulace dbáme na dodržování všech relevantních bezpečnostních standardů a právních předpisů, což zajišťuje důvěryhodnost a právní jistotu pro business partnery.

2.4 Efektivita

Využití automatizace v rámci integračních procesů nám umožňuje snížit provozní náklady a zvýšit produktivitu. Automatizované workflow a orchestrace služeb minimalizují potřebu manuálních zásahů a zvyšují přesnost a rychlost procesů. Tohoto stavu jsme dosáhli díky centrálnímu řízení integrací prostřednictvím platformy ESB, ta nám umožňuje efektivně monitorovat a spravovat všechny integrační toky, což přispívá k vyšší přehlednosti a lepší koordinaci mezi jednotlivými systémy.

3 Architektura integrací

V rámci naší organizace se zaměřujeme na implementaci moderní architektury integrací, která podporuje jak on-premise, tak cloudové prostředí. Tato hybridní přístup zajišťuje flexibilitu, škálovatelnost a bezpečnost, což jsou klíčové faktory pro úspěšné řízení IT služeb podle ITIL principů. Cílový stav architektury je ESB.

Naše integrační architektura je postavena hlavně na následujících architekturních principech:

3.1 Microservices Architecture

Naše organizace implementuje architekturu mikroslužeb, což znamená decentralizaci a rozdělení monolitických aplikací na menší, nezávislé služby. Tento přístup zajišťuje vysokou flexibilitu a usnadňuje správu jednotlivých služeb. Díky mikroservisům můžeme rychleji reagovat na změny a inovace, což nám umožňuje poskytovat kvalitnější služby našim zákazníkům v podobě businessu.

3.2 Event-Driven Architecture

Pro lepší škálovatelnost a reaktivitu využíváme architekturu řízenou událostmi. Tento přístup umožňuje systémům komunikovat prostřednictvím událostí, což zvyšuje jejich schopnost rychle reagovat na provozní incidenty. Díky tomu můžeme dosahovat vyšší efektivity a pružnosti v našich provozních procesech.

3.3 API-First Approach

Při návrhu a vývoji systémů se naše organizace řídí principem API-First. API jsou navrhována a vyvíjena jako primární prostředek komunikace mezi systémy. Tento přístup je v souladu s ITIL principy, které se zaměřují na poskytování hodnoty zákazníkům prostřednictvím dobře definovaných služeb. API-First nám umožňuje dosahovat vyšší konzistence a standardizace v naší IT infrastruktuře.

3.4 Hybridní architektura

Pro zajištění flexibility a škálovatelnosti kombinujeme on-premise a cloudová řešení. Tento hybridní přístup nám umožňuje využívat výhod obou prostředí, což zajišťuje kontinuitu služeb a splnění compliance požadavků. Díky hybridní architektuře můžeme optimalizovat naše IT zdroje a lépe podporovat business v naší organizaci. Toto je obzvláště důležité z důvodu kritické infrastruktury informací (KII), která vyžaduje vysokou míru bezpečnosti a spolehlivosti. Hybridní přístup nám umožňuje zajistit, že klíčové systémy a data jsou chráněny a zároveň flexibilně škálovatelné dle aktuálních potřeb.

4 Typy integrací

Pro celkové pochopení integrací je nutné zmínit úroveň 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 orchestraci zdrojů v hybridním prostředí, což umožňuje jednotnou správu a kontrolu napříč on-premise a cloudovými systémy.

6.3.1.1 Preferované Protokoly pro Integraci s Azure

- **REST/HTTPS** – Pro širokou škálu aplikačních a datových integrací, což podporuje snadnou správu a podporu služeb.
- **gRPC** – Pro vysoce výkonné, nízko-latentní komunikace mezi mikroservisami, což zajišťuje rychlou a efektivní komunikaci.
- **Event Grid** – Pro event-driven architekturu a notifikace, což umožňuje rychlou reakci na změny a incidenty.
- **Service Bus** – Pro messaging a integraci podnikových aplikací, což zajišťuje spolehlivou komunikaci a řízení služeb.

6.4 Integrace stávajících aplikací

Mnoho aplikací, je stále ještě integrováno point-to-point, ty budou postupně převedeny do centralizovaného integračního prostředí. Hlavní kroky zahrnují:

- **Inventarizace a Analýza** – Zmapování současných integrací a identifikace klíčových závislostí, což podporuje efektivní správu a plánování změn.
- **Standardizace API** – Vytvoření standardních API pro všechny aplikace, což zajišťuje jednotný přístup a kontrolu nad službami.
- **Refaktoring a Modernizace** – Přepsání nebo refaktoring stávajících integrací podle moderních standardů, což podporuje efektivní a bezpečné poskytování služeb.

Tabulka protokolů

Protokol	Použití	Výhody	Nevýhody	Důvod Preference/Nepreference
REST/HTTPS	Aplikační, datové	Jednoduchost, široká podpora, škálovatelnost	Omezená bezpečnost ve srovnání s jinými protokoly	Preferovaný pro svou jednoduchost a širokou podporu
SOAP	Kritické služby	Vysoká úroveň bezpečnosti, transakční podpora	Složitost, větší režie	Preferovaný pro kritické a transakční služby
MQTT	Event-driven, IoT	Nízká režie, efektivní pro nízko-šířková pásma	Omezená podpora pro složitější operace	Preferovaný pro IoT a event-driven architekturu
AMQP	Messaging	Spolehlivost, škálovatelnost	Komplexita implementace	Preferovaný pro spolehlivý a škálovatelný messaging
OData	Data, API	Standardizace, jednoduchý přístup k datům	Omezená funkčnost ve srovnání s plně funkčními API	Preferovaný pro transparentní správu dat
RFC/BAPI	SAP integrace	Efektivní volání SAP funkcí	Specifické pro SAP	Preferovaný pro spolehlivou integraci SAP
IDoc	EDI, SAP integrace	Robustní, vhodné pro velké objemy dat	Specifické pro SAP, složitost	Preferovaný pro EDI a integraci SAP
WebSocket	Real-time komunikace	Obousměrná komunikace, nízká latence	Omezená bezpečnost	Preferovaný pro real-time aplikace
gRPC	Mikroservisy	Vysoký výkon, nízká latence	Menší podpora ve srovnání s HTTP	Preferovaný pro výkonné komunikace mikroservis
FTP/SFTP	Přenos souborů	Jednoduchost, široká podpora	Zastaralost (FTP), bezpečnostní rizika (FTP)	Preferovaný (SFTP) pro bezpečný přenos souborů, FTP je nepreferovaný kvůli bezpečnostním rizikům
JMS	Messaging	Spolehlivost, asynchronní komunikace	Komplexita, omezená podpora	Preferovaný pro robustní messagingové potřeby
SMTP	Email	Široká podpora, standardní pro email	Zastaralost, omezená bezpečnost	Nepreferovaný pro datové a aplikační integrace kvůli zastaralosti
CORBA	Distribuované aplikace	Jazyková nezávislost, robustnost	Komplexita, zastaralost, velká režie	Nepreferovaný kvůli zastaralosti a komplexitě
RMI	Java aplikace	Efektivní pro Java, jednoduchost	Omezené na Java, bezpečnostní rizika	Nepreferovaný kvůli omezené použitelnosti mimo Java a bezpečnostním rizikům
Telnet	Vzdálená správa	Široká podpora	Velmi slabá bezpečnost (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

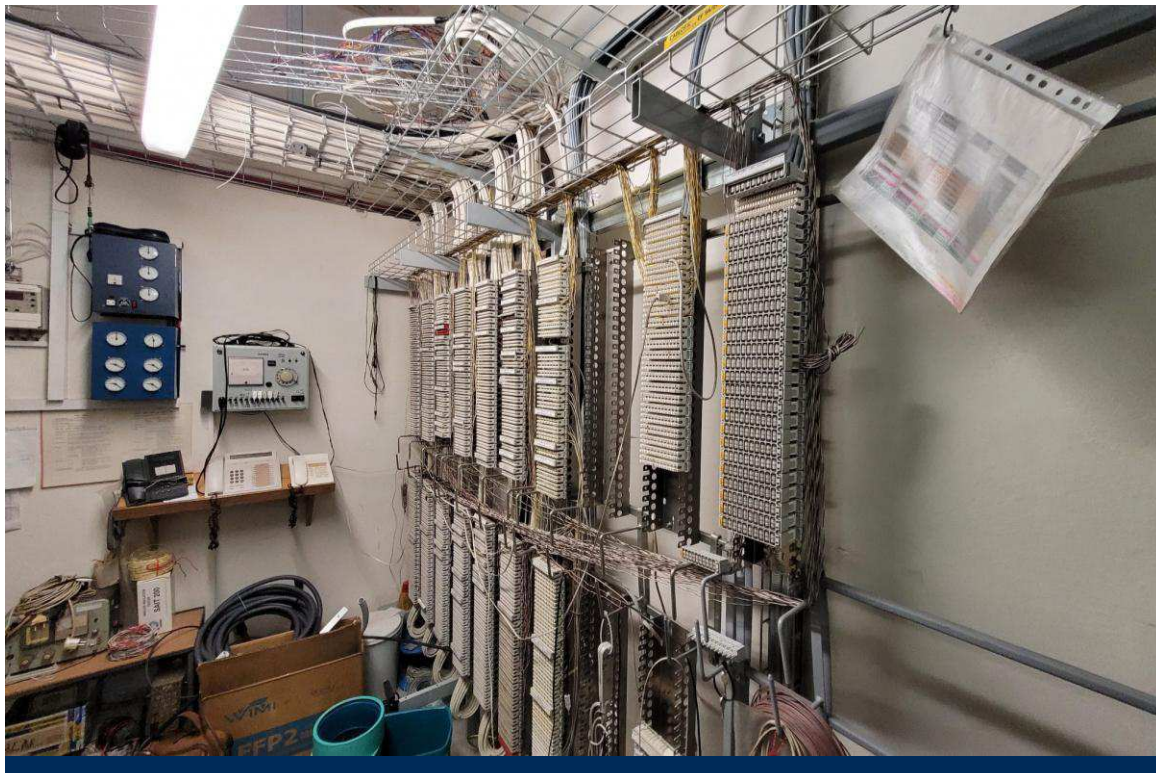
Jakékoliv nové Integrační scénáře, či změny Integračních scénářů musí projít skrze Architecture Board nebo Change management a být posouzeny v širším kontextu. Skrze jaký proces bude integrační scénář posuzován určí matice, která zahrnuje posouzení složitosti změny a její dopady. Integrační scénář následně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

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

© 2025

Datum tisku
2025-07-30

spravazeleznic.cz



Platforma SŽ Komunikační standardy

Červen 2025

Obsah

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

Seznam zkratek

API	Komplexně definované komunikační rozhraní aplikace (<i>Application Programming Interface</i>)
APN	Virtuální vyhrazená část mobilní datové sítě. Nejedná se tak o mobilní připojení k Internetu, ale k lokální síti daného zákazníka mobilního operátora.
CPS	Centrální poštovní systém Správy železnic
ICT	Informační a komunikační technologie (<i>Information and Communication Technology</i>)
O27	Odbor komunikace GŘ SŽ
SAP	Modulární ERP systém od německé firmy SAP AG
SMS	Krátká textová zpráva (<i>Short Message Service</i>)
SMTP	Základní síťový protokol pro přenos elektronické pošty (<i>Simple Mail Transfer Protocol</i>)
SŽ	Správa železnic, státní organizace
SŽT	Správa železničních informačních technologií
UAS	Logická uživatelsko-aplikační síť SŽ, zahrnuje VRF v MPLS sítích a lokální VLAN, běžně se nazývá také „Intranet SŽ“
VPN	Virtuální privátní síť (<i>Virtual Private Network</i>)

Seznam vysvětlivek

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

1 Úvod

Cílem této přílohy Platformy SŽ je popsat podporovaných komunikačních služeb a technologií, které lze v rámci Platformy SŽ využít a současně definuje služby, zařízení a technologie, které není možné z důvodu duplicity v rámci navrhovaných řešení dodávat do ICT prostředí Správy železnic.

2 Komunikační služby

Platforma Správy železnic definuje základní komunikační služby, které lze v rámci aplikací a informačních systémů využívat primárně technické notifikace. Použití k jiným účelům (například pro marketingové účely nebo komunikaci s veřejností) je možná jen po předchozím schválení ze strany Správy železnic, a to minimálně ze strany SŽT a O27.

3 SMS brána

SMS je negarantovaná služba telekomunikačních operátorů. Garantován není čas doručení ani samotné doručení SMS zprávy vůbec. SMS brána je aplikace instalovaná v prostředí SŽ napojená přímo na telekomunikačního operátora. Nejedná se tedy o použití koncového zařízení přihlášeného do veřejné mobilní telefonní sítě.

SMS brána umožňuje obousměrnou komunikaci, to znamená odesílání SMS zpráv definovaným příjemcům a příjem odpovědí na odeslané zprávy. Stejně tak umožňuje evidenci (logování) doručenek zpráv. Komunikaci se SMS 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 podporována.

4.3 Z externích sítí Správy železnic

Z externích sítí a připojení Správy železnic (VPN a APN) není služba odesílání emailových zpráv dostupná.

4.4 Mimo 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

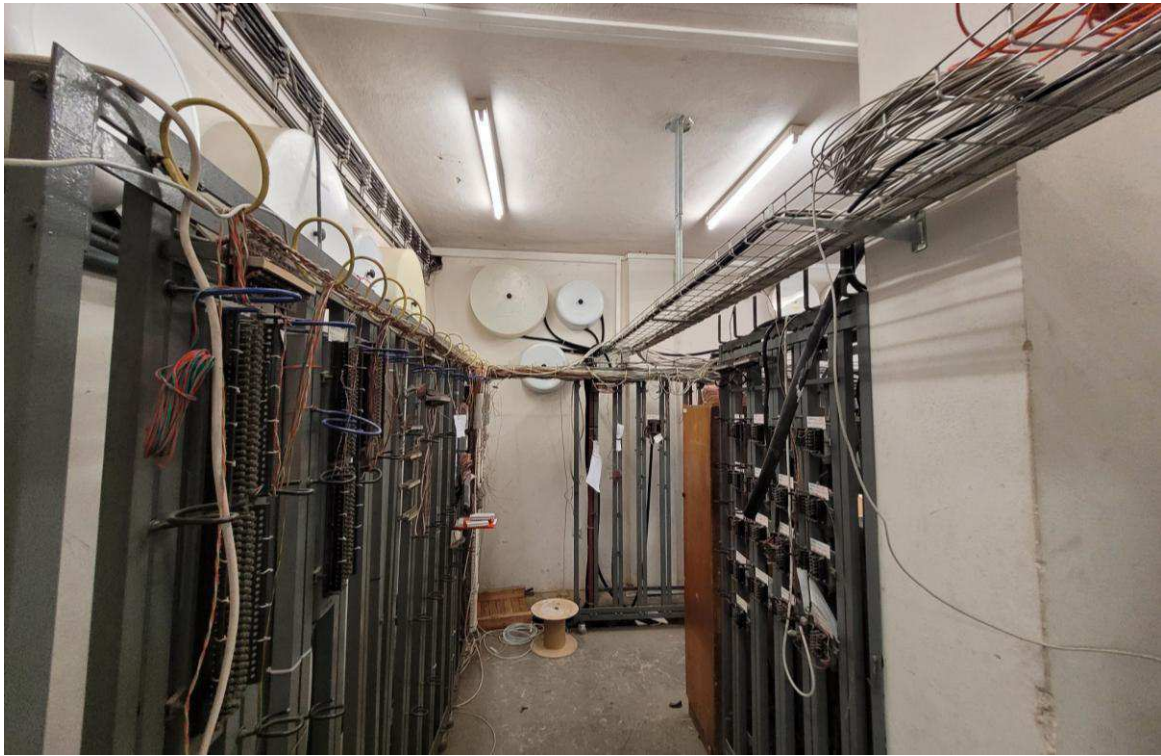
Komunikační platforma pro zajištění komunikace v rámci dispečerských pracovišť je Cisco Webex.

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

© 2025

Datum tisku
2025-07-30

spravazeleznic.cz



Platforma SŽ Standardy zálohování a disaster recovery

Červen 2025

Obsah

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

Seznam zkratek

DB	Databázová aplikace (<i>Database Engine</i>)
DR	Plán obnovy po havárii, součást kontinuity IT služeb (<i>Disaster Recovery</i>)
IBM	Americká technologická společnost (<i>International Business Machines</i>)
ICT	Informační a komunikační technologie (<i>Information and Communication Technology</i>)
LTO	Otevřený formát magnetické pásky určené pro záznam velkých objemů dat (<i>Linear Tape Open</i>)
MSSQL	Databázový server od firmy Microsoft (<i>Microsoft SQL Server</i>)
OS	Operační systém (<i>Operating System</i>)
SQL	Standardní jazyk pro manipulaci s relačními databázemi. SQL umožňuje ukládat, manipulovat a vyhledávat data v relačních databázích. SQL je založeno na dotazech (queries) na data v databázích. Dotazy lze pak definovat a modifikovat strukturu databází, vytvářet a upravovat tabulky, indexy a další prvky, vkládat a aktualizovat data, mazat data a další operace. SQL je nezávislý na platformě, což znamená, že může být použit na různých operačních systémech a s různými databázovými systémy, avšak každá databázová platforma může mít různé změny v syntaxi (<i>Structured Query Language</i>)
SŽ	Správa železnic, státní organizace
TSM	Nástroj pro zálohování, v současné době již nese název IBM Storage Protect (<i>Tivoli Storage Manager</i>)
UAS	Logická uživatelsko-aplikační síť SŽ, zahrnuje VRF v MPLS sítích a lokální VLAN, běžně se nazývá také „Intranet SŽ“

Seznam vysvětlivek

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

1 Úvod

Cílem této části Platformy SŽ je popis podporovaných služeb, technologií, a architektonických principů v oblasti zálohování a disaster recovery v ICT prostředí Správy železnic.

