SPRÁVA ŽELEZNIC

Smlouva o dílo – Log management a SIEM

Číslo smlouvy Objednatele: 73491/2024-SŽ-GŘ-O8
Číslo smlouvy Zhotovitele: SML/2023/182

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: **ALEF NULA, a. s.**
zapsaná v obchodním rejstříku vedeném městským soudem v Praze pod sp. zn. B 2727
Praha 8 – Karlín, Pernerova 691/42, PSČ 186 00
IČO 61858579, DIČ CZ61858579
Bankovní spojení: XXX
Číslo účtu: XXX
Zastoupená Ing. Milanem Zinkem, předsedou představenstva
(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 „***Log management a SIEM***", ev. č. veřejné zakázky ve Věstníku veřejných zakázek: F2023-042966/ č.j. veřejné zakázky 61441/2023-SŽ-GŘ-O8 (dále jen „**Veřejná zakázka**" a „**Zadávací řízení**") Objednatelem 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 Objednatelem vyhodnocena jako ekonomicky nejvýhodnější.

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 Smlouvy;
2) Přílohy č. 1 až 6 Smlouvy;
3) Příloha č. 7 Smlouvy – Zvláštní obchodní podmínky pro Zakázky v oblasti ICT (dále jen „**ZOP**");
4) Příloha č. 8 Smlouvy – Obchodní podmínky ke Smlouvě o dílo (dále jen „**OOP**");
5) Ostatní dokumenty zadávací dokumentace Veřejné zakázky či zmiňované ve Smlouvě.

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

Pokud nevyplývá ze Smlouvy jinak, mají pojmy s velkými počátečními písmeny význam definovány v ZOP, nebo OOP. Pro vyloučení jakýchkoliv pochybností Strany uvádějí, že pokud je ve Smlouvě obsažen článek se shodným názvem jako v ZOP, OOP nebo jiném smluvním dokumentu, neznamená to, že by článek 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 jen „**ZoKB**"), musí provádět bezpečnostní opatření (§ 5 ZoKB) v rozsahu nezbytném pro zajištění kybernetické bezpečnosti informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury. Jedním ze způsobů, jak naplnit tyto povinnosti, je implementace řešení Log management a SIEM, které bude zajišťovat jednotný sběr provozních a bezpečnostních událostí z prostředí SŽ, uchovávat je pro potřeby analýzy a archivovat je v souladu s legislativními požadavky.

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 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 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. Součástí zadávací dokumentace Veřejné zakázky je interní předpis s názvem „Provozní politika prvků v působnosti systému řízení bezpečnosti informací".

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 poskytnutí vymezených činností za účelem dodávky, implementace a podpory řešení Log management a SIEM, které bude zajišťovat jednotný sběr provozních a bezpečnostních událostí z prostředí SŽ, uchovávat je pro potřeby analýzy a archivovat je v souladu s legislativními požadavky. Bližší požadavky na Předmět díla jsou vymezeny zejména, nikoliv však výlučně, v části 2 a části 4 přílohy č. 1 *Specifikace plnění* této Smlouvy (dále jen „**Příloha č. 1**").

2.3 Provedení Díla spočívá v provedení následujících **oblastí** dílčích činností ze strany Zhotovitele podrobně definovaných v části 2 a 4 Přílohy č. 1:

Etapa

Etapa 1A

2.3.1 Před-implementační analýza dle části 2.3.1 a 4.1.1 Přílohy č. 1.

Etapa 1B

2.3.2 Instalace a konfigurace řešení, Dodávka technologií Log management a SIEM Napojení určených zdrojů logů pro etapu 1 dle části 2.3.1, 2.4, 2.4.13 a 4.1.2 a 4.1.3 Přílohy č. 1.

Etapa 2

2.3.3 Napojení určených zdrojů logů pro etapu 2 dle části 2.3.2 a 4.1.3 Přílohy č. 1.

Etapa 3

2.3.4 Tvorba a optimalizace bezpečnostní/detekční politiky řešení dle části 2.3.3 a 4.1.4. Přílohy č. 1

2.3.5 Školení dle části 4.1.5 Přílohy č. 1.

Etapa 4

2.3.6 Napojení určených zdrojů logů pro etapu 4 dle části 2.3.4 a 4.1.3 Přílohy č. 1.

Etapa 5

2.3.7 Technická podpora servisního týmu SŽ dle části 2.3.5 a 4.2.1 Přílohy č. 1.

2.3.8 Údržba řešení dle části 2.3.5 a 4.2.2 Přílohy č. 1.

Etapa 6

2.3.9 Konzultace a rozvojové aktivity dle části 4.2.3 Přílohy č. 1.

3 Místo plnění

3.1 Místem plnění Smlouvy je především sídlo Objednatele a sídla jednotlivých organizačních složek Objednatele, nebo jakákoliv jiná místa, pokud je to potřebné či vhodné za účelem 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 Smlouvy činí 5 let a 4 měsíce (dále jen „**doba trvání Smlouvy**“) ode dne účinnosti Smlouvy. Tato Smlouva však nepozbyde účinnosti dříve, než za 5 let od ukončení etapy 1B podle přílohy č. 3 Smlouvy (dále jen „**Harmonogram**“).

4.2 Harmonogram předpokládá pro zahájení plnění Etapy 1B připravenost Platformy SŽ na straně Objednatele, přičemž tato podmínka bude splněna prohlášením Objednatele o připravenosti virtualizační platformy vůči Zhotoviteli.

4.3 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.

4.4 Pokud není stanoveno jinak, je Zhotovitel povinen provádět Dílo v termínech uvedených v závazném harmonogramu realizace Díla obsaženém v Harmonogramu.

4.5 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 Smlouvy, tj. Cena díla, je uvedena pod položkou Nabídková cena celkem v příloze č. 2 Smlouvy (dále jen „**Příloha č. 2**").

5.2 Ceny, a to jak jednotkové ceny, tak nabídková cena celkem, obsažené v Příloze č. 2. Nabídková cena, 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 Smlouvy, náklady na licence apod. jsou všechny zahrnuty v cenách obsažených v Příloze č. 2).

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

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

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

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

6 Platební podmínky

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

6.1.1 První platební milník: Výzva k úhradě ve výši jednotkové ceny za položku v Příloze č. 2: E1 - Před-implementační analýza, Implementační služby (napojení určených zdrojů logů pro Etapu 1), E1 - Licence, údržba licencí a technická podpora výrobce na 60 měsíců, nebo subskripce licencí včetně údržby a technické podpory na 60 měsíců (celková cena za výčet licencí uvedených v Příloze č. 20 Zadávací dokumentace "Log management a SIEM dotazník", záložka Licence), E1 – Hardwarové prostředky, dodávané nad rámec specifikovaných Požadavků na služby Platformy SŽ, technická podpora výrobce HW na 60 měsíců, údržba a technická podpora HW dodavatele na 60 měsíců, a to nejdříve po akceptaci (bez výhrad) Etapy 1 (tedy Etapy 1A a Etapy 1B), která je tvořena činnostmi uvedenými v části 2.3.1., 2.4., 2.4.13, 4.1.1;4.1.2;4.1.3 Přílohy č. 1;

6.1.2 Druhý platební milník: Výzva k úhradě ve výši jednotkové ceny za položku v Příloze č. 2: E2 - Implementační služby (napojení určených zdrojů logů pro Etapu 2), a to nejdříve po akceptaci (bez výhrad) Etapy 2, která je tvořena činnostmi uvedenými v části 2.3.2 a 4.1.3 Přílohy č. 1;

6.1.3 Třetí platební milník: Výzva k úhradě ve výši jednotkové ceny za položku v Příloze č. 2: E3 – Tvorba a optimalizace bezpečnostní / detekční politiky řešení, Školení, a to nejdříve po akceptaci (bez výhrad) Etapy 3, která je tvořena činnostmi uvedenými v části 2.3.3, 4.1.4 a 4.1.5. Přílohy č. 1;

6.1.4 Čtvrtý platební milník: Výzva k úhradě ve výši jednotkové ceny za položku v Příloze č. 2: E4 - Implementační služby (napojení určených zdrojů logů pro Etapu 4), a to nejdříve po akceptaci (bez výhrad) Etapy 4, která je tvořena činnostmi uvedenými v části 2.3.2 a 4.1.3 Přílohy č. 1;

6.2 Zhotovitel je dále oprávněn doručit Objednateli Výzvu k úhradě za poskytování služeb Technická podpora servisního týmu SŽ dle čl. 2.3.5 a 4.2.1 Přílohy č. 1 a čl. 11 této Smlouvy, a Údržba řešení dle čl. v části 2.3.5 a 4.2.2 Přílohy č. 1 této Smlouvy, a to opakovaně po dobu trvání Smlouvy po uplynutí každého 1 měsíce ode dne akceptace (bez výhrad) Etapy 1B. Každá Výzva k úhradě dle předchozí věty může být vystavena ve výši jednotkové ceny za položku dle Přílohy č. 2 této Smlouvy: Technická podpora servisního týmu SŽ, údržba řešení.

6.3 Zhotovitel je dále oprávněn doručit Objednateli Výzvu k úhradě po akceptaci (bez výhrad) každého plnění na základě Objednávky Konzultací a rozvojových aktivit dle čl. 12 této Smlouvy, a to ve výši součinu počtu MD dle skutečně provedených MD (nejvýše dle Objednávky) a ceny za jednu MD dle příslušné položky ceny Konzultace a rozvojové aktivity 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_005/0000104. Pokud je Výzva k úhradě hrazena z více zdrojů, budou na ní uvedena všechna čísla projektů. Objednatel je oprávněn čísla projektu aktualizovat v průběhu trvání této Smlouvy a Zhotovitel je povinen tuto skutečnost akceptovat a zohlednit v rámci prováděné fakturace.

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

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 Smlouvy.

6.8 Zhotovitel se zavazuje, že bankovní účet jím určený pro zaplacení jakéhokoliv závazku Objednatele na základě Smlouvy bude od data podpisu 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 Smlouvy či v souvislosti s ní vůči jakýmkoliv pohledávkám Objednatele. Pohledávky a nároky Zhotovitele vzniklé na základě 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 Smlouvu). Jakýkoliv právní úkon učiněný Zhotovitelem v rozporu s tímto ustanovením bude považován za podstatné porušení 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 smlouvy, resp. jeho část, a to vždy do 60 kalendářních dnů od obdržení platby ze strany Objednatele za konkrétní plnění předmětu smlouvy, resp. jeho části.

7 Akceptační řízení

7.1 Akceptačnímu řízení dle části 8 ZOP a tohoto článku Smlouvy podléhají Etapy definované v čl. 2 odst. 2.3.1 až 2.3.9. této Smlouvy, tj. Etapa 1A, Etapa 1B, Etapa 2, Etapa 3, Etapa 4, Etapa 5 a Etapa 6. Pro vyloučení všech pochybností Strany výslovně uvádějí, že Etapa 1A, Etapa 1B, Etapa 2, Etapa 3, Etapa 4, Etapa 5 a Etapa 6 podléhají samostatnému Akceptačnímu řízení.

7.2 Každá Fáze plnění podléhají samostatnému Akceptačnímu řízení se považuje za ukončenou akceptací (bez výhrad) posledního dílčího plnění uvedeného pro příslušnou Etapu v části 2 a 4 Přílohy č. 1 této Smlouvy. Akceptační kritéria pro každou dílčí část jednotlivých Etap vyplývají z části 2 a 4 Přílohy č. 1 této Smlouvy, kdy Dodavatel předá Objednateli všechny části plnění uvedené v kategorii „Výstupy". U Etapy 5 předá Dodavatel Objednateli vždy do 5 dnů od skončení příslušného měsíce poskytování služeb měsíční výkaz shrnující poskytnutí dané služby za tento měsíc.

7.3 Zhotovitel bere na vědomí, že v rámci Předmětu díla může dojít k upřesnění Předmětu díla, resp. Akceptačních kritérií jednotlivých Etap. 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 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 Smlouvy podléhají rovněž práce provedené na základě Objednávek Konzultací a rozvojových aktivit dle článku 12 Smlouvy. Akceptační kritéria vyplývají ze specifikace prací uvedených v Objednávce.

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

8 Licenční ujednání

8.1 Pokud jsou výstupy dílčích činností ze strany Zhotovitele podrobně definované v části 4 Přílohy č. 1 této Smlouvy, Autorským dílem, uplatní se čl. 6.2. ZOP.

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, jehož parametry jsou podrobněji vymezeny v čl. 4.1.5 Přílohy č. 1 této Smlouvy.

10 Helpdesk

10.1 Zhotovitel se zavazuje nejpozději do dne účinnosti Smlouvy založit a po celou dobu trvání Smlouvy udržovat v provozu Helpdesk, a to za podmínek dle části 10 ZOP.

10.2 Zhotovitel se zavazuje zajišťovat Helpdesk v **Režimu 1** ve smyslu části 10 ZOP.

10.3 Helpdesk bude provozován ve třetí **úrovni (L3)** podpory ve smyslu části 10 ZOP.

11 Technická podpora servisního týmu SŽ a Údržba řešení

11.1 Zhotovitel se zavazuje v souladu s částí 4.2.1 a 4.2.2. Přílohy č. 1 této Smlouvy poskytovat Objednateli Technickou podpora servisního týmu SŽ a Údržbu řešení, a to ode dne akceptace (bez výhrad) Etapy B1 po dobu 60 měsíců.

11.2 Technická podpora servisního týmu SŽ a Údržba řešení spočívá zejména v přijímání hlášení o Incidentech přes Helpdesk a jejich následném vyřešení v souladu s podmínkami této Smlouvy.

11.3 Způsob nahlášení Incidentu je stanoven v části 11 ZOP, přičemž Ohlašovatel určí kategorii Incidentu dle odst. 1.1.19 ZOP. Určení kategorie Incidentu může být změněno, pokud Zhotovitel prokáže, že kategorie Incidentu je jiná.

11.4 Incidenty a Požadavky budou řešeny podle **servisního modelu B1** vymezeného v části 12 ZOP.

12 Služby Konzultace a rozvojové aktivity

12.1 Zhotovitel se zavazuje poskytovat Služby konzultace a rozvojové aktivity na vyžádání, které jsou blíže vymezeny v části 4.2.3 Přílohy č. 1 této Smlouvy.

12.2 Maximální souhrn Služeb konzultace a rozvojových aktivit na vyžádání činí 250 MD za celou dobu trvání Smlouvy ode dne účinnosti Smlouvy.

12.3 Objednatel v případě zájmu o provedení prací v rámci Služeb konzultace a rozvojových aktivit na vyžádání doručí Zhotoviteli objednávku prostřednictvím e-mailu Kontaktních osob uvedených v čl. 14 této Smlouvy se specifikací požadovaných prací v části 4.2.3 Přílohy č. 1 této Smlouvy, termínem provedení těchto prací a předpokládanou časovou náročností vyjádřenou v MD (dále jen „**Objednávka**“).

12.4 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 Smlouvy. Objednatel je povinen oprávněné připomínky Zhotovitele zohlednit v obsahu Objednávky.

12.5 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. 14 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.

12.6 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 a poskytnout ve vztahu k těmto pracím Objednateli licenci či jiná práva z duševního vlastnictví v rozsahu dle čl. 7.1 této Smlouvy.

13 Účast poddodavatelů a realizační tým

13.1 Zhotovitel je oprávněn plnit tuto Smlouvu výlučně prostřednictvím Poddodavatelů uvedených v příloze č. 6 této Smlouvy – Seznam poddodavatelů.

13.2 Před zapojením nového Poddodavatele do plnění Smlouvy musí být Objednateli předložen nový seznam poddodavatelů, který bude tvořit přílohu č. 6 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.

13.3 Seznam členů realizačního týmu je Přílohou č. 9 této Smlouvy. Pravidla pro realizační tým se řídí částí 14 ZOP.

14 Komunikace stran

14.1 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 Smlouvy, zejména podávají a přijímají informace o průběhu plnění Smlouvy (dále jen „**Kontaktní osoby**").

14.2 Kontaktními osobami za Objednatele jsou:

- ve věcech smluvních: XXX
- ve věcech technických: XXX
- ve věcech kybernetické bezpečnosti: XXX

Kontaktními osobami za Zhotovitele jsou:

- ve věcech smluvních: XXX
- ve věcech technických: XXX
- ve věcech kybernetické bezpečnosti: XXX

14.3 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 ke Smlouvě.

15 Smluvní pokuty

15.1 Objednatel je povinen uhradit smluvní pokutu za překročení nároků řešení na Požadavky na služby Platformy SŽ (příloha č. 5), které dodavatel definuje v listu „*Požadavky*" dle této přílohy, a to ve výši 150,00 Kč za každý bod nad celkový počet

bodů uvedených v buňce C14 na řádku označeném Dílčí body hodnotícího kritéria "Požadavky na služby Platformy SŽ" dle požadavků na služby Platformy SŽ.

15.2 Překročení nároků systému na Požadavky na služby Platformy SŽ je Objednatel oprávněn posuzovat kdykoli po dobu trvání účinnosti této Smlouvy, i kdykoliv po jejím skončení.

15.3 Jestliže Objednatel uplatní nárok na smluvní pokutu dle odstavce 15.1 této Smlouvy a následně by mu vzniklo právo požadovat vyšší smluvní pokutu dle odstavce 15.1 této Smlouvy, má Objednatel právo požadovat rozdíl mezi touto vyšší smluvní pokutou a nižší smluvní pokutou již dříve uplatněnou.

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

16 Ukončení smluvního vztahu

16.1 Objednatel je oprávněn odstoupit od 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 Smlouvy a změně oprávnění nakládat s těmito aktivy, či dojde ke změně ekvivalentní změnám výše uvedeným a tato změna bude Objednatelem vyhodnocena jako riziko bezpečnosti informací, které nelze odstranit jiným opatřením; toto ustanovení se uplatní i pro případ, že Dodavatel o takových změnách dopředu a včas neinformuje Objednatele.

16.2 Dodavatel se zavazuje dle pokynů Objednatele v souvislosti s ukončením smluvního vztahu založeného touto Smlouvou (z jakéhokoliv důvodu) provádět činnosti spočívající v součinnosti při ukončení této Smlouvy (exit plán), a to při přípravě a předání novému Dodavateli, nebo Objednateli.

16.3 Činnosti dle čl. 16.2 této Smlouvy budou provedeny v souladu s výstupem před-implementační analýzy dle čl. 4.1.1 Přílohy č. 1 této Smlouvy a jsou již zahrnuty v Ceně díla.

16.4 Dodavatel se zavazuje součinnost dle článku 16.2 této Smlouvy poskytovat s odbornou péčí, zodpovědně a do doby úplného převzetí novým dodavatelem, nebo Objednatelem.

16.5 Nesplnění kteréhokoliv požadavku na technické funkcionality řešení uvedené v kapitole 2.4. Přílohy č. 1 a v příloze č. 4 této smlouvy „Log management a SIEM dotazník" a funkcionalit uvedených v této Smlouvě bude to považováno za hrubé porušení povinností a bude důvodem pro odstoupení od této Smlouvy.

16.6 Další pravidla pro ukončení smluvního vztahu stanoví část 18 ZOP.

17 Kybernetická bezpečnost

17.1 Zhotovitel se zavazuje k zachovávání požadavků kybernetické bezpečnosti zejména dle části 20 ZOP.

17.2 Zhotovitel je významným dodavatelem, zavazuje se tedy i k zachovávání požadavků kybernetické bezpečnosti dle části 20 ZOP vztahujících se k významným dodavatelům.

18 Ochrana osobních údajů

18.1 Pokud bude v rámci plnění této Smlouvy docházet ke zpracování osobních údajů, zavazuje se Zhotovitel dodržovat opatření dle části 21 ZOP.

19 Ochrana důvěrných informací

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

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

20.1 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.

20.2 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:

20.2.1 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,

20.2.2 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**").

20.3 Je-li Zhotovitelem sdružení více osob, platí podmínky dle odstavce 20.1 a 20.2 této Smlouvy také jednotlivě pro všechny osoby v rámci Zhotovitele sdružené, a to bez ohledu na právní formu tohoto sdružení.

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

20.5 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.

20.6 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.

20.7 Ukáží-li se prohlášení Zhotovitele dle odstavce 20.1 a 20.2 této Smlouvy jako nepravdivá nebo poruší-li Zhotovitel svou oznamovací povinnost dle odstavce 20.4. nebo povinnosti dle odstavců 20.5 nebo 20.6 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.

21 Přímé platby poddodavatelům

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

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

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

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

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

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

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

21.8 V případě, že částka k úhradě již byla uhrazena Zhotoviteli, Objednatel ji uhradí poddodavateli, a následně bude o částku k úhradě snížena celková odměna Zhotovitele, a to formou započtení proti pohledávce nebo pohledávkám Zhotovitele vzniklých na základě plnění této Smlouvy. O zápočtu proti pohledávce Zhotovitele musí Objednatel Zhotovitele písemně informovat. Není-li již budoucí platba, kterou by Objednatel mohl započíst proti své pohledávce vůči Zhotoviteli, představuje částka k úhradě výši smluvní pokuty za nesplnění povinnosti dle čl. 21.1 této Smlouvy a Zhotovitel se zavazuje tuto smluvní pokutu uhradit nejpozději do 15 dnů ode dne doručení výzvy k zaplacení.

22 Další povinnosti Zhotovitele

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

22.2 Zhotovitel je povinen minimálně do 31. 12. 2035 poskytovat požadované informace a dokumentaci související s plněním 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 jim při provádění kontroly součinnost.

22.3 Zhotovitel je povinen při plnění předmětu plnění 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 Smlouvy. Zhotovitel se zavazuje výše uvedené zajistit i u svých poddodavatelů.

22.4 Plnění povinností dle čl. 22.3 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.

23 Závěrečná ujednání

23.1 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 Smlouvy, jeho ceně či hodnotě a datu uzavření této Smlouvy.

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

23.3 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.

23.4 Jestliže Strana označí za své obchodní tajemství část obsahu Smlouvy, která v důsledku toho bude pro účely uveřejnění Smlouvy v registru smluv znečitelněna, nese tato Strana odpovědnost, pokud by Smlouva v důsledku takového označení byla uveřejněna způsobem odporujícím ZRS, a to bez ohledu na to, která ze stran Smlouvu v registru smluv uveřejnila. S částmi Smlouvy, které druhá 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 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.

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

23.6 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.

23.7 Veškerá práva a povinnosti Stran vyplývající ze Smlouvy se řídí českým právním řádem.

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

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

23.10 Je-li nebo stane-li se jakékoli ustanovení Smlouvy neplatným, nezákonným nebo nevynutitelným, netýká se tato neplatnost a nevynutitelnost zbývajících ustanovení 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.

23.11 Smlouvu lze měnit pouze písemnými dodatky.

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

Přílohy

1. Specifikace plnění této Smlouvy
2. Specifikace nabídkové ceny
3. Harmonogram
4. Log management a SIEM dotazník
5. Požadavky na služby Platformy SŽ
6. Seznam poddodavatelů
7. Zvláštní obchodní podmínky pro Zakázky v oblasti ICT
8. Obchodní podmínky ke Smlouvě o dílo
9. Realizační tým
10. Platforma 2.0

Za Objednatele:

elektronicky podepsáno 8. 11. 2024

……

Bc. Jiří Svoboda, MBA
generální ředitel

Za Dodavatele:

elektronicky podepsáno 18. 11. 2024

……

Ing. Milan Zinek
předseda představenstva

Klasifikace: Veřejný dokument

SPRÁVA ŽELEZNIC

Technická specifikace

Příloha č. 1a Smlouvy

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

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

Obsah

1 Seznam zkratek

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

Přehled zkratek a pojmů:

Zkratka	Popis
API	Rozhraní pro programování aplikací (Application Programming Interface)
CDP	Centrální dispečerské pracoviště
DNS	Systém správy doménových jmen, slouží k převodu jmenných záznamů na adresy informačních systémů a evidenci dalších podpůrných informací
EPS	Jednotka určující objem logů za sekundu v počtu událostí
GB/d	Jednotka určující objem logů za den v Giga Byte
GDPR	Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
HA	Režim vysoké dostupnosti (High Availability), např. prostřednictvím redundance
HTTP	HTTP (Hypertext Transfer Protocol) je internetový protokol určený pro komunikaci s WWW servery
IOC	Indikátor kompromitace (Indicator of Compromise, IOC) je ve forenzním světě důkaz, který v kybernetickém prostředí naznačuje, že došlo k narušení kybernetické bezpečnosti
IS/ICT	Informační systémy a informační a komunikační technologie.
JSON	JavaScript Object Notation je způsob zápisu dat nezávislý na počítačové platformě, určený pro přenos dat, která mohou být organizována v polích nebo agregována v objektech
LM	Log management
MD	Člověkoden, pracovní čas jedné osoby odpovídající jednomu pracovnímu dni, tedy typicky 8 hodin (man-day)
On-premise	On-premise software je takový software, který lze instalovat a provozovat v prostorách organizace, která jej využívá
OS	Operační Systém
OT	Operational technology (OT) je hardware a software, který zjišťuje nebo způsobuje změny prostřednictvím přímého monitorování a/nebo řízení průmyslových zařízení, prostředků, procesů a událostí.
RAT	Remote Access Tool – druh škodlivého kódu, který umožňuje vzdálené ovládání napadeného systému
SATA	Počítačová sběrnice, která využívá datové rozhraní pro připojení velkokapacitních paměťových zařízení (např. pevných disků)

SIEM	Security Information and Event Management je systém pro správu bezpečnostních informací a událostí.
SLA	Dohoda o úrovni poskytovaných služeb (Service Level Agreement)
SOC	Kybernetické bezpečnostní dohledové centrum.
SSD	Solid-State Drive
SW	Software
SŽ	Správa železnic, státní organizace
SŽT	Správy železniční telematiky
Účastník	Subjekt, který se v rámci tohoto zadávacího řízení uchází o realizaci veřejné zakázky
URL	Uniform Resource Locator (URL), označovaný jako webová adresa, je odkaz na webový zdroj, který určuje jeho umístění v počítačové síti a mechanismus jeho vyhledávání
USB	Univerzální sériové rozhraní informačního systému
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
WAN	Wide Area Network je v informatice počítačová síť, která pokrývá rozlehlé geografické území
XML	Extensible Markup Language je obecný značkovací jazyk, který byl vyvinut a standardizován konsorciem W3C
ZoKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů

2 Úvod

Tento dokument je přílohou a nedílnou součástí zadávacího řízení pro výběr dodavatele veřejné zakázky „Log management a SIEM" (dále jen „veřejná zakázka"), pro organizaci Správa železnic, státní organizace (dále jen „SŽ"). Dokument popisuje technické a jiné požadavky na veřejnou zakázku.

2.1 Záměr SŽ v oblasti systému Log management a SIEM

Jedním z požadavků vyplývajících z § 22 VoKB (*Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů*) je požadavek na sběr informací o provozních a bezpečnostních činnostech a jejich ochranu před neoprávněným přístupem nebo změnou. V současné době jsou informace o provozních a bezpečnostních událostech (logy) zaznamenávány převážně jen na lokální úrovni, kde není vždy možné zaručit jejich integritu a bezpečí.

Cílem aktivity je zavést kompletní řešení pro centrální sběr a uchovávání informací o provozních a bezpečnostních událostech (logů), zaručujícím jejich integritu i všechny další požadavky kladené výše uvedenou VoKB. Toho by mělo být dosaženo nasazením centrálního log management řešení a zapojením potřebných zdrojů logů ze systémů a sítě SŽ do tohoto řešení.

Aktivita definuje implementaci systému správy logů a SIEM jako jeden z kroků zaměřujících se na zlepšení celkového stavu zabezpečení organizace (SŽ). Jedním z hlavních očekávání je zlepšit detekci hrozeb a čas potřebný k reakci tím, že se umožní monitorování a analýza logů z různých systémů v téměř reálném čase. To povede nejen ke zlepšení detekce hrozeb, ale také k rychlejší reakci v případě bezpečnostního incidentu.

Klíčovým cílem je také zajištění souladu s příslušnými bezpečnostními standardy, které se v organizaci (SŽ) uplatňují. Zavedením systému pro správu logů a SIEM chce organizace (SŽ) sledovat a vykazovat bezpečnostní události, a tím zajistit soulad s takovými normami.

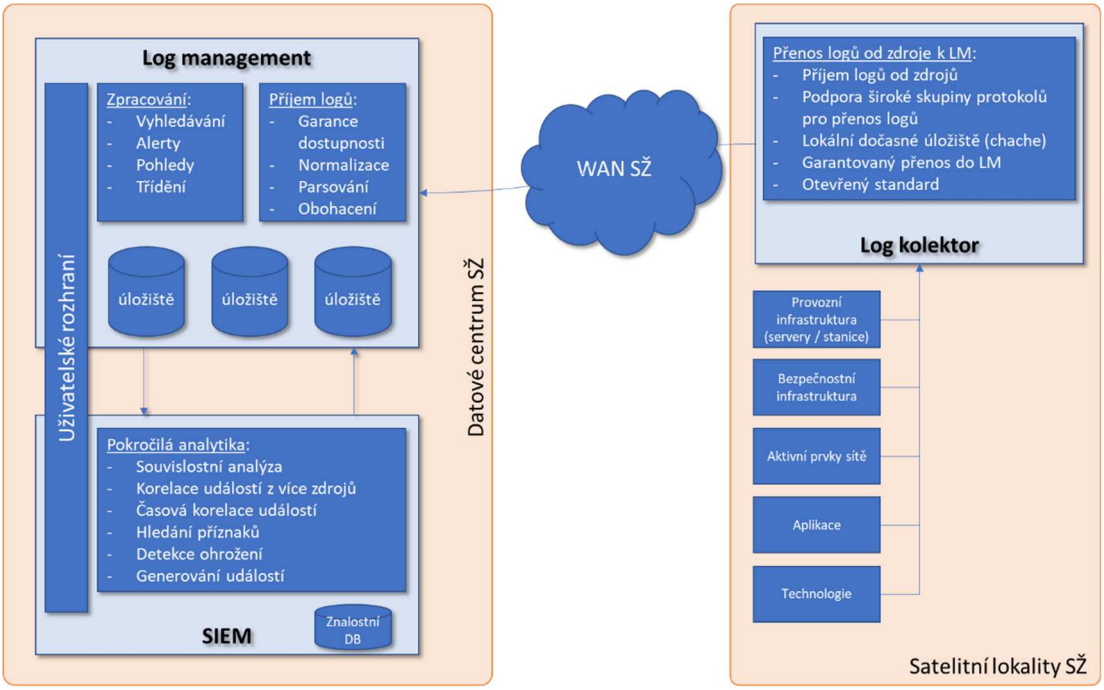
Zavedení systému správy logů a SIEM také zefektivní vyšetřování incidentů. Centralizované úložiště logů, které požadované řešení poskytne, umožní bezpečnostním týmům rychle a efektivně vyšetřovat zachycené bezpečnostní i provozní incidenty.