2 Služby zálohování

Služba zálohování ICT prostředí Správy železnic je zajištěna technologií IBM Storage Protect (dříve známý jako IBM Spectrum Protect nebo TSM). Jedná se o komplexní řešení pro fyzické fileservery, virtualizovaná prostředí a širokou škálu aplikací. IBM Storage Protect zálohuje data především s využitím technologie VMware Snapshot. Služba zálohování je dostupná v současné době jen v UAS.

Služba zálohování umožňuje 3 základní typy zálohování:

- Snapshot disku pro dosažení rychlé obnovy celého OS v Crash Consistent stavu včetně aplikační konfigurace. Zpravidla je takto zálohován pouze systémový oddíl virtualizovaného serveru. Záloha probíhá jednou denně a retence je nastavena na 30 posledních verzí.
- Záloha datových svazků připojených k jednotlivým serverům, pro dosažení maximální možné odolnosti proti náhodnému smazání či poškození apod. Záloha probíhá jednou denně, kdy se uchovává 90 posledních verzí souborů a poslední smazaná verze souboru je uchovávána 365 dní.
- Zálohy databází Oracle nebo MSSQL pomocí agentů. Záloha probíhá dvakrát denně. Přes den jsou zálohovány transakční logy databází, v noci pak vlastní databáze. Retence je nastavena na 60 posledních verzí.

Zálohy jsou řešeny lokálním backup serverem u každé virtualizační farmy, odkud jsou poté přenášeny do DR lokality a v rámci řešení offline záloh (pro další zvýšení odolnosti proti ztrátě dat) jsou zálohy dále ukládány na LTO pásky v páskové knihovně umístěné v DR lokalitě.

3 Řešení Disaster recovery

V rámci UAS byla jako DR lokalita určen objekt *Praha U2*, kam jsou pravidelně přenášeny zálohy ze všech lokálních backup serverů.

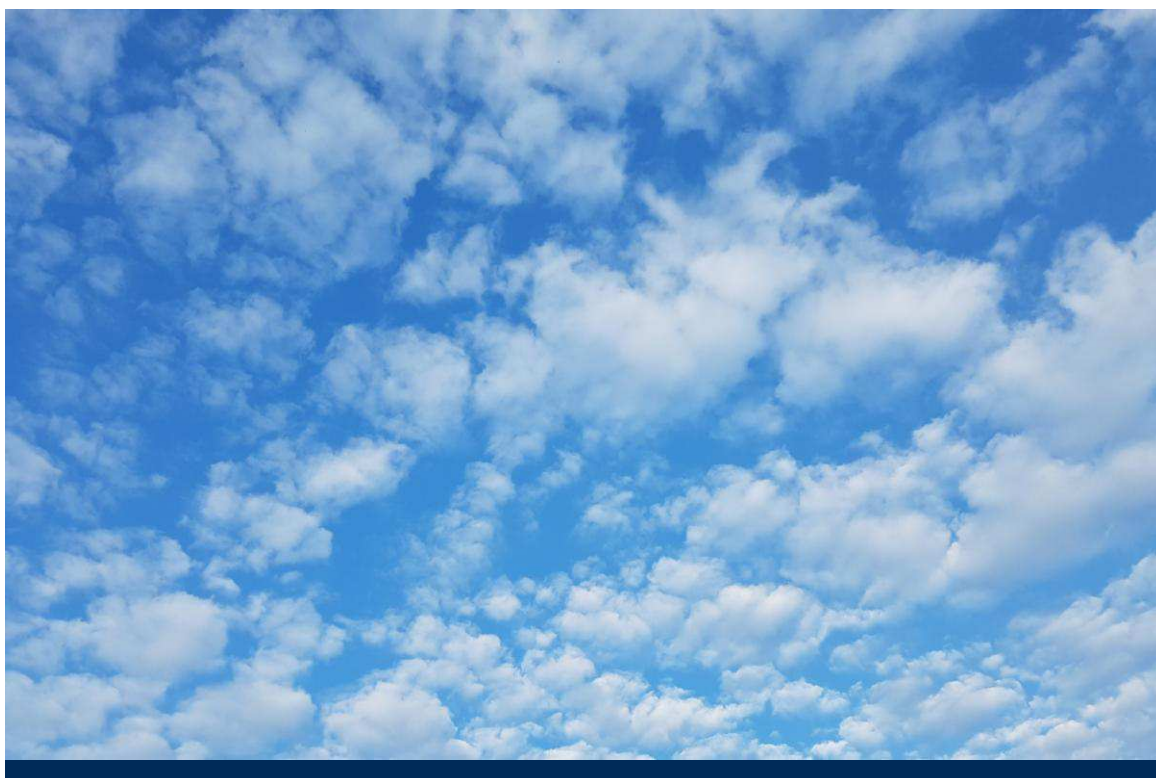
Všechny zálohy jsou pravidelně testovány a veškeré offline zálohy uložené na LTO páskách jsou pravidelně převáženy do zabezpečeného prostoru (do trezoru v jiné budově).

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

© 2025

Datum tisku
2025-07-30

spravazeleznic.cz



Platforma SŽ Cloudové prostředí

Červen 2025

Obsah

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

Seznam zkratek

AAD	Služba AD provozovaná v cloudovém prostředí MS Azure. Nový název služby je „MS EntraID“ (<i>Azure Active Directory</i>)
AD	Rozšiřitelná a škálovatelná adresářová služba, která umožňuje efektivně uspořádat síťové prostředky. Kromě informací o objektech v počítačové síti (uživatelské účty, počítače, tiskárny) umožňuje používat stromovou strukturu objektů, nastavovat globálně systémové politiky, instalovat programy na počítače nebo aplikovat kritické aktualizace v celé organizační struktuře. Má úzkou vazbu na DNS (<i>Active Directory</i>)
AWS	Cloudové prostředí firmy Amazon (<i>Amazon Web Services</i>)
DNS	Distribuovaný hierarchický jmenný systém používaný v síti Internet. Překládá názvy domén na číselné IP adresy a zpět, obsahuje informace o tom, které stroje poskytují příslušnou službu (<i>Domain Name System</i>)
ERP	Informační systém pro řízení podniku, který integruje různé oblasti podnikání, jako je například finanční řízení, řízení zásob, výroby, prodeje, nákupu a personálního řízení. Cílem je poskytovat podnikovým uživatelům přehled o celkových aktivitách a umožňovat efektivní a koordinované řízení všech procesů v rámci podniku (<i>Enterprise Resource Planning</i>)
IaaS	Typ cloudové služby, který poskytuje zákazníkům základní IT infrastrukturu jako službu, včetně serverů, úložiště, sítě a virtuálních počítačů. Tyto služby se často poskytují prostřednictvím Internetu a umožňují zákazníkům snadno a rychle využívat IT infrastrukturu bez nutnosti jejího nákupu, instalace a správy. Mezi nejznámější poskytovatele IaaS patří Amazon Web Services, Microsoft Azure a Google Cloud Platform (<i>Infrastructure as a Service</i>)
ICT	Informační a komunikační technologie (<i>Information and Communication Technology</i>)
IP	Jeden ze základních komunikačních protokolů používaných v počítačových sítích (<i>Internet Protocol</i>)
IT	Informační technologie (<i>Information Technology</i>)
M365	Globální označení služeb společnosti Microsoft, umožňující licencování jejich produktů a provoz aplikací, a to až jako on-premise řešení, či v cloudovém prostředí (<i>Microsoft 365</i>)
MS	Microsoft Corporation, americký výrobce především SW a provozovatel cloudového prostředí MS Azure
PaaS	Typ cloudové služby, která poskytuje vývojářům a IT týmům platformu pro vývoj, nasazení a správu aplikací bez nutnosti starat se o správu hardwaru a infrastruktury. Poskytovatelé PaaS nabízejí vývojové nástroje, databáze, síťové služby a další nástroje jako služby, což umožňuje vývojářům se soustředit pouze na vývoj aplikace (<i>Platform as a Service</i>)
SaaS	Model poskytování software, kdy je software hostován v cloudovém prostředí a poskytován uživatelům přes Internet. Tyto služby jsou poskytovány vývojáři software jako služby a účtovány jsou za používání (pay-as-you-go). To umožňuje uživatelům využívat software bez nutnosti investovat do hardware a IT infrastruktury (<i>Software as a Service</i>)
SAP	Modulární ERP systém od německé firmy SAP AG
SSO	Metoda jednotného přihlášení (<i>Single Sign-On</i>)
SW	Software je sada všech počítačových programů používaných v počítači, které provádějí nějakou činnost
SŽ	Správa železnic, státní organizace
SŽT	Správa železničních informačních technologií

Seznam vysvětlivek

MS Azure	Cloudové prostředí firmy Microsoft.
MS EntraID	Služba AD provozovaná v cloudovém prostředí MS Azure.
Platforma SŽ	Soubor dokumentů, rozdělený na veřejnou, interní a metodickou část, určený pro seznámení dodavatelů s ICT prostředím SŽ a současně s používanými standardy a technologiemi.
Tenant	Dedikovaný virtuální prostor v cloudovém prostředí MS Azure

1 Úvod

Cílem této části Platformy SŽ je popis podporovaných cloudových služeb, technologií, a architektonických principů v rámci tenantu provozovaného Správou železnic v cloudovém prostředí.

Důvodem je zajistit ve fázích přípravy poptávky, návrhu ICT řešení a realizace dodávky kompatibilitu se stávajícím cloudovým prostředím Správy železnic a umožnit využití pro aplikace, které splňují podmínky pro umístění v cloudovém prostředí.

2 Cloudové prostředí

U aplikací a informačních systémů, kde je to z technických a bezpečnostních důvodů možné, adoptuje Správa železnic moderní technologie včetně cloudového prostředí. S ohledem na vysoké zastoupení kritické informační infrastruktury v portfoliu Správy železnic je tento proces řízen přísnou metodikou.

V současnosti využívá Správa železnic cloudová prostředí na platformách Microsoft Azure, Amazon AWS, SAP HANA Cloud a Oracle Cloud Infrastructure, která podporují různé typy cloudových služeb:

- IaaS – infrastruktura jako služba
- PaaS – platforma jako služba
- SaaS – software jako služba

V rámci Platformy SŽ pak nabízí výhradně SaaS na platformě MS Azure, jelikož ostatní cloudová prostředí jsou v případě SŽ úzce svázána s konkrétními informačními systémy.

2.1 Microsoft Entra ID

Správa železnic provozuje ve svém ICT prostředí službu Active Directory a spolu s příchodem cloudového prostředí ho rozšířila i tam, dříve pod názvem Azure Active Directory, dnes Microsoft Entra ID.

2.2 Služby M365

Správa železnic využívá velkou část portfolia SaaS služeb poskytovaných na platformě MS Azure pod názvem M365.

3 Cloudové služby

V rámci svého v současnosti používaného cloudového prostředí na platformě Microsoft Azure jsou Platformou SŽ poskytovány následující služby.

3.1 Služba ověření proti Microsoft Entra ID

Zejména u aplikací jejichž uživatelé se pohybují mimo interní síť Správy železnic je k dispozici služba Microsoft Entra ID. Ověřování proti Microsoft Entra ID přináší vyšší bezpečnost a pohodlí uživatelů i pomocí jednotného přihlašování (SSO).

3.2 Integrace s M365

Pokud u informačního systému či aplikace předpokládá Dodavatel jakoukoli integraci s aplikacemi z rodiny M365, je nutné využít tenant Správy železnic.

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

© 2025

Datum tisku
2025-07-30

spravazeleznic.cz

Příloha č. 6 zadávací dokumentace

Seznam poddodavatelů

Účastník:

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

který podává nabídku na nadlimitní sektorovou veřejnou zakázku s názvem „**Segmentace sítě**“, č.j. **65403/2025-SŽ-GŘ-O25**, tímto předkládá v souladu s § 105 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, seznam poddodavatelů, s jejichž pomocí předpokládá plnění veřejné zakázky.

Identifikace poddodavatelů dodavatele ¹			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]	

V dne

¹ V případě více poddodavatelů zkopíruje dodavatel tabulku tolikrát, kolikrát bude třeba.

Klasifikace: Veřejný dokument



Příloha č. 7 zadávací dokumentace

Harmonogram

Fáze	Popis	Zahájení	Ukončení
F1.1	<ul style="list-style-type: none"> Zhodnocení stávající síťové infrastruktury 	od účinnosti smlouvy	do 14 týdnů
F1.2	<ul style="list-style-type: none"> Základní školení (seznámení s produktem) 	Zahájení 11 týdnů od účinnosti smlouvy	do 14 týdnů
F2.1	<ul style="list-style-type: none"> Dodávka celkem 12 kusů firewallů dle specifikace Dodávka nástroje pro centrální správu NGFW dle specifikace Dodávka požadovaných licencí Dodávka SFP+ modulů dle specifikace 	Od ukončení fáze F1.2	do 13 týdnů
F2.2	<ul style="list-style-type: none"> Specifikace změn architektury 	Od ukončení fáze F1.2	do 13 týdnů
F3.1	<ul style="list-style-type: none"> Implementace Next Generation Firewall Implementace nástroje centrální správy 	Od ukončení fáze F2.1	do 17 týdnů
F3.2	<ul style="list-style-type: none"> Příprava implementačních kroků pro realizaci vlastní segmentace (konzultace) 	Od ukončení fáze F2.2	do 17 týdnů
F4.1		Od ukončení fáze F2.2	do 17 týdnů
F4.2	<ul style="list-style-type: none"> Implementační plán pro celou uživatelskou síť 	Od ukončení fáze F2.2	do 17 týdnů
F4.3	<ul style="list-style-type: none"> Školení (odborné školení) 	Od ukončení fáze F2.2	do 17 týdnů
F5	<ul style="list-style-type: none"> Post-implementační a technická podpora 	od ukončení fáze, jež bude ukončena nejpozději ze všech předchozích fází (F3.1, F3.2, F4.1, F4.2, F4.3)	5 let
F6	<ul style="list-style-type: none"> Konzultační služby na vyžádání 	od ukončení fáze, jež bude ukončena nejpozději ze všech předchozích fází (F3.1, F3.2, F4.1, F4.2, F4.3)	5 let



Formulář pro vyplnění nabídkové ceny

Segmentace sítě v prostředí Správy železnic

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

Identifikace účastníka:

Postup pro vyplnění souboru

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

*** Platební milník B bude vypořádan po delivery uvedené fáze (F2)

*MD = člověkoder

Příloha č. 9 zadávací dokumentace

Čestné prohlášení účastníka ve vztahu k zakázaným dohodám

Účastník:

Obchodní firma/jméno [DOPLNÍ ÚČASTNÍK]

Sídlo/místo podnikání [DOPLNÍ ÚČASTNÍK]

IČO [DOPLNÍ ÚČASTNÍK]

Zastoupen [DOPLNÍ ÚČASTNÍK]

který podává nabídku na nadlimitní sektorovou veřejnou zakázku s názvem „**Segmentace sítě**“, č.j. **65403/2025-SŽ-GŘ-O25**, tímto čestně prohlašuje, že v souvislosti se zadávanou veřejnou zakázkou neuzavřel a neuzavře s jinými osobami zakázanou dohodu ve smyslu zákona č. 143/2001 Sb., o ochraně hospodářské soutěže a o změně některých zákonů (zákon o ochraně hospodářské soutěže), ve znění pozdějších předpisů.

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

V dne

Příloha č. 10 zadávací dokumentace

Čestné prohlášení ke splnění základní způsobilosti

Účastník:

Obchodní firma/jméno

[DOPLNÍ ÚČASTNÍK]

Sídlo/místo podnikání

[DOPLNÍ ÚČASTNÍK]

IČO

[DOPLNÍ ÚČASTNÍK]

Zastoupen

[DOPLNÍ ÚČASTNÍK]

který podává nabídku na nadlimitní sektorovou veřejnou zakázku s názvem „**Segmentace sítě**“, č.j. **65403/2025-SŽ-GR-O025**, tímto pro účely prokázání základní způsobilosti dle § 74 odst. 1 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**“) čestně prohlašuje, že je dodavatelem

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

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

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

V [DOPLNÍ ÚČASTNÍK] dne [DOPLNÍ ÚČASTNÍK]

Příloha č. 11 zadávací dokumentace

Seznam členů realizačního týmu

Účastník:

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

který podává nabídku na nadlimitní sektorovou veřejnou zakázku s názvem „**Segmentace sítě**“, č.j. **65403/2025-SŽ-GŘ-O25**, tímto níže předkládá seznam členů realizačního týmu, kteří se budou na plnění předmětu veřejné zakázky podílet:

Pozice člena realizačního týmu	Jméno a příjmení
Vedoucí realizačního týmu a garant řešení segmentace (PM)	
Seniorní systémový produktový inženýr, specialista NGFW a nástroje pro jeho správu	
Systémový analytik provádějící analýzu sítě SŽ a návrh řešení	
Systémový analytik provádějící analýzu sítě SŽ a návrh řešení s přihlédnutím k otázce kybernetické bezpečnosti	

V dne

Klasifikace: Diskrétní dokument



Příloha č. 13 zadávací dokumentace

Koncepce cílového stavu

Obsah

1	Seznam zkratk	3
2	Úvod	4
3	Požadavky	4
3.1	VRF	4
3.2	Segmentační firewally	5

1 Seznam zkratek

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

Zkratka	Popis
HA	(<i>High Availability</i>) je vysoká dostupnost služeb. Předpokladem řešení je použití dvou a více nezávislých zařízení s cílem zajistit funkčnost v případě výpadku.
OŘ	(<i>Oblastní ředitelství</i>) správní celek regionálního členění
SŽ	Správa železnic, státní organizace.
UAS	Logická uživatelsko-aplikační síť SŽ, zahrnuje VRF v MPLS sítích a lokální VLAN, běžně se nazývá také „Intranet SŽ“.
VRF	(<i>Virtual Routing and Forwarding</i>) Virtuální směrování a předávání je technologie, která v počítačových sítích založených na protokolu IP umožňuje souběžnou existenci více instancí směrovací tabulky v rámci sítě stejného směrovače ve stejnou dobu.