Dalším cílem implementace systému správy logů a SIEM je snížení provozních nákladů a požadavků na součinnosti. Automatizovaný sběr a analýza logů sníží manuální úsilí potřebné k vyšetřování a hlášení bezpečnostních incidentů, čímž se sníží provozní náklady. Kombinace těchto cílů umožní organizaci (SŽ) posílit její bezpečnostní pozici, zvýšit efektivitu a snížit náklady, čímž se systém správy logů a SIEM stane důležitou součástí komplexní strategie kybernetické bezpečnosti.

2.2 Předmět plnění veřejné zakázky

Předmětem aktivity je řešení Log management a SIEM, které bude zajišťovat jednotný sběr provozních a bezpečnostních událostí z prostředí SŽ, uchovávat je pro potřeby analýzy a archivovat je v souladu s legislativními požadavky (zejména s požadavky dle § 22 VoKB). Součást SIEM, která je bezpečnostní nadstavbou nad systémem Log management, bude zajišťovat detekci provozních a bezpečnostních událostí, které je možné odvodit od struktury, posloupnosti a významu zaznamenaných logů, nebo na základě předem definovaných symptomatických pravidel.

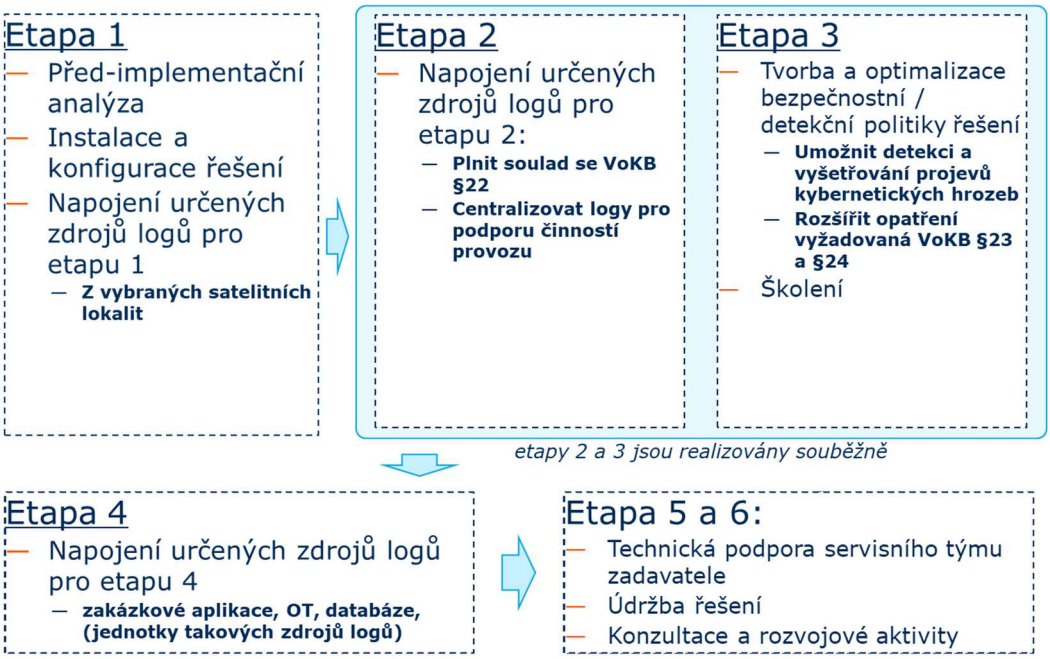
Řešení je požadováno realizovat v režimu „centralizovaném", tedy všechny logy budou přenášeny infrastrukturou SŽ na jedno centrální místo. Přenos bude realizován soustavou log kolektorů, které budou zajišťovat sběr logů od zdrojů logů a dle definovaných pravidel je předají do centrálního úložiště. Přenos logů musí být realizován spolehlivým způsobem, tedy bez ztrát logů, jejich nechtěné modifikace nebo vyzrazení.



Jednotlivé komponenty řešení budou muset umožňovat a dle požadovaných parametrů také poskytovat vysokou dostupnost. Očekáváním od vysoké dostupnosti je, že nebudou narušeny nezbytné funkcionality řešení a tím omezena možnost užívání řešení nebo porušeny zákonné a regulatorní povinnosti.

2.3 Etapy a výstupy aktivity

Aktivita Log management a SIEM bude rozdělena do jednotlivých etap, které zajistí postupnou realizovatelnost, specifikaci dílčích milníků a finanční plnění vůči dodavateli. Všechny etapy budou součástí jediné veřejné zakázky a budou jen dílčím rozdělením činností.



2.3.1 Etapa 1

V první části bude zajištěna realizace řešení pro přenos, uložení a interpretaci logů z provozní a bezpečnostní infrastruktury SŽ. Dále bude provedena instalace komponenty SIEM a všech vyžadovaných prvků vysoké dostupnosti. Pro potvrzení funkcionality první etapy, bude požadováno napojení vzorových zdrojů logů, které budou vybrány jako reprezentativní z vybraných satelitních lokalit (Brno, Plzeň) i centrální lokality (Praha U2 / CDP Praha). Zdroje logů pro tuto etapu jsou specifikovány v příloze č. 21 zadávací dokumentace „Zdroje logů - 2023-05" a označeny ve sloupci „Priorita napojení" příslušnou etapou, během níž bude vyžadováno jejich napojení.

Aktivita	Popis aktivity
Před-implementační analýza	*Popisuje způsob a podmínky nasazení technologie Log management a SIEM do prostředí SŽ.*
Instalace a konfigurace řešení	*Budou dodány všechny nezbytné softwarové komponenty řešení, potřebný hardware a licence výrobců software.* *Funkční řešení pro sběr, ukládání, vyhodnocování logů. Funkční systém pro řešení garantovaného přenosu logů infrastrukturou SŽ. Funkční rozhraní pro práci s nástrojem, vyhledávání logů a jejich interpretaci.*
Napojení určených zdrojů logů pro etapu 1	*Napojení logů z vybraných satelitních lokalit pro ověření funkční přenosové trasy od zdroje logu k systému Log management.* *Napojení logů z vybraných zdrojů k ověření výkonnostních parametrů a schopnosti řešení užívat a ovládat.*

2.3.2 Etapa 2

Tato etapa bude zaměřena na napojování všech zdrojů logů, které budou uvedeny jako zdroje logů podmiňující akceptaci díla. Tyto logy dodavatel napojí na připravené kolektory logů, zajistí jejich transport do centrálních komponent řešení Log management, připraví a nasadí všechny parsovací a normalizační politiky, aby logy byly uloženy v požadovaném formátu umožňujícím jejich další využití. Zdroje logů pro tuto etapu jsou specifikovány v příloze č. 21 zadávací dokumentace „Zdroje logů - 2023-05" a označeny ve sloupci „Priorita napojení" příslušnou etapou, během níž bude vyžadováno jejich napojení.

Aktivita	Popis aktivity
Napojení určených zdrojů logů pro etapu 2	*Dodavatel, se součinností SŽ, zajistí napojení všech určených zdrojů logů, čímž prokáže schopnost nástroje zpracovat všechny druhy logů, které SŽ pro tuto etapu specifikovala.*

2.3.3 Etapa 3

V této etapě bude vytvořena konfigurace pro vyhodnocování logů v komponentě SIEM, pravidla pro detekce symptomů v lozích a korelační pravidla. Výstupní generované události budou předávány na určené odběratele, kteří budou specifikováni v rámci přípravy před-implementační analýzy. Tato etapa bude realizována souběžně s etapou 2 a nebude se vyčkávat na dokončení napojení všech zdrojů logů definovaných pro celé dílo.

Aktivita	Popis aktivity
Tvorba a optimalizace bezpečnostní / detekční politiky řešení	*Dodané komponentě SIEM bude definován způsob nakládání s logy – tento způsob bude dodavatelem nastaven a bude ověřena jeho funkčnost.* *Nad logy, které jsou již zasílány do systému Log managementu, bude dodavatelem vytvořena sada detekčních a korelačních pravidel, kterými budou naplněny požadavky na USE-CASES SŽ, které jsou uvedeny na listu „USE-CASES" v příloze č. 21 zadávací dokumentace.* *Nad nastavenými detekcemi budou vytvořena pravidla pro integraci se systémy SŽ, jako např. JIRA, MS Teams. Důležité je, aby byla naplněna potřeba SŽ o předávání detekovaných událostí jejich zamýšleným odběratelům, tedy útvarům SOC a provoz SŽT.*
Školení pracovníků SŽ	*Pracovní týmy SŽ budou vyškoleny v:* - *administraci řešení* - *technické podpoře řešení* - *napojování zdrojů logů* - *práci s logy (hledání, třídění, interpretaci)* - *práci v nástroji SIEM* - *tvorbě detekčních a korelačních politik.*

2.3.4 Etapa 4

Etapa bude obsahovat připojování specifických vzorových zdrojů logů (jednotky množství zdrojů) u nichž je očekávána potřeba specifické úpravy nastavení komponent řešení. Mezi taková specifika patří zejména vybraná aktiva z technologických částí sítí, specifické aplikační zdroje logů a podobné. Zdroje logů pro tuto etapu jsou specifikovány v příloze č. 21 zadávací dokumentace „Zdroje logů - 2023-05" a označeny ve sloupci „Priorita napojení" příslušnou etapou, během níž bude vyžadováno jejich napojení.

Aktivita	Popis aktivity
Napojení určených zdrojů logů pro etapu 4	*SŽ vybere specifické zdroje logů, které dodavatel v této etapě připojí. Bude se jednat o napojení logů zakázkových aplikací, vybraných zařízení z prostředí OT a databázových systémů.* *Bude se jednat o jednotky takových systémů, jejichž napojením dodavatel prokáže flexibilitu řešení a možnosti, jak řešit napojení nestandardních zdrojů logů.* *SŽ bude schopno další zdroje logů napojovat ve vlastní režii, jen s možností čerpání technické podpory dodavatele řešení.*

2.3.5 Etapa 5

Aktivita	Popis aktivity
Technická podpora servisního týmu SŽ	*Technická podpora dodaného řešení a provoz Help Desku dodavatele.*
Údržba řešení	*Zajištění pravidelné údržby všech komponent dodaného řešení, a to včetně bezpečnostní údržby.*

2.3.6 Etapa 6

Aktivita	Popis aktivity
Konzultace a rozvojové aktivity	*Rozvojové aktivity, které budou souviset především ve změnami v prostředí SŽ, které mohou mít dopad na provoz řešení Log management a SIEM.*

2.4 Parametry poptávaného řešení

Všechny komponenty řešení požaduje SŽ provozovat v režimu on-premise (tedy výhradně na zařízení v infrastruktuře SŽ). Přípustná integrace s online / CLOUD službami je pouze pro aktualizační služby a získávání informací o hrozbách. Není přípustné předávat data z prostředí SŽ ke zpracování k výrobci nabízeného řešení, pokud tuto aktivitu manuálně (a pouze pro konkrétní vyšetřování) neiniciuje pracovník SŽ.

Řešení Log management a SIEM je poptáváno jako ucelené softwarové řešení, které obsahuje veškeré potřebné licence k naplnění poptávaných parametrů řešení, včetně technické podpory (maintenance nebo subscripce) výrobce nabízených komponent řešení a technické podpory dodavatele řešení, a to na dobu 5 let.

Technická podpora dodavatele bude řízena dle parametrů uvedených ve Zvláštních obchodních podmínkách pro zakázky v oblasti ICT Zadavatele (Příloha č. 7 Závazného vzoru smlouvy, který je Přílohou č. 6 zadávací dokumentace), konkrétně ustanovením kapitoly „12. SERVISNÍ MODELY". SŽ požaduje plnění v parametrech servisního modelu „B1 Závažný".

SŽ požaduje provoz Help Desku dodavatele, který bude provozován v režimu odpovídajícím specifikaci uvedené ve Zvláštních obchodních podmínkách pro zakázky v oblasti ICT Zadavatele (Příloha č. 7 Závazného vzoru smlouvy, který je Přílohou č. 6 zadávací dokumentace), konkrétně ustanovením kapitoly „10. HELPDESK". SŽ požaduje plnění Help Desku v režimu „Režim 1" a úrovni „L3".

Parametr	Jednotka	Hodnota
Celkem událostí za vteřinu	EPS	40000
Celkový denní objem logů	GB/d	1000
Počet lokalit pro umístění log kolektorů	počet	16
Celkový počet lokalit pro umístění centrálních komponent: - Jedná se o dvě pracoviště v rámci Prahy - Lokality jsou propojeny silným datovým propojem - SŽ chce využít lokalit pro geo-redundanci centrálních komponent řešení	počet	2

Minimální doba, po kterou budou logy v systému Log management uloženy	měsíců	18

2.4.1 Testovací prostředí

SŽ požaduje dodání řešení včetně testovacího prostředí, které bude obsahovat všechny komponenty řešení, licencované na nejmenší dostupné objemy, popřípadě opatřené přímo licencí pro testovací účely. Testovací prostředí musí disponovat prvky režimu vysoké dostupnosti, z důvodu možnosti jejich testování, bude však provozováno pouze v centrálním datovém centru. Testovací prostředí bude sloužit zejména k ověřování nových konfigurací, testování procesů aktualizace SW, řešení chybových stavů apod.

Pro napojení na testovací prostředí jsou vybrány jednotky zdrojů logů, které jsou specifikovány v příloze č. 21 zadávací dokumentace „Zdroje logů - 2023-05" vyplněním údaje „ANO" ve sloupci „Testovací prostředí".

2.4.2 Infrastruktura pro přenos logů

SŽ požaduje, aby přenos logů od jednotlivých zdrojů logů do centrálních komponent řešení Log management a SIEM, bylo řiditelné, zajištěno bezpečným způsobem a řešení bylo otevřené případnému napojování jiných centrálních komponent řešení.

2.4.2.1 Podpora zdrojů logů

Přenosovou infrastrukturu požaduje SŽ realizovat takovým nástrojem, který umožní integraci se zdroji logů, které jsou uvedeny v příloze č. 21 zadávací dokumentace „Zdroje logů – 2023-05", a to formou:

1. Pasivního příjmu logů, kdy log odesílá zdroj logu a využívá komunikačních protokolů:
    a. SYSLOG (TCP/UDP)
    b. HTTP/HTTPS
    c. SNMP Trap
    d. TCP
    e. UDP
    f. WEF (Windows Event Forwarder)
2. Aktivního vyčítání logů ze zdrojového systému:
    a. Office 365 Services
    b. Office 365 Activity
    c. Office 365 Message Trace
    d. Kafka
    e. Azure Event Hubs
    f. Azure Blob Storage
    g. Soubor na lokální / vzdáleném souborovém systému
    h. Databázový systém (SQL)

Zdroje logů z prostředí Microsoft systémů, které umožní předávání prostřednictvím Windows Event Forwarder, budou tento způsob využívat. Prostředí Windows Event Forwarder bude ve správě SŽ.

2.4.2.2 Dostupné parametry nastavení řešení

Řešení pro přenos logů musí umožnit nastavení filtračních pravidel, kterými bude možné již před přenosem logů do centrálních komponent řešení, nastavit filtrační pravidla pro redukci objemů přenášených logů (např. odfiltrování logů nepodstatných pro kybernetickou bezpečnost) dle jejich typu, kategorie nebo klíčových slov.

Dalším požadavkem na konfiguraci řešení je možnost upravovat parametry dočasné paměti (cache / buffer), kterou bude možné využívat k uložení logů od zdrojových systémů v případě nedostupnosti cílových centrálních komponent řešení. Požadavek na kapacitu této dočasné paměti je 5 dnů, pokud nebude v před-implemenatační analýze rozhodnuto o snížení této hodnoty. Po obnovení dostupnosti centrálních komponent řešení budou uložené logy odeslány spolehlivým a bezpečným způsobem, tedy tak, že přenos bude šifrovaný a uložení logů do centrálních komponent řešení bude potvrzováno (k vyprázdnění dočasné paměti dojde až po potvrzení uložení na centrálním úložišti).

Přenášené logy budou komprimovány, aby byl optimalizován dopad na přenosovou infrastrukturu SŽ.

2.4.2.3 Bezpečnost řešení

SŽ vyžaduje, aby všechna spojení mezi satelitními kolektory a centrálními komponentami probíhalo zabezpečeně pomocí šifrování a ochrany integrity, přičemž kryptografické algoritmy budou zabezpečeny v souladu s aktuálními doporučeními NÚKIB dle článku 20.15. Zvláštních obchodních podmínek pro zakázky v oblasti ICT (Příloha č. 7 Závazného vzoru smlouvy, který je Přílohou č. 6 zadávací dokumentace).

2.4.2.4 Otevřenost řešení

Dodané řešení pro přenos logů od zdrojů logů do centrálních komponent řešení musí podporovat otevřené komunikační standardy (alespoň SYSLOG, SNMP Trap, Kafka, TCP JSON, ELASTICSEARCH, souborový systém), kterými bude zajišťováno spojení s nástrojem Log management a SIEM. SŽ nepřipouští, aby tato spojení byla realizovatelná pouze proprietárním komunikačním protokolem výrobce řešení Log management a SIEM.

2.4.3 Řešení vysoké dostupnosti

Vysoká dostupnost je vyžadována u centrálních komponent Log management a SIEM, přičemž SŽ požaduje, aby dodavatel navrhl takové řešení, které splní minimálně následující podmínky:

1. Management rozhraní pro práci s logy a pro analýzu událostí bude provozováno v režimu vysoké dostupnosti Active-Standby nebo Active-

Active a jednotlivé komponenty budou rozloženy mezi 2 datová centra SŽ, která jsou určena k provozu centrálních komponent řešení.

2. Úložiště logů a vygenerovaných událostí (alertů) bude provozováno v režimu vysoké dostupnosti Active-Standby nebo Active-Active, přičemž všechna data musejí vždy existovat alespoň ve dvou replikách, kdy každá z replik bude vždy jedna v každém ze 2 datových center SŽ, která jsou určena k provozu centrálních komponent řešení.

2.4.4 Zálohování

SŽ požaduje dodání řešení včetně návrhu způsobu zálohování jednotlivých komponent řešení, přičemž minimálně budou požadovány následující parametry:

1. Konfigurace všech komponent řešení budou zálohovány v pravidelném cyklu minimálně 1 x denně.
2. Aplikační prostředí všech komponent řešení budou zálohována v pravidelném cyklu minimálně 1 x denně.
3. Bezpečnostní události (aletry a auditní logy Log management a SIEM), které vygenerují nástroje Log management a SIEM, budou zálohovány v pravidelném cyklu minimálně 1 x denně.
4. Data logů, která budou v nástroji Log management uloženy, nebudou podléhat potřebě zálohování – SŽ počítá s dostatečnou odolností dat v rámci jejich rozložení do úložišť ve 2 datových centrech SŽ. Řešení musí umožnit export vybraných logů (vybraných dle zdroje a typu logu) k provedení jejich zálohy na externí zálohovací zařízení SŽ.

2.4.5 Architektura úložišť

Systém Log management musí podporovat rozklad diskové kapacity na různá úložiště s různou úrovní přístupnosti a rychlosti, která jsou známa jako úložiště HOT, WARM a COLD. Tento přístup, který se často nazývá víceúrovňová architektura úložiště (tiered storage architecture) a umožňuje efektivní správu a ukládání logů s ohledem na jejich důležitost a aktuálnost.

1. Úložiště HOT: Toto úložiště je určeno pro okamžité a intenzivní zápisy logů. Jedná se o nejrychlejší a nejdražší úložiště SSD (Solid-State Drive). Logy, které jsou často přístupné a které vyžadují rychlý přístup, budou ukládány na úložišti HOT.

2. Úložiště WARM: Úložiště WARM slouží pro ukládání logů, které již nejsou tak často přístupné jako na úložišti HOT, ale stále mají určitou důležitost a potřebují být uchovávány pro analýzu, výzkum nebo případnou kontrolu. Toto úložiště je provozováno na discích s nižší rychlostí přenosu dat, jako je SATA disk.

3. Úložiště COLD: Úložiště COLD je určeno pro ukládání starých a méně důležitých logů, které jsou přístupné jen zřídka. Tato data ukládáme na pomalejších a levnějších médiích, jako jsou pásková úložiště.

Při využití víceúrovňové architektury úložiště se Log management systémy často spoléhají na různé mechanismy, jako je automatizované přesouvání logů mezi

úložišti na základě jejich věku, důležitosti nebo jiných kritérií. To umožňuje optimalizaci využití diskové kapacity a uchování logů s ohledem na jejich hodnotu a přístupnost.

SŽ vyžaduje, aby nabízené řešení umožňovalo na aplikační úrovni rozlišování druhů úložišť pro:

1. HOT úložiště, která jsou specifická tím, že jejich stáří od doby uložení do Log management není delší než 3 měsíce
2. WARM úložiště budou všechna ostatní data až do požadovaného období pro uložení 18 měsíců.

Využití úložiště úrovně COLD bude sloužit pouze pro účely archivace / zálohování vybraných druhů logů (viz. kapitola „Zálohování" této Technické specifikace) a bude dostupné pouze v lokalitách SŽ určených pro provoz centrálních komponent řešení.

2.4.6 Provozní monitoring

SŽ provozuje nástroj provozního monitoringu ZABBIX a požaduje, aby součástí dodávky byl také soupis doporučených dohledovaných parametrů a hodnot nabízeného řešení pro zajištění monitoringu operačních systémů a aplikačního prostředí dodávaného řešení. Cílem je předcházet provozním incidentům na všech komponentách Log management a SIEM, včetně všech komponent dodaných pro přenos logů od zdroje logu až po centrální komponenty.

2.4.7 Zabezpečení

Dodávané řešení a všechny jeho komponenty budou splňovat bezpečnostní doporučení výrobce (tzv. hardening) a svou vlastní konfigurací umožní dodržení souladu s požadavky ZoKB, resp. VoKB a jejích kapitol:

- § 18 Bezpečnost komunikačních sítí [písmena c) a d)]
- § 19 Správa a ověřování identit [odstavce 3, 5 písm. a) a 6 písm. a)]
- § 20 Řízení přístupových oprávnění
- § 22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů [odstavce 2 písm. d) a 2 písm. e)]
- § 26 Kryptografické prostředky [písmena a), c) a d)].

2.4.8 Log management

Kybernetické bezpečnostní řešení Log management pro SŽ s centralizovanou architekturou by mělo splňovat následující požadavky:

1. Shromažďování logů: Řešení musí umožňovat shromažďování logovacích dat z různých zdrojů v organizaci (SŽ), včetně síťových prvků, serverů, aplikací a vybraných koncových zařízení.
2. Centralizace: Veškeré logy musí být sbírány a ukládány v centrálním datovém centru. Centralizovaná architektura umožňuje snadnou správu a

analýzu dat a zajišťuje jednotný pohled na logovací informace z celé organizace.

3. Škálovatelnost: Řešení musí být schopné zvládat velké množství logovacích dat v rozsáhlé organizaci. Musí být navrženo tak, aby bylo schopné efektivně zpracovávat a ukládat logy ze všech specifikovaných satelitních lokalit (kapitola „2.4.10 Lokality určené k provozu komponent Log management a SIEM" této Technické specifikace).
4. Bezpečnostní funkce: Log management řešení musí obsahovat bezpečnostní funkce, jako je šifrování dat při přenosu, ověřování identity uživatelů systému, kontrola a řízení přístupu. To zajistí ochranu logovacích dat proti neoprávněnému přístupu a manipulaci.
5. Real-time monitoring: Řešení musí poskytovat možnost sledování logovacích událostí v reálném čase. To umožní rychlou detekci a odpověď na bezpečnostní incidenty. Požadovaná vlastnost může být sdílenou součástí se SIEM vrstvou.
6. Vyhledávání a dotazování: Řešení musí poskytovat efektivní nástroje pro vyhledávání a dotazování logovaných dat. To umožní snadnou analýzu a vyhledávání specifických informací v rozsáhlých datových sadách.
7. Reporting a vizualizace: Řešení musí poskytovat možnosti tvorby reportů a vizualizace logovacích dat. To umožní vytváření přehledných reportů a grafů, které usnadní prezentaci a analýzu logovacích informací pro bezpečnostní tým, provoz a popř. i management.
8. Auditovatelnost: Řešení musí splňovat požadavky na auditovatelnost, což zahrnuje sledování a záznam veškerých aktivit týkajících se logování i analýzy dat a auditovatelnost aktivit privilegovaných uživatelů systému Log management. To je důležité pro dodržování regulací a standardů v oblasti kybernetické bezpečnosti.
9. Rozšiřitelnost: Log management řešení musí být navrženo tak, aby bylo snadno rozšiřitelné a přizpůsobitelné rostoucím potřebám organizace (SŽ). To zahrnuje možnost přidávat nové zdroje logů a rozšiřovat kapacitu systému bez výrazného poklesu výkonu.

Celkově řečeno, kybernetické bezpečnostní řešení Log managementu s centralizovanou architekturou by mělo SŽ umožňovat efektivní shromažďování, analýzu, sledování a ochranu logovacích dat z různých zdrojů v celé organizaci (SŽ). Splnění těchto požadavků pomůže organizaci (SŽ) zlepšit svou schopnost detekovat, reagovat a předcházet kybernetickým hrozbám a incidentům a vyhovět požadavkům vyplývajícím ze ZoKB a VoKB.

2.4.9 SIEM

Nedílnou součástí požadovaného řešení je také komponenta SIEM (Security Information and Event Management), která poskytne rozšířené funkcionality pro analýzu bezpečnostních událostí a monitorování hrozeb. Kybernetické

bezpečnostní řešení SIEM pro SŽ s centralizovanou architekturou by mělo splňovat následující požadavky:

1. Detekce a analýza hrozeb: SIEM řešení musí poskytovat pokročilou detekci a analýzu bezpečnostních hrozeb. To zahrnuje monitorování aktivit a událostí v reálném čase, vyhledávání anomálií, identifikaci známých indikátorů kompromitace (IOC) a podporu pro vyhledávání souvislostí mezi různými událostmi.

2. Korelace událostí: Funkce pro korelaci událostí je klíčovou součástí SIEM řešení. Tímto způsobem lze identifikovat spojitosti a vzorce mezi různými událostmi a aktivitami v prostředí. To umožňuje identifikovat sofistikované hrozby a předcházet jim dříve, než způsobí větší škody.

3. Pravidla a upozornění: SIEM musí umožňovat vytváření pravidel a upozornění pro rychlou identifikaci a reakci na bezpečnostní události. Administrátoři by měli mít možnost definovat specifická pravidla a podmínky, na jejichž základě systém vygeneruje upozornění na potenciální bezpečnostní incidenty.

4. Integrace s Log managementem: SIEM musí být plně integrované s nabízeným Log management řešením. Tím se zajišťuje, že logy z různých zdrojů jsou k dispozici pro analýzu a monitorování bezpečnostních událostí a zároveň poskytuje holistický pohled na bezpečnostní situaci organizace (SŽ). Toto však neznamená, že všechny logy uložené v prostředí Log management budou zpracovávány komponentou SIEM. SŽ požaduje, aby bylo možné licenčně rozlišit data ukládaná jen v Log management a data, která budou určena ke zpracování v komponentě SIEM.

5. Vizualizace a reporting: SIEM řešení by mělo poskytovat možnosti vizualizace dat a tvorby reportů. To umožňuje uživatelům snadno sledovat a analyzovat bezpečnostní události prostřednictvím interaktivních grafů, tabulek a dashboardů. Reporty pak umožňují prezentaci důležitých informací managementu a auditům.

6. Sledování souladu: SIEM by měl poskytovat funkcionalitu pro sledování souladu s příslušnými bezpečnostními předpisy, normami a regulacemi, jako je například GDPR, ZoKB. Tím se organizaci (SŽ) umožní dodržování požadovaných standardů a předpokladů v oblasti ochrany dat a informací.

7. Rozšiřitelnost a výkon: SIEM by měl být navržen s ohledem na vysokou škálovatelnost a výkon. To umožní efektivní zpracování velkých objemů dat a událostí, které vznikají v rozsáhlých a dynamických prostředích SŽ.

SIEM řešení s centralizovaným Log managementem by mělo poskytovat pokročilé funkce pro detekci, analýzu a monitorování bezpečnostních událostí. Integrace s existujícími nástroji, vizualizace dat, správa incidentů a podpora souladu s regulacemi jsou další klíčové aspekty, které budou zohledněny při výběru SIEM řešení.