2 Úvod

Tento dokument je přílohou a nedílnou součástí zadávací dokumentace k veřejné zakázce s názvem „Segmentace sítě“. Dokument popisuje požadavky na segmentaci uživatelsko-aplikační sítě (UAS) ze strany organizace Správy železnic, státní organizace (dále jen SŽ), které jsou relevantní k poskytnutí účastníkům zadávacího řízení.

3 Požadavky

Implementace segmentace UAS bude vyžadovat pečlivé plánování a koordinaci, zejména vzhledem k rozsahu sítě a počtu dotčených systémů. Důležité bude zachování funkčnosti kritických služeb během celého procesu implementace.

3.1 VRF

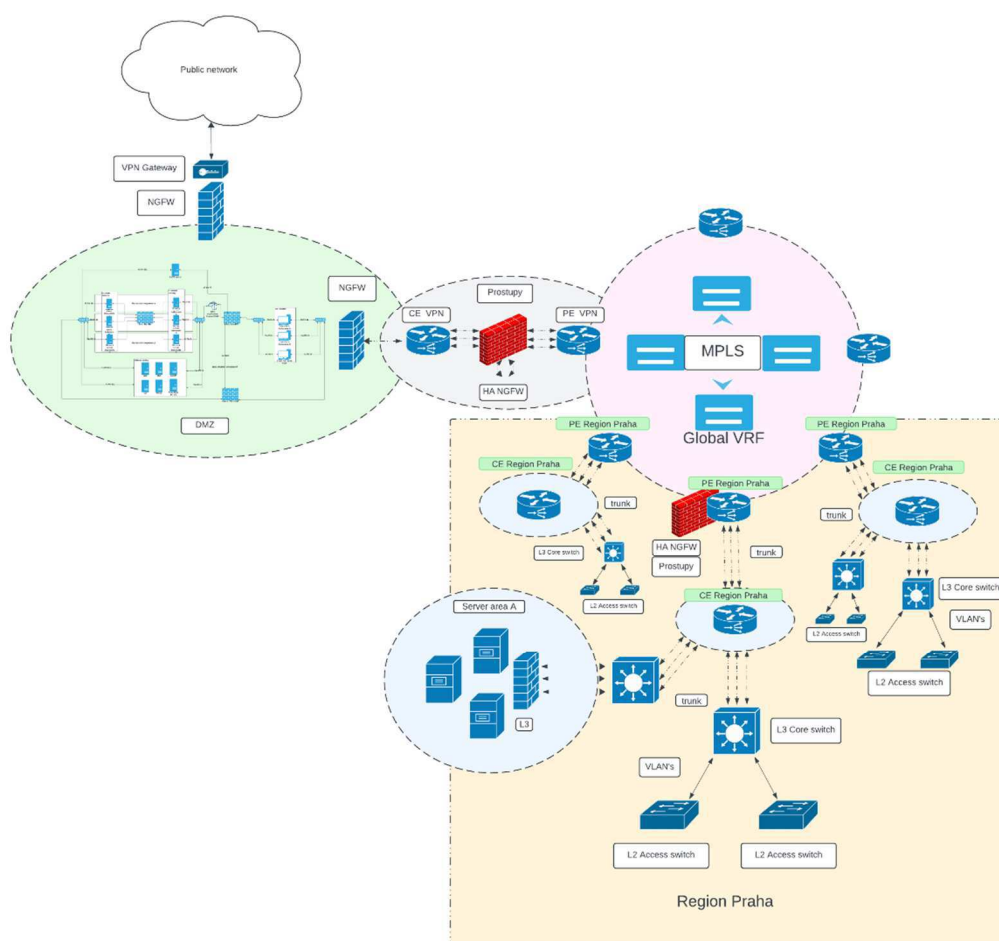
Samotná segmentace proběhne díky technologii VRF (Virtual Routing and Forwarding), která umožní logické oddělení různých částí sítě. Rozdělení reflektuje jak bezpečnostní požadavky, tak i praktické potřeby organizace vycházející z požadavků zákona o kybernetické bezpečnosti v návaznosti na níže popsané skupiny VRF. Každý segment bude mít jednoznačně definovaná pravidla pro komunikaci s ostatními segmenty, což významně zvýší celkovou bezpečnost sítě. Zároveň každé oblastní ředitelství bude vybaveno dvojicí nově implementovaných firewallů, do kterých bude sveden provoz celého oblastního ředitelství pro zvýšení úrovně provozního zabezpečení s možností detailní inspekce provozu v aplikační rovině. Nové firewally budou zapojeny v HA režimu.

V současné době je celá uživatelská síť sjednocena v jedné VRF s názvem `szdc_global`. Předpoklad ze strany Zadavatele je vytvoření nových VRF popsaných v následující tabulce.

Číslo	VRF	Popis
1	Global (<code>szdc_global</code>)	Současná, již vytvořená VRF
2	Users	Všechny uživatelské zařízení, zejména PC
3	Printers	Tiskárny, tiskové servery
4	Network monitoring	Monitoring síťových prvků
5	Server monitoring	Monitoring serverů
6	Guest	Striktně oddělená síť pro hosty
7	IoT	Media, dotykové panely, videokonference
8	Servery	Serverová komunikace
9 - x		Případné další VRF

3.2 Segmentační firewally

Každé oblastní ředitelství (ORŽ) bude vybaveno dvojicí nově implementovaných firewallů, do kterých bude sveden provoz celého oblastního ředitelství pro zvýšení úrovně provozního zabezpečení s možností detailní inspekce provozu v aplikační rovině. Dvojice budou zapojeny v HA režimu.



Obrázek 1 – Předpokládaný způsob zapojení nových segmentačních firewallů

Příloha č. 14 zadávací dokumentace – **Účastník předloží pouze v případě postupu dle čl. 24 zadávací dokumentace**

Čestné prohlášení

v souvislosti s ustanovením § 3 odst. 1 zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů (dále jen „ZRS“)

Účastník:

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

který podává nabídku na nadlimitní sektorovou veřejnou zakázku s názvem „**Segmentace sítě**“, č.j. **65403/2025-SŽ-GR-025**, tímto čestně prohlašuje, že dále uvedené údaje a další skutečnosti uvedené či jinak řádně označené ve smlouvě na plnění předmětu veřejné zakázky, jež je součástí jeho nabídky (dále jen „**smlouva**“), považuje účastník za obchodní tajemství ve smyslu ustanovení § 504 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**obchodní tajemství**“ a „**občanský zákoník**“), nebo se jedná o jiné informace, které nemohou být v registru smluv uveřejněny na základě ustanovení § 3 odst. 1 ZRS:

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

Účastník tímto čestně prohlašuje, že údaje a skutečnosti uvedené ve smlouvě, která je nedílnou součástí nabídky, označené jako obchodní tajemství, naplňují současně všechny definiční znaky obchodního tajemství, tak jak je vymezeno v ustanovení § 504 občanského zákoníku, tj. obchodní tajemství tvoří konkurenčně významné, určitelné, ocenitelné a v příslušných obchodních kruzích běžně nedostupné skutečnosti, které souvisejí se závodem a jejichž vlastník zajišťuje ve svém zájmu odpovídajícím způsobem jejich utajení. Účastník dále čestně prohlašuje, že nese veškerou odpovědnost v případě, že část obsahu smlouvy, která se týká obchodního tajemství účastníka a která v důsledku toho bude pro účely uveřejnění smlouvy v registru smluv znečitelněna, pokud by smlouva v důsledku takového označení byla uveřejněna způsobem odporujícím ZRS, a to bez ohledu na to, zda byla smlouva uveřejněna prostřednictvím registru smluv ze strany zadavatele nebo účastníka.

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

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

V dne

Příloha č. 15 zadávací dokumentace

Čestné prohlášení účastníka o střetu zájmů

Účastník:

Obchodní firma/jméno [DOPLNÍ ÚČASTNÍK]

Sídlo/místo podnikání [DOPLNÍ ÚČASTNÍK]

IČO [DOPLNÍ ÚČASTNÍK]

Zastoupen [DOPLNÍ ÚČASTNÍK]

který podává nabídku v řízení na zadání nadlimitní sektorové veřejné zakázky s názvem „**Segmentace sítě**“, č.j. **65403/2025-SŽ-GR-O25** (dále jen „**Veřejná zakázka**“ a „**Zadávací řízení**“), tímto čestně 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
- žádní poddodavatelé, jimiž prokazuje kvalifikaci v Zadávacím řízení, **nejsou** obchodní společností, ve které veřejný funkcionář uvedený v ust. § 2 odst. 1 písm. c) Zákona o střetu zájmů nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti.

Účastník dále čestně prohlašuje, že dostane-li se Účastník nebo poddodavatel, jímž prokazoval kvalifikaci v Zadávacím řízení, do střetu zájmů dle § 4b Zákona o střetu zájmů, a to kdykoliv až do okamžiku ukončení Zadávacího řízení, oznámí tuto skutečnost bez zbytečného odkladu zadavateli Veřejné zakázky.

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

V dne

Příloha č. 16 zadávací dokumentace

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

Účastník:

Obchodní firma/jméno

[DOPLNÍ ÚČASTNÍK]

Sídlo/místo podnikání

[DOPLNÍ ÚČASTNÍK]

IČO

[DOPLNÍ ÚČASTNÍK]

Zastoupen

[DOPLNÍ ÚČASTNÍK]

který podává nabídku na nadlimitní sektorovou veřejnou zakázku s názvem „**Segmentace sítě**“, č.j. **65403/2025-SŽ-GŘ-O25** (dále jen „**Veřejná zakázka**“ a „**Zadávací řízení**“), tímto čestně prohlašuje, že:

- a. on sám jakožto dodavatel, ani jeho poddodavatelé, nejsou osobami, na něž se vztahuje zákaz zadání veřejné zakázky ve smyslu § 48a zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů,
- b. on sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti v Zadávacím řízení, ani žádný z jeho poddodavatelů nebo jiných osob, jejichž způsobilost je využívána ve smyslu evropských směrnic o zadávání veřejných zakázek, **nejsou** osobami dle článku 5k nařízení Rady (EU) č. 833/2014 ze dne 31. července 2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, ve znění pozdějších předpisů,
- c. on sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti v Zadávacím řízení, ani žádný z jeho poddodavatelů nebo jiných osob, jejichž způsobilost je využívána ve smyslu evropských směrnic o zadávání veřejných zakázek, **nejsou** osobami dle článku 2 nařízení Rady (EU) č. 269/2014 ze dne 17. března 2014, o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, ve znění pozdějších předpisů, a dalších prováděcích předpisů k tomuto nařízení Rady (EU) č. 269/2014 anebo osobami dle čl. 2 nařízení Rady (ES) č. 765/2006 ze dne 18. května 2006 o omezujících opatřeních vzhledem k situaci v Bělorusku a k zapojení Běloruska do ruské agrese proti Ukrajině, ve znění pozdějších předpisů anebo osobami dle čl. 2 nařízení Rady (EU) č. 208/2014 ze dne 5. března 2014 o omezujících opatřeních vůči některým osobám, subjektům a orgánům vzhledem k situaci na Ukrajině, ve znění pozdějších předpisů (**tzv. sankční seznamy**).

Účastník dále čestně prohlašuje, že přestane-li on sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti v Zadávacím řízení, nebo některý z jeho poddodavatelů nebo jiných osob, jejichž způsobilost je využívána ve smyslu evropských směrnic o zadávání veřejných zakázek, splňovat výše uvedené podmínky, k nimž se toto čestné prohlášení vztahuje, a to kdykoliv až do okamžiku ukončení Zadávacího řízení, oznámí tuto skutečnost bez zbytečného

odkladu, nejpozději však **do 3 pracovních dnů** ode dne, kdy přestal splňovat výše uvedené podmínky, k nimž se toto četné prohlášení vztahuje, zadavateli Veřejné zakázky.

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

V [DOPLNÍ ÚČASTNÍK] dne [DOPLNÍ ÚČASTNÍK]

Odpovědi účastníků 1. kola PTK

[illegible]

14	Jaký protokol je použit pro integraci s jinou klastrou? Uveďte, na které úrovni se provádí implementace realizována (např. Virtual VDP) a jaké jsou klíčové technické výzvy/zajímavosti dostupnost a redundance?	ANO	Floating IP Address and Virtual MAC Address	https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/high-availability/ha-concepts/floating-ip-address-and-virtual-mac-address?id=3076c147-7084-430a-b041-2a9b0a6e3411				ANO	Podle typu platformy - cluster o 8 nodech (FPR 3100) nebo 16 (FPR 4200) ude v clusteru. Řešení přes CCX spoj. V clusteru se automaticky delegují fyzická jednotky klad symetricky. Připojení celého clusteru je na úrovni L2 balancování (LACP) k připojení nebo multibond připojení. Není potřeba žádný L3 balancer. K dispozici je clustering - rozložení např. do dvou DC. Více zde: https://www.cisco.com/c/en/us/solutions/securing/secure-firewall/management-center/device-config/760/management-center-device-config-760/device-ops-cluster-ops-760.html#bookSearch=true	ANO	Je využitelná propojení pomocí konektoru ClusterXL, je vyžadována IP adresa pro každý z segmentů terminovaný na firewalu, rozdíl mezi virtuální technologií VMAC v rámci ClusterXL.	ANO	https://paloaltonetworks.com/docs/ENPC/RSI_20_ClusterXL_Architecture/Content/Topics-ClusterXL-Introduction-to-ClusterXL.html#ClusterXL-Introduction-to-ClusterXL	ANO		
15	Podporuje řešení OT protokoly? Uveďte, zda je připravena řešení a specifikace, které kompatibility OT protokoly jsou podporovány.	ANO	https://www.paloaltonetworks.com/docs/OT-security				ANO	ANO, Modbus, IEC 61850, OPC UA, IEC 61850plus (přehrávání přes TCP), Modbus/TCP, ISA10009 pro OT nabízí navíc rozšíření podporu OT protokolů, včetně HART, Modbus, OPC, CIP a IEC 61850-3, IEC 61850-4, IEC 61850-5, IEC 61850-6, IEC 61850-7, IEC 61850-8, IEC 61850-9, IEC 61850-10, IEC 61850-11, IEC 61850-12, IEC 61850-13, IEC 61850-14, IEC 61850-15, IEC 61850-16, IEC 61850-17, IEC 61850-18, IEC 61850-19, IEC 61850-20, IEC 61850-21, IEC 61850-22, IEC 61850-23, IEC 61850-24, IEC 61850-25, IEC 61850-26, IEC 61850-27, IEC 61850-28, IEC 61850-29, IEC 61850-30, IEC 61850-31, IEC 61850-32, IEC 61850-33, IEC 61850-34, IEC 61850-35, IEC 61850-36, IEC 61850-37, IEC 61850-38, IEC 61850-39, IEC 61850-40, IEC 61850-41, IEC 61850-42, IEC 61850-43, IEC 61850-44, IEC 61850-45, IEC 61850-46, IEC 61850-47, IEC 61850-48, IEC 61850-49, IEC 61850-50, IEC 61850-51, IEC 61850-52, IEC 61850-53, IEC 61850-54, IEC 61850-55, IEC 61850-56, IEC 61850-57, IEC 61850-58, IEC 61850-59, IEC 61850-60, IEC 61850-61, IEC 61850-62, IEC 61850-63, IEC 61850-64, IEC 61850-65, IEC 61850-66, IEC 61850-67, IEC 61850-68, IEC 61850-69, IEC 61850-70, IEC 61850-71, IEC 61850-72, IEC 61850-73, IEC 61850-74, IEC 61850-75, IEC 61850-76, IEC 61850-77, IEC 61850-78, IEC 61850-79, IEC 61850-80, IEC 61850-81, IEC 61850-82, IEC 61850-83, IEC 61850-84, IEC 61850-85, IEC 61850-86, IEC 61850-87, IEC 61850-88, IEC 61850-89, IEC 61850-90, IEC 61850-91, IEC 61850-92, IEC 61850-93, IEC 61850-94, IEC 61850-95, IEC 61850-96, IEC 61850-97, IEC 61850-98, IEC 61850-99, IEC 61850-100, IEC 61850-101, IEC 61850-102, IEC 61850-103, IEC 61850-104, IEC 61850-105, IEC 61850-106, IEC 61850-107, IEC 61850-108, IEC 61850-109, IEC 61850-110, IEC 61850-111, IEC 61850-112, IEC 61850-113, IEC 61850-114, IEC 61850-115, IEC 61850-116, IEC 61850-117, IEC 61850-118, IEC 61850-119, IEC 61850-120, IEC 61850-121, IEC 61850-122, IEC 61850-123, IEC 61850-124, IEC 61850-125, IEC 61850-126, IEC 61850-127, IEC 61850-128, IEC 61850-129, IEC 61850-130, IEC 61850-131, IEC 61850-132, IEC 61850-133, IEC 61850-134, IEC 61850-135, IEC 61850-136, IEC 61850-137, IEC 61850-138, IEC 61850-139, IEC 61850-140, IEC 61850-141, IEC 61850-142, IEC 61850-143, IEC 61850-144, IEC 61850-145, IEC 61850-146, IEC 61850-147, IEC 61850-148, IEC 61850-149, IEC 61850-150, IEC 61850-151, IEC 61850-152, IEC 61850-153, IEC 61850-154, IEC 61850-155, IEC 61850-156, IEC 61850-157, IEC 61850-158, IEC 61850-159, IEC 61850-160, IEC 61850-161, IEC 61850-162, IEC 61850-163, IEC 61850-164, IEC 61850-165, IEC 61850-166, IEC 61850-167, IEC 61850-168, IEC 61850-169, IEC 61850-170, IEC 61850-171, IEC 61850-172, IEC 61850-173, IEC 61850-174, IEC 61850-175, IEC 61850-176, IEC 61850-177, IEC 61850-178, IEC 61850-179, IEC 61850-180, IEC 61850-181, IEC 61850-182, IEC 61850-183, IEC 61850-184, IEC 61850-185, IEC 61850-186, IEC 61850-187, IEC 61850-188, IEC 61850-189, IEC 61850-190, IEC 61850-191, IEC 61850-192, IEC 61850-193, IEC 61850-194, IEC 61850-195, IEC 61850-196, IEC 61850-197, IEC 61850-198, IEC 61850-199, IEC 61850-200, IEC 61850-201, IEC 61850-202, IEC 61850-203, IEC 61850-204, IEC 61850-205, IEC 61850-206, IEC 61850-207, IEC 61850-208, IEC 61850-209, IEC 61850-210, IEC 61850-211, IEC 61850-212, IEC 61850-213, IEC 61850-214, IEC 61850-215, IEC 61850-216, IEC 61850-217, IEC 61850-218, IEC 61850-219, IEC 61850-220, IEC 61850-221, IEC 61850-222, IEC 61850-223, IEC 61850-224, IEC 61850-225, IEC 61850-226, IEC 61850-227, IEC 61850-228, IEC 61850-229, IEC 61850-230, IEC 61850-231, IEC 61850-232, IEC 61850-233, IEC 61850-234, IEC 61850-235, IEC 61850-236, IEC 61850-237, IEC 61850-238, IEC 61850-239, IEC 61850-240, IEC 61850-241, IEC 61850-242, IEC 61850-243, IEC 61850-244, IEC 61850-245, IEC 61850-246, IEC 61850-247, IEC 61850-248, IEC 61850-249, IEC 61850-250, IEC 61850-251, IEC 61850-252, IEC 61850-253, IEC 61850-254, IEC 61850-255, IEC 61850-256, IEC 61850-257, IEC 61850-258, IEC 61850-259, IEC 61850-260, IEC 61850-261, IEC 61850-262, IEC 61850-263, IEC 61850-264, IEC 61850-265, IEC 61850-266, IEC 61850-267, IEC 61850-268, IEC 61850-269, IEC 61850-270, IEC 61850-271, IEC 61850-272, IEC 61850-273, IEC 61850-274, IEC 61850-275, IEC 61850-276, IEC 61850-277, IEC 61850-278, IEC 61850-279, IEC 61850-280, IEC 61850-281, IEC 61850-282, IEC 61850-283, IEC 61850-284, IEC 61850-285, IEC 61850-286, IEC 61850-287, IEC 61850-288, IEC 61850-289, IEC 61850-290, IEC 61850-291, IEC 61850-292, IEC 61850-293, IEC 61850-294, IEC 61850-295, IEC 61850-296, IEC 61850-297, IEC 61850-298, IEC 61850-299, IEC 61850-300, IEC 61850-301, IEC 61850-302, IEC 61850-303, IEC 61850-304, IEC 61850-305, IEC 61850-306, IEC 61850-307, IEC 61850-308, IEC 61850-309, IEC 61850-310, IEC 61850-311, IEC 61850-312, IEC 61850-313, IEC 61850-314, IEC 61850-315, IEC 61850-316, IEC 61850-317, IEC 61850-318, IEC 61850-319, IEC 61850-320, IEC 61850-321, IEC 61850-322, IEC 61850-323, IEC 61850-324, IEC 61850-325, IEC 61850-326, IEC 61850-327, IEC 61850-328, IEC 61850-329, IEC 61850-330, IEC 61850-331, IEC 61850-332, IEC 61850-333, IEC 61850-334, IEC 61850-335, IEC 61850-336, IEC 61850-337, IEC 61850-338, IEC 61850-339, IEC 61850-340, IEC 61850-341, IEC 61850-342, IEC 61850-343, IEC 61850-344, IEC 61850-345, IEC 61850-346, IEC 61850-347, IEC 61850-348, IEC 61850-349, IEC 61850-350, IEC 61850-351, IEC 61850-352, IEC 61850-353, IEC 61850-354, IEC 61850-355, IEC 61850-356, IEC 61850-357, IEC 61850-358, IEC 61850-359, IEC 61850-360, IEC 61850-361, IEC 61850-362, IEC 61850-363, IEC 61850-364, IEC 61850-365, IEC 61850-366, IEC 61850-367, IEC 61850-368, IEC 61850-369, IEC 61850-370, IEC 61850-371, IEC 61850-372, IEC 61850-373, IEC 61850-374, IEC 61850-375, IEC 61850-376, IEC 61850-377, IEC 61850-378, IEC 61850-379, IEC 61850-380, IEC 61850-381, IEC 61850-382, IEC 61850-383, IEC 61850-384, IEC 61850-385, IEC 61850-386, IEC 61850-387, IEC 61850-388, IEC 61850-389, IEC 61850-390, IEC 61850-391, IEC 61850-392, IEC 61850-393, IEC 61850-394, IEC 61850-395, IEC 61850-396, IEC 61850-397, IEC 61850-398, IEC 61850-399, IEC 61850-400, IEC 61850-401, IEC 61850-402, IEC 61850-403, IEC 61850-404, IEC 61850-405, IEC 61850-406, IEC 61850-407, IEC 61850-408, IEC 61850-409, IEC 61850-410, IEC 61850-411, IEC 61850-412, IEC 61850-413, IEC 61850-414, IEC 61850-415, IEC 61850-416, IEC 61850-417, IEC 61850-418, IEC 61850-419, IEC 61850-420, IEC 61850-421, IEC 61850-422, IEC 61850-423, IEC 61850-424, IEC 61850-425, IEC 61850-426, IEC 61850-427, IEC 61850-428, IEC 61850-429, IEC 61850-430, IEC 61850-431, IEC 61850-432, IEC 61850-433, IEC 61850-434, IEC 61850-435, IEC 61850-436, IEC 61850-437, IEC 61850-438, IEC 61850-439, IEC 61850-440, IEC 61850-441, IEC 61850-442, IEC 61850-443, IEC 61850-444, IEC 61850-445, IEC 61850-446, IEC 61850-447, IEC 61850-448, IEC 61850-449, IEC 61850-450, IEC 61850-451, IEC 61850-452, IEC 61850-453, IEC 61850-454, IEC 61850-455, IEC 61850-456, IEC 61850-457, IEC 61850-458, IEC 61850-459, IEC 61850-460, IEC 61850-461, IEC 61850-462, IEC 61850-463, IEC 61850-464, IEC 61850-465, IEC 61850-466, IEC 61850-467, IEC 61850-468, IEC 61850-469, IEC 61850-470, IEC 61850-471, IEC 61850-472, IEC 61850-473, IEC 61850-474, IEC 61850-475, IEC 61850-476, IEC 61850-477, IEC 61850-478, IEC 61850-479, IEC 61850-480, IEC 61850-481, IEC 61850-482, IEC 61850-483, IEC 61850-484, IEC 61850-485, IEC 61850-486, IEC 61850-487, IEC 61850-488, IEC 61850-489, IEC 61850-490, IEC 61850-491, IEC 61850-492, IEC 61850-493, IEC 61850-494, IEC 61850-495, IEC 61850-496, IEC 61850-497, IEC 61850-498, IEC 61850-499, IEC 61850-500, IEC 61850-501, IEC 61850-502, IEC 61850-503, IEC 61850-504, IEC 61850-505, IEC 61850-506, IEC 61850-507, IEC 61850-508, IEC 61850-509, IEC 61850-510, IEC 61850-511, IEC 61850-512, IEC 61850-513, IEC 61850-514, IEC 61850-515, IEC 61850-516, IEC 61850-517, IEC 61850-518, IEC 61850-519, IEC 61850-520, IEC 61850-521, IEC 61850-522, IEC 61850-523, IEC 61850-524, IEC 61850-525, IEC 61850-526, IEC 61850-527, IEC 61850-528, IEC 61850-529, IEC 61850-530, IEC 61850-531, IEC 61850-532, IEC 61850-533, IEC 61850-534, IEC 61850-535, IEC 61850-536, IEC 61850-537, IEC 61850-538, IEC 61850-539, IEC 61850-540, IEC 61850-541, IEC 61850-542, IEC 61850-543, IEC 61850-544, IEC 61850-545, IEC 61850-546, IEC 61850-547, IEC 61850-548, IEC 61850-549, IEC 61850-550, IEC 61850-551, IEC 61850-552, IEC 61850-553, IEC 61850-554, IEC 61850-555, IEC 61850-556, IEC 61850-557, IEC 61850-558, IEC 61850-559, IEC 61850-560, IEC 61850-561, IEC 61850-562, IEC 61850-563, IEC 61850-564, IEC 61850-565, IEC 61850-566, IEC 61850-567, IEC 61850-568, IEC 61850-569, IEC 61850-570, IEC 61850-571, IEC 61850-572, IEC 61850-573, IEC 61850-574, IEC 61850-575, IEC 61850-576, IEC 61850-577, IEC 61850-578, IEC 61850-579, IEC 61850-580, IEC 61850-581, IEC 61850-582, IEC 61850-583, IEC 61850-584, IEC 61850-585, IEC 61850-586, IEC 61850-587, IEC 61850-588, IEC 61850-589, IEC 61850-590, IEC 61850-591, IEC 61850-592, IEC 61850-593, IEC 61850-594, IEC 61850-595, IEC 61850-596, IEC 61850-597, IEC 61850-598, IEC 61850-599, IEC 61850-600, IEC 61850-601, IEC 61850-602, IEC 61850-603, IEC 61850-604, IEC 61850-605, IEC 61850-606, IEC 61850-607, IEC 61850-608, IEC 61850-609, IEC 61850-610, IEC 61850-611, IEC 61850-612, IEC 61850-613, IEC 61850-614, IEC 61850-615, IEC 61850-616, IEC 61850-617, IEC 61850-618, IEC 61850-619, IEC 61850-620, IEC 61850-621, IEC 61850-622, IEC 61850-623, IEC 61850-624, IEC 61850-625, IEC 61850-626, IEC 61850-627, IEC 61850-628, IEC 61850-629, IEC 61850-630, IEC 61850-631, IEC 61850-632, IEC 61850-633, IEC 61850-634, IEC 61850-635, IEC 61850-636, IEC 61850-637, IEC 61850-638, IEC 61850-639, IEC 61850-640, IEC 61850-641, IEC 61850-642, IEC 61850-643, IEC 61850-644, IEC 61850-645, IEC 61850-646, IEC 61850-647, IEC 61850-648, IEC 61850-649, IEC 61850-650, IEC 61850-651, IEC 61850-652, IEC 61850-653, IEC 61850-654, IEC 61850-655, IEC 61850-656, IEC 61850-657, IEC 61850-658, IEC 61850-659, IEC 61850-660, IEC 61850-661, IEC 61850-662, IEC 61850-663, IEC 61850-664, IEC 61850-665, IEC 61850-666, IEC 61850-667, IEC 61850-668, IEC 61850-669, IEC 61850-670, IEC 61850-671, IEC 61850-672, IEC 61850-673, IEC 61850-674, IEC 61850-675, IEC 61850-676, IEC 61850-677, IEC 61850-678, IEC 61850-679, IEC 61850-680, IEC 61850-681, IEC 61850-682, IEC 61850-683, IEC 61850-684, IEC 61850-685, IEC 61850-686, IEC 61850-687, IEC 61850-688, IEC 61850-689, IEC 61850-690, IEC 61850-691, IEC 61850-692, IEC 61850-693, IEC 61850-694, IEC 61850-695, IEC 61850-696, IEC 61850-697, IEC 61850-698, IEC 61850-699, IEC 61850-700, IEC 61850-701, IEC 61850-702, IEC 61850-703, IEC 61850-704, IEC 61850-705, IEC 61850-706, IEC 61850-707, IEC 61850-708, IEC 61850-709, IEC 61850-710, IEC 61850-711, IEC 61850-712, IEC 61850-713, IEC 61850-714, IEC 61850-715, IEC 61850-716, IEC 61850-717, IEC 61850-718, IEC 61850-719, IEC 61850-720, IEC 61850-721, IEC 61850-722, IEC 61850-723, IEC 61850-724, IEC 61850-725, IEC 61850-726, IEC 61850-727, IEC 61850-728, IEC 61850-729, IEC 61850-730, IEC 61850-731, IEC 61850-732, IEC 61850-733, IEC 61850-734, IEC 61850-735, IEC 61850-736, IEC 61850-737, IEC 61850-738, IEC 61850-739, IEC 61850-740, IEC 61850-741, IEC 61850-742, IEC 61850-743, IEC 61850-744, IEC 61850-745, IEC 61850-746, IEC 61850-747, IEC 61850-748, IEC 61850-749, IEC 61850-750, IEC 61850-751, IEC 61850-752, IEC 61850-753, IEC 61850-754, IEC 61850-755, IEC 61850-756, IEC 61850-757, IEC 61850-758, IEC 61850-759, IEC 61850-760, IEC 61850-761, IEC 61850-762, IEC 61850-763, IEC 61850-764, IEC 61850-765, IEC 61850-766, IEC 61850-767, IEC 61850-768, IEC 61850-769, IEC 61850-770, IEC 61850-771, IEC 61850-772, IEC 61850-773, IEC 61850-774, IEC 61850-775, IEC 61850-776, IEC 61850-777, IEC 61850-778, IEC 61850-779, IEC 61850-780, IEC 61850-781, IEC 61850-782, IEC 61850-783, IEC 61850-784, IEC 61850-785, IEC 61850-786, IEC 61850-787, IEC 61850-788, IEC 61850-789, IEC 61850-790, IEC 61850-791, IEC 61850-792, IEC 61850-793, IEC 61850-794, IEC 61850-795, IEC 61850-796, IEC 61850-797, IEC 61850-798, IEC 61850-799, IEC 61850-800, IEC 61850-801, IEC 61850-802, IEC 61850-803, IEC 61850-804, IEC 61850-805, IEC 61850-806, IEC 61850-807, IEC 61850-808, IEC 61850-809, IEC 61850-810, IEC 61850-811, IEC 61850-812, IEC 61850-813, IEC 61850-814, IEC 61850-815, IEC 61850-816, IEC 61850-817, IEC 61850-818, IEC 61850-819, IEC 61850-820, IEC 61850-821, IEC 61850-822, IEC 61850-823, IEC 61850-824, IEC 61850-825, IEC 61850-826, IEC 61850-827, IEC 61850-828, IEC 61850-829, IEC 61850-830, IEC 61850-831, IEC 61850-832, IEC 61850-833, IEC 61850-834, IEC 61850-835, IEC 61850-836, IEC 61850-837, IEC 61850-838, IEC 61850-839, IEC 61850-840, IEC 61850-841, IEC 61850-842, IEC 61850-843, IEC 61850-844, IEC 61850-845, IEC 61850-846, IEC 61850-847, IEC 61850-848, IEC 61850-849, IEC 61850-850, IEC 61850-851, IEC 61850-852, IEC 61850-853, IEC 61850-854, IEC 61850-855, IEC 61850-856, IEC 61850-857, IEC 61850-858, IEC 61850-859, IEC 61850-860, IEC 61850-861, IEC 61850-862, IEC 61850-863, IEC 61850-864, IEC 61850-865, IEC 61850-866, IEC 61850-867, IEC 61850-868, IEC 61850-869, IEC 61850-870, IEC 61850-871, IEC 61850-872, IEC 61850-873, IEC 61850-874, IEC 61850-875, IEC 61850-876, IEC 61850-877, IEC 61850-878, IEC 61850-879, IEC 61850-880, IEC 61850-881, IEC 61850-882, IEC 61850-883, IEC 61850-884, IEC 61850-885, IEC 61850-886, IEC 61850-887, IEC 61850-888, IEC 61850								