2.4.10 Lokality určené k provozu komponent Log management a SIEM

Typ lokality	Adresa lokality	Účel
CDP	V Trianglu 2474, Praha 9	Centrální komponenty LM / SIEM
Datové centrum	Pod Táborem 369/8a, Praha 9	Centrální komponenty LM / SIEM
Datové centrum	Kulkova 1, Brno (Maloměřice)	Satelitní log kolektor
Datové centrum	Škroupova 1017/11, Plzeň	Satelitní log kolektor
Datové centrum /CDP	Tovární 3286, Přerov	Satelitní log kolektor
Oblastní ředitelství	ATU, Ostrava	Satelitní log kolektor
Oblastní ředitelství	Kounicova 26, Brno	Satelitní log kolektor
Oblastní ředitelství	Pávovská 2, Jihlava	Satelitní log kolektor
Oblastní ředitelství	Křižíkova 552, Praha 1	Satelitní log kolektor
Oblastní ředitelství	Pernerova 2819/2a, Praha 2	Satelitní log kolektor
Oblastní ředitelství	Riegrovo náměstí 1660, Hradec Králové	Satelitní log kolektor
Oblastní ředitelství	ATU, Pardubice	Satelitní log kolektor
Oblastní ředitelství	Sušická 1168/23, Plzeň	Satelitní log kolektor
Oblastní ředitelství	A. Trägera 2899/90, České Budějovice	Satelitní log kolektor
Oblastní ředitelství	Železničářská 1386/31, Ústí nad Labem	Satelitní log kolektor
Organizační jednotka	Kounicova 26, Brno	Satelitní log kolektor
Organizační jednotka	Nerudova 773/1, Olomouc	Satelitní log kolektor
Technologická / sdělovací místnost	Wilsonova 300/8, Praha 2	Satelitní log kolektor
Technologická / sdělovací místnost	Havlíčkova 1011, Praha 1	Satelitní log kolektor

2.4.11 Požadavky na technické funkcionality řešení

Všechny parametry požadované v tomto dokumentu a přílohách zadávací dokumentace jsou pro dodavatele závazné a SŽ vyžaduje jejich naplnění.

Požadavky na vybrané funkcionality poptávaného řešení, které SŽ vyžaduje splnit technickými prostředky, a u nichž Účastník musí popsat způsob, kterým jím nabízené řešení naplní požadavek, jsou specifikovány v přiloženém dotazníku „Log management a SIEM dotazník“, který je Přílohou č. 20 zadávací dokumentace;

v tomto dotazníku Účastník potvrdí připravenost nabízeného řešení splnit vybrané požadavky a vyplní způsob, kterým je každý požadavek naplněn. Účastník do přiloženého dotazníku doplní také soupis všech licencí nabízeného řešení, kterým zajistí naplnění požadovaných funkcionalit.

SŽ upozorňuje, že nesplnění kteréhokoliv požadavku na technické funkcionality řešení uvedeného v přiloženém dotazníku, povede k vyloučení Účastníka ze zadávacího řízení. V případě, že bude nesplnění takového požadavku odhaleno až v průběhu realizace plnění, bude to považováno za hrubé porušení povinností dle přílohy č. 6 zadávací dokumentace – Závazného vzoru smlouvy a bude důvodem pro odstoupení od této smlouvy.

2.4.12 Požadavky na specifikaci virtualizačních prostředků Zadavatele

V souvislosti se schválenou strategií IS/ICT SŽ, konkrétně cílem zajištění dlouhodobého koncepčního a efektivního rozvoje IS/ICT, požaduje SŽ využití možností jeho hardwarové a virtualizační platformy pro jednotlivé komponenty poptávaného řešení. Popis platformy je uveden v příloze č. 4 zadávací dokumentace, která je označena jako „Platforma SŽ 2.0".

Pro veškeré prostředky, ve všech lokalitách určených k provozu řešení Log management a SIEM, které je možné provozovat v platformě SŽ, vyplní Účastník specifikaci technických požadavků na platformu SŽ, a to do připraveného listu „Požadavky" v Příloze č. 19 zadávací dokumentace, která je označena jako „Požadavky na služby Platformy SŽ pro Log Management a SIEM".

Jedná se zejména o následující parametry:

- Požadovaný počet kusů daného řešení
- Požadovaný počet Core
- Požadovaná velikost RAM
- Požadovaná velikost diskového prostoru na úložišti typu COLD storage
- Požadovaná velikost diskového uložiště v úložišti typu HOT/WARM storage
- Požadovaná velikost diskového uložiště pro zálohování (BACKUP).

Náklady na rozšíření virtualizační platformy SŽ do požadovaných parametrů, nebude Účastník uvádět jako součást nabídkové ceny, tedy do svých nákladů. SŽ bude hodnotit nároky nabízeného řešení na virtualizační platformu pomocí bodovacího systému, na základě celkového požadovaného výpočetního výkonu uvedeného v listu „Požadavky", který je součástí Přílohy č. 19 zadávací dokumentace.

SŽ limituje celkové požadavky na výpočetní výkon a kapacitu, který je připraven pro účely projektu nabídnout, takto:

Parametr výkonu a kapacity	Maximální povolená hodnota

Počet v CPU	1046
Kapacita RAM (GB)	4877
Kapacita disků (GB)	1860000

2.4.13 Dodávka hardwarových a softwarových prostředků

Výjimkou, kdy není nutné využití platformy SŽ, jsou samozřejmě komponenty řešení, které virtualizaci neumožňují. V takovém případě uvede dodavatel veškeré náklady na hardware, který je součástí dodávaného řešení a nebude provozován v platformě SŽ, do své cenové kalkulace a učiní jej součástí své dodávky.

Pokud bude součástí nabízeného řešení také dodávka technických a programových prostředků, bude Účastník respektovat, že:

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 provedla SŽ analýzu rizik související s předmětnou veřejnou zakázkou na dodávky, jak je jeho povinností podle § 5 a § 8 VOKB. V návaznosti na to SŽ identifikovala rizika spojená s výše uvedenými technickými a programovými prostředky jako neakceptovatelná, a současně opatření k jejich zvládání, kterým je nepřipuštění použití těchto prostředků v rámci plnění veřejné zakázky.

SŽ 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.

2.5 Oblasti, které nejsou předmětem plnění veřejné zakázky

- Instalace a správa virtualizační platformy, která zajišťuje prostor pro provoz komponent řešení Log management a SIEM.

- Instalace a správa operačních systémů, které jsou součástí nabízených instancí virtualizační platformy SŽ, pokud dodavatel nebude vyžadovat instalaci specifického OS, nebo provádění zásahů do standardní instalace.
- Provozní monitoring HW a virtualizačního prostředí SŽ, které zajišťuje provoz jednotlivých komponent řešení Log management a SIEM.
- Úprava a konfigurace zdrojů logů pro účely jejich integrace na komponenty řešení Log management a SIEM.
- Provoz archivačního systému pro dlouhodobé uložení logů mimo prostředí řešení Log management a SIEM.

3 Současný stav a popis prostředí

Současný stav ICT prostředí SŽ je popsán v přiložených dokumentech:

- Analýza prostředí – architektura prostředí SŽ (Příloha č. 2 zadávací dokumentace)
- Analýza prostředí – popis prostředí sítě UAS (Příloha č. 3 zadávací dokumentace)
- Platforma 2.0 - souhrn podporovaných infrastrukturních služeb, technologií, a architektonických principů, která definuje základní rámec pro návrh řešení ICT (Příloha č. 4 zadávací dokumentace)

4 Požadavky na plnění

SŽ očekává dodávku komplexního řešení, která se bude sestávat z jednorázových projektových činností, dodávky nástroje se souvisejícími technickými komponenty a průběžných služeb dodavatele řešení.

4.1 Jednorázové projektové činnosti

Jednorázové projektové činnosti jsou nedílnou součástí dodávaného řešení, jsou zahrnuty mezi akceptační milníky a je k nim vázána etapizace dodávky a fakturace.

4.1.1 Před-implementační analýza

	Před-implementační analýza
Popis	Před-implementační analýza popisuje způsob a podmínky nasazení technologie Log management a SIEM do prostředí SŽ. Dokument musí popisovat charakteristiku dodávaného technického řešení, popis jednotlivých jeho komponent, navrhovaný způsob zapojení do prostředí SŽ a samozřejmě způsob integrace zdrojů logů. Dokument musí mít charakter detailní technické specifikace pro všechny uvažované implementační postupy, na jejichž předběžném schválení závisí umožnění provádět technické zásahy do prostředí SŽ.

Výstupy	Výstupem tohoto kroku bude dokument obsahující alespoň:
	• Popis dodávaného technického řešení a jeho komponent
	• Návrh architektury dodávaného řešení v prostředí SŽ
	• Detailní popis implementačních kroků
	• Detailní technická specifikace
	  ○ Umístění technologií
	  ○ Napájení
	  ○ Síťové segmenty pro správu technologie
	  ○ IP adresace
	  ○ HW požadavky na virtualizační platformu SŽ
	  ○ Požadavky na síťové prostupy
	  ○ Požadavky na přístup do internetu
	  ○ Požadavky na vzdálený přístup pro správu technologie
	  ○ Požadavky na systémový monitoring
	  ○ Postup napojení zdrojů logů do Log management / SIEM
	• Revizi USE-CASES, které jsou uvedeny v listu „USE-CASES" v příloze č. 21 zadávací dokumentace, zadaných v rámci TS a doporučení dalších USE-CASES dodavatelem
	• Požadované součinnosti na SŽ
	• Návrh akceptačních testů
	• Katalog projektových rizik a návrh způsobu jejich ošetření
	• Specifikace kroků, součinností dodavatele a jejich rozsah v MD, při ukončení projektu (exit plán), které budou součástí poskytované služby

	• Detailní harmonogram implementace řešení

4.1.2 Instalace a konfigurace řešení

	Instalace a konfigurace řešení
Popis	V této části projektu dojde k dodání, instalaci a konfiguraci všech komponent technického řešení Log management a SIEM, které naplní požadavky předmětu veřejné zakázky a naplní specifika projektu uvedená v dokumentu před-implementační analýza.
Výstupy	Výstupem tohoto kroku bude funkční technické řešení Log management a SIEM, které bude: • Obsahovat všechny potřebné licence, předplatné a technické podpory výrobce. • Dodáno s nezbytným hardwarem pro komponenty, které není vhodné provozovat ve virtuálním prostředí SŽ. • Nasazeno na všech požadovaných lokalitách pro etapu 1 včetně komponent pro přenos logů od zdroje do centrálních úložišť. • V souladu se schválenou architekturou. • Zcela funkční pro výkon funkce Log management a SIEM, tak jak SŽ požaduje v této Technické specifikaci. • Napojeno na systémový monitoring SŽ (systém Zabbix). • Schopno vyhovět definovaným akceptačním testům v rozsahu specifikovaným v před-implementační analýze a schváleným SŽ.

4.1.3 Napojení určených zdrojů logů

	Napojení určených zdrojů logů
Popis	V této části projektu dojde k napojení určených zdrojů logů, které SŽ určila k napojení do prostředí Log management a SIEM pro odpovídající etapu projektu. Zdroje logů jsou zvlášť specifikovány pro etapu 1, etapu 2 a etapu 4 v příloze č. 21 zadávací dokumentace „Zdroje logů - 2023-05" uvedením odpovídající etapy ve sloupci „Priorita napojení".

Výstupy	Výstupem tohoto kroku bude funkční napojení zdroj logů na Log management a SIEM a bude obsahovat:
	• Nasazení komponent infrastruktury pro přenos logů ze satelitních lokalit do centrálních úložišť řešení (nad rámec komponent instalovaných v etapě 1).
	• Provedení technické integrace se zdrojem logu
	  ○ Výběr komunikačního protokolu
	  ○ Výběr typů logových zpráv.
	• Nastavení přenosové platformy pro zajištění garantovaného odeslání logů od zdrojového systému k centrálním prvkům řešení Log management a SIEM.

	• Ověření přenosu logů od zdroje do centrálního úložiště. • Nastavení zpracování logů od zdrojů pro podporu další datové analýzy (parsing). • Nastavení normalizace logů, pokud je to vyžadováno řešením pro naplnění požadavků uvedených v technické specifikaci a požadavcích na detekční USE-CASES, které jsou uvedeny v listu „USE-CASES" v příloze č. 21 zadávací dokumentace. • Nastavení retenční politiky pro logy.

4.1.4 Tvorba a optimalizace bezpečnostní / detekční politiky řešení

	Tvorba a optimalizace bezpečnostní / detekční politiky řešení
Popis	V této části projektu bude dodavatelem provedeno vyhodnocení účinnosti nasazeného řešení Log management a SIEM, bude upravena bezpečnostní / detekční pravidla a zdokumentovány všechny provedené konfigurační úpravy, které vedou k vyšší efektivitě detekce kybernetických bezpečnostních událostí pro analytický tým SOC SŽ.
Výstupy	Výstupem tohoto kroku bude funkční technické řešení Log management a SIEM, které bude mít upravenu bezpečnostní / detekční politiku tak, že bude minimalizován objem falešných detekcí, které by musel analytický tým SOC zpracovávat. SŽ požaduje provedení alespoň následujících činností: • Zohlednění reálných dostupných IP adresací SŽ v detekčních politikách. • Upřesnění konkrétních druhů validních aktiv SŽ zaznamenaných v komunikacích, které jsou důležité pro fungování detekčních pravidel (DNS, SMTP, WEB, NTP, PROXY, MS AD). • Vytvoření specifických detekčních politik (tzv. detekčních use-cases), dle specifikace SŽ, které jsou specifikovány v příloze č. 21 zadávací dokumentace „Zdroje logů - 2023-05." v listu „USE-CASES". • Aplikace výjimek, které doporučí SŽ. • Předávání detekovaných událostí jejich odběratelům, kterými budou pracoviště SOC, nebo provozní tým SŽT. Všechny upravené konfigurace budou zdokumentovány a předány jako výstup této části projektu.

4.1.5 Školení

	Školení
Popis	V této části projektu bude dodavatelem provedeno zaškolení technického servisního týmu SŽ a týmu Security Operations Center SŽ. Cílem je přenesení znalostí o správě dodaných nástrojů a předání rutinní správy na tým SŽ. Druhé specifické školení by se mělo hlouběji zaměřit na školení práce s řešením Log management a SIEM, jehož odběratelem bude pracoviště SOC SŽ.

Výstupy	Výstupem tohoto kroku bude realizované školení se zaměřením na využívání a správu technického řešení Log management a SIEM:
	• Prezenční školení servisního týmu SŽ. SŽ nominuje 8 pracovníků a bude požadovat naplnění časové dotace alespoň 3 MD.
	  ○ komponenty systému
	  ○ konfigurační parametry komponent
	  ○ ladění výkonnostních a kapacitních parametrů řešení
	  ○ troubleshooting
	  ○ update a upgrade.
	• Prezenční školení týmu SOC SŽ v prostorách výrobce zakončené certifikací účastníků. SŽ nominuje 4 pracovníky a bude požadovat naplnění časové dotace alespoň 3 MD.
	  ○ zaměření na užívání nástroje Log management a SIEM
	  ○ tvorba a úprava detekčních pravidel
	  ○ vyšetřování a analýza událostí
	  ○ aktivní vyhledávání kybernetických hrozeb.

4.2 Průběžné služby dodavatele řešení

4.2.1 Technická podpora servisního týmu SŽ

	Technická podpora servisního týmu zadavatele
Popis	Technická podpora bude řízena dle parametrů uvedených ve Zvláštních obchodních podmínkách pro zakázky v oblasti ICT SŽ (Příloha č. 7 Závazného vzoru smlouvy, který je Přílohou č. 6 zadávací dokumentace), konkrétně v ustanovení kapitoly „12. SERVISNÍ MODELY“. SŽ požaduje plnění v parametrech servisního modelu „B1 Závažný“. SŽ požaduje provoz Help Desku dodavatele, který bude provozován v režimu odpovídajícím specifikaci uvedené ve Zvláštních obchodních podmínkách pro zakázky v oblasti ICT SŽ (Příloha č. 7 Závazného vzoru smlouvy, který je Přílohou č. 6 zadávací dokumentace), konkrétně v ustanovení kapitoly „10. HELPDESK“. SŽ požaduje plnění Help Desku v režimu „Režim 1“ a úrovni „L3“.
Výstupy	Výstupem tohoto bude poskytnutí služby dle parametrů požadovaných SŽ a definovaných v servisní smlouvě s dodavatelem.

4.2.2 Údržba řešení

	Údržba řešení
Popis	Dodavatel zajistí pravidelnou údržbu všech komponent dodaného řešení, a to včetně bezpečnostní údržby. Cílem je, aby byl zajištěn provoz řešení v aktuální verzích produktu, které budou považovány za stabilní a bezpečné. Dodavatel zajistí aplikaci výrobcem vydávaných opravných balíčků, nových funkcionalit a bezpečnostních záplat. Průběžně prováděné a pravidelné činnosti zahrnují (prováděné min. 1x měsíčně): • Aktivní sledování a využívání nových postupů v oblasti zabezpečení systémů a komunikací. • Průběžné aplikování bezpečnostních oprav od výrobců. • Udržování aktuálnosti SW verzí dodaného řešení, a to minimálně v režimu aktuální MAJOR verze a MINOR verze ne starší než 2 vydání. Případné výjimky musí schválit SŽ. • Sběr podkladů pro aktualizaci dokumentace / evidence aktiv SŽ. • Pravidelná profylaxe systémových prostředků systému, včetně návrhu řešení nalezených problémů nebo rozvoje systému. • Kontrola provozních systémových logů s následným řešením případných incidentů. • Kontrola funkčnosti a bezpečnosti úložiště hesel. • Vypracování protokolu o údržbě s detailním popisem veškerých nalezených nedostatků a postupu pro jejich odstranění.
Výstupy	Výstupem tohoto bude poskytnutí služby dle parametrů požadovaných SŽ.

4.2.3 Konzultace a rozvojové aktivity

	Konzultace a rozvojové aktivity

Popis	Dodavatel poskytne SŽ služby konzultace na vyžádání. Maximální souhrn těchto služeb bude činit 250 MD za celou dobu trvání smlouvy, čerpání bude probíhat dle konkrétních potřeb SŽ. Jedná se o rozvojové aktivity, které budou souviset především s:
	- změnami v prostředí SŽ, které mohou mít dopad na provoz řešení Log management a SIEM.
	- integrací prostředí Log management a SIEM na procesy Security Operations Center
	  o Incident Response
	  o Forenzní analýza
	  o Sběr IoC.
	- pokročilou analýzou dat.
	- zajištěním udržitelnosti prostředí Log management a SIEM.

Výstupy	Výstupem tohoto bude poskytnutí služby konzultace na vyžádání podle potřeb SŽ.

5 Akceptační milníky

Plnění musí být dodáno v níže uvedených etapách. Každá z níže uvedených etap (tj. každý řádek níže uvedené tabulky) musí být SŽ separátně akceptována nejpozději v termínu uvedeném v harmonogramu. SŽ akceptuje výstupy dané Etapy, jestliže je dodavatel provedl v šíři a kvalitě požadované v zadávací dokumentaci této veřejné zakázky.

Etapa	**Popis**	**Kapitola obsahující požadavky**
Etapa 1A	Jednorázové projektové činnosti: - Před-implementační analýza	4.1.1
Etapa 1B	Jednorázové projektové činnosti: - Instalace a konfigurace řešení - Napojení určených zdrojů logů pro etapu 1	4.1.2 4.1.3
Etapa 2	Jednorázové projektové činnosti: - Napojení určených zdrojů logů pro etapu 2	4.1.3
Etapa 3	Jednorázové projektové činnosti: - Tvorba a optimalizace bezpečnostní / detekční politiky řešení - Školení	4.1.4 4.1.5
Etapa 4	Jednorázové projektové činnosti: - Napojení určených zdrojů logů pro etapu 4	4.1.3
Etapa 5	Průběžné služby dodavatele řešení: - Technická podpora servisního týmu SŽ - Údržba řešení	4.2.1 4.2.2
Etapa 6	Průběžné služby dodavatele řešení: - Konzultace a rozvojové aktivity	4.2.3

Klasifikace: Diskrétní dokument

SPRÁVA ŽELEZNIC

Příloha č. 1b Smlouvy – Analýza prostředí – architektura prostředí SŽ

Dokument se neuveřejňuje

Klasifikace: Diskrétní dokument

SPRÁVA ŽELEZNIC

Příloha č. 1c Smlouvy – Analýza prostředí – popis prostředí sítě UAS

Dokument se neuveřejňuje

Nabídková cena

Účastník vyplní **ve sloupci E** ("Jednotková cena (bez DPH, v CZK)") jednotkovou cenu **v Kč bez DPH** za každou část (etapu) dodávky řešení: E1, E2, E3, E4, E5 a E6 v řádcích 11 až 18.

V případě, že formulář obsahuje červeně zbarvenou celkovou nabídkovou cenu, nabídka pravděpoboně obsahuje nesprávně vyplněné údaje, které mohou vést až k vyloučení účastníka ze zadávacího řízení.

Maximální a nepřekročitelná cena veřejné zakázky (nesmí být překročena v řádku 19): 95 000 000 CZK

Etapa	Část dodávky	Odkaz na kapitolu TS	Jednotková cena (bez DPH, v CZK)	Počet jednotek	jedn.	Nabídková cena (bez DPH, v CZK)
E1	Před-implementační analýza, Implementační služby (napojení určených zdrojů logů pro Etapu 1)	4.1.1;4.1.2;4.1.3	2 152 000 CZK	1	-	2 152 000,00 CZK
E1	Licence, údržba licencí a technická podpora výrobce na 60 měsíců , nebo supskripce licencí včetně údržby a technické podpory na 60 měsíců (celková cena za výčet licencí uvedených v Příloze č. 20 zadávací dokumentace "Log management a SIEM dotazník", záložka Licence)	2.4	46 074 356 CZK	1	-	46 074 356,00 CZK
E1	Hardwarové prostředky, dodávané nad rámec specifikovaných Požadavků na služby Platformy SŽ, technická podpora výrobce HW na 60 měsíců, údržba a technická podpora HW dodavatele na 60 měsíců*	2.4.13	0 CZK	1	-	0,00 CZK
E2	Implementační služby (napojení určených zdrojů logů pro Etapu 2)	4.1.3	3 581 600 CZK	1	-	3 581 600,00 CZK
E3	Tvorba a optimalizace bezpečnostní / detekční politiky řešení, Školení	4.1.4;4.1.5	1 792 000 CZK	1	-	1 792 000,00 CZK
E4	Implementační služby (napojení určených zdrojů logů pro Etapu 4)	4.1.3	1 480 000 CZK	1	-	1 480 000,00 CZK
E5	Technická podpora servisního týmu SŽ, údržba řešení	4.2.1; 4.2.2	130 407 CZK	60	měsíc	7 824 420,00 CZK
E6	Konzultace a rozvojové aktivity	4.2.3	16 000 CZK	250	MD**	4 000 000,00 CZK
	NABÍDKOVÁ CENA CELKEM					**66 904 376,00 CZK**

**MD = člověkoden

* Tuto položku může dodavatel ocenit i hodnotou 0, a to v případě, že z jeho strany nebudou dodávány žádné další hardwarové prostředky nad rámec specifikovaných Požadavků na služby Platformy SŽ (viz čl. 18.3 zadávací dokumentace).

SPRÁVA ŽELEZNIC

Příloha č. 3 Smlouvy

HARMONOGRAM PLNĚNÍ

Etapa	Popis	Odkaz na kapitolu v TS	Termín zahájení	Požadovaný termín dokončení
Etapa 1A	• Před-implementační analýza	4.1.1	Od účinnosti smlouvy	1 měsíc
Etapa 1B	• Instalace komponent LM • Napojení určených zdrojů logů (z vybraných lokalit) • Dodávka produktových licencí včetně podpory výrobce v délce 60 měsíců	4.1.2 4.1.3	Od ukončení Etapy 1A, nebo od připravenosti Platformy SŽ	3 měsíce
Etapa 2	• Napojení všech určených zdrojů logů pro etapu 2	4.1.3	Od ukončení Etapy 1B	8 měsíců
Etapa 3	• Tvorba a optimalizace bezpečnostní / detekční politiky řešení • Školení	4.1.4 4.1.5	Od ukončení Etapy 1B	8 měsíců
Etapa 4	• Napojení určených zdrojů logů pro etapu 4	4.1.3	Od ukončení Etapy 2	4 měsíce
Etapa 5	• Technická podpora servisního týmu SŽ • Údržba řešení	4.2.1 4.2.2	Od ukončení Etapy 1B	60 měsíců
Etapa 6	• Konzultace a rozvojové aktivity	4.2.3	Od účinnosti smlouvy	Do konce účinnosti smlouvy