27	Můžete popsat, jak budete integrovat NGFW s existující infrastrukturou zákazníků?	NE							ANO	V případě dalšího definovaných cílů a kvalitativní zprávy o projektové dokumentaci probíhá implementace bez dopadu na provoz.	ANO	Detailní analýza sdělovacího vstupu včetně analýzy komponent konfigurace stávající bezpečnostní technologie. Upravení nového řešení na doporučené softwarové verzi. Konfigurace nového NGFW řešení. Tvorba bezpečnostních politik. Připojení NGFW do sítě a nastavení v režimu detekce. Testování a monitorování se zákazníkem. Přepnutí do režimu prevent a optimalizace nastavení. Školení administrátorů, kteří budou nově NGFW řešení spravovat.		ZVOLTE	Integrace NGFW s existující infrastrukturou zákazníků probíhá vždy individuálně, v závislosti na specifické potřebě a požadavky každého klienta. Provozujeme proslavený přístup, kdy úzce spolupracujeme se zákazníkem na optimalizaci celého procesu. Konkrétní detaily implementace však podléhají dohodě o možnostech (RTO) a namířena je výhradně sdělovací informací, rád s vámi prodiskutujeme možnosti v rámci individuální konzultace.		ANO	Viz. předchozí bod.	
28	Uveďte, kolik zakázek, na téma implementace segmentace, jste realizovali v uplynulých 5 letech?	ANO	3						Částečně	Bude upřesněno dle kritérií VŘ	ANO	13	V uplynulých 5 letech jsme realizovali více než 13 zakázek zaměřených na implementaci sdělovací segmentace. Tyto projekty zahrnovaly návrh a implementaci bezpečnostních sítí, které přispívají k bezpečnosti a integritě s dalšími bezpečnostními prvky.	ZVOLTE	V závislosti na rozsahu a časovém omezení se tato realizace pohybuje v desítkách, možná stovech. Náklady implementace nelze jednoduše formulovat, ale jsou součástí standardní sdělovací správy.		ANO		
29	Uveďte, kolik zakázek, na téma implementace segmentace, jste realizovali v uplynulých 5 letech?	ANO	10+						Částečně	Bude upřesněno dle kritérií VŘ	ANO	52	V uplynulých 5 letech jsme realizovali více než 52 zakázek zaměřených na implementaci sdělovací segmentace. V rámci těchto projektů jsme nastavovali a konfigurovali firewally. Řešení nemovných výstupů, nastavovali pravidla segmentace provozu a implementovali pravidla bezpečnosti politiky.	ZVOLTE	Stejně jako předchozí bod		ANO		
30	Uveďte, zda-li máte jednotlivých firewál typu Cisco, platíte certifikát z oblasti zaměření CCNP nebo CCIE. Uplatňujete to i u ostatních certifikátů.	ANO	1x CCNP						ANO	Certifikovaných odborníků máme k dispozici dostatečný počet.	ANO	stávající certifikát CC	předložíme na vyžádání	ANO	Ano jsme Cisco Gold partner		ANO		
31	Uveďte, zda-li máte jednotlivých firewál typu Cisco, platíte certifikát, který garantuje znalost dodávky firewalů resp. schopnost jejich konfigurace a administrace. Uveďte, který jednotlivých certifikátů.	ANO	2x PCNSE						ANO	Bude upřesněno dle kritérií VŘ	ANO	platné certifikáty CCSP (A), CCSP (Blue 1), CCSE (2), CCSE (2)	předložíme na vyžádání	ANO	Jsem Check Point Elite partner		ANO		
32	Uveďte, zda-li máte certifikát, který by garantoval znalost verze i na realizaci typu v jednotlivých verzích.	ANO	certifikace pro jiné sdělovací verze i na úrovni expert, certifikace na IPAM						ZVOLTE	Certifikovaný Projekt management u Zadávatel (např. Prince2), Objednatel (např. Prince2).	ANO	PRINCE2, ZOKB, Systém jakosti ISO 9001, ITIL, Foundation Certificate IT Service Management	předložíme na vyžádání	ZVOLTE	Togaf, CISP, CISA, Prince 2, IPMA		ANO		
33	Uveďte, zda-li jste realizovali 3 a více zakázek na implementaci segmentace v rámci 3 mil a více?	NE							ZVOLTE	Bude upřesněno dle kritérií VŘ	ANO	3	Bude upřesněno realizováno více než 10 zakázek na implementaci segmentace sítí s rozpočtem 5 milionů Kč a více. Tyto projekty zahrnovaly návrh a implementaci segmentačních strategií se zaměřením na bezpečnostní prvky, které přispívají k optimalizaci sdělovacího provozu. Cílem bylo zvýšit odolnost sítí vůči kybernetickým hrozbám. (Jako např. Bero a.s., Dobrá nemocnice Kladno a.s.,)	ANO			ZVOLTE		
34	Uveďte, zda-li jste realizovali 3 a více implementací segmentace firewalů v rámci projektů segmentace v období 5 mil a více?	ANO							ZVOLTE	Bude upřesněno dle kritérií VŘ	ANO	5	Realizovali jsme více než 3 implementace segmentačních firewalů v rámci projektů sdělovací segmentace v rozsahu přesahujícím 5 mil. Kč. V těchto projektech jsme nastavovali firewally, nastavovali pravidla politiky, nastavovali jejich konfiguraci dle bezpečnostních standardů a implementovali pravidla mechanismy řízení provozu a sdělovacího provozu. (Stanislav mladá firma, U.S. Steel Kladno, s.r.o., Východočeská zdravotní a.s., Východočeská zdravotní, řádný podnik), kromě těchto implementací jsme v mnoha dalších zakázkách prováděli revidování, nastavení a sdělování, čímž jsme zajišťovali jejich dlouhodobou sdělovou stabilitu a bezpečnost.	ANO			ZVOLTE		
35	Uveďte, zda-li jste realizovali 3 a více implementací segmentace firewalů pro sdělování sdělovacího provozu v rámci projektů segmentace v období 5 mil a více?	NE							ZVOLTE	Bude upřesněno dle kritérií VŘ	ANO	6	Realizovali jsme více než 3 implementace segmentačních nástrojů pro sdělování sdělovacího provozu v rámci projektů segmentace v období 5 mil. Kč. Tyto projekty zahrnovaly návrh a implementaci segmentačních strategií se zaměřením na bezpečnostní prvky, které přispívají k optimalizaci sdělovacího provozu. Cílem bylo zvýšit odolnost sítí vůči kybernetickým hrozbám. (Jako např. Bero a.s., Dobrá nemocnice Kladno a.s.,)	ANO		Některé realizace jsou v klasifikovaných režimech. Z tohoto pohledu může být obtížnější nebo nemožné je vyjádřit jako referenci.	ZVOLTE		

Doplňné nad rámec dotazů ke zvážení Závazkem pro eventuelní budoucí VR - Technologie NGFW (Účastník 3)

36	Umožňuje nabízené řešení monitorovat bezpečnostních incidentů pomocí netflow exportu?	ANO	NSFL je Cisco FW specifická implementace Netflow exportu optimalizovaná pro bezpečnostní monitoring. Podporuje optimální běh netflow informací pro firewalu analýzu a monitorování bezpečnostních událostí.	
37	Umožňuje FW funkci blokování provozu z ovládacích panelů, URL, seznamů, seznamů URL, seznamů adres, seznamů IPAM a seznamů? Pokud ano, jakým způsobem?	ANO	ACL s URL filtrací, příkladně Security Intelligence filtrace s databází na úrovni DNS nebo URL. Možnost definovat i vlastní objekty.	
38	Umožňuje FW generovat ať se jedná o jednotlivé adresy, Vyhledání k předpokládanému režimu a způsoby, kterými byl FW schopen v ACL.	ANO	Od verze FTD 7.7 je k dispozici	
39	Umožňuje FW kontrolu typu sdělovacího provozu, bezpečnostní role sdělovacího provozu a další ACL a autentizace. Popište způsoby, jakými.	ANO	Identičné ve spojení s Cisco ISE a využití SGT	
40	Umožňuje FW detekci nebezpečných sdělovacích aplikací i bez jejich dešifrování?	ANO	Encrypted Visibility Engine	
41	Možnost dynamického mapování IP adres sdělovacího provozu do symbolických názvů a použití těchto sdělovacích a příslušných pravidel.	ANO	Dynamic Attribute Connector synchronizuje značky definované pro státní, OS, např. do objektů, které lze použít v ACL.	
42	Ověření a dokumentování API	ANO	Ano. Praktické příklady např. https://developer.cisco.com/secure-firewall-management-center/	
43	Možnost detekce a dešifrování SD-WAN	ANO	Ano, pomocí Smart engine	
44	Z důvodu zvýšení ochrany před novými typy útoků, které budoucí bezpečnostní řešení a dynamického sdělovacího provozu, je ochrana před novými nebo čerstvými typy útoků.	ANO	Ano, SnortML umožňuje detekci útoků bez nutnosti vytváření nových signatur. Sítí zvyšuje schopnost systému odhalit zero-day útoky. Více zde: https://www.cisco.com/c/en/us/solutions/cisco-secure-firewall/secure-firewall-machine-learning-based-exploit-detection.html , source=chugai.com	
45	Podpora a typy rozhraní	ANO	Doporučujeme zvážet nepoužívat atypické rozhraní 40G a 80G, kompatibility stávajících sdělovacích prvků sítí s 25G, s možností nahrazení např. 4x10G.	

Předběžná tržní konzultace - „Segmentace sítě“

Příloha č. 17 Zadávací dokumentace - Dotazy k ceně - Indikace nákladů (uvedené částky jsou bez DPH)

Dotazy k pracnosti

ID Účastníka	ID	Položka indikace nákladů	Předpokládaný počet MD	Předpokládané náklady v Kč	Upřesnění	Poznámka
	1	Jaký je Váš odhad ceny pro etapu „Analýza stávající síťové infrastruktury“ (v Kč bez DPH), kde etapa obsahuje fáze: -Dokumentace stávající síťové infrastruktury -Inventarizace síťových zařízení a jejich konfigurací -Mapování současných síťových toků a závislostí -Mapování aplikací a služeb třetích stran -Popis stávajícího prostředí Klíčový výstup dodavatele: Dokument, analyzující síťovou infrastrukturu, která bude popisovat stávající prostředí SŽ v detailu potřebném pro návrh segmentace sítě na základě dodaných podkladů od zadavatele.	40	800 000 Kč	Cenu uveďte celkově za jednotlivou etapu, případné poznámky k rozkladu uveďte v doplňujícím komentáři.	
	2	Jaký je Váš odhad ceny pro etapu „Specifikace změn architektury segmentované sítě“ (v Kč bez DPH), kde etapa obsahuje fáze: -Základní specifikace -Definice VRF instancí a jejich účelu -Definice postupu konfiguračních prací Klíčový výstup dodavatele: Dokument architektury, zobrazující navrhované změny ve vazbě na segmentaci sítě.	30	600 000 Kč	Cenu uveďte celkově za jednotlivou etapu, případné poznámky k rozkladu uveďte v doplňujícím komentáři	
	3	Jaký je Váš odhad ceny pro etapu „Implementace / Realizace“ (v Kč bez DPH), kde etapa obsahuje fáze: -Příprava prostředí -Nastavení VRF v testovacím prostředí -Implementace směrovacích protokolů -Příprava operačních procedur -Zátěžové testy -Bezpečnostní testování -Optimalizace konfigurace -Školení na nové technologie -Dodávka požadovaného HW -Rollout plán pro celou uživatelskou síť (akceptace zadavatelem) Klíčový výstup dodavatele: Aktivní kroky implementační na základě dvou předešlých fází dle upřesnění zadavatele, směřující k naplnění segmentace uživatelské sítě.	100	2 000 000 Kč	Cenu uveďte celkově za jednotlivou etapu, případné poznámky k rozkladu uveďte v doplňujícím komentáři.	
	4	Jaký je náklad na dlouhodobé poskytnutí administrátora síťových prvků CISCO nad rámec realizačního týmu projektu: - Konfigurace L2/L3 switchů, routerů, firewallů - Vytížení kolísavé 16-40 hodin za pracovní týden	1	18 000 Kč	Cenu uveďte jako náklad na 1 MD (8 pracovních hodin) specialisty	
	Náklady pracnost celkem:		3 400 000 Kč			

Dotazy k ceně poptávaného hardware NGFW, podpory a licencí

Id	Položka indikace nákladů	Investiční náklady v Kč	Provozní náklady na 5 let v Kč	Upřesnění	Poznámka
1	Uveďte cenu za 2 kusy – Next Generation Firewall dle konfigurace A.	5 443 200 Kč	0 Kč	Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivý firewall dle přílohy č. 2 – Specifikace NGFW	Palo Alto Networks PA-5420 with redundant AC power supplies
2	Uveďte cenu za 10 kusů – Next Generation Firewall dle konfigurace B.	10 509 600 Kč	0 Kč	Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivý firewall dle přílohy č. 2 – Specifikace NGFW	Palo Alto Networks PA-3420 with redundant AC power supplies
3	Uveďte cenu za podporu a aktualizaci požadovaných bezpečnostních služeb celkově po dobu 60 měsíců. - (8x5) - (24x7)	16 794 500 Kč	3 600 000 Kč	Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivou položku.	

4	Uvedte cenu za licence a maintenance po dobu 60 měsíců spolu se specifikací, jaké licence jsou třeba.	100 965 000 Kč	0 Kč	Cenu uveďte (v Kč bez DPH), případně do komentáře přidejte další poznámky	Additional 10 virtual systems (1 to 11) for PA-3420 Advanced Threat Prevention subscription 5 year term for device in an HA pair, PA-3420 Advanced DNS Security subscription 5 year term for device in an HA pair, PA-3420 PA-3420, DLP subscription, for one (1) device in an HA pair, 5 years (60 months) term. PA-3420, IoT subscription, does not require data lake, for one (1) device in an HA pair, 5 years (60 months) term. Advanced Threat Prevention subscription 5 year term for device in an HA pair, PA-5420 Advanced DNS Security subscription 5 year term for device in an HA pair, PA-5420 PA-5420, DLP subscription, for one (1) device in an HA pair, 5 years (60 months)
5	Uvedte cenu za „firewall management tool“ spolu s náklady na licence a maintenance, support po dobu 60 měsíců.	556 000 Kč	0 Kč	Cenu uveďte (v Kč bez DPH), případně do komentáře přidejte další poznámky jako je způsob „subscription“, o jaký se jedná nástroj atd.	Panorama central management software, 25 devices Partner enabled premium support 5 year term, Panorama 25 devices
Náklady HW celkem:		134 268 300 Kč	3 600 000 Kč		

Dotazy k ceně poptávaného hardware NGFW, podpory a licencí

Id	Položka indikace nákladů	Investiční náklady v Kč	Provozní náklady na 5 let v Kč	Upřesnění	Poznámka
1	Uvedte cenu za 2 kusy – Next Generation Firewall dle konfigurace A.	0 Kč	0 Kč	Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivý firewall dle přílohy č. 2 – Specifikace NGFW	
2	Uvedte cenu za 10 kusů – Next Generation Firewall dle konfigurace B.	0 Kč	0 Kč	Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivý firewall dle přílohy č. 2 – Specifikace NGFW	
3	Uvedte cenu za podporu a aktualizaci požadovaných bezpečnostních služeb celkově po dobu 60 měsíců. - (8x5) - (24x7)	0 Kč	0 Kč	Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivou položku.	
4	Uvedte cenu za licence a maintenance po dobu 60 měsíců spolu se specifikací, jaké licence jsou třeba.	0 Kč	0 Kč	Cenu uveďte (v Kč bez DPH), případně do komentáře přidejte další poznámky	
5	Uvedte cenu za „firewall management tool“ spolu s náklady na licence a maintenance, support po dobu 60 měsíců.	0 Kč	0 Kč	Cenu uveďte (v Kč bez DPH), případně do komentáře přidejte další poznámky jako je způsob „subscription“, o jaký se jedná nástroj atd.	
Náklady HW celkem:		0 Kč	0 Kč		

Dotazy k pracnosti

Id	Položka indikace nákladů	Předpokládaný počet MD	Předpokládané náklady v Kč	Upřesnění	Poznámka
----	--------------------------	------------------------	----------------------------	-----------	----------

1	<div>Jaký je Váš odhad ceny pro etapu „Analýza stávající síťové infrastruktury“ (v Kč bez DPH), kde etapa obsahuje fáze:</div> <div><div>-Dokumentace stávající síťové infrastruktury</div><div>-Inventarizace síťových zařízení a jejich konfigurací</div><div>-Mapování současných síťových toků a závislostí</div><div>-Mapování aplikací a služeb třetích stran</div><div>-Popis stávajícího prostředí</div></div> <div>Klíčový výstup dodavatele: Dokument, analyzující síťovou infrastrukturu, která bude popisovat stávající prostředí SŽ v detailu potřebném pro návrh segmentace sítě na základě dodaných podkladů od zadavatele.</div>	150	4 200 000 Kč	<div>Cenu uveďte celkově za jednotlivou etapu, případné poznámky k rozkladu uveďte v doplňujícím komentáři.</div>	
2	<div>Jaký je Váš odhad ceny pro etapu „Specifikace změn architektury segmentované sítě“ (v Kč bez DPH), kde etapa obsahuje fáze:</div> <div><div>-Základní specifikace</div><div>-Definice VRF instancí a jejich účelu</div><div>-Definice postupu konfiguračních prací</div></div> <div>Klíčový výstup dodavatele: Dokument architektury, zobrazující navrhované změny ve vazbě na segmentaci sítě.</div>	50	1 400 000 Kč	<div>Cenu uveďte celkově za jednotlivou etapu, případné poznámky k rozkladu uveďte v doplňujícím komentáři</div>	
3	<div>Jaký je Váš odhad ceny pro etapu „Implementace / Realizace“ (v Kč bez DPH), kde etapa obsahuje fáze:</div> <div><div>-Příprava prostředí</div><div>-Nastavení VRF v testovacím prostředí</div><div>-Implementace směrovacích protokolů</div><div>-Příprava operačních procedur</div><div>-Zátěžové testy</div><div>-Bezpečnostní testování</div><div>-Optimalizace konfigurace</div><div>-Školení na nové technologie</div><div>-Dodávka požadovaného HW</div><div>-Rollout plán pro celou uživatelskou síť (akceptace zadavatelem)</div></div> <div>Klíčový výstup dodavatele: Aktivní kroky implementační na základě dvou předešlých fází dle upřesnění zadavatele, směřující k naplnění segmentace uživatelské sítě.</div>	130	3 640 000 Kč	<div>Cenu uveďte celkově za jednotlivou etapu, případné poznámky k rozkladu uveďte v doplňujícím komentáři.</div>	
4	<div>Jaký je náklad na dlouhodobé poskytnutí administrátora síťových prvků CISCO nad rámec realizačního týmu projektu:</div> <div><div>- Konfigurace L2/L3 switchů, routerů, firewallů</div><div>- Vytížení kolísavé 16-40 hodin za pracovní týden</div></div>	1	24 000 Kč	<div>Cenu uveďte jako náklad na 1 MD (8 pracovních hodin) specialisty</div>	

Náklady pracnost celkem:

9 240 000 Kč

Dotazy k ceně poptávaného hardware NGFW, podpory a licenci

Id	Položka indikace nákladů	Investiční náklady v Kč	Provozní náklady na 5 let v Kč	Upřesnění	Poznámka
1	Uveďte cenu za 2 kusy – Next Generation Firewall dle konfigurace A.	4 683 000 Kč		<div>Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivý firewall dle přílohy č. 2 – Specifikace NGFW</div>	uvedená cena je za HW, ale nelze koupit samotný HW, musí se objednat včetně SNT a subscriptions, tzn. prvotní investiční náklady zahrnují položky 3 a 4 (v případě nákupu na 60 měsíců, může být koupeno prvotně na kratší dobu)
2	Uveďte cenu za 10 kusů – Next Generation Firewall dle konfigurace B.	15 036 000 Kč		<div>Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivý firewall dle přílohy č. 2 – Specifikace NGFW</div>	uvedená cena je za HW, ale nelze koupit samotný HW, musí se objednat včetně SNT a subscriptions, tzn. prvotní investiční náklady zahrnují položky 3 a 4 (v případě nákupu na 60 měsíců, může být koupeno prvotně na kratší dobu)
3	Uveďte cenu za podporu a aktualizaci požadovaných bezpečnostních služeb celkově po dobu 60 měsíců. <div>- (8x5)</div> <div>- (24x7)</div>	0 Kč	42 222 000 Kč	<div>Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivou položku.</div>	pro NGFW konf. A 14 650 000,- Kč, konf. B 27 607 000,- Kč celkem
4	Uveďte cenu za licence a maintenance po dobu 60 měsíců spolu se specifikací, jaké licence jsou třeba.	0 Kč	10 793 000 Kč	<div>Cenu uveďte (v Kč bez DPH), případně do komentáře přidejte další poznámky</div>	8X5XNBD

5	Uvedte cenu za „firewall management tool“ spolu snáklady na licence a maintenance, support po dobu 60 měsíců.	174 000 Kč	240 000 Kč	Cenu uveďte (v Kč bez DPH), případně do komentáře přidejte další poznámky jako je způsob „subscription“, o jaký se jedná nástroj atd.	FMC Management
Náklady HW celkem:		19 893 000 Kč	53 255 000 Kč		

Dotazy k ceně poptávaného hardware NGFW, podpory a licencí

Id	Položka indikace nákladů	Investiční náklady v Kč	Provozní náklady na 5 let v Kč	Upřesnění	Poznámka
1	Uvedte cenu za 2 kusy – Next Generation Firewall dle konfigurace A.	0 Kč	0 Kč	Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivý firewall dle přílohy č. 2 – Specifikace NGFW	
2	Uvedte cenu za 10 kusů – Next Generation Firewall dle konfigurace B.	0 Kč	0 Kč	Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivý firewall dle přílohy č. 2 – Specifikace NGFW	
3	Uvedte cenu za podporu a aktualizaci požadovaných bezpečnostních služeb celkově po dobu 60 měsíců. - (8x5) - (24x7)	0 Kč	0 Kč	Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivou položku.	
4	Uvedte cenu za licence a maintenance po dobu 60 měsíců spolu se specifikací, jaké licence jsou třeba.	0 Kč	0 Kč	Cenu uveďte (v Kč bez DPH), případně do komentáře přidejte další poznámky	
5	Uvedte cenu za „firewall management tool“ spolu snáklady na licence a maintenance, support po dobu 60 měsíců.	0 Kč	0 Kč	Cenu uveďte (v Kč bez DPH), případně do komentáře přidejte další poznámky jako je způsob „subscription“, o jaký se jedná nástroj atd.	
Náklady HW celkem:		0 Kč	0 Kč		

Dotazy k pracnosti

Id	Položka indikace nákladů	Předpokládaný počet MD	Předpokládané náklady v Kč	Upřesnění	Poznámka
1	Jaký je Váš odhad ceny pro etapu „Analýza stávající síťové infrastruktury“ (v Kč bez DPH), kde etapa obsahuje fáze: -Dokumentace stávající síťové infrastruktury -Inventarizace síťových zařízení a jejich konfigurací -Mapování současných síťových toků a závislostí -Mapování aplikací a služeb třetích stran -Popis stávajícího prostředí Klíčový výstup dodavatele: Dokument, analyzující síťovou infrastrukturu, která bude popisovat stávající prostředí SŽ v detailu potřebném pro návrh segmentace sítě na základě dodaných podkladů od zadavatele.	500	8 000 000 Kč	Cenu uveďte celkově za jednotlivou etapu, případné poznámky k rozkladu uveďte v doplňujícím komentáři.	odhadujeme cca 6 osob po dobu 9 měsíců
2	Jaký je Váš odhad ceny pro etapu „Specifikace změn architektury segmentované sítě“ (v Kč bez DPH), kde etapa obsahuje fáze: -Základní specifikace -Definice VRF instancí a jejich účelu -Definice postupu konfiguračních prací Klíčový výstup dodavatele: Dokument architektury, zobrazující navrhované změny ve vazbě na segmentaci sítě.	160	2 560 000 Kč	Cenu uveďte celkově za jednotlivou etapu, případné poznámky k rozkladu uveďte v doplňujícím komentáři	
3	Jaký je Váš odhad ceny pro etapu „Implementace / Realizace“ (v Kč bez DPH), kde etapa obsahuje fáze: -Příprava prostředí -Nastavení VRF v testovacím prostředí -Implementace směrovacích protokolů -Příprava operačních procedur -Zátěžové testy -Bezpečnostní testování -Optimalizace konfigurace -Školení na nové technologie -Dodávka požadovaného HW -Rollout plán pro celou uživatelskou síť (akceptace zadavatelem) Klíčový výstup dodavatele: Aktivní kroky implementační na základě dvou předešlých fází dle upřesnění zadavatele, směřující k naplnění segmentace uživatelské sítě.	160	2 560 000 Kč	Cenu uveďte celkově za jednotlivou etapu, případné poznámky k rozkladu uveďte v doplňujícím komentáři.	Pouze pro vybranou pilotní lokalitu po optimalizaci a vyčištění sítě Objednatelem.

3

4	Jaký je náklad na dlouhodobé poskytnutí administrátora síťových prvků CISCO nad rámec realizačního týmu projektu: - Konfigurace L2/L3 switchů, routerů, firewallů - Vytížení kolísavé 16-40 hodin za pracovní týden	1	16 000 Kč	Cenu uveďte jako náklad na 1 MD (8 pracovních hodin) specialisty	
Náklady pracnost celkem:		13 120 000 Kč			

Dotazy k ceně poptávaného hardware NGFW, podpory a licenci

Id	Položka indikace nákladů	Investiční náklady v Kč	Provozní náklady na 5 let v Kč	Upřesnění	Poznámka
1	Uveďte cenu za 2 kusy – Next Generation Firewall dle konfigurace A.	4 462 685 Kč	0 Kč	Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivý firewall dle přílohy č. 2 – Specifikace NGFW	2 231 342 Kč
2	Uveďte cenu za 10 kusů – Next Generation Firewall dle konfigurace B.	10 024 000 Kč	0 Kč	Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivý firewall dle přílohy č. 2 – Specifikace NGFW	1 002 400 Kč
3	Uveďte cenu za podporu a aktualizaci požadovaných bezpečnostních služeb celkově po dobu 60 měsíců. - (8x5) - (24x7)	10 582 658 Kč	0 Kč	Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivou položku.	1 630 016 Kč (A) 723 263 Kč (B)
4	Uveďte cenu za licence a maintenance po dobu 60 měsíců spolu se specifikací, jaké licence jsou třeba.	33 480 160 Kč	0 Kč	Cenu uveďte (v Kč bez DPH), případně do komentáře přidejte další poznámky	
5	Uveďte cenu za „firewall management tool“ spolu s náklady na licence a maintenance, support po dobu 60 měsíců.	140 014 Kč	0 Kč	Cenu uveďte (v Kč bez DPH), případně do komentáře přidejte další poznámky jako je způsob „subscription“, o jaký se jedná nástroj atd.	Doplnění stávajícího FMC
Náklady HW celkem:		58 689 517 Kč	0 Kč		

Dotazy k ceně poptávaného hardware NGFW, podpory a licenci

Id	Položka indikace nákladů	Investiční náklady v Kč	Provozní náklady na 5 let v Kč	Upřesnění	Poznámka
1	Uveďte cenu za 2 kusy – Next Generation Firewall dle konfigurace A.	4 462 685 Kč	0 Kč	Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivý firewall dle přílohy č. 2 – Specifikace NGFW	2 231 342 Kč
2	Uveďte cenu za 10 kusů – Next Generation Firewall dle konfigurace B.	10 024 000 Kč	0 Kč	Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivý firewall dle přílohy č. 2 – Specifikace NGFW	1 002 400 Kč
3	Uveďte cenu za podporu a aktualizaci požadovaných bezpečnostních služeb celkově po dobu 60 měsíců. - (8x5) - (24x7)	10 582 658 Kč	0 Kč	Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivou položku.	1 630 016 Kč (A) 723 263 Kč (B)
4	Uveďte cenu za licence a maintenance po dobu 60 měsíců spolu se specifikací, jaké licence jsou třeba.	33 480 160 Kč	0 Kč	Cenu uveďte (v Kč bez DPH), případně do komentáře přidejte další poznámky	- Kč
5	Uveďte cenu za „firewall management tool“ spolu s náklady na licence a maintenance, support po dobu 60 měsíců.	140 014 Kč	0 Kč	Cenu uveďte (v Kč bez DPH), případně do komentáře přidejte další poznámky jako je způsob „subscription“, o jaký se jedná nástroj atd.	Doplnění stávajícího FMC
Náklady HW celkem:		58 689 517 Kč	0 Kč		

Dotazy k pracnosti - Varianta A (dodáno včetně podrobné kalkulace ve formátu pdf)

Id	Položka indikace nákladů	Předpokládaný počet MD	Předpokládané náklady v Kč	Upřesnění	Poznámka
1	Jaký je Váš odhad ceny pro etapu „Analýza stávající síťové infrastruktury“ (v Kč bez DPH), kde etapa obsahuje fáze: -Dokumentace stávající síťové infrastruktury -Inventarizace síťových zařízení a jejich konfigurací -Mapování současných síťových toků a závislostí -Mapování aplikací a služeb třetích stran -Popis stávajícího prostředí Klíčový výstup dodavatele: Dokument, analyzující síťovou infrastrukturu, která bude popisovat stávající prostředí SŽ v detailu potřebném pro návrh segmentace sítě na základě dodaných podkladů od zadavatele.	10	154 000 Kč	Cenu uveďte celkově za jednotlivou etapu, případné poznámky k rozkladu uveďte v doplňujícím komentáři.	

1	<div>Jaký je Váš odhad ceny pro etapu „Analýza stávající síťové infrastruktury“ (v Kč bez DPH), kde etapa obsahuje fáze: -Dokumentace stávající síťové infrastruktury -Inventarizace síťových zařízení a jejich konfigurací -Mapování současných síťových toků a závislostí -Mapování aplikací a služeb třetích stran -Popis stávajícího prostředí Klíčový výstup dodavatele: Dokument, analyzující síťovou infrastrukturu, která bude popisovat stávající prostředí SŽ v detailu potřebném pro návrh segmentace sítě na základě dodaných podkladů od zadavatele.</div>	30	462 000 Kč	<i>Cenu uveďte celkově za jednotlivou etapu, případné poznámky k rozkladu uveďte v doplňujícím komentáři.</i>	
2	<div>Jaký je Váš odhad ceny pro etapu „Specifikace změn architektury segmentované sítě“ (v Kč bez DPH), kde etapa obsahuje fáze: -Základní specifikace -Definice VRF instancí a jejich účelu -Definice postupu konfiguračních prací Klíčový výstup dodavatele: Dokument architektury, zobrazující navrhované změny ve vazbě na segmentaci sítě.</div>	20	308 000 Kč	<i>Cenu uveďte celkově za jednotlivou etapu, případné poznámky k rozkladu uveďte v doplňujícím komentáři</i>	
3	<div>Jaký je Váš odhad ceny pro etapu „Implementace / Realizace“ (v Kč bez DPH), kde etapa obsahuje fáze: -Příprava prostředí -Nastavení VRF v testovacím prostředí -Implementace směrovacích protokolů -Příprava operačních procedur -Zátěžové testy -Bezpečnostní testování -Optimalizace konfigurace -Školení na nové technologie -Dodávka požadovaného HW -Rollout plán pro celou uživatelskou síť (akceptace zadavatelem) Klíčový výstup dodavatele: Aktivní kroky implementační na základě dvou předešlých fází dle upřesnění zadavatele, směřující k naplnění segmentace uživatelské sítě.</div>	30	495 500 Kč	<i>Cenu uveďte celkově za jednotlivou etapu, případné poznámky k rozkladu uveďte v doplňujícím komentáři.</i>	cena vč. školení Check Point Certified System Administrator, 3dny, 1 člověk
4	<div>Jaký je náklad na dlouhodobé poskytnutí administrátora síťových prvků CISCO nad rámec realizačního týmu projektu: - Konfigurace L2/L3 switchů, routerů, firewallů - Vytížení kolísavé 16-40 hodin za pracovní týden</div>	1	15 400 Kč	<i>Cenu uveďte jako náklad na 1 MD (8 pracovních hodin) specialisty</i>	
Náklady pracnost celkem:			1 265 500 Kč		

Dotazy k ceně poptávaného hardware NGFW, podpory a licencí

Id	Položka indikace nákladů	Investiční náklady v Kč	Provozní náklady na 5 let v Kč	Upřesnění	Poznámka
1	Uveďte cenu za 2 kusy – Next Generation Firewall dle konfigurace A.	0 Kč	0 Kč	<i>Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivý firewall dle přílohy č. 2 – Specifikace NGFW</i>	
2	Uveďte cenu za 10 kusů – Next Generation Firewall dle konfigurace B.	35 366 031 Kč	0 Kč	<i>Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivý firewall dle přílohy č. 2 – Specifikace NGFW</i>	Podrobný položkový rozpad konfigurace FW, licencí a maintenance je součástí nabídky jako Příloha č. 5
3a	Uveďte cenu za podporu a aktualizaci požadovaných bezpečnostních služeb celkově po dobu 60 měsíců. - (8x5)	0 Kč	2 772 000 Kč	<i>Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivou položku.</i>	
3b	Uveďte cenu za podporu a aktualizaci požadovaných bezpečnostních služeb celkově po dobu 60 měsíců. - (24x7)	0 Kč	5 544 000 Kč	<i>Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivou položku.</i>	
4	Uveďte cenu za licence a maintenance po dobu 60 měsíců spolu se specifikací, jaké licence jsou třeba.	0 Kč	0 Kč	<i>Cenu uveďte (v Kč bez DPH), případně do komentáře přidejte další poznámky</i>	Cena za licence a maintenance je zahrnuta v pořizovací ceně FW, podrobný položkový rozpad viz Příloha č. 5
5	Uveďte cenu za „firewall management tool“ spolu snáklady na licence a maintenance, support po dobu 60 měsíců.	2 222 511 Kč	0 Kč	<i>Cenu uveďte (v Kč bez DPH), případně do komentáře přidejte další poznámky jako je způsob „subscription“, o jaký se jedná nástroj atd.</i>	Firewall management tool není potřeba kupovat pro obě varianty A i B zvlášť, stačí pouze 1x CPAP-NGSM600M-BASE, kapacitně je počítáno s 12ks firewallu pro Mangement.
Náklady HW celkem:		37 588 542 Kč	8 316 000 Kč		