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

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

Id	Oblast LM&SIEM	Požadovaná funkcionalita systému	Splnění požadavku (Ano/Ne)	Způsob naplnění
1	Platforma	Architektura škáluje na běžném spotřebním hardware bez omezení na úložný prostor (možnost přidání hardware dle potřeby): - Horizontální škálování (přidání hardware výpočetního uzlu dle potřeby, clusterování) - Vertikální škálování (povýšení HW prostředků jednoho uzlu)	Ano	Popis celé architektury nabízeného řešení je popsán v samostatné Příloze č. 21 - Splunk architektura.pdf Obě varianty škálování jsou popsané v příloze.
2	Platforma	Automatická komprese indexovaných dat pro redukci nároků na úložný prostor	Ano	Všechna příchozí data se ukládají v raw podobě a Splunk tato data automaticky indexuje. Lze nastavit algoritmus z ZSTD, LZ4 a GZIP.
3	Platforma	Celé řešení je možné spravovat pomocí Grafického rozhraní.	Ano	Všechny komponenty systému se spravují přes Webové rozhraní dostupné přes HTTP nebo HTTPS.
4	Platforma	Celé řešení je možné spravovat pomocí konfiguračních souborů, nebo přes API volání (pro řešení automatizace)	Ano	Všechny konfigurační funkce jsou dostupné přes REST API a zároveň lze i konfigurovat přímo pomocí textových souboru
5	Platforma	Centralizovaná správa a monitoring funkčnosti všech SIEM komponent	Ano	Splunk umožňuje centrální správu a distribuci konfigurací z jednoho místa. K tomu slouží Splunk Deployment server. Z tohoto jednoho místa jsou distribuované konfigurace na všechny ostatní komponenty. Pro monitoring je pak určená role Monitoring Console. Tento server vyhodnocuje logy a metriky ze všech komponent a na jednom místě sdružuje několik dashboardů s různým pohledem na provozovanou Splunk infrastrukturu a zobrazuje stav jednotlivých komponent.
6	Platforma	Flexibilní nastavení uchování dat s možností odstupňování řízení toho, co se stane s postupně stárnoucími daty. Neaktuální data mohou být přesunuta na externí (levnější) datové úložiště k archivaci a (nebo) smazána.	Ano	Splunk podporuje víceúrovňové hierarchické ukládání dat. Pro každou úroveň lze definovat různé parametry ovlivňující kdy se data z dané úrovně začnou přesouvat do nižší/další úrovně. Data / logy se zapisují ve větších blocích tzv buckety. Celé buckety jsou pak přenášeny mezi jednotlivými úrovněmi úložiště. Hot - zde jsou data zapisována, jedná se o aktivní oblast náročnou na čtená a zápis. Warm - jedná se o buckety s aktuálními daty, ale už zde nedochází k zápisu (jedná se již o ReadOnly buckety). Předpokládá se, že tato data budou často prohledávána a proto vyžaduje rychlé úložiště - rychlé čtení. Cold - starší data s nižší pravděpodobností ke čtení. Ukládána na pomalejší zařízení s větší kapacitou. Frozen - offline úložiště
7	Platforma	Flexibilní nastavení uchování dat: - Nezávislost na technologii uložení dat - Může uchovávat indexovaná data, jak dlouho bude potřeba – dny, měsíce, roky - Odstupňované řízení toho, co se stane s postupně stárnoucími daty. - Neaktuální data je možné řízeně provozovat na levnějším datovém úložišti a nebo smazána.	Ano	Viz bod 6 Splunk je softwarová platforma. Není nijak závislá na technologiích pro uložení dat. Je pouze vyžadována podpora dané technologie v operačním systému.
8	Platforma	Informace o času poslední dostupnosti každé z komponent SIEMu	Ano	Monitorování systému zajišťuje role Monitoring Console. Zde je vidět i čas dostupnosti každé komponenty. Viz bod 5
9	Platforma	Instalovatelné na běžně dostupný hardware dle vlastního výběru, včetně virtualizace Vmware	Ano	Jedná se o software platformu. Instaloval lze na standardní HW, nebo je podporovaná virtualizace VMWare, Hyper-V nebo KVM. Také lze instalovat do kontejnerů Docker/Kubernetes.
10	Platforma	Instalovatelné na všechny hlavní operační systémy (Windows, Linux, HP/UX, AIX, FreeBSD, Solaris, …)	Ano	Aktuálně jsou podporované operační systémy: - Microsoft Windows 2019+ - Linux s kernel 3.x, 4.x nebo 5.4+
11	Platforma	Jeden produkt integrující jak funkce pro Log management i SIEM (nejsou oddělená datová úložiště a uživatelská rozhraní pro Log management a SIEM)	Ano	Splunk Enterprise (LogManagement) definuje uložiště, SIEM je řešen nadstavbou Splunk Enterprise Security, která je vybudovaná na Splunk Enterprise. SIEM část nemá možnost je tak zajištěno že je jedno uložiště dat.
12	Platforma	Jednotné uživatelské rozhraní pro všechny systémové funkcionality včetně vyhledávání, reportování, tvorbu pravidel, správu systému (transportní vrstva může mít samostatné uživatelské rozhraní)	Ano	Všechny komponenty mají stejné webové rozhraní a všechny konfigurace a nastavení se provádí přes toto webové rozhraní.
13	Platforma	Možnost distribuované architektury – rozložení zátěže, redundance, rychlejší odezva management konzole a možností rozprostření dílčích systémových funkcionalit (rolí) mezi více prvků celého řešení s centrální správou	Ano	Viz bod 1. Rozdělením jednotlivých rolí na samostatné servery se docílí rozložením zátěže. Další škálování může být do šířky přidáním více serverů pro stejnou roli. Tím je i automaticky řešena vysoká dostupnost dané role. Systém automaticky rozkládá zátěž přes všechny servery (pro danou roli). Všechny validované architektury (včetně distribuovaných) jsou popsány výrobcem v dokumentu SVA - https://www.splunk.com/en_us/pdfs/tech-brief/splunk-validated-architectures.pdf
14	Platforma	Možnost instalace on-premis, v cloudu nebo kombinovaný hybridní přístup	Ano	Splunk podporuje všechny 3 možnosti. On-premis je možné na vlastním HW. V případě Cloud varianty je možné více přístupů. Je možné zprovoznit Splunk v rámci vlastního Cloudu (AWS, ASURE …) nebo v rámci Splunk Cloudu, kde se o celou infrastrukturu stará přímo Splunk. Hybridní přístup je také možný, je možní mát část infrastrukturu v cloudu a část On-prem.
15	Platforma	Možnost nasadit veškeré klíčové prvky v HA modu. V HA modu nemusí být části, které při výpadku krátkodobě (min 1 den) neovlivní jakkoliv funkcionalitu systému	Ano	Všechny klíčové komponenty lze instalovat v režimu vysoké dostupnosti (HA). Pro různé role jsou definovaná jiná doporučení k instalaci vysoké dostupnosti. Každá vrstva Splunk infrastruktury (viz bod 1) lze instalovat v režimu N+1. Při výpadku jednoho prvku, běží celý systém dál bez jakéhokoliv výpadku. Ostatní komponenty a prvky detekují výpadek a zajistí potřebnou změnu v komunikaci. V tomto stavu může běžet celý systém i několik dní.
16	Platforma	Možnost přístupu a vzdálené správy přes WebUI a CLI	Ano	Splunk umožňuje správu jak ve webovém prostředí WebUI, tak lze i spravovat systém pomocí CLI přes SSH protokol. https://docs.splunk.com/Documentation/Splunk/latest/Admin/AbouttheCLI
17	Platforma	Možnost snadno přeposílat data do jakéhokoliv externího systému nebo logovacího nástroje: - V době indexování mohou být původní data přeposílána protokolem syslog přes TCP, UDP nebo jako prostý TCP stream - V době indexování může systém přeposlat vybrané, transformované a/nebo o kontext obohacené události jako soubor nebo syslogem přes TCP či UDP	Ano	Pro sběr a směrování logů využíváme nástroj společnosti Cribl. Ten zajišťuje tyto hlavní stavební bloky (hlavní funkce): - Collect - Reduce - Shape - Route - Replay Pomocí uživatelem definovaných Pipelines lze definovat potřebné úpravy zpráv, filtrace, směrování na vybraný cíl a případně i úpravu zpráv jen pro vybraný cíl. Seznam možný zdrojů a cílů je zde: - https://docs.cribl.io/stream/sources/ - https://docs.cribl.io/stream/destinations
18	Platforma	Možnost využití nestrukturovaných souborů a datového skladu bez pevného schématu (bez relační database s pevným schématem)	Ano	Splunk ukládá data v takovém stavu v jakém je přijme. Využívá přístupu Schema-on-Read. Tedy data se ukládají v nestrukturované podobě a případná struktura se vytváří až při přístupu k datům / při vyhledávání.
19	Platforma	Musí podporovat vývojové nástroje (SDK) psané nad API pro jazyky, např.: - Python - Java - JavaScript - PHP - Ruby - C#	Ano	Splunk podporuje Python, Java, JavaScript, C# https://dev.splunk.com/enterprise/docs/devtools
20	Platforma	Podpora instalaci do virtuálního prostředí i na fyzický hardware (bez omezení na konkrétní virtualizační platformu)	Ano	Instalace není omezena na fyzický HW, je možné řešení instalovat jak na HW, virtuální prostředí i cloud - viz bod 9
21	Platforma	Poskytuje webové rozhraní pro koncové uživatele (nevyžaduje instalaci tlustého klienta)	Ano	Pro přístup se v základním nastavení používá webové prostřední. Tlustý klient k dispozici není.
22	Platforma	Pouze software - bez vazby na uzavřenou fyzickou appliance	Ano	Ano, řešení je distribuováno jako balíček, který je možné instalovat bez uzavřené fyzické appliance - viz bod 9
23	Platforma	Produkt bude integrovat jak funkce Log managementu, tak SIEMu. Nejsou oddělená datová úložiště a uživatelská rozhraní pro Log management a SIEM	Ano	stejná odpověď jako u otázky 11
24	Platforma	Řešení ukládá audit akcí provedených administrátory Log managementu a SIEMu. Systém provádí nativně audit veškerých změn v konfiguraci, bez ohledu na to, jakým způsobem byla změna provedena, včetně přímého zápisu do konfiguračních souborů. Auditní logy se musí ukládat na jedno společné místo a všechna auditní data musí být dostupná a prohledávatelná přes UI. Podpora odesílání auditních logů na úložiště mimo dodávané řešení Log management a SIEM, např. protokolem SYSLOG.	Ano	Veškeré změny v systému, které provádí uživatel přes CLI, WebUI nebo API jsou ukládány do speciálního auditního logu. Před vlastním zápisem do auditního logu jsou data také uložena do indexu. Díky tomu nelze data před indexováním změnit. Pokud by někdo chtěl změnit konfigurační soubory přímo, tak to lze, pak je v systému ještě funkce ConfigTracker. Ta monitoruje a vyhodnocuje přímou editaci změn v konfiguračních souborech. Jakákoliv změna je detekována a uložena ve speciálním Indexu. Všechny auditní data jsou uložena v indexech a jsou prohledávatelná z UI standardním způsobem, jako ostatní logy. Auditní logy lze odeslat i do externích systémů pomocí Syslog protokolu.
25	Platforma	Schopnost replikace dat k udržování násobku identických kopií indexovaných dat k zajištění dostupnosti a věrnosti dat, odolnosti proti neočekávané události (katastrofě) a zlepšení výkonnosti vyhledávání.	Ano	Splunk index cluster umožňuje definovat replikační faktor, který udává počet kopii, které mají být v rámci clusteru uloženy. Každá kopie je na jiném Splunk index serveru. Při zpracování dotazů se posílá požadavek na všechny index server a tím se rozkládá zátěž přes všechny servery, kde jsou data uložena. Tím dochází i k rychlejšímu zpracování dotazů.

26	Platforma	Schopnost udržovat si původní časové známky pro každou událost a poradit si s časovými známkami z různých časových zón	Ano	Splunk v rámci příjmu dat provede extrakci časové známky z logu. Pokud časová známka obsahuje časovou zónu, dokáže s ní pracovat. Pro servery, které nepošlají časovou zónu, lze v systému tato zóna definovat. Všechny dotazy se pak interně zpracovávají v UTC čase.
27	Platforma	Schopnost uložit různá data do různých indexů pro optimalizaci vyhledávání nebo pro oddělení dat (řízení přístupu dle rolí uživatelů, tzv. RBAC)	Ano	Splunk umožňuje rozdělit data do různých indexů kdy každému indexu lze definovat skupina uživatelů, která s daným indexem může pracovat.
28	Platforma	Schopnost vytvářet indexy a datová úložiště sumarizující surová strojová data a následně spustit vyhledávání/reporty nad těmito agregacemi pro zrychlení výkonu	Ano	Řešení umožnuje vytvářet tzv. "summary indexy" a nad nimi provádět vyhledávání. https://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Usesummaryindexing
29	Platforma	Systém není prototypem vyvinutým pro účel této zakázky; veškerou funkcionalitu musí být dodavatel schopen na vyžádání zadavatele demonstrovat	Ano	Řešení je postaveno na existujících produktech Splunk a Cribl. Jedná se o řešení provozované několik let u zákazníků po celém světě. https://www.splunk.com/ https://cribl.io/
30	Platforma	Systém umožňuje kompletní správu řešení pomocí automatizačních nástrojů (ansible, Puppet a dalších)	Ano	Řešení umožňuje konfiguraci pomocí konfiguračních souborů, CLI a API. Je tedy možné využít automatizačních nástrojů. Pro Ansible existuje i dokumentované řešení přímo od výrobce - https://splunk.github.io/splunk-ansible/
31	Platforma	Systém umožňuje rozšíření pomocí dalších placených i neplacených modulů	Ano	Dostupný seznam je k dispozici na https://splunkbase.splunk.com/
32	Platforma	Systém umožňuje snadné vytváření vlastních modulů např. pro možnost zpracování specifického formátu vstupních dat	Ano	Systém má dokumentované vývojové možnosti a lze vytvářet vlastní moduly. Dokumentace pro vývoj vlastních modulu https://dev.splunk.com/enterprise/docs/developapps/ Případně dokumentace týkající se parsování dat je zde: https://docs.splunk.com/Documentation/Splunk/9.1.1/Data/Overviewofeventprocessing
33	Platforma	Škálovatelná architektura, která nasazená u zákazníků zpracovává více jak 10TB dat denně	Ano	viz bod 1, Množství dat není omezeno, záleží jen na dostupných HW prostředcích
34	Platforma	Umožňuje vyhledávat nad distribuovaným uložištěm (uložená data ve vzdálených lokalitách)	Ano	Vyhledávací servery posílají vyhledávací dotaz na všechny servery, kde jsou data uložena. Tedy bez ohledu na to, v jaké lokalitě servery jsou uloženy. Vyhledání probíhá nad celým distribuovaným úložištěm.
35	Platforma	Veškerá systémová nastavení jsou konfigurovatelná přes uživatelské rozhraní (WebUI), příkazovou řádku (CLI) nebo změnou souborů	Ano	viz bod 16, veškeré nastavení provedené přes WebUI nebo CLI se zapisuje do konfiguračních souborů, které administrátor může měnit i přímo změnou na souborovém systému.
36	Platforma	Veškerou konfiguraci je možné uložit a spravovat jako kód ve strukturované textové formě (například yaml,json,xml a dalších)	Ano	Konfigurační soubory jsou uložené v textové podobně odpovídající INI/TOML formátu. viz bod 4 a 30
37	Platforma	Všechny reporty a dashboardy je možné upravit v WebUI nebo přímou editací příslušných konfiguračních souborů	Ano	Viz bod 30, reporty jsou v systému uloženy jako samostatné soubory ve formátu XML
38	Platforma	Výrobce poskytuje veřejné uložiště dostupných nadstavbových aplikací (modulů)	Ano	viz bod 31
39	Platforma	Infrastruktura pro přenos logů od zdroje k centrálním úložištím musí podporovat oba směry komunikací, tedy: - PUSH, kdy spojení navazuje prvek na vzdálené satelitní lokalitě - PULL, kdy spojení navazuje centrální komponenta řešení Log management a SIEM	Ano	Podporované jsou oba způsoby komunikace. V případě PUSH jsou data odesílána ze zdroje dat a spojení je navazováno z tohoto zařízení, typicky se jedná o komunikaci pomocí syslog protokolu nebo pomocí Splunk Universal Forwarder agenta. U PULL je spojení navazováno ze zařízení k tomu určeného - Splunk Heavy Forwarder. Zde jsou instalované moduly a aplikace, které zajišťují stahování dat ze vzdálených zařízení, typicky se jedná o přístup do databáze, čtení dat pomocí REST API, a podobně.
40	Platforma	Využívá implementace technologie MapReduce pro rychlé a distribuované vyhledávání	Ano	Komponenta SearchHead zajišťuje spuštění a zpracování prohledávacího dotazu. Po analyzování dotazu a optimalizaci se vytvoří speciální konfigurační balíček a ten se pošle na Index vrstvu. Zde se dotaz rozloží mezi všechny servery, které mají uložena prohledávaná data (index a časové okno). Každý server par provádí lokální prohledávání uložených dat. Na nalezená data je aplikovaný parsing a následně předzpracování dat. Redukovaná data (výsledek dotazu) se pošle zpět na SearchHead server, který o data žádal. Jednotlivé výsledky ze všech serverů se dále skládají a zpracovávají. Detailní popis https://docs.splunk.com/Documentation/Splunk/9.1.1/DistSearch/Parallelreduceoverview
41	Platforma	Využívá nestrukturované soubory a datový sklad bez pevného schématu (bez relační databáze s pevným schématem, což může být úzkým hrdlem nebo kritickým bodem selhání)	Ano	Splunk ukládá data v takovém stavu v jakém je přijme. Další úpravy jsou prováděny nad originálním stavem, kdy tento stav nemění.
42	Platforma	Zasílání alertů při výpadku komponent	Ano	Splunk Monitoring Console monitoruje stav jednotlivých komponent. Provádí se analýza metrik a interních logů. Při výpadku je možné nastavit alerting a definovat požadovanou akci - například odeslání emailem.
43	Platforma	Systém v rámci HA nasazení podporuje Active-Active režim nebo Cluster se všemi aktivními členy, je tím zaručen bezvýpadkový provoz.	Ano	Detailní popis HA je v bodu 15. Pokud dojde k výpadku jednoho serveru, ostatní komponenty toto dokáži detekovat a automaticky přesměrují svoji komunikaci na jiný server.
44	Platforma	Zpracování dotazů musí být rozloženo přes všechny členy, kde jsou uložena data. Přidáním nového člena dojde k dalšímu rozložení zátěže a tím pádem ke zrychlení zpracování dotazů.	Ano	Zpracování dotazů se vždy provádí na všech členech tzv Index clusteru. Tedy na všech serverech, kde jsou uložená data. Přidáním dalšího člena automaticky dojde k rozšíření clusteru a nový člen se ihned začne zapojovat do zpracování dotazů (pro data, která má již indexovaná nebo replikovaná).
45	Platforma	Systém nepotřebuje provádět reindexaci již uložených dat, pokud dojde ke změně ve zpracovávání(parsing/normalizace) dat, změna se okamžitě projeví i v historických datech).	Ano	K parsingu dat dochází ve Splunku vždy v době vyhledávání. Tedy pokud je nutno změnit parsing neprovádí se žádná reindexace a nový parsing je aktivní ihned na všechna data.
46	Platforma	Řešení je možné provozovat v běžně používaných kontejnerových platformách (Docker, Kubernets, ...).	Ano	Ano, řešení lze provozovat v kontejnerových platformách docker a Kubernetes - viz bod 9
47	Platforma	Systém umožňuje definovat kde jsou v rámci operačního systému uložena data, konfigurace a interní logy.	Ano	Pomocí nastavení ve Splunku a nejlépe i v kombinaci s nastavení v operačním systému lze oddělit kde je uložen Splunk, kde jsou uloženy konfigurace, kam se zapisují logy a jde se ukládají indexovaná data.
48	Licencování	Licence není vázaná na instalovanou topologii - počet lokalit systému Log management a SIEM	Ano	Licence je vázaná pouze na počet přijatých dat za den
49	Licencování	Licence není vázaná na počet uživatelů ani počet zařízení zasílajících logy	Ano	Licence není vázaná na počet uživatelů. Licence je vázaná pouze na počet přijatých dat za den
50	Licencování	Licence nesmí omezovat výkon, nebo propustnost dat systému v případě překročení licence	Ano	Licence neomezuje výkon. Vždy se zpracovávají všechna data a výkon není žádným způsobem omezován (jen výkonem daných HW zdrojů - CPU/vCPU). Licence se vyhodnocuje zpětně za předchozí den.
51	Licencování	Licenční model je založen na objemu dat zpracovaných za 24 hodin, nebo počtu událostí za sekundu průměrovaných za časové období delší než 1 hodina, což umožní pojmout případné chvilkové špičky v objemu přijímaných informací.	Ano	Viz Bod 49+50
52	Licencování	Při překročení objemu zpracovaných dat za den, nebo EPS za období delší než 1 hodinu, nedojde k zastavení/zahazování nových příchozích dat	Ano	Viz bod 50
53	Licencování	Systém umožňuje zpracovávat nárazové špičky zpracovávaných dat bez omezení	Ano	Viz bod 50
54	Zpracování a zdroje dat	Agent pro Linux, min. CentOS, Debian	Ano	U Linux systémů má Splunk podmínky pouze na verze Linuxového jádra a CPU architektury. Seznam podporovaných Linuxu je https://docs.splunk.com/Documentation/Splunk/9.1.1/Installation/Systemrequirements#Unix_operating_systems
55	Zpracování a zdroje dat	Agent pro Windows (min. Server 2008 R2)	Ano	Agenta Splunk Universal Forwarder lze instalovat na všechny aktuálně podporované verze Windows (2012+). Sběr dat z již neaktuálních Windows a nepodporovaných ze strany výrobce Microsoft je možný, a lze využít starších verzi agenta. Pro podporu Server 2008 R2 je potřeba použít starší verze Splunk Universal forwarderu (verze 7.2.10). Toto verzi je možné posílat na poslední verze Splunku https://docs.splunk.com/Documentation/VersionCompatibility/current/Matrix/Compatibilitybetweenforwardersandindexers
56	Zpracování a zdroje dat	Datové zdroje zahrnují jakoukoliv aplikaci, operační systém nebo systém ať už fyzický, virtuální nebo v cloudu, půjde-li o člověkem čitelná data)	Ano	Splunk systém dokáže indexovat a prohledávat jakoukoliv textovou (člověkem čitelnou) informaci. Pomocí Addonů a scriptů se lze připojit na libovolnou existující aplikaci, sledovat soubory nebo přijímat data přes síť. V případě i binárních (ne textových) dat, lze pomocí modulů převézt tato data do textové podoby a zajistit tak uložení a prohledávání.
57	Zpracování a zdroje dat	Nebude potřeba vytvářet datové schéma nebo připravit vyhledávací dotazy ještě před indexováním	Ano	Splunk využívá funkcionality Schema-On-Read. To znamená, že všechna přijatá data uloží na disk a jakýkoliv parsing a případné vytváření schématu se provádí až při prohledávání dat.
58	Zpracování a zdroje dat	Řešení bude schopno pracovat s novými zdroji dat nebo změnami ve formátech logů u existujících datových zdrojů.	Ano	Viz bod 57
59	Zpracování a zdroje dat	Řešení může indexovat víceřádkové nebo komplexní logy událostí	Ano	Splunk umožňuje více možností jak pracovat s víceřádkovým logem. Jedním z nich je například parametr EVENT_BREAKER definující pravidlo pro rozpoznání oddělovače mezi eventy. https://docs.splunk.com/Documentation/Splunk/9.1.1/admin/Propsconf

60	Zpracování a zdroje dat	Schopnost importovat data pro indexaci z Hadoop platformy	Ano	V Systému Splunk lze definovat tzv Virtuální Index. V tomto případě se jedná o data, která nejsou přímo přijata a indexovaná systémem Splunk, ale o externí data. Tímto způsobem lze využívat i externí data uložená v systému Hadoop. Protože se jedná o Index, jsou data standardním způsobem i prohledávatelná a analyzovatelní v UI. https://docs.splunk.com/Documentation/Splunk/9.1.1/HadoopAnalytics/Virtualindexes
61	Zpracování a zdroje dat	Schopnost indexovat a připravit pro vyhledávání všechna originální data bez jakékoliv modifikace (bez normalizace/redukce dat)	Ano	Splunk přijímá a ukládá data tak jak přišla. Neprovádí se žádná úprava/modifikace. Vyhledávání se provádí vždy nad uloženými daty.
62	Zpracování a zdroje dat	Schopnost indexovat všechna původní nemodifikovaná data a jejich zpřístupnění při vyhledávání a generování reportů (bez předem definovaného schématu nebo normalizace/redukce dat). Žádná data se indexováním nikdy neztratí	Ano	viz bod 61 a 57
63	Zpracování a zdroje dat	Schopnost přijímat data přes širokou škálu mechanizmů využívajících agentů i bez nich: - Dodavatelem podporovaný "univerzální agent" - agent musí mít schopnost šifrovat komunikaci na centrální komponenty log management řešení, zadržovat data v cache, rozkládat zátěž na více indexátorů, posílat data přes TCP, explicitně potvrzovat přijetí - Syslog - Netflow (Netflow v5, Netflow v9, sFlow, IPFIX) - SNMP události - XML - CSV - JSON - Windows WMI - Čtení ze souborů uložených lokálně na indexátoru nebo přístupných vzdáleně jakýmikoliv běžně dostupnými protokoly (CIFS, SMB, NFS, apod.) - HTTP protokolem přímo z aplikací - Proprietární protokoly (např. Checkpoint OPSEC LEA, HPE Arcsight CEF, apod.) - Vlastní vstupy (Skriptované vstupy, modulární vstupy - vlastní technologické moduly)	Ano	Splunk Universal Forwarder i Cribl Edge jsou agenti, kteří se instaluji na zdrojové zařízení. Oba agenti podporují šifrování dat do nadřízeného a dále až na index vrstvu. V případě nefunkční komunikace lze zapnout permanentní cache na disku. Komunikace s nadřízeným prvkem je vždy rozkládána mezi všechny prvky. Všechny komunikace běží nad TCP protokolem a jsou vždy potvrzované. Lze i zapnout explicitní potvrzování od Indexační vrstvy pomocí Indexer acknowledgment - https://docs.splunk.com/Documentation/Splunk/9.1.1/Data/AboutHECIDXAck. Všechny zmíněné mechanismy je možné v systému přijímat.
64	Zpracování a zdroje dat	Schopnost připojit se přímo do tabulky SQL databáze a extrahovat obsah pro indexaci	Ano	Pro čtení a indexování dat z SQL lze využít rozšíření Splunk DB Connect. Po přidání příslušného ovladače pro konkrétní verzi SQL serveru lze číst data z tabulky (TABLE) nebo z pohledu (VIEW).
65	Zpracování a zdroje dat	Schopnost získat a automaticky analyzovat jakýkoliv zdroj dat (textových, binárních) bez omezení na konkrétní verzi nástroje. V případě, že systém v konkrétní verzi nebude schopen získat nebo interpretovat požadovaná data automaticky, musí být natolik robustní a flexibilní, že zákazník nebo dodavatel jsou schopni doplnit funkčnosti vlastními silami – kombinací prostředků systému nebo s pomocí externích nástrojů.	Ano	Systém je robustní a disponuje velkými možnostmi jak přijímat a analyzovat data. K dispozici jsou i popsané SDK a API, pomocí kterých lze dopsat i další možnosti. Již hotová řešení jsou dostupná na splunkbase.splunk.com. Dodavatel má praktické zkušenosti s implementováním a vývojem modulů pro příjem dat na přání zákazníka.
66	Zpracování a zdroje dat	Schopnost zpracovávat 1 TB dat denně	Ano	Celé řešení je navrženo pro příjem 1TB dat a to včetně výpadku jednoho virtuálního serveru.
67	Zpracování a zdroje dat	Systém je schopen nad logy provádět datové obohacení a normalizaci. Normalizací se rozumí sjednocení formátu logů stejného typu z různých zdrojů. Log je extrahován a zaveden do příslušného jednotného schématu Za normalizaci se nepovažuje prostá extrakce datových polí z logů.	Ano	Datové obohacení se provádí před ukládáním dat nebo až při zpracování dotazů. Obohatit logy lze pomocí již uložených jiných logu, nebo z externích zdrojů. Pro normalizace se používá funkcionalita DataModel. Ta vytváří definovaný předpis (schéma). Uživatel si může tyto datamodely vytvářet sám, nebo lze využít existujícího doporučení - Splunk CIM. https://docs.splunk.com/Documentation/CIM/5.2.0/User/Overview
68	Zpracování a zdroje dat	Systém provádí sběr libovolných logů z OS Linux, přičemž umožňuje sbírat výstupy custom skriptů	Ano	Pomocí instalovaných agentů lze monitorovat a přijímat data z libovolných logů uložených na daném počítači. Případně lze psát vlastní aplikace nebo scripty, které zajistí sběr dat. Podpora skriptovacích jazyků je omezena jen podporované jazyky v daném OS. Pro OS Linux je to například Bash, Python, ...
69	Zpracování a zdroje dat	Systém sbírá libovolné logy z OS Windows, včetně informací z komponenty Windows perfmon, přičemž umožňuje sbírat výstupy custom skriptů minimálně v jazyce Windows Powershell	Ano	Pomocí instalovaných agentů lze monitorovat a přijímat data z libovolných logů uložených na daném počítači. Případně lze psát vlastní aplikace nebo scripty, které zajistí sběr dat. Podpora skriptovacích jazyků je omezena jen podporou v daném OS. Pro OS Windows je to například Cmd, PowerShell, Python, ...
70	Zpracování a zdroje dat	Systém umožňuje definovat kde jsou jednotlivá data uložena, v případě lokalit je možné definovat v jaké lokalitě mají být uložena	Ano	Na základě pravidel je možní definovat v agentu, kam má příslušná data posílat k zaindexování. Může se jednat o samostatný Index Server, o Index Cluster nebo o MultiSite Cluster. V případě MultiSite Clusteru se pak mohou data směrovat do příslušné lokality.
71	Zpracování a zdroje dat	Systém umožňuje tagování (označování) jednotlivých logů a událostí dle libovolných kritérií	Ano	Je možné využít přiřazení hodnoty EventType a následné přidání tag. Každá zpráva může mít více EventType a každý EventType může mít více Tagů. Pro každý EventType lze definovat i barvu, která se použije při zobrazení události v UI.
72	Zpracování a zdroje dat	Systém zajišťuje dostupnost provozních a bezpečnostních logů v nezměněném tvaru, tak jak byl poslán ze zdrojového zařízení	Ano	Splunk přijímá data v originálním formátu a až následně ve fázi hledání data upravuje podle požadavku.
73	Zpracování a zdroje dat	Systém zpracovává data z neomezeného počtu zařízení (do systému je možné zasílat data z jakéhokoliv počtu typu zařízení s neomezeným počtem datových zdrojů)	Ano	Viz bod 49 Systém nekontroluje odkud mu přicházejí data, přijímá data ze všech zdrojů.
74	Zpracování a zdroje dat	Univerzální index: - Sběr a zpracování a uložení jakékoliv textové informace bez ohledu na zdroj, objem, rychlost, proměnlivost, rozmanitost a strukturu dat v reálném čase - Indexování všech informací v původním nezměněném tvaru - Automatické doplnění časové značky ke každé události, pokud chybí	Ano	Splunk při zpracování dat nerozlišuje, co nebo od koho daná data přišla. Má vytvořenou universální platformu pro ukládání textových dat. Tato data se indexují včetně dalších metadat pro jejich rychlejší zpracování. Vždy se data indexují v podobě, jak přišla. Ke každému logu se přidávají navíc prohledávatelná metadata: host, source, sourcetype a timestamp. Pokud vstupní data neobsahují časovou známku, pak automaticky Splunk použije aktuální čas jako timestamp.
75	Zpracování a zdroje dat	Uživatel může nastavit klasifikaci a normalizaci vstupních dat	Ano	Pro příchozí data lze nastavit nebo změnit klasifikaci. Na základě správné klasifikace se pak provádí normalizace, kterou si uživatel opět může změnit.
76	Zpracování a zdroje dat	Zdroje dat nebo oblasti dat, které mohou být indexovány a jsou relevantní pro technologická prostředí: - SCADA zařízení - Systémy průmyslové automatizace (ICS) - Výrobní systémy (CNC systémy, výrobní linky) - Data z fyzických visaček zaměstnanců (badge) - Radiofrekvenční identifikátory (RFID) - GPS data - Vlastní aplikace - PCAP soubory	Ano	Pro všechny vypsané technologie lze zajistit příjem dat: - Nativní podpora - Existující rozšiřující modul - Vlastní vývoj
77	Zpracování a zdroje dat	Zdroje dat nebo oblasti dat, které mohou být indexovány: - Firewally a VPN - IDS/IPS systémy - Autentizační systémy (vč. LDAP a Active Directory) - DLP systémy - Anti-malware nástroje - Automatizované nástroje pro analýzu malware - Webová bezpečnost a webová proxy - Emailová bezpečnost - Skenery zranitelností - Monitory integrity souborů - Web aplikační firewally - Logy operačního systému (koncové stanice a servery) - Email server - Web server - DHCP/DNS - Network Flows (NetFlow, sFlow, Jflow, IPFIX, atd.) - Síťová zařízení (směrovač, přepínač, balancer zátěže, atd.) - Databáze a sálové počítače (IBM zSeries, atd.) - Zařízení pro ukládání velkých objemů dat (NAS, SAN, atd.) - Logy hypervisorů (VMWare, KVM, Citrix Xen, Hyper-V) a virtuálních serverů - Tiketovací systémy (Service desky) - Záznamy o hovorech (CDR) - Mobilní zařízení a MDM systémy - Nástroje pro správu serverů a koncových stanic (MS System Center, atd.) - Hostovaná prostředí virtuální systémů MS AZURE, AWS, Google, Cloudové aplikace - Sociální platformy (Twitter, Facebook, Foursquare, atd.) - ERP and CRM systémy - Aplikace	Ano	Splunk není omezen na zdrojové technologie, je možné vybrat z více jak 2700 aplikací, https://splunkbase.splunk.com/apps , nebo lze vytvořit vlastní aplikaci