Dotazy k pracnosti

Id	Položka indikace nákladů	Předpokládaný počet MD	Předpokládané náklady v Kč	Upřesnění	Poznámka
1	Jaký je Váš odhad ceny pro etapu „Analýza stávající síťové infrastruktury“ (v Kč bez DPH), kde etapa obsahuje fáze: -Dokumentace stávající síťové infrastruktury -Inventarizace síťových zařízení a jejich konfigurací -Mapování současných síťových toků a závislostí -Mapování aplikací a služeb třetích stran -Popis stávajícího prostředí Klíčový výstup dodavatele: Dokument, analyzující síťovou infrastrukturu, která bude popisovat stávající prostředí SŽ v detailu potřebném pro návrh segmentace sítě na základě dodaných podkladů od zadavatele.	120	2 100 000 Kč	<i>Cenu uveďte celkově za jednotlivou etapu, případné poznámky k rozkladu uveďte v doplňujícím komentáři.</i>	V závislosti na detailu informací o prostředí a nutnosti fyz. přístupu.
2	Jaký je Váš odhad ceny pro etapu „Specifikace změn architektury segmentované sítě“ (v Kč bez DPH), kde etapa obsahuje fáze: -Základní specifikace -Definice VRF instancí a jejich účelu -Definice postupu konfiguračních prací Klíčový výstup dodavatele: Dokument architektury, zobrazující navrhované změny ve vazbě na segmentaci sítě.	35	612 500 Kč	<i>Cenu uveďte celkově za jednotlivou etapu, případné poznámky k rozkladu uveďte v doplňujícím komentáři</i>	
3	Jaký je Váš odhad ceny pro etapu „Implementace / Realizace“ (v Kč bez DPH), kde etapa obsahuje fáze: -Příprava prostředí -Nastavení VRF v testovacím prostředí -Implementace směrovacích protokolů -Příprava operačních procedur -Zátěžové testy -Bezpečnostní testování -Optimalizace konfigurace -Školení na nové technologie -Dodávka požadovaného HW -Rollout plán pro celou uživatelskou síť (akceptace zadavatelem) Klíčový výstup dodavatele: Aktivní kroky implementační na základě dvou předešlých fází dle upřesnění zadavatele, směřující k naplnění segmentace uživatelské sítě.	200	3 500 000 Kč	<i>Cenu uveďte celkově za jednotlivou etapu, případné poznámky k rozkladu uveďte v doplňujícím komentáři.</i>	Nemáme představu o rozsahu a aktuální konfiguraci sítě. Není možné konkrétně stanovit, takže náš odhad vychází z nejpravděpodobnějšího scénáře.
4	Jaký je náklad na dlouhodobé poskytnutí administrátora síťových prvků CISCO nad rámec realizačního týmu projektu: - Konfigurace L2/L3 switchů, routerů, firewallů - Vytížení kolísavé 16-40 hodin za pracovní týden	1	17 500 Kč	<i>Cenu uveďte jako náklad na 1 MD (8 pracovních hodin) specialisty</i>	
Náklady pracnost celkem:			6 212 500 Kč		

Dotazy k ceně poptávaného hardware NGFW, podpory a licenci

Id	Položka indikace nákladů	Investiční náklady v Kč	Provozní náklady na 5 let v Kč	Upřesnění	Poznámka
1	Uveďte cenu za 2 kusy – Next Generation Firewall dle konfigurace A.	6 384 448 Kč	0 Kč	<i>Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivý firewall dle přílohy č. 2 – Specifikace NGFW</i>	
2	Uveďte cenu za 10 kusů – Next Generation Firewall dle konfigurace B.	8 553 670 Kč	0 Kč	<i>Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivý firewall dle přílohy č. 2 – Specifikace NGFW</i>	
3	Uveďte cenu za podporu a aktualizaci požadovaných bezpečnostních služeb celkově po dobu 60 měsíců. - (8x5) - (24x7)	17 087 650 Kč	0 Kč	<i>Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivou položku.</i>	
4	Uveďte cenu za licence a maintenance po dobu 60 měsíců spolu se specifikací, jaké licence jsou třeba.	21 637 420 Kč	0 Kč	<i>Cenu uveďte (v Kč bez DPH), případně do komentáře přidejte další poznámky</i>	
5	Uveďte cenu za „firewall management tool“ spolu snáklady na licence a maintenance, support po dobu 60 měsíců.	1 846 791 Kč	0 Kč	<i>Cenu uveďte (v Kč bez DPH), případně do komentáře přidejte další poznámky jako je způsob „subscription“, o jaký se jedná nástroj atd.</i>	
Náklady HW celkem:		55 509 979 Kč	0 Kč		

Dotazy k ceně poptávaného hardware NGFW, podpory a licenci

Id	Položka indikace nákladů	Investiční náklady v Kč	Provozní náklady na 5 let v Kč	Upřesnění	Poznámka
1	Uveďte cenu za 2 kusy – Next Generation Firewall dle konfigurace A.	0 Kč	0 Kč	<i>Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivý firewall dle přílohy č. 2 – Specifikace NGFW</i>	

2	Uvedte cenu za 10 kusů – Next Generation Firewall dle konfigurace B.	0 Kč	0 Kč	Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivý firewall dle přílohy č. 2 – Specifikace NGFW	
3	Uvedte cenu za podporu a aktualizaci požadovaných bezpečnostních služeb celkově po dobu 60 měsíců. - (8x5) - (24x7)	0 Kč	0 Kč	Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivou položku.	
4	Uvedte cenu za licence a maintenance po dobu 60 měsíců spolu se specifikací, jaké licence jsou třeba.	0 Kč	0 Kč	Cenu uveďte (v Kč bez DPH), případně do komentáře přidejte další poznámky	
5	Uvedte cenu za „firewall management tool“ spolu s náklady na licence a maintenance, support po dobu 60 měsíců.	0 Kč	0 Kč	Cenu uveďte (v Kč bez DPH), případně do komentáře přidejte další poznámky jako je způsob „subscription“, o jaký se jedná nástroj atd.	
Náklady HW celkem:		0 Kč	0 Kč		

Dotazy k pracnosti

Id	Položka indikace nákladů	Předpokládaný počet MD	Předpokládané náklady v Kč	Upřesnění	Poznámka
1	Jaký je Váš odhad ceny pro etapu „Analýza stávající síťové infrastruktury“ (v Kč bez DPH), kde etapa obsahuje fáze: -Dokumentace stávající síťové infrastruktury -Inventarizace síťových zařízení a jejich konfigurací -Mapování současných síťových toků a závislostí -Mapování aplikací a služeb třetích stran -Popis stávajícího prostředí Klíčový výstup dodavatele: Dokument, analyzující síťovou infrastrukturu, která bude popisovat stávající prostředí SŽ v detailu potřebném pro návrh segmentace sítě na základě dodaných podkladů od zadavatele.	0	0 Kč	Cenu uveďte celkově za jednotlivou etapu, případně poznámky k rozkladu uveďte v doplňujícím komentáři.	Bez poskytnuté dokumentace a dalších detailů, nejsme schopni kvalifikovaně odhadnout pracnost.
2	Jaký je Váš odhad ceny pro etapu „Specifikace změn architektury segmentované sítě“ (v Kč bez DPH), kde etapa obsahuje fáze: -Základní specifikace -Definice VRF instancí a jejich účelu -Definice postupu konfiguračních prací Klíčový výstup dodavatele: Dokument architektury, zobrazující navrhované změny ve vazbě na segmentaci sítě.	0	0 Kč	Cenu uveďte celkově za jednotlivou etapu, případně poznámky k rozkladu uveďte v doplňujícím komentáři	Bez poskytnuté dokumentace a dalších detailů, nejsme schopni kvalifikovaně odhadnout pracnost.
3	Jaký je Váš odhad ceny pro etapu „Implementace / Realizace“ (v Kč bez DPH), kde etapa obsahuje fáze: -Příprava prostředí -Nastavení VRF v testovacím prostředí -Implementace směrovacích protokolů -Příprava operačních procedur -Zátěžové testy -Bezpečnostní testování -Optimalizace konfigurace -Školení na nové technologie -Dodávka požadovaného HW -Rollout plán pro celou uživatelskou síť (akceptace zadavatelem) Klíčový výstup dodavatele: Aktivní kroky implementační na základě dvou předešlých fází dle upřesnění zadavatele, směřující k naplnění segmentace uživatelské sítě.	0	0 Kč	Cenu uveďte celkově za jednotlivou etapu, případně poznámky k rozkladu uveďte v doplňujícím komentáři.	Bez poskytnuté dokumentace a dalších detailů, nejsme schopni kvalifikovaně odhadnout pracnost.
4	Jaký je náklad na dlouhodobé poskytnutí administrátora síťových prvků CISCO nad rámec realizačního týmu projektu: - Konfigurace L2/L3 switchů, routerů, firewallů - Vytížení kolísavé 16-40 hodin za pracovní týden	0	0 Kč	Cenu uveďte jako náklad na 1 MD (8 pracovních hodin) specialisty	Bez poskytnuté dokumentace a dalších detailů, nejsme schopni kvalifikovaně odhadnout pracnost.
Náklady pracnost celkem:		0 Kč			

Dotazy k ceně poptávaného hardware NGFW, podpory a licencí

Id	Položka indikace nákladů	Investiční náklady v Kč	Provozní náklady na 5 let v Kč	Upřesnění	Poznámka
1	Uvedte cenu za 2 kusy – Next Generation Firewall dle konfigurace A.	15 834 528 Kč	0 Kč	Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivý firewall dle přílohy č. 2 – Specifikace NGFW	2x FW Ceny jsou přepočítány z USD dle aktuálního kurzu, který se může v čase měnit.

2	Uvedte cenu za 10 kusů – Next Generation Firewall dle konfigurace B.	12 550 920 Kč	0 Kč	Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivý firewall dle přílohy č. 2 – Specifikace NGFW	10xFW Ceny jsou přepočítány z USD dle aktuálního kurzu, který se může v čase měnit.
3	Uvedte cenu za podporu a aktualizaci požadovaných bezpečnostních služeb celkově po dobu 60 měsíců. - (8x5) - (24x7)	0 Kč	0 Kč	Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivou položku.	viz bod níže
4	Uvedte cenu za licence a maintenance po dobu 60 měsíců spolu se specifikací, jaké licence jsou třeba.	177 409 296 Kč	0 Kč	Cenu uveďte (v Kč bez DPH), případně do komentáře přidejte další poznámky	Ceny jsou přepočítány z USD dle aktuálního kurzu, který se může v čase měnit.
5	Uvedte cenu za „firewall management tool“ spolu s náklady na licence a maintenance, support po dobu 60 měsíců.	2 297 984 Kč	0 Kč	Cenu uveďte (v Kč bez DPH), případně do komentáře přidejte další poznámky jako je způsob „subscription“, o jaký se jedná nástroj atd.	Ceny jsou přepočítány z USD dle aktuálního kurzu, který se může v čase měnit.
Náklady HW celkem:		208 092 728 Kč	0 Kč		

Dotazy k ceně poptávaného hardware NGFW, podpory a licencí

Id	Položka indikace nákladů	Investiční náklady v Kč	Provozní náklady na 5 let v Kč	Upřesnění	Poznámka
1	Uvedte cenu za 2 kusy – Next Generation Firewall dle konfigurace A.	0 Kč	0 Kč	Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivý firewall dle přílohy č. 2 – Specifikace NGFW	Duplicita s tabulkou výše.
2	Uvedte cenu za 10 kusů – Next Generation Firewall dle konfigurace B.	0 Kč	0 Kč	Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivý firewall dle přílohy č. 2 – Specifikace NGFW	Duplicita s tabulkou výše.
3	Uvedte cenu za podporu a aktualizaci požadovaných bezpečnostních služeb celkově po dobu 60 měsíců. - (8x5) - (24x7)	0 Kč	0 Kč	Cenu uveďte celkově (v Kč bez DPH) a do komentáře za jednotlivou položku.	Duplicita s tabulkou výše.
4	Uvedte cenu za licence a maintenance po dobu 60 měsíců spolu se specifikací, jaké licence jsou třeba.	0 Kč	0 Kč	Cenu uveďte (v Kč bez DPH), případně do komentáře přidejte další poznámky	Duplicita s tabulkou výše.
5	Uvedte cenu za „firewall management tool“ spolu s náklady na licence a maintenance, support po dobu 60 měsíců.	0 Kč	0 Kč	Cenu uveďte (v Kč bez DPH), případně do komentáře přidejte další poznámky jako je způsob „subscription“, o jaký se jedná nástroj atd.	Duplicita s tabulkou výše.
Náklady HW celkem:		0 Kč	0 Kč		

Předběžná tržní konzultace - „Segmentace sítě"

Příloha č. 17 Zadávací dokumentace - Specifikace Next generation FW

Kapacitní specifikace Varianta A

ID Účastníka	Požadovaná vlastnost	Požadovaná hodnota vlastnosti	Hodnota vlastnosti navrhovaného zařízení
2	Typ zařízení	Fyzické ve standardním provedení do rozvaděče o šířce 19 palců.	1RU do 19" Rack
	Název zařízení (specifikujte navrhovaná zařízení)	Uvedte, o jaký se jedná výrobek/společnost	Cisco Secure Firewall 4215
	Minimální počet 40 Gbps rozhraní	2	2x 40/100G QSFP+/QSFP28
	Minimální počet 10 Gbps rozhraní	2	8x 1/10/25/50G SFP/SFP+/SFP28/SFP56
	Dosažitelná reálná propustnost při zapnutých funkcionalitách Firewall, IPS, Aplikační kontrola, Web/URL filtering, Antivirus	Minimálně 20 Gbps provozu označovaného jako „Enterprise Mix traffic“.	65Gbps (1024B Avg)
	SSL/TLS inspekce až do propustnosti	Minimálně 20 Gbps.	20Gbps
	Celková minimální propustnost	90 Gbps	90Gbps
	Minimální propustnost NGFW	60 Gbps	65Gbps

Kapacitní specifikace Varianta B

Požadovaná vlastnost	Požadovaná hodnota vlastnosti	Hodnota vlastnosti navrhovaného zařízení
Typ zařízení	Fyzické ve standardním provedení do rozvaděče o šířce 19 palců.	1RU do 19" Rack
Název zařízení (specifikujte navrhovaná zařízení)	Uvedte o jaký se jedná výrobek/společnost	Cisco Secure Firewall 3130
Minimální počet 25 Gbps rozhraní	2	8x 1/10/25G SFP/SFP+/SFP28
Minimální počet 10 Gbps rozhraní	2	8x 1/10/25G SFP/SFP+/SFP28
Dosažitelná reálná propustnost při zapnutých funkcionalitách Firewall, IPS, Aplikační kontrola, Web/URL filtering, Antivirus	Minimálně 4 Gbps provozu označovaného jako „Enterprise Mix traffic“.	38Gbps (1024B Avg)
SSL/TLS inspekce až do propustnosti	Minimálně 4 Gbps.	9.7Gbps
Celková minimální propustnost	15 Gbps	42Gbps
Minimální propustnost NGFW	10 Gbps	38Gbps

Společné požadavky pro obě varianty

Požadovaná vlastnost	Požadovaná hodnota vlastnosti	Hodnota vlastnosti navrhovaného zařízení
Propustnost SSL/TLS inspekce	Minimálně TLS 1.2 a TLS 1.3.	Podpora dekrypcce (TLS Proxy) pro SSL v3.0, TLS v1.0, TLS v1.1, TLS v1.2, TLS v1.3, QUIC
Interní virtualizace	Zařízení budou rozdělena na dva samostatné klastry, každý klastr musí být možné rozdělit minimálně na 5 samostatných administrativně nezávislých virtuálních zařízení, a to bez nutnosti pořízení dodatečné licence.	Zařízení podporují multi-instance funkcionalitu (podpora až 10x instancí na 4215, 7x instancí na 3130), High-availability cluster & možnost rozdělit virtuální HA instance v rámci dohledu - FMC Multi-domain funkcionality pro zajištění samostatných administrativních domén
Podpora pravidel na základě	Firewallová pravidla umožňují řízení provozu na základě uživatelské identity a uživatelských skupin, ve kterých je uživatelská identita členem.	Podpora získání identit a atributů z MS AD / Azure EntraID / OpenLDAP & mapping infromace pro uživatele můžeme získat Pasivně - ISE-PIC (Syslog, WMI, LDAP, REST API), ISE (dot1x/SXP), TS Agent & Aktivně - Captive Portal, RA VPN, ZTNA (SAML IdP)
Způsoby ověřování uživatelů či napojení na autentizační systémy	Podpora proaktivního ověřování pomocí protokolu LDAP, Kerberos, RADIUS a TACASC+. Dále je požadována SSO funkcionalita na základě proaktivního vyčítání událostí o přihlášení ze systému Active Directory.	Podpora LDAP, RADIUS, Kerberos, SSO
Módy vysoké dostupnosti klastru	Podpora režimů Active-Active a Active-Passive.	Ano Active-Active (Clustering), Active-Standby (High-Availability)
Aplikační kontrola	Detekce a řízení síťových aplikací. Minimálně 4000 rozpoznávaných aplikací.	Ano nyní 7376x rozpoznatelných aplikací (https://appid.cisco.com/home)
URL filtrace	Automatické řízení přístupů k webovým službám na základě reputace a kategorií.	Ano
Antivirus	Ochrana před škodlivým softwarem procházejícím firewall v reálném čase.	Ano AMPfN / Secure Malware Analytics (1-to-1 (TI), local AV, fuzzy-fingerprinting, Spero (Machine learning) , IOC, Retrospection & File trajectory, Sandboxing)
Směrování provozu	Podpora statického, policy based a dynamického směrování provozu.	Statické směrování, ECMP, PBR, application aware/Qos based based routing, Dynamic Routing – BGP, OSPFv2, OSPFv3, EIGPR ,RIP, BFD, Multcats Routing

	Velikost lokálního úložiště	Minimálně 100 GB.	Ano (4215 – 2x 900GB RAID1 SED – Self-Encrypting Drive, 3130 – 1x 900GB SED – Self-Encrypting Drive) SSD
	Ochrana proti DoS a DDoS útokům	Ano.	SNORT Rules (IPS) obsahují specifická pravidla pro ochranu před DoS/DDoS, Security Intelligence (CnC, Bots, Attackers ...), PortScan Detection/Prevention
	Podpora pravidel na základě identit uživatelů	Ano.	Ano
	Podpora ICAP – variantní informace ve smyslu (je – není)	Specializovaný protokol, který umožňuje webovým serverům a proxy serverům přenášet filtrování obsahu, antivirovou kontrolu, vkládání reklam, prevenci ztráty dat (DLP) a další výpočetně náročné úlohy na externí servery ICAP.	Podpora ICAP není. Lokální funkce DLP/AV/Interactive Block – SDD (Sensitive Data Detection v rámci SNORT) pro DLP, malware protection – AMPfN/Malware Analytics pro AV funkce & Interactive Block pro zobrazení vlastního content. Pro specifický content filtering doporučujeme externí zařízení (např. Cisco SWA – Secure Web Appliance / SEG – Secure Email Gateway)
	Další funkcionality	Antibot, Ochrana DNS.	Security Intelligence (antibot), DNS Inspection Policies / Umbrella policies, Encrypted Visibility Engine (EVE), Zero Trust Application Policies
	Podpora IPS/IDS	Pokročilé funkcionality (skenování portů, OS Fingerprinting, IP Fragmentaci, Buffer Overflow, testování SIDS atd).	Podpora IPS/IDS – preprocesory řeší základní IP kontrolu (FCS, Checksum, defragmentace/reassembly, TCP normalizace (Flags), App/OS/User/IOC detection, port scanning, port independent detection atp.)