78	Zpracování a zdroje dat	Systém musí být schopen zpracovávat, vyhodnocovat a zobrazovat metrická data, přičemž podporuje práci s časovými řadami.	Ano	Splunk disponuje speciálním indexem pro ukládání Metrik. Metrická data se ukládají odlišným způsobem než logy. Jedná se o hodnoty s časovou značkou opatřenými dalšími doplňkovými daty - dimenze. Zpracování dat se provádí pomocí nejrůznějších metod pro časové řady (hodnoty v čase). Jedná se o efektivnější zpracování dat než by zpracování serializovaných dat do textového logu.
79	Integrace	Integrace s CMDB databází (Change Management Database) nebo databází aktiv s informacemi o aktivech včetně: - Jméno zařízení, IP, MAC, lokalita, důvěrnost, vztah k normám, apod. - Umožní mapovat IP na jméno zařízení a naopak.	Ano	Je možné vyčítat data ze CMDB pomocí API nebo pravidelného exportu a následně provádět obohacování dat. Lze zajistit i integraci v UI, tedy proklik při analýze logů přímo do CMDB.
80	Integrace	Integrace s korporátními adresáři (AD, LDAP, atd.) pro extrakci informací o zaměstnancích včetně: - Uživatelská jména, křestní jména, příjmení, telefon, nadřízený, oddělení, lokalita, privilegia, atribut o sledování, začátek a ukončení pracovního poměru a další atributy zaměstnanců - Dovolí možnost korelovat více uživatelský jmen zpět k jedinému zaměstnanci	Ano	Pro integraci s AD/LDAP lze využít rozšiřující modul https://splunkbase.splunk.com/app/1151. Ten zajišťuje import dat z AD/LDAP do Splunku, a konkrétní importované atributy se řeší formou konfigurace konektoru. Tato importovaná data pak vstupují do SIEM modulu Asset and Identity Management. Zde lze korelovat uživatelské jména a vytvářet unikátního uživatele pro další zpracování v SIEMu.
81	Integrace	Možnost snadné integrace s lidsky čitelnými zdroji informací o hrozbách, ať už jsou zdarma, komerční nebo od jakékoliv třetí strany	Ano	Splunk využívá Threat Intelligence Management kde jsou přednastavené threatlisty, nebo je možné definovat vlastní zdroje.
82	Integrace	Možnost využít externích zdrojů dat pro obohacení událostí přidáním dalšího kontextu (souvislosti), a/nebo vytvoření specifičtějšího korelačního vyhledávacího dotazu)	Ano	Obohacení událostí může být provedeno z interních dat nebo z externích. V případě externích se může jednat o integrované systémy, nebo i o veřejně dostupná data z internetu. Pomocí již hotových aplikací lze takto přidat obohacení například o: - informace o IP adrese - https://splunkbase.splunk.com/app/4070 - reputace souboru - https://splunkbase.splunk.com/app/5864
83	Integrace	Nabízí REST API, aby externím systémům, aplikacím a dashboardům zpřístupnil indexovaná data, vyhledávací příkazy a další funkce	Ano	Všechny funkce jsou dostupné přes API. Toto API je kompletně dokumentované na https://docs.splunk.com/Documentation/Splunk/latest/RESTREF/RESTprolog Pro integraci reportů v externím dashboardu lze využít funkční EmbedReport - https://docs.splunk.com/Documentation/SplunkCloud/9.0.2305/Report/Embedscheduledreports Případně lze využít i přímo Search API - https://docs.splunk.com/Documentation/Splunk/9.1.1/RESTTUT/RESTsearches
84	Integrace	Nabízí zdarma více jak 2000 veřejně dostupných nadstavbových aplikací (modulů) pro integraci s produkty třetích stran, vytvoření případů užití a celkové zkrácení doby nutné k zisku očekávaného výsledku	Ano	Na SplunkBase je dostupných cca 2700 addonů a aplikací pro Splunk - https://splunkbase.splunk.com/
85	Integrace	Web API pro napojení softwaru třetích stran (zpracování událostí, logů, alarmů, seznamů)	Ano	Splunk má všechny API zdokumentované na stránkách dev.splunk.com. V případě Web API se týká primárně podpora Javascriptu viz https://dev.splunk.com/enterprise/docs/devtools/javascript/sdk-javascript nebo https://docs.splunk.com/Documentation/JavaScriptSDK
86	Integrace	Upozornění na nově vzniklý alert v SIEMu je vyžadováno integrovat jako notifikaci s platformou MS TEAMS. Skupina definovaných příjemců obdrží notifikaci v platformě MS TEAMS v případě výskytu detekované události.	Ano	Pro integraci s Microsoft Teams lze využít specializovaného addonu nebo nakonfigurovat integraci přímo ve Splunku. Ve MS Teams je nutná přípravná práce v podobě zajištění příchozího Webhook a ten se použije při vytváření Custom akce v alertu. Zde se provede vytvoření JSON struktury, vložení dat z alertu a odeslání na Webhook. Následně při vytvoření Alertu se vytvoří i zpráva v MS Teams.
87	Integrace	Systém musí umožnit integraci s nástrojem "Jupyter Notebook" pro lepší podporu datové analytiky s využitím programovacího jazyka Python.	Ano	Integrace je možná. Detailní nastavení je dostupná na stránkách výrobce - https://www.splunk.com/en_us/blog/platform/configure-jupyter-notebook-to-interact-with-splunk-enterprise-the-splunk-machine-learning-toolkit.html
88	Integrace	Řešení musí být schopné obousměrné integrace s tiketovacím systémem zákazníka (ATLASSIAN - JIRA) z důvodu: - automatického zakládání alertů jako bezpečnostní tikety (SIEM -> JIRA) - synchronizace stavu řešení tiketu OPEN / CLOSED zpět do nástroje SIEM (JIRA -> SIEM)	Ano	Splunk lze integrovat i s řešením od společnosti Atlassian (Jira nebo Jira ServiceDesk). Existují již hotové "add-ons", které tuto oboustrannou vazbu již zajišťují, popřípadě lze i vytvořit vlastní integraci dle detailní specifikace zákazníka, anebo dle bezpečnostních politik zákazníka.
89	Obohacení dat	Možnost přidat nové zdroje bezpečnostních informací, ať už volně dostupných nebo komerčních či proprietárních	Ano	Viz bod 81
90	Obohacení dat	Možnost využít externích zdrojů dat pro obohacení událostí přidáním dalšího kontextu (souvislosti), a/nebo vytvoření specifičtějšího korelačního vyhledávacího dotazu	Ano	Viz bod 81
91	Obohacení dat	Nová externí data (threat feed, obohacení dat) mohou být aplikována na již dříve indexovaná data pro usnadnění vyhledání nebo reportování, které jde zpět do historie v řádu dnů, měsíců či let.	Ano	Viz bod 81. Data je možné prohledávat zpětně.
92	Obohacení dat	Při normalizaci lze provádět datový enrichment (Doplnit jméno počítače na základě jeho IP adresy, doplnit lokalitu dle GEO informace, provést dotaz do LDAP apod.)	Ano	Je možné doplnit DNS jméno na základě DNS dotazu, nebo informace z CMDB. Je možné získat GEO informace pomocí příkazu iplocation, případně lze využít externích geolokací například pomocí IPInfo. Lze dělat i další obohacení - WhoIs, LDAP, …
93	Obohacení dat	Systém vede evidenci aktiv a identit a jejich klasifikaci, která je využívána pro výpočet kritičnosti událostí a incidentů. Evidenci je možno plnit ručně nebo z externích zdrojů	Ano	SIEM obsahuje modul Asset and Identity Management, který zajišťuje tuto funckionalitu. https://docs.splunk.com/Documentation/ES/7.2.0/Admin/Manageassetsandidentities
94	Vyšetřování a reakce	Case management a definice workflow musí být integrální součástí SIEM řešení	Ano	Case management i workflow jsou nedílnou součástí SIEMu. Case management je popsán zde: https://docs.splunk.com/Documentation/ES/7.2.0/Admin/Iroverview Workflow je popsáno zde: https://docs.splunk.com/Documentation/Splunk/latest/Knowledge/CreateworkflowactionsinSplunkWeb
95	Vyšetřování a reakce	Dotaz do uložených dat může být tvořen manuálně přímo v dotazovacím poli nebo s využitím „průvodce" (wizzardu)	Ano	Uživatel může psát dotazy pomocí dotazovacího jazyku SPL. Druhou možností je využít funkce Splunk Datasets, kde se pomocí průvodce v UI vytváří tzv Table View - https://lantern.splunk.com/Splunk_Platform/Product_Tips/Data_Management/Using_Table_Views_to_prepare_data_without_SPL
96	Vyšetřování a reakce	Dotazy umožní uživateli získávat data na základě kdo, co, kdy a kde	Ano	Uživatel má dvě možnosti jakým způsobem se dotazuje na data. Jedním přístupem je full-text prohledávání. Druhým způsobem je dotazování na základě hodnot a klíče/pole (field). Tyto pole se vytvářejí při zpracování dotazu na základě tzv parsingu. Po dokončení parsingu má uživatel dostupné pole jak systémové tak i vyparsované z vlastní zprávy. - Kde - lze využít field host, source - Kdy - timestamp události - Co - vlastní log popřípadě specifické pole - Kdo - pokud je informace obsažena v logu, pak bývá ve parsovaném fieldu typicky - user, src_user, dest_user, apod.
97	Vyšetřování a reakce	Flexibilní a uživatelsky intuitivní vyhledávací jazyk pro tvorbu vlastních dotazů, reportů a korelačních pravidel včetně možnosti vytváření vlastních „parserů" dat umožňujících samostatně a jednoduše tvořit bez závislosti na placené asistenci nebo rozšířeních tvůrce technologie či technologického partnera) – s využitím regulárních výrazů, průvodců (wizzards) apod. S pomocí vyhledávacího jazyka lze kdykoliv vytvořit jakýkoliv korelační scénář.	Ano	Splunk si vyvinul vlastní vyhledávací jazyk inspirovany tim nejlepším z SQL a Linuxu. Z Linuxu si vzal možnost řetězit příkazy pomocí pipeline '|'. Z SQL si vzal základní sestavováním dotazu a skládání podmínek pomocí logických operátorů. SPL dotazovací jazyk je jediným jazykem v systému a je použít v celém systému Splunk. Pro méně znalé uživatele lze využít Datasets a Analytics Workspace, kdy pomocí Průvodců(Wizardů) lze sestavit SPL dotaz v UI. Výsledkem je pak kompletní SPL dotaz. Pomocí regulárních výrazů v příkazu 'rex' lze přímo v SPL dotazu dokončit parsování polí. Korelační scénář je z pohledu Splunku uložený dotaz v jazyku SPL s dalším nastavením - jako například provedení workflow akce.
98	Vyšetřování a reakce	Jednotlivé dotazy lze do sebe „vnořovat"	Ano	Jazyk SPL umožňuje tzv. vnořené dotazy (https://docs.splunk.com/Documentation/Splunk/9.1.1/SearchTutorial/Useasubsearch), přičemž výsledková množina vnořeného dotazu slouží jako vstup do nadřazeného dotazu.
99	Vyšetřování a reakce	Jednotlivé příkazy vyhledávacího dotazu je možné řetězit podobně jako v unixových systémech, čímž je vytvořena jedna komplexní podmínka aplikovaná na data v dashboardu	Ano	Splunk SPL dotazovací jazyk (https://docs.splunk.com/Documentation/Splunk/9.1.1/SearchTutorial/Usethesearchlanguage nebo https://docs.splunk.com/Documentation/Splunk/9.1.1/Search/Aboutsearchlanguagesyntax) využívá to nejlepší ze SQL a *nix syntaxe, což mj. umožňuje zřetězení operací a podmínek v dotazech pomocí operátoru "|".
100	Vyšetřování a reakce	Ke každému vyhledávání je možné zobrazit detailní (debug) informace pro odladění chyb ve vyhledávání	Ano	Splunk web GUI poskytuje nástroj "Job Inspector" (https://docs.splunk.com/Documentation/Splunk/latest/Search/Viewsearchjobpropertieswiththe JobInspector), který nabízí detailní přehled o jednotlivých fázích provádění SPL dotazu včetně informací potřebných k odladění chyb a optimalizaci každého dotazu.
101	Vyšetřování a reakce	Možnost zadání ad-hoc dotazu do vyhledávacího pole pomocí vyhledávacího jazyka	Ano	Splunk umožňuje kdykoliv zadat tzv. ad hoc dotaz (https://docs.splunk.com/Splexicon:Adhocsearch) , jehož zpracování má vždy prioritu před naplánovanými dotazy (scheduled searches). Jako dotazovací jazyk se používá SPL - https://docs.splunk.com/Documentation/Splunk/9.1.1/SearchReference/UnderstandingSPLsyntax

102	Vyšetřování a reakce	Možnost definice vlastních vyhledávacích příkazů, které můžou být využiti v grafickém prostředí pro vyhledávání a práci s indexovanými daty	Ano	Splunk podporuje rozšíření funkcionalit SPL o vlastní vyhledávací funkce (tzv. custom search commands). Postup je popsán na https://dev.splunk.com/enterprise/docs/devtools/customsearchcommands/ . Tyto příkazy je možné využívat jak v dotazovacím poli aplikace Search and Reporting, tak i ve vizuálním návrháři dashboardů.
103	Vyšetřování a reakce	Možnost definovat workflow včetně provedení automatické a semiautomatické akce: až po ověření a schválení analytikem (ten prověří, zda se nejedná o false positive)	Ano	Krok ověření nebo schválení analytikem je zakončen změnou stavu u události. Na tento stav lze navázat jiný samostatný seznam akcí, které může operátor semiautomatizovaně spustit, případně pomocí samostatného jobu lze zajistit automatické spuštění.
104	Vyšetřování a reakce	Možnost definovat workflow včetně provedení automatické a semiautomatické akce: ihned po detekci incidentu	Ano	Na každé detekční pravidlo lze navázat i tzv Adaptive Response Action, které se automaticky provádějí ihned po detekci. Slouží například k obohacení události o další data, nebo k integraci s externím ticket systémem apod.
105	Vyšetřování a reakce	Možnost prohledávat celý text na jakékoliv pole v indexovaných datech na základě klíčových dat a časových úseků v rozsahu konkrétní nebo relativní časové okno na úrovni M/D/m/s	Ano	Splunk SPL umožňuje vyhledávání jak pomocí pojmenovaných polí/atributů, tak i v režimu full text search. Je možné pracovat jak s originálním logem v původním tvaru, ale také v rámci SPL dotazu definovat klíčová pole díky tzv. Schema on Read. Časová kritéria pro dotaz nejsou nijak omezena, je možné hledat real time, případně specifikovat časový interval jak konkrétními hodnotami data a času, tak relativně vztaženo k aktuálnímu okamžiku. https://docs.splunk.com/Documentation/Splunk/9.1.1/Search/Selectiti merangestoapply https://docs.splunk.com/Documentation/Splunk/9.1.1/SearchReference/Commontimeformatvariables
106	Vyšetřování a reakce	Možnost prohledávat celý text, jakékoliv pole v indexovaných datech na základě: - Klíčových slov - Časové úseky - Konkrétní nebo relativní časová okna na úrovni měsíce, dne, minuty, vteřiny - Logické operátory („AND“, „OR“, „XOR“,“NOT“, atd.) - Regulární výrazy - Syntaxe zástupných (wildcard) meta znaků	Ano	viz bod 105, samozřejmá je podpora logických operátorů (https://docs.splunk.com/Documentation/Splunk/9.1.1/SearchReference/UnderstandingSPLsyntax#Boolean_operators) i wildcards (https://docs.splunk.com/Documentation/Splunk/9.1.1/SearchReference/UnderstandingSPLsyntax#Fields_and_wildcard_fields). Regulární výrazy jsou hlavním nástrojem pro extrakci datových polí a to jak během tzv. indexing time, ale také v době spuštění dotazu (https://docs.splunk.com/Documentation/Splunk/9.1.1/SearchReference/Rex)
107	Vyšetřování a reakce	Možnost spustit více souběžných dotazů	Ano	Splunk umožňuje běh více dotazů na najednou. Spouštění jednotlivých dotazů lze naplánovat v čase, mj. pomocí cron scheduleru. Omezení max. počtu současně spuštěných dotazů je dáno zejména možnostmi HW. Čím více prostředků (zejména CPU jader), tím více SPL dotazů můžeme spustit. Pokud dojde k překročení limitu, Splunk zařadí dotaz do fronty a spustí jej jakmile je potřebná HW kapacita k dispozici.
108	Vyšetřování a reakce	Možnost uložení finálního dotazu jako dashboard, report, alert nebo novou událost	Ano	Jednotlivé dotazy je možné přímo uložit do libovolného dashboardu, případně je lze uložit jako reportu (savedsearch) a ten následně napojit jakožto zdroj na dashboard. Z výsledků dotazu je také možné snadno vytvořit nové události pomocí příkazu collect (https://docs.splunk.com/Documentation/Splunk/9.1.1/SearchReference/Collect).
109	Vyšetřování a reakce	Možnost volitelného „vzorkování“ – rychlejší prezentace výsledků zobrazením každého n-tého paketu	Ano	v rámci grafického prostředí je možné zvolit při vyhledávání parametr sampling a zvolit si tak vzorkování výsledkové množiny podle potřeby (https://docs.splunk.com/Documentation/Splunk/9.1.1/Search/Retrieveasamplesetofevents). Toto nastavení má vliv na prohledávané události tak i na prohledávané packety.
110	Vyšetřování a reakce	Musí podporovat využití Machine Learning nástrojů pro indentifikaci opakujících se vzorů v datech, detekci anomálií a prediktivní analýzu dat	Ano	Splunk nabízí ucelenou sadu nástrojů a algoritmů ML v rámci Machine Learning Toolkit (https://www.splunk.com/en_us/products/machine-learning.html). Aplikace je instalována jako součást balíku Splunk Enterprise Security, ale je dostupná i samostatně na SplunkBase (https://splunkbase.splunk.com/app/2890).
111	Vyšetřování a reakce	Musí umožňovat nad daty provádět statistické výpočty a analýzy (min, max, median ...)	Ano	Splunk podporuje komplexní sadu statistických výpočtů. Dokumentace je uvedena na https://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Stats#Stats_function_options
112	Vyšetřování a reakce	Podpora akce: Odeslání emailu	Ano	Pro každý alert/report je možné vybrat response action s akcí Send Email https://docs.splunk.com/Documentation/ES/7.2.0/Admin/Configureadaptiveresponse. V těle mailu lze nadefinovat vlastní text, vypsat výsledky běhu alertu nebo je případně připojit jako přílohu.
113	Vyšetřování a reakce	Podpora akce: Spuštění skriptu	Ano	V rámci response action je podporována akce Run a script https://docs.splunk.com/Documentation/ES/7.2.0/Admin/Configureadaptiveresponse, která umožní spustit libovolný externí script nebo příkaz.
114	Vyšetřování a reakce	Podpora akce: Založení tiketu v interním case tracking systému	Ano	Je možné spustit response action s akcí Create Notable event https://docs.splunk.com/Documentation/ES/7.2.0/Admin/Configureadaptiveresponse. Jsou také k dispozici add-ony poskytující integraci např. se ServiceNow, PagerDuty, JIRA atd.
115	Vyšetřování a reakce	Podpora akce: Zápis do souboru	Ano	Je možné spustit response action s akcí Run a script s přesměrováním výstupu do souboru https://docs.splunk.com/Documentation/ES/7.2.0/Admin/Configureadaptiveresponse Případně lze vytvořit custom akci, nebo custom workflow a přizpůsobit akci konkrétním potřebám.
116	Vyšetřování a reakce	Podpora vyhodnocovaní událostí z webového rozhraní	Ano	Všechny události je možné vyhodnocovat přes Webové rozhraní dostupné na HTTP nebo HTTPS. Je možné zde také obohatit události o další atributy např. z externích zdrojů, doplnit kontext o další vyhledávací dotazy, případně dodat informace o dalších assetech, dotčených danou událostí, doplnit screenshoty atd. V rámci investigation workflow pak je možné přehledně zobrazit průběh investigace v čase, přidané poznámky a artefakty včetně informací, kdy a kdo do investigace čím přispěl.
117	Vyšetřování a reakce	Provádět statistické operace pro nalezení extrému (anomálie)	Ano	Dotazovací jazyk SPL (Splunk Processing Language) poskytuje rozsáhlou podporu pro provádění statistických operací. Například můžete použít příkazy jako stats, timechart nebo tstats k výpočtu statistických metrik (min, max, avg, stdev atd.) na základě kterých lze detekovat anomálie. Jsou také k dispozici funkce statistického rozložení jako např. percentil aj. Možné metody identifikace anomálií jsou popsány přehledně na https://docs.splunk.com/Documentation/Splunk/latest/Search/Findandremovingoutliers
118	Vyšetřování a reakce	Schopnost stanovit “normál” a pak aplikovat výše uvedené statistické operace pro nalezení extrému (anomálie), jež může být pokročilou hrozbou (APT), na kterou nelze aplikovat signaturu	Ano	Splunk poskytuje ucelenou sadu nástrojů pro odhalení a obranu proti APT. Kromě identifikace normálních vzorců chování u uživatelů ("baselining") a detekci anomálií je to také podpora procesů Risk Managementu, Asset Identification a scoring i Vulnerability management. Detailní popis je zde: https://www.splunk.com/en_us/blog/learn/apts-advanced-persistent-threats.html
119	Vyšetřování a reakce	Statistická analýza včetně: - Počet výskytů, počet unikátních výskytů, součet - Nejběžnější hodnoty, nejméně běžné hodnoty polí - Minimum, maximum - Průměr, modus, medián, atd. - Standardní odchylka, rozptyl - Identifikace anomálních hodnot ve výsledcích, které mohou být nepravidelné, neobvyklé - Statistická korelace mezi atributy - Shlukování událostí podle jejich podobnosti k sobě samým jako jedna událost - Ořezávání extrémních numerických hodnot ve vybraných polích při statistické korelaci - První a poslední nalezená hodnota - Percentil - Predikované hodnoty (dotaz se dívá na historická data, aby matematicky předpověděl budoucí hodnoty) - Sloučení, rozdíl nebo průnik individuálních nebo vícero výsledků hledání - Hledej vztahy mezi páry atributů porovnáním hodnot prvního atributu vůči hodnotám druhého atributu	Ano	Splunk umožňuje statistické výpočty. Dokumentace je uvedena na https://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Stats. Pro predikci hodnot na základě dat z minulosti je k dispozici např. příkaz "predict" (viz https://docs.splunk.com/Documentation/Splunk/9.1.1/SearchReference/Predict), pro pokročilejší modelování pak lze využít Machine Learning Toolkit.
120	Vyšetřování a reakce	Systém umožňuje notifikaci přes email, SMS, MS TEAMS, s možností definovat pravidla pro zasílání na různé adresy podle kritičnosti zdroje nebo celkového vyhodnoceného rizika události	Ano	Splunk podporuje odeslání notifikace pomocí SMS více způsoby. Jedním způsobem je využití API rozhraní u operátora SMS, dalším způsobem je odeslání specifického emailu na operátora SMS služby a poslední možností je využití lokální SMS brány. Pro všechny způsoby existuje plná podpora v systému. Příklad existujících addonů: https://splunkbase.splunk.com/app/4046 https://splunkbase.splunk.com/app/2865 Integrace MS Teams viz bod 86
121	Vyšetřování a reakce	Systém umožňuje vyhledávání log záznamů, událostí a incidentů dle zadané kombinace tagů a dalších podmínek (dle časových kritérií, typu zdroje, IP adresy, uživatele)	Ano	viz bod 105. SPL nijak neomezuje množinu atributů, podle kterých lze vyhledávat. Je možno i během provádění dotazu přidat vlastní nová pole a podmínky libovolně kombinovat. Obohacení o tzv. tagy je samozřejmostí.

122	Vyšetřování a reakce	Ve vyhledávacím dotazu je možné se odkázat na jakékoliv pole nebo atribut z přijaté události a v podmínce očekávat konkrétní hodnotu (např. uživatel je z konkrétní skupiny v Active Directory, IP adresa je z konkrétní sítě (IP rozsah, výčet IP, CIDR formát, atd.), název aplikace odpovídá regulárnímu výrazu nebo řetězci apod.)	Ano	viz bod 121 Systém podporuje i dotazování pomocí CIDR - https://docs.splunk.com/Documentation/Splunk/9.1.1/SearchReference/Search#CIDR_matching
123	Vyšetřování a reakce	Vyhledávací dotaz může být jednoduše uložen, sdílen nebo upraven v rámci systému	Ano	Dotaz je může být uložen jako report, alert nebo obecně saved search. Tyto dotazy je možné sdílet mezi uživateli nebo aplikacemi, případně v rámci celého systému. Sdílení se řídí podle nastavených přístupových práv.
124	Vyšetřování a reakce	Výhledávání a vizualizace pokrývají základní oblasti pro dohled a analýzu – přístupy, koncová zařízení, síťová komunikace, zúčastněné entity (lidé a zařízení)	Ano	Splunk Enterprise Security poskytuje více jak 100 vizualizací (Dashboardů) které v základu dělí na Security Inteligence(User Inteligence, Web Inteligence …), Security Domain (Access, Network, Domain, Identity), Cloud security (Microsoft 365 …). Pod každou kategorii jsou dostupné další upřesňující podkategorie.
125	Vyšetřování a reakce	Vyhledávání může být v reálném čase nebo naplánované	Ano	V grafickém prostředí je možné pod položkou Time Range Picker zvolit vyhledávání v reálném čase, nebo v libovolném časovém okně. Je možné provádění jednotlivých dotazů naplánovat tak, aby se nám pravidelně předpočítaly a z každého běhu tak získat požadovaný výsledek. https://docs.splunk.com/Documentation/Splunk/9.1.1/Search/Aboutrealtimesearches
126	Vyšetřování a reakce	Systém umožňuje definovat jakékoliv vlastní příkazy. Tyto příkazy je možné používat minimálně v rámci vyhledávání, korelací a reportů. Vlastní příkazy je možné za sebou řetězit a není omezeno, v jaké části vyhledávání je možné je použít.	Ano	Splunk umožňuje definovat vlastní příkazy, které se pak stávají rovnocennou součástí množiny příkazů/funkcí SPL. Tyto příkazy lze pomoci operátoru "|" řetězit a kombinovat podle potřeby a v libovolné části SPL dotazu. Postup je popsán https://dev.splunk.com/enterprise/docs/devtools/customsearchcommands/
127	SIEM	Automatická aktualizace parsovacích pravidel pro zpracování logů od výrobce zařízení	Ano	Pokud systém má přístup do internetu na speciální server vendora, provádí automatickou kontrolu aktuálnosti všech komponent a také všech přídavných modulů. Z důvodů zabezpečení správné funkce, neprovádí systém automatickou aktualizaci žádné komponenty, tedy ani žádného modulu a ani parsovacích pravidel. Nové pravidla mohou být v kolizi z jinými uživatelskými nastaveními anebo uživatelským parsingem. Proto vždy doporučujeme jakékoliv aktualizace předem ověřit, než se nainstalují. Pokud by ale byla vyžadována automatická aktualizace, lze zajistit naplánováním potřebného scriptu i pravidelnou aktualizaci.
128	SIEM	Definice časového okna pro sledování korelace (okno aspoň 1 týden)	Ano	časové okno pro sledování korelace není omezeno. Tedy korelace může být provedena i nad všemi uloženými daty.
129	SIEM	Desítky korelačních vyhledávacích dotazů: - Existující dotazy mohou být snadno modifikovány a vytvořeny tak nové dotazy - Každý dotaz má automaticky přiřazenu konfigurovatelnou hodnotu závažnosti, vlastníka a stav	Ano	Splunk Enterprise Security obsahuje 80+ integrovaných pravidel. Splunk nabízí pomocí aplikace dalších cca 1400 připravených korelací. Tyto korelace lze podle potřeby upravovat a dále rozšiřovat. https://splunkbase.splunk.com/app/3449
130	SIEM	Detailní pohled na každý incident, který zahrnuje: - Automaticky doplněný kontext o aktivech a identitách z externích zdrojů - Původní události, které představují incident - Historie postupu zpracování události (workflow) – kdo, co, kde, kdy, jak, čím, … - Rozbalovací nabídka možností ke každému relevantnímu poli, která usnadňuje směrovat vyšetřování další cestou - Rozbalovací nabídka možností ke každé události, která usnadňuje směrovat vyšetřování další cestou - Možnost manuálně změnit závažnost incidentu, vlastníka, status a stejně tak přidat k incidentu poznámku	Ano	Splunk umožnuje řešit události na dvou místech. První místo kde jsou dostupné veškeré události je Incident Review. Slouží pro prvotní analýzu a rozhodnutí zda je záchyt relevantní nebo zda se jedná o False-Positive. Je zde možné měnit stav události/incidentu, přidávat/měnit řešitele a zobrazovat další klíčové informace. Pokud je potřeba náročnější řešení/investigaci události, lze vytvořit samostatnou investigaci k danému incidentu. K investigaci pak přísluší samostatný dashboard poskytující detailní informace o postupu šetření incidentu. K dispozici je také workflow, časová osa, kde jsou vidět zaznamenané události a komentáře uživatelů k incidentu. Umožnuje snadno dohledávat další informace podle detekovaných assetů. Je tak k dispozici celkový pohled na incident, jeho stav, kdo incident řeší a jednotlivé kroky šetření. více https://docs.splunk.com/Documentation/ES/7.2.0/User/IncidentReviewdashboard a https://docs.splunk.com/Documentation/ES/7.2.0/User/Timelines
131	SIEM	Hlídání prahových hodnot (např. počítání přenesených bajtů)	Ano	Splunk umožnuje počítat statistiku (např. počet přenesených bajtů, průběžně i sumárně) a při překročení prahové hranice vyvolat specifickou akci (například poslat email, nebo založit ticket v externím IMS)
132	SIEM	Je možno sledovat stav řešení incidentů a měnit jejich důležitost	Ano	Je možné využít Splunk ES dashboard Incident review, který ukazuje přehled jednotlivých stavů událostí. Zde je možné i doplnit další podstatné údaje pro investigaci, případně měnit závažnost.
133	SIEM	Jeden dotaz nebo report může zahrnout všechna indexovaná data	Ano	Jazyk SPL neomezuje množinu prohledávaných dat, pomocí wildcards je možno jedním dotazem provést vyhledání ve všech indexovaných datech. Jediným limitem jsou nadefinovaná přístupová oprávnění uživatele, který dotaz spouští.
134	SIEM	K dispozici musí být funkce typu „Tail" zobrazující aktuálně příchozí logy na základě podmínek definovaných analytikem	Ano	Pro zobrazení záznamů a zároveň soustavný monitoring přírůstků v log streamu je k dispozici tzv. Real-time search (https://docs.splunk.com/Splexicon:Realtimesearch). Tento mechanismus umožňuje na základě zadaného klouzavého okna v čase (např. 30s) zobrazit živý pohled na stream dat tak, jak přichází do Splunku. Případně existuje příkaz "TAIL", pomocí kterého lze zobrazit poslední X logů - https://docs.splunk.com/Documentation/Splunk/9.1.1/SearchReference/Tail
135	SIEM	K incidentu je možno přiřadit výsledky dalšího vyhledávání souvislostí	Ano	K incidentu v rámci šetření pomocí Investigations je možné přidávat další výsledky vyhledávání, komentáře a další atributy jako např. geolokační informace apod. Vlastnosti assetů, pokud jsou dohledány v databázi Asset&Identity Management, jsou doplněny automaticky.
136	SIEM	Každé korelační pravidlo má automaticky přiřazenu konfigurovatelnou hodnotu závažnosti, vlastníka a stavu (dotazu lze nastavit uvedené defaultní hodnoty)	Ano	Každé korelační pravidlo má definovanou závažnost, tzv. risk score. Tato závažnost se následně upravuje podle dalších kritérií jako je např. důležitost assetu, ke kterému se událost vztahuje. V rámci investigation workflow lze přednastavené hodnoty vždy upravit a případně incident přidělit jinému vlastníkovi. Sadu přednastavených atributů určuje a spravuje Splunk Enterprise Security administrátor.
137	SIEM	Korelace logů mezi různými zdroji a typy zařízení	Ano	Korelace není omezena na jednotlivé zdroje dat. Jazyk SPL umožňuje vyhledávat napříč všemi zdroji. Viz také bod 133
138	SIEM	Korelace na základě počtu výskytů nebo naopak na základě chybějícího logu	Ano	Korelace je možné vyhodnocovat jak na základě hodnot v konkrétním poli/polích se kterým se pracuje v korelačním pravidle, tak i např. v závislosti na počtu vrácených výsledků. Je také možné upravit podmínku tak, aby byla splněna v případě neexistence/nedohledání konkrétního záznamu. Pro zjednodušení reportingu výpadku logů vznikla i specializovaná aplikace - https://splunkbase.splunk.com/app/3247
139	SIEM	Korelační pravidla musí umožňovat provázání a vizualizace s frameworkem MITRE ATT&CK	Ano	Jednotlivá korelační pravidla vycházejí z frameworku MITRE ATT&CK. Z něj také odvozují svoji identifikaci a v přehledném dashboardu aplikace Splunk Security Essentials je graficky znázorněno mapování dat a definovaných use cases na tento framework, včetně identifikace chybějících datových zdrojů. https://splunkbase.splunk.com/app/3435
140	SIEM	Modul pro sledování shody s nařízením GDPR	Ano	Pomocí rozšíření GDPR Compliance lze analyzovat a vyhodnocovat uložené logy, zda neobsahují citlivá data z pohledu GDPR. Rozšíření poskytuje tři ridhboardy - Identifikace citlivých dat a kategorizace, Přístup k citlivým datům a Přenos citlivých dat.
141	SIEM	Monitoring v reálném čase, varování na známé i neznámé (tzv. APT) hrozby	Ano	Na známé i neznámé hrozby můžeme reagovat s využitím RBA (Risk Based Alerting), pomocí vyhodnocování a baseliningu chování uživatelů (UBA), případně zapojit Machine Learning pro vyhodnocení odchylek v "normálním" provozu. Viz také bod 118
142	SIEM	Možnost definicí korelace v grafickém rozhraní a jejich následné vyhodnocení nad zpracovanými daty	Ano	Korelace se dají definovat jak v grafickém prostředí (viz bod 95) tak i pomocí textových konfiguračních souborů. Vyhodnocení je následně dostupné v dashboardu Incident review.
143	SIEM	Možnost definovat vlastní parsovací pravidla pro zpracování nepodporovaných logů na základě regulárních výrazů.	Ano	Splunk umožňuje tvorbu vlastních modulů pro parsing nepodporovaných technologií a zdrojů dat. Je k dispozici kompletní SDK pro vývoj, příklady a dokumentace. Při definici regulárních výrazů pro parsing datového streamu je také možné využít interaktivního průvodce ve Splunk GUI.
144	SIEM	Možnost manuálně změnit závažnost incidentu, vlastníka, status a stejně tak přidat k incidentu poznámku	Ano	Jednotlivé parametry incidentu je možné měnit v rámci Splunk ES v dashboardu Incident review, dále pak při následném vyhodnocování a řešení v rámci workflow v Investigations. Viz také bod 136
145	SIEM	Možnost řetězení korelací	Ano	Splunk Enterprise Security podporuje možnost řetězení korelačních dotazů pomocí Sequence templates. Korelace je možné řetězit na základě definovaného pořadí událostí, podle specifických atributů, případně jejich kombinace. Kompletní popis je k dispozici na https://docs.splunk.com/Documentation/ES/7.2.0/Admin/Sequencecorrelationsearches

146	SIEM	Musí umožnit provádět pokročilé analytické behaviorální analýzy v reálném čase	Ano	Splunk podporuje provádět pokročilé behaviorální analýzy. Systém poskytuje více možných řešení a přístupů. Dostupné jsou standardní analytické funkce, lze využít Machine Learning modul, lze využít aplikaci Splunk App for Behavioral Profiling nebo lze využít externích knihoven jako například pro jazyk python knihovny pandas a numpy.
147	SIEM	Porovnávání hodnot ve vybraných atributech události	Ano	Pro porovnání hodnot ve vybraných atributech je možné využít příkaz eval, který obsahuje funkce jako if, case, … viz https://docs.splunk.com/Documentation/Splunk/9.1.1/SearchReference/CommonEvalFunctions nebo https://docs.splunk.com/Documentation/Splunk/9.1.1/SearchReference/Eval
148	SIEM	Řešení musí korelovat informace o správě identit a přístupů s ostatními strojovými daty shromážděnými v infrastruktuře, aby porozumělo chování uživatelů a identifikoval neobvyklou aktivitu uživatelů.	Ano	Systém si vytváří tzv baseline pro identity a entity a následně provádí analýzu, zda chování odpovídá dříve definované baseline. Pokud je chování odlišné, pak se detekuje anomálie. K této funkcionalitě jsou dostupná i sada reportů a dashboardů
149	SIEM	Řešení musí poskytovat techniky detekce hrozeb včetně pokročilé korelace, rozpoznávání vzorů, blacklistu a whitelistingu a statistické analýzy	Ano	Techniky detekce lze rozdělit na 3 kategorie. První kategorií jsou detekce podle paternu (vzorky, opakující se akce, blacklisty) včetně využití statistické analýzy. Druhá kategorie jsou pokročilé korelace pomoci Risk Base Alerting (RBA). Sledují se příznaky chování, které se následně vyhodnocují. Poslední kategorii jsou pravidla založená na Machine Learning, kde se sledují odchylky od standartního chování. Ve všech případech lze aplikovat blacklisty a whitelisty.
150	SIEM	Řeší všechny hlavní případy užití SIEM nástroje včetně (nejen): - Log management - Dokumentace a audit průběhu šetření v čase (log book) - Forenzní přístup (dashboardy, nástroje, workflow) - Tvorba vlastních bezpečnostních reportů, reportů na soulad s normami, vizualizace - Monitoring v reálném čase, varování na známé i neznámé (tzv. APT) hrozby - Schopnost provádět korelace přes více datových zdrojů a hledání specifických vzorů - Dlouhodobá retence dat	Ano	Jednotlivé body jsou zodpovězeny v přechozích otázkách. Splunk jakožto analytická platforma pro práci s big daty využívá přístupu "one platform - many lenses". Nad jednotnou datovou základnou pro Log management i SIEM tak umožňuje jak práci s vlastními logy, tak i detekci hrozeb napříč všemi zdroji dat. Díky využití jazyka SPL a prací s originálními daty, uchovávanými v původním tvaru, nejsou jeho možnosti omezovány. Viz popis na https://www.splunk.com/en_us/products/splunk-enterprise-security-features.html Pro podporu forenzní analýzu jsou ve Splunk připravené dashboardy, rozdělené do skupin. Tyto dashboardy jsou přístupné formou akce přímo z vyšetřovaného incidentu a automaticky jsou vyplněné potřebné filtry podle polí z incidentu.
151	SIEM	Schopnost provádět korelace přes více datových zdrojů a hledání specifických vzorů	Ano	Splunk umožňuje prohledávat všechna data, která jsou v rámci platformy zaindexována. Viz také bod 133. Je možné hledat specifické vzory napříč všemi datovými zdroji/technologiemi. Jsou k dispozici nástroje Machine Learningu pro hledání specifických vzorů v datech, které využívá např. Splunk ES dashboard Access Anomalies.
152	SIEM	SIEM počítá baselines pro identifikaci nestandardního chování konkrétních zdrojů logů	Ano	Jak již bylo odpovězeno v otázce 146, 148, 141 a 118, Splunk dokáže počítat baseline a detekovat odchylky, dokáže využít Machine Learning modulu, popřípadě i Behaviorální analytiku. Všechny tyto možnosti lze aplikovat na libovolný objekt, tedy na Asset/zařízení, na uživatele a tak i na celý zdroj logů.
153	SIEM	SIEM umožňuje zpracování dat ze skenerů zranitelností	Ano	V rámci Common Information Model je připraven standardní dataset Vulnerabilities (https://docs.splunk.com/Documentation/CIM/5.2.0/User/Vulnerabilities) který umožňuje sdružit data z různých zdrojů skenerů zranitelnosti. Nezávisle na technologii pak pomocí normalizace dat tyto informace zpřístupňuje pro vyhledání, zpracování a zobrazení v dashboardech.
154	SIEM	Sledování odchylek vůči baseline	Ano	Ke sledování odchylek je možné použít statistickou analýzu nebo Machine Learning pravidla. Pravidla se naučí chování podle připraveného vzorku a pokud je odchylka větší než definovaný threshold oproti baseline, vytvoří se událost.
155	SIEM	Systém automaticky počítá míru rizika (risk score) pro jednotlivá aktiva a identity dle jejich klasifikace a reálně zjištěných událostí a incidentů	Ano	Splunk využívá Risk Based Alerting přístupu, kdy je jednotlivým aktivům v rámci Asset managementu přiřazena priorita/závažnost. Tato priorita je pak brána v úvahu při vyhodnocování korelačních pravidel, která se vztahují ke konkrétnímu assetu. RBA tak umožňuje stanovit risk score incidentu v závislosti na závažnosti jednotlivých dotčených aktiv, a spustit alert teprve při překročení definované úrovně rizika. Tím významně přispívá ke snížení počtu tzv. False positive alertů. Mimo to Splunk ES poskytuje dashboard Risk Analysis, ve kterém přehledně zobrazuje a kategorizuje aktiva podle aktuální míry rizika. Zde je např. možné identifikovat assety, u kterých došlo k výraznému nárůstu aktivity apod.
156	SIEM	Systém obsahuje 100+ připravených korelačních pravidel	Ano	Splunk Enterprise Security obsahuje v základu 90+ korelačních pravidel. Tento základ lze doplnit pomocí Splunk ES Update Content add-onu (https://splunkbase.splunk.com/app/3449) o dalších 1400+ korelačních pravidel, které jsou pravidelně doplňovány a aktualizovány. Korelační pravidla vycházejí z MITRE ATT&CK frameworku.
157	SIEM	Systém obsahuje workflow pro podporu řešení detekovaných událostí a incidentů. Incidenty je možno přiřadit řešiteli.	Ano	Každou událost/incident lze přiřadit řešiteli, případně řešitel může řešení incidentu předat na jiného řešitele. Workflow pro definici přechodu stavů pro incident nebo pro investigaci je plně konfigurovatelné. Lze definovat nové stavy a definovat přechody mezi stavy https://docs.splunk.com/Documentation/ES/7.2.0/Admin/Investigationstatus
158	SIEM	Systém počítá risk score dle zdroje a cíle události nebo incidentu a na základě toho je stanovena závažnost aktuálně detekované události	Ano	viz bod 155
159	SIEM	Systém průběžně hodnotí rizika a poskytuje up-to-date informace o stavu rizik	Ano	viz bod 155. Kategorizace assetů podle rizik je dostupná v dashboardu Risk Analysis.
160	SIEM	Systém umožňuje automatické stahovaní Threat feed z internetu/externího zdroje dat	Ano	Splunk poskytuje modul Threat Intelligence Management, kde je možné spravovat přednastavené zdroje threats. Informace z těchto zdrojů lze využít pro vyhodnocení, případně obohacení incidentů, viz popis na https://docs.splunk.com/Documentation/ES/7.2.0/Admin/Includedthreatintelsources. Je též možné přidat vlastní zdroje, postup zde: https://docs.splunk.com/Documentation/ES/7.2.0/Admin/Addthreatintelcustomlookup
161	SIEM	Systém umožňuje automatické vyhodnocování událostí na základě informací obsažených v Threat feed	Ano	Splunk Threat Intelligence pravidelně automaticky aktualizuje seznamy hrozeb z nastavených a povolených zdrojů. Data přicházející do Splunk platformy jsou pak kontrolována oproti tomuto seznamu během indexace a začlenění do datových modelů, se kterými pracuje splunk ES. Pokud je nalezena shoda, automaticky se založí Alert. Detailní popis funkce threat intelligence frameworku je dostupný na https://dev.splunk.com/enterprise/docs/devtools/enterprisesecurity/threatintelligenceframework/
162	SIEM	Systém umožňuje přidávat Risk score na jednotlivé assety (uživatel, it zařízení, uživatelsky definované,...), čímž může být ovlivněna závažnost detekovaných událostí.	Ano	Splunk umožňuje v rámci spouštění korelačních pravidel mimo vytváření alertů (notable event) také vytvářet risk score, které se přidává jednotlivých assetům/identitám nalezeným v rámci detekce. Tato Risk score je možné následně agregovat do souhrnné informace o rizikovosti jednotlivých assetů/identit. Toto skóre můžeme také propojit se zachycenými událostmi v rámci notable event a pokud je Riziko na daném assetu velké, je možné zvýšit závažnost detekované události. Tedy ke zvýšení závažnosti dojde na základě předchozího vývoje Risk Score.
163	SIEM	Uzivatel si muže definovat vlastní parsing, který neovlivňuje další uživatele ani zbytek systému	Ano	Každý uživatel Splunku využívá globální konfiguraci, kterou si může podle své potřeby upravit. Úpravy konfigurace, jakou je mj. i parsing data streamu, se ukládají v uživatelském profilu, který je oddělený od ostatních uživatelů. Je tak zajištěno, že tyto změny ostatní uživatele neovlivní. Zároveň mají tyto lokální změny prioritu v konfiguraci před ostatními konfiguracemi, takže jsou platné pouze v kontextu daného uživatele. Pokud je administrátorem Splunk deploymentu přiděleno uživateli odpovídající oprávnění, je pak možné lokální změny zpřístupnit i ostatním uživatelům v rámci konkrétní aplikace nebo případně celé Splunk instance. Viz také https://docs.splunk.com/Documentation/Splunk/9.1.1/Admin/Whereto findtheconfigurationfiles#Configuration_file_precedence
164	SIEM	Ke každému incidentu obsahuje časovou osu, kde je možno sledovat veškeré akce řešitelů	Ano	Ve Splunk ES v modulu zaměřeném na investigaci incidentů je k dispozici přehledná časová osa, kde jsou vidět jednotlivé události v životním cyklu incidentu, aktuální stav a komentáře. https://docs.splunk.com/Documentation/ES/7.2.0/User/Reviewaninvestigation

165	Reporting	Dostupné vizualizace by měly zahrnovat: - Čárový graf - Časový graf - Plošný graf - Sloupcový graf vertikální - Sloupcový graf horizontální - Jediná hodnota s trendem (růst, pokles) - Koláčový graf - Bodový graf - Bublinový graf - Ciferníkový (budíkový) ukazatel - Graf typu teploměr (zobrazení hodnoty ve vztahu k rozsahu) - Geolokační mapa - Graf zobrazující rozložení hodnot v geografických regionech - Kruhový graf - Výplňový graf - Tabulky (vč. doplňkových funkcí jako jsou automatické sumy, procentuálních vyjádření, číslování řádků, atd.)	Ano	Všechny požadované typy vizualizací jsou v Splunk Enterprise k dispozici. Další možnosti grafické reprezentace výsledků dotazů, jejich porovnání a vyhodnocování jsou dostupné v podobě zásuvných modulů (vizualizačních add-onů) na https://splunkbase.splunk.com/apps?keyword=visualization. V případě specifických požadavků je také možné vyvinout vlastní vizualizační add-on podle dokumentace na https://dev.splunk.com/enterprise/docs/developapps/visualizedata/displaydataview/splunkplatformcustom/
166	Reporting	Každý uživatel má možnost definovat vlastní reporty	Ano	Uživatel si může definovat vlastní report nebo dashboard, který je uložen v jeho osobním prostoru a nijak neovlivňuje ostatní uživatele. V závislosti na administrátorem přidělených oprávnění je následně možné tento privátní dashboard nebo report zpřístupnit i ostatním uživatelům, popsáno na https://docs.splunk.com/Documentation/Splunk/9.1.1/SearchTutorial/Aboutdashboards#Change_dashboard_permissions
167	Reporting	Komplexní, efektní zobrazení více metrik pomocí unifikovaných zástupných symbolů (síťový prvek, grafy, budíky, hodnoty apod.) s libovolným rozvržením po celé obrazovce včetně mapování symbolů a jejich aktuálních hodnot do grafického podkladu (síťová topologie, mapa apod.) pro názornější interpretaci	Ano	Je možné využít Splunk Dashboard studio které podporuje " drag and drop actions" a umisťování jednotlivých prvků libovolně na dashboard. Lze si nakreslit schéma sítě a na vybraná místa zobrazovat příslušné hodnoty - ukázka https://www.splunk.com/en_us/blog/platform/dashboards-ga-introducing-splunk-dashboard-studio.html
168	Reporting	Možnost exportu dashboardů do PDF souborů a naplánování jejich odesílání dalším uživatelům emailem	Ano	Systém umožňuje ruční nebo i automatické generování PDF z existujících reportů a dashboardů. Podle naplánovaného schématu se pak spouští příslušné reporty, převedou se do PDF a odešlou se emailem k definovaným adresátům.
169	Reporting	Možnost integrace s externími vizualizačními nástroji (D3, Tableau, apod.) pro další grafické formy výstupu	Ano	Externí vizualizační je možné využít. V rámci Splunk app base jsou dostupné zdarma : https://splunkbase.splunk.com/apps?keyword=visualization. Případně lze i opačně integrovat Splunk do externího vizualizačního systému jako například Tableau - https://help.tableau.com/current/pro/desktop/en-us/examples_splunk.htm
170	Reporting	Možnost vytváření šablon reportů	Ano	Ve Splunku se šablony reportů a dashboardů sdružují do samostatné aplikace, kde se i spravují. Do této aplikace je možné uložit existující šablony nebo si tam přidat další vlastní šablony. K těmto šablonám dashboardům pak mají ostatní uživatelé právo číst a pokud jej chtějí použít, stačí si tyto šablony zkopírovat a následně upravit.
171	Reporting	Přehledná evidence a audit využití licencí s včasným varováním o přiblížení se a překroční limitu	Ano	K dispozici je přehledový Dashboard, který nabízí aktuální přehled o využití licence. K dispozici je 30 denní pohled na předešlé využití. V rámci Splunk Alertů je k dispozici pravidlo s hlášením překročení licence. Úpravou pravidla lze reportovat i blížící se limit.
172	Reporting	Reporting v SIEMu musí nabízet výstupy podle ISO 2700x (přičemž požadujeme minimálně ISO 27002)	Ano	Reporty podle normy ISO27002 obsahuje SIEM modul. Protože ale nejsou z pohledu normy dostupné jednoduše a přehledně, vytvořili jsme addon, který všechny výstupy definované v části 6.8 ISO 27002 sdružují na jedno místo.
173	Reporting	Reporty a dashboardy obsahují možnosti jednoduchého filtrování pomocí formulářových polí a pomoci uživatelům zúžit záběr jen na data, která je zajímají	Ano	Filtrování je možné několika metodami. Je možné využít obecný filtr(Text), kdy si uživatel pomocí SPL definuje upřesňující dotaz, dále jsou k dispozici Radio, Dropdown, Checkbox, Multiselect.
174	Reporting	Reporty jsou poskytovány ve formě grafů a tabulek, přičemž tyto mohou být obsaženy v jedno reportu vícenásobně	Ano	Vizualizace dotazů lze libovolně nastavit - vybrat ze široké palety vizualizací nebo zobrazit v podobě tabulky. Pro jeden dotaz může být přiřazeno více reportů s rozdílnou vizualizací.
175	Reporting	Řešení musí umožnit snadné vytváření široké palety vizualizací (ne jen pevně dané, předpřipravené reporty)	Ano	Řešení umožňuje uživateli vytvořit vlastní klasické reporty, nebo využít novější řešení, které využívá " drag and drop actions" a přizpůsobit si dashboard podle svých potřeb. Splunk má k dispozici pro reporting definovanou sadu vizualizací, kterou lze pomocí addonů dále rozšiřovat a případně si lze naspat svůj addon se svojí vizualizací.
176	Reporting	Snadný tisk událostí, tabulek a vizualizací	Ano	V rámci vytvořeného vyhledávání, nebo dashboardu je možné exportovat data (https://docs.splunk.com/Documentation/SplunkCloud/9.0.2305/Search/ExportdatausingSplunkWeb) nebo je vytisknout.
177	Reporting	Systém obsahuje předdefinované a modifikovatelné reporty	Ano	Splunk obsahuje předddefinované reporty viz odpověď 182. Všechny reporty je možné dále upravovat nebo kopírovat.
178	Reporting	Systém provádí audit veškerých změn v konfiguraci	Ano	Systém provádí kompletní audit všech změn provedený pomocí Webového rozhraní, pomocí API a nebo i přímou změnou konfiguračních souborů. Veškerá auditní data jsou dostupná pro další zpracování.
179	Reporting	Systém umožní tvorbu bezpečnostních reportů, reportů na shodu s normami a vizualizace	Ano	Systém umožňuje vytvoření reportů podle potřeby uživatele.
180	Reporting	U všech grafů lze snadno změnit nadpis, legendu, popisy os a další nastavení	Ano	Pro tvorbu a editaci grafických dashboardů Splunk poskytuje následující možnosti: Přehledné web GUI rozhraní, kde lze návrh graficky upravovat, dále pokročilejší režim editace přímo zdrojového kódu (XML), případně design pomocí komponenty Dashboard studio. Typ grafického zobrazení a jeho atributy jako nadpis, popisy os atd. lze měnit, viz https://docs.splunk.com/Documentation/Splunk/9.1.1/Viz/Editdashboardpanelvisualizations a https://docs.splunk.com/Documentation/Splunk/9.1.1/Viz/ChartConfigurationReference#Area.2C_Bubble.2C_Bar.2C_Column.2C_Line.2C_and_Scatter_charts
181	Reporting	Uživatelské rozhraní typu „drag and drop“ umožňuje jak ne-technikům, tak technikům vytvořit komplikované reporty bez nutnosti manuálního zadávání vyhledávacích příkazů nebo porozumění formátu základních dat	Ano	Je možné využít funkce Splunk Datasets, kde se pomocí průvodce v UI vytváří tzv Table View - https://lantern.splunk.com/Splunk_Platform/Product_Tips/Data_Management/Using_Table_Views_to_prepare_data_without_SPL Pro vytvoření reportu lze využít Dashboard Studio, kde i ne technik může vytvořit požadovaný report - https://www.splunk.com/en_us/blog/platform/dashboards-ga-introducing-splunk-dashboard-studio.html
182	Reporting	Více jak 150 reportů a dashboardů organizovaných do logických skupin pokrývajících (nejen): - Celkové bezpečnostní riziko - Incidenty - Nezpracované události - Bezpečnostní analýzy - Externí zdroje hrozeb - Anomálie, extrémy - Audit systému samotného SIEM systému - Přehled korelačních pravidel s kontextem „story“ a všech náležitostí k realizaci	Ano	V součtu nabízí Splunk systém rozhodně více jak 150 předkonfigurovaných reportů a dashboardů. Největší část více jak 100 dashboardů a více jak 100 reportů je obsažena v části SIEM, kde jsou dashboardy rozděleny do hierarchického stromu. Další dashboardy a reporty obsahují technologické Addony zajišťující příjem, parsován a normalizaci dat.
183	Reporting	Vizualizace musí být schopné aktualizovat se v reálném čase	Ano	Jednotlivá vyhledávání a na ně navázané vizualizace mohou běžet v reálném čase, nebo v definovaném okně s pravidelnou aktualizací.
184	Reporting	Vizualizace musí být schopné jasně zvýraznit extrémy/anomálie vyžadující další pozornost a šetření	Ano	Řešení pro zvýraznění je opět více. Jako základ se bere podbarvení extrémních hodnot v tabulkové vizualizaci nebo například obarvení sloupců s extrémy u bar grafu. Dále lze do grafických vizualizací (chart, timechart) přidávat graf thresholdu. A také je možné do grafu přidávat i anotace s poznámkou o extrému - https://docs.splunk.com/Documentation/Splunk/latest/Viz/ChartEventAnnotations
185	Reporting	Všechny reporty a dashboardy mohou být plně modifikovány	Ano	Všechny dashboardy je možné podle potřeby uživatele upravit. Úprava je možná v grafickém prostředí nebo pomocí konfiguračních souborů
186	Reporting	Všechny reporty a dashboardy podporují možnost „drill-down“, čímž se lze dostat z high-level reportu/dashboardu k detailnímu reportu/dashboardu či k přímo původním událostem v řádu sekund	Ano	V dashboardech a jejich jednotlivých vizualizačních komponentách (grafy, tabulky, obrázky) Splunk umožňuje interaktivní přechod na další prvky, tzv. drilldown. Je podporováno několik typů drilldown akcí, jako např. zobrazení množiny eventů, která je výsledkem dotazu generujícího data pro daný graf, nebo proklik na zadanou webovou stránku, případně pak přechod na další dashboard, zobrazující další úroveň informací. Samozřejmostí je možnost předání runtime parametrů, tzv. tokenů, sloužících jako vstupní hodnoty pro zobrazení spouštěného dashboardu. Detailní popis mechanismu je na https://docs.splunk.com/Documentation/Splunk/9.1.1/Viz/DrilldownIntro
187	Reporting	Všechny vizualizace podporují procházení proklikáváním s cílem přejít z přehledu do původních událostí ve vteřinách	Ano	Viz bod 186

188	Zabezpečení	Flexibilní kontrola přístupu na základě rolí (RBAC) pro řízení přístupu uživatelů a přístupů přes API. Umožňuje omezovat přístup ke specifickým datovým zdrojům, datovým typům, specifickým pohledům, reportům a dashboardům.	Ano	Splunk řídí přístup pomocí skupin. Jednotlivým skupinám je možné nastavovat různá práva od přístupu k jednotlivému reportu až pro přístup k jednotlivým indexům. https://docs.splunk.com/Documentation/Splunk/9.1.1/Security/Aboutusersandroles
189	Zabezpečení	Generování hashe v době indexování. Systém umožní pomocí vyhledávání zjistit, zda s daty nebylo manipulováno	Ano	V době indexování dat systém může generovat hashe. Provádí se tak na menším bloku dat (data slice). Tyto hashe jsou ukládány do samostatného souboru. Při uzavření bucketu je tento soubor s hashy dále podepsán, aby bylo možné detekovat změnu. Pomocí Splunk scriptu lze pravidelně kontrolovat integritu dat a výstup lze indexovat pro následnou kontrolu. Více na https://docs.splunk.com/Documentation/Splunk/9.1.1/Security/Dataintegritycontrol
190	Zabezpečení	Integrace s Active Directory včetně autorizace a autentizace	Ano	Autentizace i autorizace je podporovaná se systémem Microsoft Active directory. Propojit lze pomocí LDAP protokolu nebo pomocí SSO. Autorizace probíhá pomocí mapování skupin v Active Directory na interní skupiny ve Splunk systému - detaily zde https://docs.splunk.com/Documentation/Splunk/9.1.1/Security/MapLDAPgroupstoSplunkroles https://docs.splunk.com/Documentation/Splunk/9.1.1/Security/Mapgroupstoroles
191	Zabezpečení	K dispozici jsou tyto metody autentizace: - Lokální autentizace - Common Access Card - Vícefaktorová autentizace – s více možnostmi zadání sekundárních autentizačních údajů - LDAP/Active Directory - Proxy SSO - SSO přes SAML - SSO přes reverse proxy - Univerzální API pro skriptovanou autentizaci pro externí systémy (RADIUS, PAM, atd.)	Ano	Všechny požadované autentizace jsou ve Splunku podporovány a ke všem zmíněným typům existuje přesný popis jak daný typ autentizace nastavit.
192	Zabezpečení	Monitoring své vlastní konfigurace a využití s cílem udržet si kompletní, auditní záznamy o tom, kdo přistupuje k systému, jaké dotazy spouští, na jaké reporty se dívá, jaké konfigurační změny provádí a další	Ano	Splunk Enterprise monitoruje všechny komponenty a ukládá několik auditních logů, které se následně indexují. Jedná se primárně o přístup na API a přístup na Webové rozhraní. Dále si systém kontroluje změnu v konfiguračních souborech, jakákoliv změna je zaznamenána do speciálního indexu ConfigTracker.
193	Zabezpečení	Šifrovaný provoz mezi agentem a Log management a SIEM řešením s podporou uživatelských SSL certifikátů	Ano	Pro sběr dat pomocí agenta je navrženo využití Cribl Edge. Ten má podporu šifrování komunikace, podporu uživatelských certifikátů a podporu KMS pro snazší správu - https://docs.cribl.io/edge/securing-and-monitoring Pokud by bylo potřeba využít Splunk Agenta, tak i ten podporuje šifrování komunikace pomocí klientského/uživatelského certifikátu.
194	Zabezpečení	Tok mezi instancemi je zabezpečen pomocí certifikátů	Ano	Interní komunikace mezi instancemi probíhá přes API, které je automaticky zabezpečeno selfsign certifikáty. Tyto certifikáty lze nahradit podepsanými certifikáty z preferované CA. Další komunikace jako je přístup na WEB, příjem dat lze zapnout do režimu SSL/TLS a tedy zabezpečit pomocí certifikátu.
195	Zabezpečení	Zabezpečený tok dat mezi instancemi distribuované architektury přes SSL/TLS.	Ano	stejné s bodem 194
196	Podpora produktu	Enterprise podpora v režimu 24/7/365 (email, telefon, webový portál)	Ano	Splunk nabízí dvě základní úrovně podpory - standard a premium, obě v režimu 24/7. Odlišnosti spočívají zejména v době reakce na zadaný incident v závislosti na jeho prioritě. Detailní informace jsou dostupné na https://www.splunk.com/en_us/customer-success/support-programs.html. Pro návrhy změn a vylepšení Splunk platformy je také k dispozici portál pro evidenci požadavků: https://ideas.splunk.com/
197	Podpora produktu	Široká aktivní komunita uživatelů a vývojářů diskutující otázky v odborných fórech.	Ano	Splunk má širokou a velmi aktivní komunitu. Portál je k dispozici na https://community.splunk.com/, rozčleněný na jednotlivá fóra podle tematických okruhů. Zde lze položit dotaz, vyhledávat v již zodpovězených otázkách anebo získat informace o školeních a certifikacích. Pokročilejší uživatelé, případně dodavatelé technologií, pak přispívají vlastními doplňkovými moduly, tzv. add-ony, které rozšiřují funkcionalitu Splunk platformy, jejich zveřejněním na portále https://splunkbase.splunk.com/. Další možností komunikace s komunitou může být i kanál na Slack. Více na https://docs.splunk.com/Documentation/Community/current/community/AboutCommunity
198	Podpora produktu	Webový portál s bezplatně a volně přístupnou kompletní a detailní produktovou dokumentací	Ano	Veškerá dokumentace výrobce je zdarma dostupná na webu https://docs.splunk.com/Documentation. Je k dispozici jak část týkající se základních funkcionalit platformy Splunk jako je Log management, tak i popis řešení Enterprise Security. Pro vývojáře je pak dostupná stránka https://dev.splunk.com

Licence

Účastník vyplní ve sloupcích C a D za každý potřebný typ licence, údržby licence a subskripce licencí jejich název a počet.
Požadavky na licence jsou definovány technickými požadavky na poptávané řešení.