Kapacitní specifikace Varianta A

ID Účastníka	Požadovaná vlastnost	Požadovaná hodnota vlastnosti	Hodnota vlastnosti navrhovaného zařízení
4	Typ zařízení	Fyzické ve standardním provedení do rozvaděče o šířce 19 palců.	Fyzické ve standardním provedení do rozvaděče o šířce 19 palců.
	Název zařízení (specifikujte navrhovaná zařízení)	Uvedte, o jaký se jedná výrobek/společnost	29100 / Check Point
	Minimální počet 40 Gbps rozhraní	2	2
	Minimální počet 10 Gbps rozhraní	2	2
	Dosažitelná reálná propustnost při zapnutých funkcionalitách Firewall, IPS, Aplikační kontrola, Web/URL	Minimálně 20 Gbps provozu označovaného jako „Enterprise Mix traffic“.	47 Gbps
	SSL/TLS inspekce až do propustnosti	Minimálně 20 Gbps.	103 Gbps
	Celková minimální propustnost	90 Gbps	47 Gbps
	Minimální propustnost NGFW	60 Gbps	130 Gbps

Kapacitní specifikace Varianta B

Požadovaná vlastnost	Požadovaná hodnota vlastnosti	Hodnota vlastnosti navrhovaného zařízení
Typ zařízení	Fyzické ve standardním provedení do rozvaděče o šířce 19 palců.	Fyzické ve standardním provedení do rozvaděče o šířce 19 palců.
Název zařízení (specifikujte navrhovaná zařízení)	Uvedte o jaký se jedná výrobek/společnost	9300 / Check Point
Minimální počet 25 Gbps rozhraní	2	4
Minimální počet 10 Gbps rozhraní	2	8
Dosažitelná reálná propustnost při zapnutých funkcionalitách Firewall, IPS, Aplikační kontrola, Web/URL filtering, Antivirus	Minimálně 4 Gbps provozu označovaného jako „Enterprise Mix traffic“.	28
SSL/TLS inspekce až do propustnosti	Minimálně 4 Gbps.	33
Celková minimální propustnost	15 Gbps	9
Minimální propustnost NGFW	10 Gbps	28

Společné požadavky pro obě varianty

Požadovaná vlastnost	Požadovaná hodnota vlastnosti	Hodnota vlastnosti navrhovaného zařízení
Propustnost SSL/TLS inspekce	Minimálně TLS 1.2 a TLS 1.3.	TLS 1.2, TLS 1.3
Interní virtualizace	Zařízení budou rozdělena na dva samostatné klastry, každý klastr po dvou nodech. Každý klastr musí být možné rozdělit minimálně na 5 samostatných administrativně nezávislých virtuálních zařízení, a to bez nutnosti pořízení dodatečné licence.	Zařízení budou rozdělena na dva samostatné klastry, každý klastr po dvou nodech. Každý klastr musí být možné rozdělit minimálně na 5 samostatných administrativně nezávislých virtuálních zařízení.

	Podpora pravidel na základě	Firewallová pravidla umožňují řízení provozu na základě uživatelské identity a uživatelských skupin, ve kterých je uživatelská identita členem.	Firewallová pravidla umožňují řízení provozu na základě uživatelské identity a uživatelských skupin, ve kterých je uživatelská identita členem.
	Způsoby ověřování uživatelů či napojení na autentizační systémy	Podpora proaktivního ověřování pomocí protokolu LDAP, Kerberos, RADIUS a TACASC+. Dále je požadována SSO funkcionalita na základě proaktivního vyčítání událostí o přihlášení ze systému Active Directory.	Podpora proaktivního ověřování pomocí protokolu LDAP, Kerberos, RADIUS a TACASC+. Dále je požadována SSO funkcionalita na základě proaktivního vyčítání událostí o přihlášení ze systému Active Directory.
	Módy vysoké dostupnosti klastru	Podpora režimů Active-Active a Active-Passive.	Podpora režimů Active-Active a Active-Passive.
	Aplikační kontrola	Detekce a řízení síťových aplikací. Minimálně 4000 rozpoznávaných aplikací.	Detekce a řízení síťových aplikací. Minimálně 4000 rozpoznávaných aplikací.
	URL filtrace	Automatické řízení přístupů k webovým službám na základě reputace a kategorií.	Automatické řízení přístupů k webovým službám na základě reputace a kategorií.
	Antivirus	Ochrana před škodlivým softwarem procházejícím firewall v reálném čase.	Ochrana před škodlivým softwarem procházejícím firewall v reálném čase.
	Směrování provozu	Podpora statického, policy based a dynamického směrování provozu.	Podpora statického, policy based a dynamického směrování provozu.
	Velikost lokálního úložiště	Minimálně 100 GB.	Minimálně 100 GB.
	Ochrana proti DoS a DDoS útokům	Ano.	DoS Ano, pro DDos není firewall vhodná platforma.
	Podpora pravidel na základě identit uživatelů	Ano.	Ano
	Podpora ICAP – variantní informace ve smyslu (je – není)	Specializovaný protokol, který umožňuje webovým serverům a proxy serverům přenášet filtrování obsahu, antivirovou kontrolu, vkládání reklam, prevenci ztráty dat (DLP) a další výpočetně náročné úlohy na externí servery ICAP.	Ano
	Další funkcionality	Antibot, Ochrana DNS.	Ano
	Podpora IPS/IDS	Pokročilé funkcionality (skenování portů, OS Fingerprinting, IP Fragmentaci, Buffer Overflow, testování SIDS atd).	Ano

Kapacitní specifikace Varianta A

ID Účastníka	Požadovaná vlastnost	Požadovaná hodnota vlastnosti	Hodnota vlastnosti navrhovaného zařízení
5	Typ zařízení	Fyzické ve standardním provedení do rozvaděče o šířce 19 palců.	29100
	Název zařízení (specifikujte navrhovaná zařízení)	Uvedte, o jaký se jedná výrobek/společnost	29100
	Minimální počet 40 Gbps rozhraní	2	2
	Minimální počet 10 Gbps rozhraní	2	2
	Dosažitelná reálná propustnost při zapnutých funkcionalitách Firewall, IPS, Aplikační kontrola, Web/URL filtering, Antivirus	Minimálně 20 Gbps provozu označovaného jako „Enterprise Mix traffic“.	47 Gbps
	SSL/TLS inspekce až do propustnosti	Minimálně 20 Gbps.	103 Gbps
	Celková minimální propustnost	90 Gbps	47 Gbps
	Minimální propustnost NGFW	60 Gbps	130 Gbps

Kapacitní specifikace Varianta B

Požadovaná vlastnost	Požadovaná hodnota vlastnosti	Hodnota vlastnosti navrhovaného zařízení
Typ zařízení	Fyzické ve standardním provedení do rozvaděče o šířce 19 palců.	9300
Název zařízení (specifikujte navrhovaná zařízení)	Uvedte o jaký se jedná výrobek/společnost	9300
Minimální počet 25 Gbps rozhraní	2	4 porty 10/25G
Minimální počet 10 Gbps rozhraní	2	4 porty 10/25G
Dosažitelná reálná propustnost při zapnutých funkcionalitách Firewall, IPS, SSL/TLS inspekce až do propustnosti	Minimálně 4 Gbps provozu označovaného jako „Enterprise Mix traffic“.	9 Gbps
SSL/TLS inspekce až do propustnosti	Minimálně 4 Gbps.	5,1
Celková minimální propustnost	15 Gbps	70 Gbps
Minimální propustnost NGFW	10 Gbps	28,2

Společné požadavky pro obě varianty

Požadovaná vlastnost	Požadovaná hodnota vlastnosti	Hodnota vlastnosti navrhovaného zařízení
Propustnost SSL/TLS inspekce	Minimálně TLS 1.2 a TLS 1.3.	Specifikace podmínek
Interní virtualizace	Zařízení budou rozdělena na dva samostatné klastry, každý klastr po dvou nodech. Každý klastr musí být možné rozdělit minimálně na 5 samostatných administrativně nezávislých virtuálních zařízení, a to bez nutnosti pořízení dodatečné licence.	Licence na 6 VSX
Podpora pravidel na základě	Firewallová pravidla umožňují řízení provozu na základě uživatelské identity a uživatelských skupin, ve kterých je uživatelská identita členem.	ANO
Způsoby ověřování uživatelů či napojení na autentizační systémy	Podpora proaktivního ověřování pomocí protokolu LDAP, Kerberos, RADIUS a TACASC+. Dále je požadována SSO funkcionalita na základě proaktivního vyčítání událostí o přihlášení ze systému Active Directory.	ANO s výjimkou TACACS+
Módy vysoké dostupnosti klastru	Podpora režimů Active-Active a Active-Passive.	ANO

	Aplikační kontrola	Detekce a řízení síťových aplikací. Minimálně 4000 rozpoznávaných aplikací.	Více než 4500
	URL filtrace	Automatické řízení přístupů k webovým službám na základě reputace a kategorií.	ANO
	Antivirus	Ochrana před škodlivým softwarem procházejícím firewall v reálném čase.	ANO
	Směrování provozu	Podpora statického, policy based a dynamického směrování provozu.	ANO
	Velikost lokálního úložiště	Minimálně 100 GB.	480 GB
	Ochrana proti DoS a DDoS útokům	Ano.	ANO
	Podpora pravidel na základě identit uživatelů	Ano.	ANO
	Podpora ICAP – variantní informace ve smyslu (je – není)	Specializovaný protokol, který umožňuje webovým serverům a proxy serverům přenášet filtrování obsahu, antivirovou kontrolu, vkládání reklam, prevenci ztráty dat (DLP) a další výpočetně náročné úlohy na externí servery ICAP.	ANO
	Další funkcionality	Antibot, Ochrana DNS.	ANO
	Podpora IPS/IDS	Pokročilé funkcionality (skenování portů, OS Fingerprinting, IP Fragmentaci, Buffer Overflow, testování SIDS atd).	ANO

Příloha č. 18 zadávací dokumentace

PROFESNÍ ŽIVOTOPIS

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

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

VZDĚLÁNÍ

[DOPLNÍ DODAVATEL] <i>Dodavatel doplní nejvyšší dokončené vzdělání</i>	[DOPLNÍ DODAVATEL]
[DOPLNÍ DODAVATEL]	[DOPLNÍ DODAVATEL]

PROFESNÍ A DALŠÍ CERTIFIKÁTY

[DOPLNÍ DODAVATEL] <i>Dodavatel doplní datum obdržení autorizace / osvědčení / certifikátu ve formátu DD/MM/YY</i>	[DOPLNÍ DODAVATEL] <i>Dodavatel doplní zejména certifikáty prokazující odbornou způsobilost</i>
[DOPLNÍ DODAVATEL]	[DOPLNÍ DODAVATEL]

POZICE V REALIZAČNÍM TÝMU

[DOPLNÍ DODAVATEL]

PROFESNÍ PRAXE

[DOPLNÍ DODAVATEL] <i>Dodavatel doplní dobu profesní praxe na konkrétní pozici ve formátu mm/rrrr - mm/rrrr, případně zaměstnavatele</i>	[DOPLNÍ DODAVATEL] <i>Dodavatel doplní označení pozice a rovněž stručný popis vykonávaných činností, ze kterého bude vyplývat naplnění požadavků dle čl. 12 zadávací dokumentace</i>
[DOPLNÍ DODAVATEL]	[DOPLNÍ DODAVATEL]

ZKUŠENOSTI PRO ÚČELY PROKÁZÁNÍ TECHNICKÉ KVALIFIKACE

<i>Dodavatel uvede objednatele významné zakázky:</i>	<i>Dodavatel uvede název a popis předmětu plnění významné zakázky, ze</i>	<i>Dodavatel uvede celkový finanční objem významné</i>	<i>Dodavatel uvede dobu realizace (datum od-do)</i>
--	---	--	---

<i>název, IČO, sídlo, místo podnikání, kontakt k ověření realizované významné zakázky (telefonní a e-mailový kontakt na kontaktní osobu)</i> [DOPLNÍ DODAVATEL]	<i>kterého bude vyplývat naplnění požadavků dle čl. 12.2 zadávací dokumentace</i> [DOPLNÍ DODAVATEL]	<i>zakázky</i> [DOPLNÍ DODAVATEL]	[DOPLNÍ DODAVATEL]
[DOPLNÍ DODAVATEL]	[DOPLNÍ DODAVATEL]	[DOPLNÍ DODAVATEL]	[DOPLNÍ DODAVATEL]

ZKUŠENOSTI PRO ÚČELY HODNOCENÍ V RÁMCI DÍLČÍHO HODNOTÍČÍHO KRITÉRIA „ZKUŠENOSTI ČLENŮ REALIZAČNÍHO TÝMU“

<i>Dodavatel uvede objednatele významné zakázky: název, IČO, sídlo, místo podnikání, kontakt k ověření realizované významné zakázky (telefonní a e-mailový kontakt na kontaktní osobu)</i> [DOPLNÍ DODAVATEL]	<i>Dodavatel uvede název a popis předmětu plnění významné zakázky, ze kterého bude vyplývat naplnění požadavků dle čl. 17.3 zadávací dokumentace</i> [DOPLNÍ DODAVATEL]	<i>Dodavatel uvede celkový finanční objem významné zakázky</i> [DOPLNÍ DODAVATEL]	<i>Dodavatel uvede dobu realizace (datum od-do)</i> [DOPLNÍ DODAVATEL]
[DOPLNÍ DODAVATEL]	[DOPLNÍ DODAVATEL]	[DOPLNÍ DODAVATEL]	[DOPLNÍ DODAVATEL]

Tento strukturovaný životopis je určen pro účely podání nabídky do veřejné zakázky s názvem „**Segmentace sítě**“, č.j. 65403/2025-SŽ-GR-O25.

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

V [DOPLNÍ DODAVATEL] dne [DOPLNÍ DODAVATEL]

Podpis člena realizačního týmu

titul, jméno, příjmení
[DOPLNÍ DODAVATEL]

Příloha č. 19 zadávací dokumentace

Čestné prohlášení o splnění technické kvalifikace – seznam významných služeb

Účastník:

Obchodní firma/jméno [DOPLNÍ ÚČASTNÍK]

Sídlo/místo podnikání [DOPLNÍ ÚČASTNÍK]

IČO [DOPLNÍ ÚČASTNÍK]

Zastoupen [DOPLNÍ ÚČASTNÍK]

který podává nabídku na nadlimitní sektorovou veřejnou zakázku s názvem „**Segmentace sítě**“, č.j. **65403/2025-SŽ-GŘ-O25**, tímto čestně prohlašuje, že za posledních 5 let před zahájením zadávacího řízení realizoval alespoň 1 významnou zakázku splňující požadavky dle čl. 12.1.1 písm. a) a b) zadávací dokumentace.

Objednatel významné zakázky Název, IČO, sídlo, místo podnikání, kontakt k ověření realizované významné zakázky (telefonní a e-mailový kontakt na kontaktní osobu)	Název a předmět plnění významné zakázky	Celkový finanční objem významné zakázky	Doba realizace (datum od-do, v rámci 5 kalendářních let nazpět před zahájením zadávacího řízení)

V dne