Druh licence		Název licence	počet
Licence Log management a SIEM	Perpetuální licence		
	Údržba perp. licencí		
	Subskripce licencí	SE-T-LIC-ST Splunk Enterprise - Term License with Standard Success Plan - GB/day	1000
		ES-T-LIC-ST Splunk Enterprise Security - Term License with Standard Success Plan - GB/day	1000
		CLS-S Cribl-Suite On-Prem Standard - Priced based on the expected Quantity of GB/Day consumed.	1000
		SE-T-LIC-TEST Splunk Enterprise - Term License - Standard support - GB/day (Dev/Test)	1
		ES-T-LIC-TEST Splunk Enterprise Security - Term License - Standard support - GB/day (Dev/Test)	1
Ostatní licence (OS apod.)	Ostatní licence - subskripce		
	Ostatní licence - perpetuální		
	Údržba ostatních licencí		

SPRÁVA ŽELEZNIC

Příloha č. 5 Smlouvy

Požadavky na služby Platformy SŽ pro Log Management a SIEM

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

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

Příloha č. 19: Požadavky na služby Platformy SŽ pro Log Management a SIEM

Základní informace

- Tento soubor je přílohou zadávací dokumentace veřejné zakázky "Log management a SIEM".
- V tomto souboru účastník zadávacího řízení vyplní své požadavky na služby Platformy SŽ pro Log Management a SIEM.
- Pro účely projektu Log Management a SIEM jsou určeny a povoleny k výběru pouze Infrastrukturní služby platformy.
- Detailní popis služeb je uveden v Příloze č. 4 zadávací dokumentace Platforma SŽ 2.0: Vymezení služeb.
- Pro účely projektu Log Management a SIEM jsou parametry infrastrukturních služeb uvedených v detailním popisu upřesněny, nebo nahrazeny následovně:
    - Článek 5.1.1 Platformy 2.0 – pro projekt Log Management a SIEM je upřesněno, že budou dodávány v rámci virtualizačního prostředí virtuální jádra, přičemž minimální frekvence používaných fyzických CPU je 2GHz.
    - Článek 5.1.2 Platformy 2.0 – služby datového úložiště jsou pro účely projektu Log Management a SIEM nahrazeny popisem uvedeným v rámci Přílohy č. 1 ZD Technická specifikace, článek 2.4.5. a následujícími technickými parametry:
        - COLD Storage poskytuje úložiště s minimální rychlostí 500 IOPS (operací za sekundu).
        - HOT/WARM Storage poskytuje úložiště s minimální rychlostí 2.000 IOPS (operací za sekundu).
        - Úložiště pro zálohování – Backup zálohování je realizována zálohovacími servery s diskovým polem a páskovou knihovnou
- Požadované služby musí pokrýt všechny infrastrukturní požadavky nabízeného řešení tak, aby jej bylo možné nasadit a provozovat v parametrech definovaných Zadávací dokumentací zadávacího řízení.
- Účastník veřejné zakázky vyplní požadavky nabízeného řešení na Platformu SŽ do formuláře na listu "Požadavky".
- Tyto vyplněné požadavky slouží jako podklad pro výpočet dílčích bodů pro dílčí hodnotící kritérium "Požadavky na služby Platformy SŽ" - výpočet probíhá
  na listu "Požadavky" na základě jednotkových hodnot uvedených na listu "Jednotkové_body"
- Instrukce k vyplnění jsou obsaženy na příslušném listu.

Obsah tohoto souboru

List	Popis listu	Odkaz
Požadavky **VYPLŇUJE ÚČASTNÍK**	Obsahuje: - Instrukce k vyplnění formuláře - Formulář pro vyplnění požadavků účastníka na Platformu SŽ - Výsledný počet dílčích bodů za kritérium "Požadavky na služby Platformy SŽ"	zde
Příklad Nevyplňuje účastník.	- Zpracovaný příklad vyplnění požadavků	zde
Jednotkové_Body Nevyplňuje účastník.	Přehled bodového hodnocení pro jednotlivé služby Platformy.	zde

V tomto XLSX souboru upravujte pouze buňky označené těmito barvami:

	Buňky k vyplnění
	Buňky k výběru z předefinovaných možností (Dropdown)

Seznam služeb, které si účastník může nakonfigurovat je uveden v tabulce níže. Detailnější popis těchto služeb najdete v Příloze č. 4 zadávací dokumentace "Platforma SŽ 2.0".

Služba	Popis	IaaS/PaaS	Kategorie služeb
Win.VMware.x86_64	Služba virtualizace s OS Windows	IaaS	Infrastrukturní služba
RHEL.VMware.x86_64	Služba virtualizace s OS RHEL	IaaS	Infrastrukturní služba
SLES.VMware.x86_64	Služba virtualizace s OS SLES	IaaS	Infrastrukturní služba

Požadavky dodavatele na služby Platformy SŽ pro Log Management a SIEM a výpočet dílčích bodů hodnotícího kritéria "Požadavky na služby Platformy SŽ"

Popis:

Na tomto listu účastník definuje požadavky nabízeného řešení na služby Platformy SŽ pro Log Management a SIEM. Výpočet dílčích bodů hodnotícího kritéria "Požadavky na služby Platformy SŽ" probíhá dle interní nákladové náročnosti požadovaných služeb Platformy SŽ.
Počet celkových dílčích bodů se vypočte následovně: počet kusů * (zvolený počet Core * jednotkové body + zvolená velikost GB:RAM * jednotkové body + ... + zvolená velikost GB:Backup * jednotkové body). Jednotkové body jsou uvedeny na listu "Jednotkové_Body".

Instrukce:

Jeden řádek tabulky odpovídá jedné požadované službě.

Do sloupce ***Služba (B)*** účastník vybírá požadovanou službu z Platfformy SŽ

Sloupec ***Typ služby (C)*** automaticky doplní o jakou kategorii Služeb se jedná.

Ve sloupcích **Core (E), GB:RAM (F), GB:COLD Storage (G), GB:HOT/WARM Storage (H) a GB:Backup (I)** účastník volí požadovaný sizing služby. Ve sloupci **Počet kusů (D)** účastník zvolí celkový počet kusů dané konfigurace. Obecně přípustné hodnoty jsou 0 a celá

Sloupec ***Core (E)*** obsahuje počet virtuálních jader v rámci virtualizačního prostředí, přičemž minimální frekvence používaných fyzických CPU je 2 GHz.

Ve sloupci ***GB:COLD Storage (G)*** účastník specifikuje kapacitní požadavky na diskové úložiště pro dlouhodobé uložení dat typu COLD storage, dle schématu víceúrovňové architektury úložiště, který je provozován na discích typu HDD. Tento typ úložiště je k dispozici jen v lokalitách centrálního zpracování dat, nikoliv v lokalitách, kde budou umístěny jen kolektory dat (logů). Tento typ úložiště je provozován v georedundantním režimu a nebude dále jinak zálohován. COLD Storage poskytuje úložiště s minimální rychlostí **500 IOPS** (operací za sekundu).

Ve sloupci ***GB:HOT/WARM Storage (H)*** účastník specifikuje kapacitní požadavky na provozní diskové úložiště kategorie HOT a/nebo WARM, dle schématu víceúrovňové architektury úložiště. HOT/WARM Storage poskytuje úložiště s minimální rychlostí **2000 IOPS** (operací za sekundu).

Ve sloupci ***GB:Backup (I)*** účastník specifikuje kapacitní požadavky na službu zálohování, která je realizována zálohovacími servery s

Počet bodů za konfigurovanou službu je možné vidět ve sloupci **P**, přičemž součet za všechny konfigurované služby je uveden v buňce **C14 (Dílčí body kritéria "Požadavky na služby Platformy SŽ")**.

Dílčí body hodnotícího kritéria "Požadavky na služby Platformy SŽ" dle požadavků na služby Platformy SŽ.	-

Pro každou vybranou službu je povinné nenulovou hodnotou vyplnit sloupce B, D, E, F, sloupec I může nabývat i nulových hodnot. Dále je nezbytné vyplnit alespoň jeden ze sloupců G a H a dále sloupec Q.

Seznam vybraných služeb musí pokrýt infrastrukturní požadavky nabízeného řešení tak, aby jej bylo možné nasadit a provozovat v parametrech definovaných zadávací dokumentací zadávacího řízení, zejména včetně pokrytí produkčního i testovacího prostředí (prosím označte ve sloupci Q), pokrytí potřeb zálohování a potřeb všech komponent - centrálních i satelitních.

Pokud se Vám zobrazují hodnoty červeně, překročili jste povolený limit stanovený v technické specifikaci (2.4.12)

Vyberte službu z nabídky Platformy SŽ		Zvolte požadovaný počet kusů daného řešení	Zvolte požadovaný počet Core	Zvolte požadovanou velikost RAM	Zvolte požadovanou velikost diskového prostoru na dlouhodobém úložišti typu COLD storage	Zvolte požadovanou velikost diskového úložiště v lokálním provozním úložišti typu HOT nebo WORM storage	Zvolte požadovanou velikost diskového úložiště pro zálohování		Zvolte prostředí	Určete využití dané konfigurace	
Služba	**Typ služby**	**Počet kusů**	**Core**	**GB:RAM**	**GB: COLD Storage**	**GB: HOT/WARM Storage**	**GB:Backup**	**Celkový počet bodů za službu**	**Prostředí**	**Účel**	**Popis**

Příklad vyplnění: Vyhodnocení náročnosti požadavků dodavatele na IT Infrastrukturu SŽ

Popis:

Na tomto listu je ukázán možný způsob vyplnění Požadavků na Platformu SŽ.

Celkové bodové ohodnocení požadavků dodavatele:	**2334373**

Vyberte službu z nabídky Platformy SŽ		Zvolte požadovaný počet kusů daného řešení	Zvolte požadovaný počet Core	Zvolte požadovanou velikost RAM	Zvolte požadovanou velikost diskového prostoru na dlouhodobém úložišti typu COLD storage	Zvolte požadovanou velikost diskového úložiště v lokálním provozním úložišti typu HOT nebo WORM storage	Zvolte požadovanou velikost diskového úložiště pro zálohování		Zvolte prostředí	Určete využití dané konfigurace	
Služba	**Typ služby**	**Počet kusů**	**Core**	**GB:RAM**	**GB: COLD**	**GB: HOT/WARM**	**GB:Backup (COLD)**	**Celkový počet bodů za službu**	**Prostředí**	**Účel**	**Popis**
RHEL.VMware.x86_64	Infrastrukturní služba	4	56	128	65 536	8 192	256	532 854	PROD	Centrální komponenta	Sekundární lokalita
RHEL.VMware.x86_64	Infrastrukturní služba	10	72	128	77 824	8 192	256	1 553 316	PROD	Centrální komponenta	Primární lokalita
RHEL.VMware.x86_64	Infrastrukturní služba	5	16	32	-	2 048	100	42 655	PROD	Satelitní komponenta	Syslog
RHEL.VMware.x86_64	Infrastrukturní služba	28	12	16	-	1 536	100	176 106	PROD	Satelitní komponenta	Syslog remote
RHEL.VMware.x86_64	Infrastrukturní služba	2	48	64	1 024	1 024	100	29 442	TEST	Centrální komponenta	Primární lokalita

Bodové ohodnocení nákladnosti služeb v Platformě SŽ

Popis:

Dílčí body za jednotku IT služeb SŽ.

Tabulka slouží jako vstup pro hodnocení požadavků účastníka ve VZ (kritérium "Požadavky na služby Platformy SŽ").

Služba	Typ služby	Iaas	Body Základ	Body Core	Body GB:RAM	Body GB:COLD	Body GB:HOT/WARM	Body GB:Backup (COLD)
Win.VMware.x86_64	**Infrastrukturní služba**		**0,00**	**553,66**	**46,14**	**1,54**	**2,29**	**1,00**
RHEL.VMware.x86_64	**Infrastrukturní služba**		**0,00**	**200,68**	**16,72**	**1,54**	**2,29**	**1,00**
SLES.VMware.x86_64	**Infrastrukturní služba**		**0,00**	**173,85**	**14,49**	**1,54**	**2,29**	**1,00**

SPRÁVA ŽELEZNIC

Příloha č. 6 Smlouvy

Seznam poddodavatelů

Účastník:

Obchodní firma/jméno	ALEF NULA, a.s.
Sídlo/místo podnikání	Pernerova 691/42, 186 00 Praha
IČO	61858579
Zastoupen	Ing. Milanem Zinkem, předsedou představenstva

který podává nabídku na nadlimitní sektorovou veřejnou zakázku s názvem **„Log management a SIEM", č.j. 61441/2023-SŽ-GŘ-O8**, nevyužije k provádění předmětu plnění dle Smlouvy žádné poddodavatele.

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

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

SPRÁVA ŽELEZNIC

Příloha č. 7 Smlouvy

Zvláštní obchodní podmínky pro Zakázky v oblasti ICT

OBSAH

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

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

1. VÝKLAD POJMŮ

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

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

a. Specifikaci provedeného Plnění;

b. Akceptační kritéria;

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

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

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

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

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

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

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

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

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

1.10. **Doba vyřešení** je pro každou kategorii Incidentů uvedena ve Smlouvě 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.

1.11. **Doba zahájení řešení incidentu (RTI)** je Doba, která uplyne od času nahlášení Incidentu Ohlašovatelem prostřednictvím Helpdesku a okamžikem předání řešení Incidentu na skupinu řešitelů.

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

1.13. **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).

1.14. **Dostupnost** znamená stav Softwaru, 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 v celém jeho rozsahu nebo jeho podstatné části, přičemž Software se považuje za Dostupný, je-li přístupný a použitelný pro všechny uživatele Softwaru.

1.15. **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.

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

1.17. **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).

1.18. **GUI** znamená grafické uživatelské rozhraní.

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

1.20. **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.

1.21. **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

1.22. **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.

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

1.24. **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.*

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

1.26. **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*.

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

1.28. **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.

1.29. **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.

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

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

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

1.33. **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.

1.34. **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.

1.35. **Ohlašovatel** znamená uživatel Předmětu Smlouvy; případně osoba určená Objednatelem dle vymezení parametrů Helpdesku

a. pro úroveň L1 Helpdesku uživatele Softwaru;

b. pro úroveň L2 Helpdesku osoby určené Objednatelem dle jeho potřeb zajišťující úroveň L1 podpory;

c. pro úroveň L3 Helpdesku člen Realizačního týmu určený Dodavatelem dle jeho potřeby zajišťující úroveň L2 podpory.

1.36. **Opční právo** představuje vyhrazenou změnu závazku v souladu s ustanovením § 100 odst. 3 ZZVZ ze Smlouvy spočívající v pořízení dalšího obdobného Plnění od vybraného uchazeče v rámci zadávacího řízení Veřejné zakázky, tj. od Dodavatele dle Smlouvy.

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

1.38. **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.

1.39. **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.*

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

1.41. **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

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

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

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

1.45. **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*.

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

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

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

1.49. **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.

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

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

1.52. **Helpdesk** je Software provozovaný Dodavatelem nebo Objednatelem sloužící ke komunikaci Stran v průběhu provádění Plnění dle Smlouvy, v rámci něhož bude evidován postup Dodavatele při provádění Plnění dle Smlouvy a zároveň bude sloužit jako kontaktní místo Dodavatele pro nahlašování požadavků, otázek, odpovědí a další zaznamenávání průběhu provádění Plnění dle Smlouvy.

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

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

1.55. **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.

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

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

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

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

d. Software, o kterém to stanoví Smlouva.

1.57. **Smlouva** uzavřená na základě zadávacího řízení Veřejné zakázky vztahující se k ICT, která se řídí těmito ZOP.

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

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

1.60. **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.

1.61. **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.

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

1.63. **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.

1.64. **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.

1.65. **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.

1.66. **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).

1.67. **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.

1.68. **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.

1.69. **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.

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

1.71. **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).

1.72. **Zdrojový kód** znamená zápis kódu počítačového programu (Softwaru) v programovacím jazyce, který je uložen v jednom nebo více editovatelných souborech, čitelný, opatřený komentáři vysvětlujícími jeho jednotlivé části alespoň ve standardu obvyklém pro open source projekty a procesy, ve spustitelném formátu odpovídajícím programovacímu jazyku a

Produkčnímu prostředí, včetně ověřeného a podrobného postupu nezbytného pro sestavení plně funkčního strojového kódu, a v podobě, aby jej bylo možné zkompilovat do strojového kódu bez nutnosti provedení jiných úprav než kompilace v souladu s postupem k sestavení.

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

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

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

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

1.77. 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.

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;

b. poskytovat Plnění dle Smlouvy alespoň v závazných parametrech kvality dle Smlouvy a SLA, a to zejména dodržování stanoveného Servisního modelu dle článku 12.2. ZOP;

c. 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;

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

e. 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;

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

g. 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;

h. 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;

i. 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. Software

6.1.1. V případě, že je Software Autorské dílo vznikající v průběhu Plnění, Dodavatel postupuje na Objednatele oprávnění k výkonu majetkových práv autorských k takovému Autorskému dílu (ve formě strojového i Zdrojového kódu) tak, aby Objednatel byl oprávněn takové Autorské dílo užít v maximálním možném rozsahu včetně oprávnění k provádění změn a předání novému dodavateli.

6.1.2. Dodavatel prohlašuje, že Autorské dílo dle článku 6.1.1. ZOP bylo vytvořeno zaměstnanci či Poddodavateli jako zaměstnanecké dílo ve smyslu § 58 odst. 1 a 7 Autorského zákona, a že je oprávněn k postoupení výkonu majetkových práv v souladu s tímto článkem 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.

6.1.3. 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 článkem. S povinností převodu oprávnění k výkonu majetkových práv se pojí povinnost předání Zdrojového kódu dle čl. 7 ZOP.

6.1.4. Dodavatel dále prohlašuje, že má svolení autora/ů k zásahům do Autorského díla dle článku 6.1.1. ZOP ve smyslu § 58 odst. 4 Autorského zákona a tato svolení se vztahují na jakékoliv třetí osoby, jež budou vykonávat autorská majetková práva k tomuto Autorskému dílu.

6.1.5. Dodavatel dále prohlašuje, že vyloučil oprávnění autorů dle ustanovení § 58 odst. 3 Autorského zákona i vůči všem budoucím vykonavatelům autorských majetkových práv k Autorskému dílu dle článku 6.1.1. ZOP.

6.1.6. Dodavatel dále převádí veškerá zvláštní práva pořizovatele k Databázím pořízeným v průběhu provádění 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.

6.1.7. K ostatním majetkovým hodnotám, které spadají pod pojem Software a zároveň nespadají pod definici Autorského díla, uděluje Dodavatel Objednateli oprávnění v rozsahu dle článku 6.1.8. ZOP. Ustanovení článku 6.2. ZOP tímto nejsou dotčena.

6.1.8. 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 oprávněn dotčené části upravovat, zpracovávat, spojovat s jinými díly a jinak zasahovat do osobnostních autorských práv. Dodavatel odpovídá za zajištění těchto souhlasů.

6.1.9. Dodavatel není oprávněn pro účely vývoje Softwaru použít software licencovaný pod FOSS licencemi, jejichž podmínky by stanovovaly Objednateli povinnost sdělovat nebo jinak šířit Software nebo jeho části včetně Zdrojových kódů třetím osobám, nebo umožnit jim změny, úpravy či jiné zásahy do Softwaru nebo jeho části.

6.1.10. Dodavatel se zavazuje nahradit veškerou Újmu, která vznikne Objednateli v důsledku nesplnění jakýchkoliv povinností dle článku 6.1. ZOP. V případě, že jakákoliv třetí osoba bude uplatňovat vůči Objednateli jakékoliv nároky spojené se Softwarem nebo jeho částí v důsledku domnělého porušení svých autorských práv, zavazuje se Dodavatel hradit nároky, které Objednatel účelně vynaložil na ochranu zájmů Objednatele v této věci (včetně právního zastoupení), a to až do právního

vyřešení nároků třetích osob; tímto není dotčena povinnost dle první věty tohoto bodu.

6.2. Standardní Software

6.2.1. V případech, kdy je součástí Předmětu Smlouvy dodání Standardního Softwaru, Dodavatel poskytuje nevýhradní licenci, čímž se rozumí nevýhradní nevýlučné oprávnění Autorské dílo užít v souladu s dalšími podmínkami článku 6.2. ZOP, přičemž nevýhradní licence je poskytována Objednateli dále za následujících podmínek, není-li ve Smlouvě či v Příloze Smlouvy *Specifikace Plnění* stanoveno výslovně jinak:

a. Nevýhradní oprávnění k výkonu práva užít (licenci, resp. podlicenci) Autorské dílo včetně práva užít další Autorská díla a vytěžovat a zužitkovat Databáze, jež jsou určeny ke společnému užívání se Standardním Softwarem a za tímto účelem jsou společně distribuovány, a to všemi způsoby odpovídajícími účelu, pro který jsou taková Autorská díla, resp. Databáze, určeny, a to na dobu trvání majetkových práv autorských, nebo alespoň na dobu trvání Smlouvy.

b. Dodavatel je povinen zajistit poskytnutí podpory (subscription/licence maintenance) Standardního Softwaru, tj. zajistit poskytování nejnovějších verzí Standardního Softwaru získaných z důvěryhodných zdrojů Objednateli a dalších služeb v souladu se standardními licenčními podmínkami Standardního Softwaru, na dobu trvání majetkových práv autorských, pokud je to možné, jinak alespoň na dobu trvání Smlouvy.

c. Dodavatel je povinen poskytnout Objednateli o zajištění oprávnění ke Standardnímu Softwaru písemné prohlášení a na výzvu Objednatele tuto skutečnost prokázat.

d. Oprávnění musí vždy umožňovat Objednateli používání Standardního Softwaru pro interní potřeby Objednatele a jemu podřízených složek, organizací, částí nebo s ním propojených právnických osob.

6.2.2. Licence se vztahuje ve stejné míře jako ke Standardnímu Softwaru na:

a. Aktualizaci, Modernizaci a Zásadní modernizaci;

b. Dokumentaci specifikovanou v Příloze Smlouvy *Specifikace Plnění*;

c. Dokumentaci nad rámec Dokumentace dle předchozího bodu;

d. právo zužitkovat a vytěžovat Databáze, pokud jde o jiné Databáze než dle Smlouvy; a pokud tyto souvisí a jsou vhodné či nezbytné k naplnění účelu a Předmětu Smlouvy;

e. loga či jiné předměty duševního vlastnictví, které se Standardním Softwarem souvisí a jsou vhodné či nezbytné k užití spolu se Standardním Softwarem.

6.2.3. Je-li Standardní Software nebo Dokumentace vytvářena, upravována anebo jinak modifikována pro potřeby Objednatele, je Objednateli v takovém případě udělována licence k takto pro Objednatele vytvořeným či modifikovaným částem Standardního Softwaru nebo Dokumentace, včetně práva dané části jakkoliv měnit, udělit podlicenci nebo licenci zcela či z části postoupit a použít takové části Standardního Softwaru či Dokumentace k jakémukoliv účelu, v jakémkoliv množství, na jakémkoliv území, jakýmkoliv způsobem a na dobu trvání majetkových práv autorských, a to vše i prostřednictvím třetí osoby.

6.2.4. Pokud se jedná o Standardní Software a Dodavatel není oprávněn udělit alespoň nevýhradní licenci, pak se Dodavatel zavazuje udělit či zajistit udělení nevýhradního oprávnění k výkonu práva užít (licenci, resp. podlicenci) veškerá Autorská díla a k výkonu práva vytěžovat a zužitkovat Databáze, a to všemi způsoby odpovídajícími účelu, pro který je takové Autorské dílo, resp. Databáze, určeno, a to alespoň na dobu trvání Smlouvy. Dodavatel je povinen zajistit poskytnutí podpory Standardního Softwaru dle tohoto článku, tj. zajistit poskytování nejnovějších verzí Standardního Softwaru Objednateli získaných z důvěryhodných zdrojů a dalších služeb v souladu s jeho standardními licenčními podmínkami, na dobu trvání Smlouvy. Dodavatel je povinen poskytnout Objednateli písemné prohlášení o zajištění oprávnění ke Standardnímu Softwaru a na výzvu Objednatele tuto skutečnost prokázat. Oprávnění dle tohoto článku musí vždy umožňovat Objednateli používání Standardního Softwaru pro interní potřeby Objednatele a jemu podřízených složek, organizací, částí nebo s ním propojených právnických osob.

6.2.5. V ostatních parametrech se udělení licence řídí licenčními podmínkami výrobce Standardního Softwaru.

6.2.6. Ustanovení čl. 6.1. ZOP a 6.3. ZOP a jeho podčlánků se pro Standardní Software nepoužijí.

6.3. Software vztahující se k Hardwaru

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

6.3.2. Ustanovení čl. 6.1. ZOP a jeho podčlánků a 6.2. ZOP a jeho podčlánků se pro Software vztahující se k Hardwaru nepoužijí.

6.4. Odměna za poskytnutí oprávnění dle článku 6. ZOP je zahrnuta v Ceně za Plnění dle Smlouvy.

7. ZDROJOVÝ KÓD A DOKUMENTACE

7.1. Zdrojový kód bude předáván Objednateli na datovém nosiči vždy na konci Akceptačního řízení, nebo za podmínek stanovených ve Smlouvě, zejména pokud bude smluvní vztah ukončen bez provedení Akceptačního řízení.

7.2. Na datovém nosiči dat musí být viditelně označen „Zdrojový kód" s označením části Modifikace a jeho verze a den předání Zdrojového kódu. O předání nosiče dat bude oběma Smluvními stranami sepsán a podepsán písemný předávací protokol.

7.3. Povinnost Dodavatele předávat Zdrojový kód se přiměřeně použije i pro jakékoliv opravy, změny, doplnění, upgrade nebo update Zdrojového kódu v rámci následného provádění Plnění anebo v rámci záručních oprav. Zdrojový kód musí obsahovat podrobný popis a komentář každého zásahu do Zdrojového kódu.

7.4. Objednatel nebude v průběhu provádění Plnění sám anebo prostřednictvím jiných osob zasahovat do Zdrojového kódu nasazeného anebo fungujícího v Produkčním prostředí či Testovacím prostředí.

7.5. Dodavatel je povinen předat Objednateli příslušnou Dokumentaci a Zdrojový kód ve standardní podobě (to nejméně v kvalitě obvyklé pro open source projekty), vždy obsahující následující:

a. Kompletní Zdrojové kódy celého díla.

b. Uživatelskou příručku obsahující konkrétní popis uživatelského prostředí, funkcí a postupů pro zaškolení zaměstnanců.

c. Administrátorskou příručku, popisující všechny parametry, které lze konfigurovat a popis dopadů změny konfigurace do systému.

d. Technickou dokumentaci systému, pakliže se jedná o vícevrstvou architekturu, popis každé vrstvy zvlášť:

(i) Datová vrstva – popis datové vrstvy, čili tabulek v databázi včetně vazeb mezi tabulkami a včetně E-R schémat.

(ii) Aplikační vrstva – popis jádra systému, jeho funkcí, služeb a rozhraní. Dokumentace musí obsahovat kompletní popis architektury jádra systému, výčet a podrobný popis všech jeho funkcí, přehled a popis služeb, které jádro poskytuje dalším komponentám systému, modulům a knihovnám.

(iii) Prezentační vrstva – Dokumentace systému musí obsahovat drátové modely všech obrazovek uživatelského rozhraní včetně popisu funkcí prvků každé obrazovky.

e. Popis konfigurace provozního prostředí systému (serverová strana i klientská strana).

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

(i) mapování souborových systémů;

(ii) požadavky na operační paměť a procesory;

(iii) konfigurační parametry jednotlivých podpůrných Softwarových prostředků (např. specifika pro nastavení databáze, aplikačního serveru, webového serveru apod.).

g. Objednatel požaduje, aby tato Dokumentace byla ve formátech XML DocBook (zdrojové) a PDF (export z XML zdroje pro snadnou distribuci uživatelům) nebo případně v jiném formátu, který Objednatel schválí po vzájemné dohodě s Dodavatelem. Všechny Dokumentace musí být verzované, opatřené seznamem autorů, přehledem změn jednotlivých verzí a musí být obsahově úplné pro tu část systému, kterou popisují.

h. Řešení musí obsahovat návod na používání systému (uživatelský manuál) a popis systému – jeho vlastností, strukturu projektu, použité technologie (technická dokumentace). Součástí řešení je i Dokumentace a automaticky generovaná dokumentace (Javadoc). Součástí Dokumentace musí být zip archiv se zdrojovými soubory řešení a programátorskou dokumentací.

7.6. V případě jakýchkoli pochybností o správnosti předání Zdrojového kódu se bude uvedené posuzovat podle svého účelu, tedy zejména následné možnosti provádět samostatně či prostřednictvím třetích osob opravy, změny, doplnění, upgrady nebo updaty Zdrojového kódu. Za nesprávné předání se přitom považuje takové předání, které v důsledku vede ke znemožnění či podstatnému ztížení práce se Zdrojovým kódem ve výše uvedeném smyslu.

8. AKCEPTAČNÍ ŘÍZENÍ

8.1. Předání a převzetí Předmětu Smlouvy, včetně předání a převzetí výstupů provádění Plnění, dokumentů majících charakter výstupů Předmětu Plnění a Zdrojových kódů, probíhá na základě Akceptačního řízení, tj. postupným provedením akceptačních procesů a podepsáním Akceptačního/ch protokolu/ů.

8.2. Akceptační řízení zahrnuje porovnání skutečných vlastností Provádění Plnění se specifikací Plnění dle Smlouvy a Akceptačními kritérii. Podrobnější rozsah Akceptačních kritérií je součástí Přílohy Smlouvy *Specifikace Plnění*.

8.3. Plnění dle Smlouvy a jakékoliv jeho části, které podléhají Akceptačnímu řízení, jsou provedeny skončením Akceptačního řízení dotčené části Plnění, v případě Plnění jako celku skončením Akceptačního řízení Plnění jako celku.

8.4. Na Akceptační řízení se uplatní následující pravidla:

a. Dodavatel je povinen písemně informovat Objednatele nejméně čtrnáct (14) dní předem o termínu předání výstupu k Akceptačnímu řízení, nedohodnou-li se Strany jinak;

b. Dodavatel předá Objednateli výstup provádění Plnění k realizaci Akceptačního řízení; Akceptační řízení může být zahájeno pouze v případě, že výstup provádění Plnění, který je předmětem takového Akceptačního řízení, je umístěn v Produkčním anebo Testovacím prostředí nebo byl jiným způsobem Dodavatelem skutečně předán Objednateli a ten se s ním mohl seznámit; Objednatel na žádost Dodavatele potvrdí převzetí výstupů k Akceptačnímu řízení v Helpdesku, e-mailem, anebo prostřednictvím ISDS; převzetím k Akceptačnímu řízení anebo potvrzením ve smyslu tohoto článku je zahájeno Akceptační řízení;

c. po provedení všech nezbytných činností v rámci Akceptačního řízení se Objednatel i Dodavatel zavazují podepsat příslušný protokol potvrzující provedení výstupu provádění Plnění anebo výsledek Testů výstupů provádění Plnění připravený Dodavatelem a upravený a vyplněný Objednatelem (Akceptační protokol). Akceptační protokol obsahuje:

(i) Specifikaci provedeného Plnění;

(ii) Akceptační kritéria;

(iii) informace o průběhu Testů, jsou-li prováděny;

(iv) další informace a dokumenty nezbytné pro provedení Akceptačního řízení provedeného Plnění nebo jeho části.

d. v případě nutnosti opakování činností v rámci Akceptačního řízení v důsledku uvedení výroku „Neakceptováno" v Akceptačním protokolu Dodavatel Objednateli opět předá výstup k opětovnému provedení činností v rámci Akceptačního řízení (další kolo

Akceptačního řízení) a Dodavatel připraví nový Akceptační protokol vztahující se k dalšímu kolu Akceptačního řízení;

e. je-li součástí Plnění několik výstupů, pak každý z takových výstupů podléhá samostatnému Akceptačnímu řízení;

f. Akceptační řízení konkrétního výstupu končí a výstup se považuje za provedený podpisem Akceptačního protokolu Objednatelem s uvedeným výrokem „Akceptováno" nebo odstraněním vytčených vad výstupu v případě vyznačení „Akceptováno s výhradou" a potvrzením odstranění takových vytčených vad Objednatelem na Akceptačním protokolu, který obsahoval vytčené vady.

8.5. Objednatel je povinen po provedení ověření kvality výstupu v rámci Akceptačního řízení Dodavateli podepsat Akceptační protokol a akceptovat výstup provádění Plnění, případně oznámit Dodavateli vady výstupu provádění Plnění, které brání jeho provedení včetně určení Kategorie vady A, B, C.

8.6. Výstupy provádění Plnění jsou způsobilé k akceptaci Objednatelem, pokud:

a. naplňují Akceptační kritéria a nevykazují žádné vady, pak Objednatel vyznačí na Akceptačním protokolu „Akceptováno"; nebo

b. naplňují Akceptační kritéria a vykazují vady, které nebrání tomu, aby výstup provádění Plnění sloužil svému účelu bez významnějších omezení pro Objednatele (zejména organizačních, časových, nákladových apod.), anebo v případě Softwaru při Testech či provozu v souhrnu nevykazují více vad, než připouští Akceptační kritéria, pak Objednatel vyznačí na Akceptačním protokolu „Akceptováno s výhradou".

V jiných případech vyznačí Objednatel na Akceptačním protokolu „Neakceptováno".

8.7. V případě splnění Akceptačních kritérií je Objednatel povinen do 30 dnů od zahájení Akceptačního řízení vyznačit na Akceptačním protokolu výrok „Akceptováno". V případě nesplnění Akceptačních kritérií Objednatel vyznačí do 30 dnů od zahájení Akceptačního řízení na Akceptačním protokolu výrok „Neakceptováno" a uvede všechna Akceptační kritéria, která považuje za nesplněná s uvedením, v čem spočívá jejich nesplnění. Objednatel není povinen výše uvedené lhůty dodržet, dojde-li k prodloužení Akceptačního řízení z důvodu na straně Dodavatele.

8.8. Pokud Objednatel akceptuje výstup provádění Plnění svým podpisem a vyznačením výroku „Akceptováno s výhradou", které na Akceptačním protokolu uvede společně s uvedením vad, které nebrání akceptaci, zavazuje se Dodavatel k odstranění těchto vad ve lhůtách výslovně stanovených v Akceptačním protokolu, a pokud nejsou takové, pak lhůtách přiměřených stanovených Objednatelem v rámci odstraňování vad vyznačených v Akceptačním protokolu s výrokem „Akceptováno s výhradou" postupují Strany dle předchozích ustanovení tohoto článku až do odstranění všech vad vyznačených v Akceptačním protokolu s výrokem „Akceptováno s výhradou".

8.9. V případě neschválení výstupu provádění Plnění vyznačením na Akceptačním protokolu „Neakceptováno" odstraní Dodavatel vady uvedené v Akceptačním protokolu ve lhůtách výslovně stanovených v Akceptačním protokolu Objednatelem, a pokud nejsou takové, pak lhůtách přiměřených. Do odstranění vad bránících akceptování je výstup provádění Plnění považován za neakceptovaný (neprovedený). Po odstranění vad uvedených v Akceptačním protokolu Dodavatel předá znovu výstup provádění Plnění Objednateli k dalšímu kolu Akceptačního řízení a Objednatel postupuje obdobně podle předchozích ustanovení tohoto článku a specifických podmínek Akceptačního řízení uvedených v tomto článku.

8.10. Akceptační řízení se užije i na akceptaci a schválení výkazů či reportů, je-li jejich pravidelné zasílání Objednateli součástí Plnění.

Akceptační řízení však bude v takovém případě probíhat pouze následovně:

a. výkaz a report, včetně všech jeho součástí, se považuje za akceptovaný doručením Dodavateli sdělení Objednatele, že Objednatel jej považuje za úplný a správný, a souhlasí s vystavenou fakturou; nebo

b. marným uplynutím lhůty pro posouzení úplnosti a správnosti faktury, která se týká stejného období jako výkaz a report, bez vznesení připomínek ze strany Objednatele.

9. ŠKOLENÍ

9.1. Dodavatel provede zaškolení příslušných zaměstnanců Objednatele pro Software nebo Hardware v termínu dle Smlouvy, a pokud takový termín není, pak v termínu určeném Objednatelem po dohodě s Dodavatelem.

9.2. Součástí školení je i poskytnutí Dokumentace pro provedení školení a komplexní administraci Softwaru nebo užívání Hardwaru tak, aby na základě Dokumentace byli účastníci absolvující školení schopni samostatně (bez zásahů Dodavatele) ovládat Software nebo Hardware.

9.3. Účelem provedení školení je seznámení účastníků školení se Softwarem nebo Zařízením do té míry, aby jej byli schopni samostatně užívat v souladu se svým pracovním zařazením u Objednatele.

9.4. Požadavek na školení bude stanoven ve Smlouvě. Pokud Smlouva či její Příloha obsahuje požadavek na provedení školení, provede Dodavatel seznámení zaměstnanců Objednatele s Předmětem Smlouvy za podmínek, jež jsou uvedeny v tomto článku.

9.5. 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 do dne 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 Ohlašovatelům a dalším pověřeným uživatelům dle pokynů Objednatele, včetně Objednatelem určeného počtu přístupů. Helpdesk bude fungovat prostřednictvím webové adresy, elektronické pošty nebo telefonního čísla;

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 v jednom z následujících režimů, který je vymezen ve Smlouvě:

a. **Režim 1:**

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

b. **Režim 2:**

7x24, tj. dvacet čtyři (24) hodin sedm (7) dní v týdnu prostřednictvím elektronické pošty na adrese určené Dodavatelem.

c. **Režim 3:**

5×8, tj. v Pracovních dnech v době od 9:00 do 17:00 na telefonním čísle určeném Dodavatelem.

10.4. Helpdesk v režimu 1 dle článku 10.3. ZOP zahrnuje mimo jiné příjem a evidenci 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.

10.5. Helpdesk bude dostupný pouze pro Objednatele a Ohlašovatele.

10.6. Helpdesk je provozován v některé z těchto úrovní podpory, která je vymezena ve Smlouvě:

a. první úroveň (L1) – nahlášení Incidentu Ohlašovatelem je prováděno nahlášením Objednateli či pověřené osobě Objednatele, který Incident vyhodnotí a případně předá Incident jako Incident Dodavateli do druhé úrovně podpory;

b. druhá úroveň (L2) – nahlášení Incidentu Ohlašovatelem Dodavateli v případě, že Incident nebyl vyřešen v první úrovni podpory – je prováděno nahlášením Ohlašovatelem přes Helpdesk Dodavateli;

c. třetí úroveň (L3) – nahlášení Incidentu eskalační úrovni podpory Dodavatele nebo nahlášení Dodavatelem třetí osobě, která je oprávněna anebo schopna vyřešit Incident, pokud nebyl vyřešen v druhé úrovni podpory – je prováděno nahlášením Ohlašovatelem přes Helpdesk eskalační úrovni Dodavatele anebo Dodavatelem třetí osobě.

10.7. Ohlašovatelem s přístupem do Helpdesku

a. je pro úroveň L1 Helpdesku uživatel Softwaru nebo Hardwaru;

b. jsou pro úroveň L2 Helpdesku osoby určené Objednatelem dle jeho potřeb zajišťující úroveň L1 podpory;

c. je pro úroveň L3 Helpdesku člen Realizačního týmu určeného Dodavatelem dle jeho potřeby zajišťující úroveň L2 podpory.

11. NAHLÁŠENÍ INCIDENTU

11.1. Hlášení o Incidentu Dodavateli bude provedeno Ohlašovatelem, a to přímým zadáním Incidentu do Helpdesku, odesláním e-mailu nebo telefonátem na kontaktní číslo Helpdesk, 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 čl. 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.

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

11.4. 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.

11.5. Není-li v Servisní smlouvě, jejích přílohách anebo Technické specifikaci stanoveno jinak, ustanovení článku 11. ZOP se použijí přiměřeně i na nahlášení a evidování Požadavků; v takovém případě se za Čas nahlášení Incidentu považuje Čas nahlášení Požadavku.

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 řešení Incidentů kategorie A	Doba řešení Incidentů kategorie B	RTO	RPO	Doba zpracování Požadavku	Doba řešení Požadavku kategorie A	Doba řešení 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 nejsou započítávány:

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

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

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

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

12.5. Nedostupnost Softwaru dle článku 0. ZOP se nepovažuje za nedosažení sjednaných parametrů Dostupnosti dle Smlouvy a nebude započítána do výpočtu dle článku 12.6. a 12.7. ZOP.

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

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

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

$$Doba\ výpadku = \sum_{i}^{n} T_i$$

kde:

Σ je celková doba všech výpadků Softwaru za vyhodnocované období

T_i je doba jednotlivého výpadku Softwaru

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

13. ÚČAST PODDODAVATELŮ

13.1. Poddodavatele, jejichž prostřednictvím Dodavatel prokazoval kvalifikaci ve Veřejné zakázce, je Dodavatel povinen využívat při Plnění Smlouvy po celou dobu jejího trvání v rozsahu, v jakém jimi prokazoval kvalifikaci. Poddodavatele, jimiž Dodavatel prokazoval kvalifikaci ve Veřejné zakázce, lze vyměnit pouze s předchozím listinným souhlasem Objednatele, který může být dán výlučně za předpokladu, že tyto osoby budou nahrazeny osobami splňujícími kvalifikaci požadovanou ve Veřejné zakázce ve stejném rozsahu jako nahrazované osoby.

13.2. Dodavatel se zavazuje, že při poskytování Plnění pro Objednatele budou všichni Poddodavatelé, které Dodavatel využívá k poskytnutí Plnění dle Smlouvy, dodržovat veškeré požadavky vyplývající ze Smlouvy a Příloh Smlouvy. Dodavatel odpovídá za to, že jeho Poddodavatelé nebudou jednat v rozporu s ujednáními Smlouvy a jejími Přílohami, kterou mezi sebou uzavřeli Dodavatel a Objednatel.

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

14. REALIZAČNÍ TÝM

14.1. Pokud je takový požadavek součástí Zadávací dokumentace, je Dodavatel povinen předat Objednateli seznam osob, které budou členy Realizačního týmu, který se bude podílet na Plnění dle Smlouvy. Členy Realizačního týmu lze měnit pouze s předchozím listinným souhlasem Objednatele, který může být dán výlučně za předpokladu, že tyto osoby budou nahrazeny osobami splňujícími kvalifikaci požadovanou ve Veřejné zakázce ve stejném rozsahu jako nahrazované osoby. 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 článku 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. SMLUVNÍ POKUTY

16.1. Poruší-li Dodavatel některou ze svých povinností stanovených v Příloze Smlouvy *Specifikace Plnění*, zejména pak pokud poruší SLA, resp. stanovený servisní model dle článku 12.2. ZOP, je Objednatel oprávněn požadovat zaplacení smluvní pokuty ve výši stanovené v článku 16.2. ZOP, pokud nejsou ve Smlouvě výslovně zakotveny jiné sankce, které vylučují aplikaci článku 16.2. ZOP.

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

a. poruší-li Dodavatel svoji povinnost řádně a včas provést Plnění ve výši 0,01 % z celkové ceny Plnění (dále jen „Cena") za každý započatý den prodlení až do řádného splnění této povinnosti;

b. poruší-li Dodavatel svoji povinnost řádně a včas provést jakoukoliv část Plnění ve výši 0,02 % z ceny takové části Plnění za každý započatý den prodlení až do řádného splnění této povinnosti; v případě, že by smluvní pokuty dle čl. 16.2. písm. a. a čl. 16.2. písm. b. ZOP měly běžet vůči Dodavateli zároveň, vzniká za takové období Objednateli nárok pouze dle čl. 16.2. písm. a.

c. poruší-li Dodavatel povinnost udělit nebo zajistit Objednateli ze strany třetí osoby/třetích osob udělovaná oprávnění v rozsahu práv duševního vlastnictví ve výši 5 % z Ceny za každé jednotlivé porušení;

d. poruší-li Dodavatel povinnost řádně a včas předat Objednateli Zdrojový kód a veškerou související Dokumentaci, ve výši 0,05 % z Ceny za každý započatý den prodlení;

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

f. poruší-li Dodavatel svoji povinnost dodržet sjednanou Dobu vyřešení Incidentu, ve výši:

(i) ve výši 0,003 % z Ceny v případě každé započaté hodiny/den prodlení nad rámec sjednané Doby vyřešení v případě každého Incidentu kategorie A;

(ii) ve výši 0,003 % z Ceny v případě každé započaté hodiny/den prodlení nad rámec sjednané Doby vyřešení v případě každého Incidentu kategorie B;

(iii) ve výši 0,001 % z Ceny v případě každé započaté hodiny/den prodlení nad rámec sjednané Doby vyřešení v případě každého Incidentu kategorie C;

g. v případě prodlení nad rámec sjednané lhůty pro odstranění vad v Produkčním prostředí:

(i) Vada kategorie A ve výši 0,003 % z Ceny za každou započatou hodinu/den v případě každé Vady;

(ii) Vada kategorie B ve výši 0,003 % z Ceny za každou započatou hodinu/den v případě každé Vady;

(iii) Vada kategorie C ve výši 0,001 % z Ceny za každou započatou hodinu/den v případě každé Vady;

h. V případě, že Dodavatel nedodrží Dostupnost stanovenou servisním modelem dle článku 12. 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 %	3 % z ceny poskytovaného Plnění odpovídající vyhodnocovanému období dle čl. 12.8 ZOP

2 do 5 %	5 % z ceny poskytovaného Plnění odpovídající vyhodnocovanému období dle čl. 12.8 ZOP
5 do 10 %	8 % z ceny poskytovaného Plnění odpovídající vyhodnocovanému období dle čl. 12.8 ZOP
10 % a více	16 % z ceny poskytovaného Plnění odpovídající vyhodnocovanému období dle čl. 12.8 ZOP

i. v případě prodlení Dodavatele reagovat na Požadavek Objednatele v době řešení incidentu uvedené v článku 12.2. ZOP ve výši z 0,007 z % Ceny za každý jednotlivý případ;

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

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

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

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

16.3. Pro smluvní pokuty stanovené v čl. 16.2. písm. f. a g. ZOP platí, že je-li lhůta pro splnění stanovena v hodinách, je smluvní pokuta počítána za každou započatou hodinu, je-li lhůta pro splnění stanovena ve dnech či pracovních dnech, je smluvní pokuta počítána za každý započatý den.

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

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

16.6. Za každý den prodlení s úhradou Smluvní pokuty je Objednatel oprávněn požadovat po Dodavateli úhradu úroků z prodlení ve výši stanovené obecně závaznými právními předpisy.

17. ZÁRUKA ZA JAKOST A PRÁVA Z VADNÉHO PLNĚNÍ

17.1. Společná ustanovení

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

17.1.2. Objednatel je oprávněn Vady, které se vyskytnou v průběhu záruční doby, nahlásit Zhotoviteli bez zbytečného odkladu od okamžiku, kdy je zjistil. Lhůta bez zbytečného odkladu činí vždy nejméně devadesát (90) dnů.

17.1.3. Dodavatel odpovídá za vady zjevné, skryté i právní, které měl výstup provádění Plnění v době akceptace Objednatelem, a dále za ty, které se na něm vyskytnou v záruční době, a zavazuje se, vedle dalších nároků Objednatele, je bezplatně odstranit.

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

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

17.1.6. Dodavatel neodpovídá za vady Plnění vzniklé:

a. provozováním Díla Objednatelem v rozporu s Dokumentací;

b. neoprávněným nebo neodborným zásahem či nesprávným užitím Díla Objednatelem;

c. vadami IT prostředí Objednatele.

17.2. Záruka vztahující se k Softwaru

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

17.2.2. V době trvání záruční doby je Dodavatel povinen odstraňovat vady ve lhůtách uvedených v tabulce níže. Lhůty stanovené v hodinách běží pouze v Pracovní dny osm (8) hodin denně v době od 9:00 do 17:00 hodin (režim 5x8). Lhůty stanovené v hodinách se mimo dobu uvedenou v předchozí větě staví a pokračují dále v běhu během další bezprostředně následující doby počítání. Strany pro zamezení pochybnostem prohlašují, že toto se netýká lhůt stanovených v Pracovních dnech ani počítání doby prodlení v rámci výpočtu smluvních pokut.

Produkční prostředí

Kategorie vady	Lhůta k odstranění počítaná od nahlášení vady Objednatelem
Vada kategorie A – kritická	do 4 hodin[1]
Vada kategorie B – střední	do 17:00 třetího Pracovního dne od nahlášení vady[2]
Vada kategorie C – nízká	do 17:00 pátého Pracovního dne od nahlášení vady[3]

Testovací prostředí

Kategorie vady	Lhůta k odstranění počítaná od nahlášení vady Objednatelem
Vada kategorie A – kritická	do 17:00 druhého Pracovního dne od nahlášení vady[4]
Vada kategorie B – střední	do 17:00 pátého Pracovního dne od nahlášení vady[5]
Vada kategorie C – nízká	do 17:00 desátého Pracovního dne od nahlášení vady[6]

17.3. Záruka vztahující se k Hardwaru

17.3.1. Poskytuje-li výrobce anebo Dodavatel kterékoliv části Hardwaru na své výrobky anebo služby záruku za jakost delší, než je záruka za jakost dle tohoto článku, zavazuje se Dodavatel udělit Objednateli nebo na Objednatele postoupit danou záruku za jakost tak, aby Objednatel byl oprávněn po skončení záruky za jakost uplatnit nároky ze záruky za jakost bez nutnosti součinnosti ze strany Dodavatele.

17.3.2. Zjevné vady Hardware a dalších hmotných věcí je Objednatel povinen u Dodavatele reklamovat v rámci Akceptačního řízení. V případě, že Objednatel zjistí vady hmotných věcí po akceptaci, je povinen tyto vady bez zbytečného odkladu reklamovat u Dodavatele.

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

18. UKONČENÍ SMLUVNÍHO VZTAHU

18.1. Obecně k odstoupení od Smlouvy:

a. Strany sjednávají, že vznikne-li Objednateli nárok na odstoupení od Smlouvy, může podle své volby odstoupit od Smlouvy v celém rozsahu či jen od některé části Plnění určené Objednatelem.

b. Strany se dohodly na vyloučení použití § 1978 odst. 2 Občanského zákoníku, který stanoví, že marné uplynutí dodatečné lhůty stanovené k plnění může mít za následek odstoupení od této Smlouvy bez dalšího.

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

c. Dodavatel nemá právo odstoupit od Smlouvy v případě nevhodných příkazů Objednatele či poskytnutí nevhodné věci Objednatelem dle § 2595 Občanského zákoníku.

18.2. Objednatel je oprávněn odstoupit od Smlouvy, v případě, že:

a. Dodavatel je v prodlení s plněním dle Smlouvy či jakékoliv části Plnění déle než 30 dnů a nezjedná nápravu ani do 15 dnů od doručení písemného oznámení Objednatele o takovém prodlení.

b. Dodavatel je v prodlení s Plněním dle Smlouvy déle než 60 dnů, a to i bez nutnosti zaslání předchozího upozornění.

c. Nastane některý ze zákonem stanovených případů a zejména v případech podstatného porušení povinností Dodavatele stanovených ve Smlouvě. Za podstatné porušení povinností Dodavatele se považuje zejména:

(i) Dodavatel je opakovaně v prodlení s prováděním Plnění dle Smlouvy;

(ii) prohlášení Dodavatele učiněné na základě Smlouvy se ukáže jako nepravdivé;

(iii) Dodavatel bez upozornění a relevantního odůvodnění nepoužil k Plnění člena Realizačního týmu, ač k tomu byl povinen; nebo

(iv) Dodavatel poruší některou z povinností uvedenou v čl. 20. ZOP opakovaně nebo závažným způsobem.

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 čl. 13.2. ZOP nebo čl. 13.3. ZOP nebo Poddodavatel Dodavatele poruší některou z povinností vyplývající z požadavků dle čl. 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 čl. 4.2. ZOP.

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

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

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

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

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

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

19. ZMĚNY SMLOUVY A ZMĚNOVÉ ŘÍZENÍ

19.1. Není-li ve Smlouvě nebo jejích Přílohách stanoveno jinak, může být Smlouva měněna nebo zrušena pouze v listinné podobě, a to v případě změn Smlouvy číslovanými dodatky, který musí být podepsány oběma Stranami a uzavřeny v souladu se ZZVZ.

19.2. Pokud je ve Smlouvě upraveno Opční právo, vyhrazuje si Objednatel v souladu s ustanovením § 100 odst. 3 ZZVZ vyhrazenou změnu závazku z této Smlouvy spočívající v pořízení dalšího obdobného Plnění od vybraného účastníka v rámci zadávacího řízení Veřejné zakázky, tj. od Dodavatele dle Smlouvy. Předmětem plnění Opčního práva je poskytnutí dalšího obdobného Plnění dle Smlouvy tak, jak bylo podrobně vymezeno včetně dalších zákonných náležitostí vyhrazené změny závazku dle § 100 odst. 3 ZZVZ v Zadávací dokumentaci předmětné Veřejné zakázky.

19.3. Objednatel je oprávněn do uplynutí tří (3) let od nabytí účinnosti Smlouvy kdykoliv uplatnit toto Opční právo, a to i opakovaně do vyčerpání limitů Opčního práva definovaných v Zadávací dokumentaci. Vyhrazená změna závazku ze Smlouvy bude Stranami projednána v rámci jednacího řízení bez uveřejnění dle § 66 ZZVZ, které bude zahájeno Objednatelem v souladu s tímto ustanovením, a jehož výsledkem bude uzavření listinného dodatku k této Smlouvě či uzavření nové smlouvy mezi Objednatelem nebo Dodavatelem.

20. KYBERNETICKÁ BEZPEČNOST

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

20.2. Dodavatel se při plnění Smlouvy zavazuje postupovat v souladu se ZKB, VKB a souvisejícími právními předpisy, dodržovat zásady bezpečnosti informací, Interní předpisy Objednatele a z nich vyplývající povinnosti týkající se bezpečnostních opatření, provozní řády prostor Objednatele, rozhodnutí, opatření obecné povahy, či jiný správní akt NÚKIB či jiného správního orgánu anebo závazné podmínky pro Objednatele stanovené orgánem veřejné moci ukládající Objednateli další povinnosti ve smyslu ZKB a VKB, včetně upozorňování a zajištění hlášení Kybernetických bezpečnostních událostí a Kybernetických bezpečnostních incidentů Objednateli, jakož i další bezpečnostní politiky, metodiky a postupy, se kterými byl Objednatelem seznámen.

20.3. Dodavatel je povinen seznámit se s bezpečnostními požadavky Objednatele uvedenými ve Smlouvě, jejích přílohách, těchto ZOP, Interních předpisech Objednatele a seznámit s nimi osoby podílející se na plnění Smlouvy dle potřeby s ohledem na charakter jejich plnění s přihlédnutím k zajištění bezpečnosti informací. Kontaktní osoba Dodavatele je povinna splnění povinnosti dle předchozí věty Objednateli potvrdit do 30 dnů od uzavření Smlouvy. Pokud je to potřebné, je Dodavatel povinen provést školení bezpečnostních požadavků dle tohoto odstavce a dále je provádět v pravidelných intervalech, nejméně 1x ročně. Dodavatel je také povinen aktivně vynucovat dodržování takových bezpečnostních požadavků dotčenými osobami na straně Dodavatele. Za porušení těchto pravidel osobami uvedenými v tomto odstavci odpovídá Dodavatel tak, jako by je porušil sám.

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

a. politiku řízení přístupu, na základě které přidělí oprávnění k výkonu činností jednotlivým rolím svých fyzických osob (přístup pro více osob na jednom účtu je nežádoucí a lze pouze se souhlasem Objednatele) podílejících se na plnění Smlouvy (zaměstnanci, programátoři podnikatelé apod.) v nejmenším možném a nutném rozsahu tak, aby měly přístup k aktivům Objednatele pouze ty osoby, které takový přístup skutečně potřebují k výkonu činností týkajících se předmětu Plnění dle Smlouvy; není-li ve Smlouvě ujednáno jinak, je Dodavatel dále povinen průběžně monitorovat a zaznamenávat přístupy všech osob účastnících se na Plnění dle Smlouvy, a to v rozsahu, aby bylo možné jednoznačně určit uživatele, čas a provedenou činnost, jakož i vyhodnocovat oprávněnost těchto přístupů (logování přístupů) a tuto svou povinnost v politice řízení přístupu zohlednit a Dodavatel musí umožnit a poskytnout součinnost na jejich integraci do systému bezpečnostního monitoringu (SIEM), systému pro správu logů a centrální úložiště logů Objednatele;

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

20.5. Kontaktní osoba Dodavatele je povinna před započetím Plnění, nejpozději však do 30 dnů od uzavření Smlouvy, určit a popsat veškerá dotčená primární i podpůrná aktiva na straně Dodavatele potřebná pro plnění Smlouvy. Dodavatel je povinen při nakládání s veškerými aktivy (dotčenými aktivy Dodavatele a Objednatele) postupovat tak, aby chránil jejich důvěrnost, dostupnost a integritu a zavést přiměřená opatření na jejich ochranu. Dodavatel je povinen řídit rizika spojená s Plněním dle Smlouvy minimálně dle standardů požadovaných normou ISO 27001 a případně dle Interních předpisů, pokud obsahují závazná pravidla pro řízení rizik. Dodavatel je povinen bez zbytečného odkladu po uzavření Smlouvy kontaktní osobu Objednatele informovat o způsobu řízení rizik a o zbytkových rizicích souvisejících s Plněním Smlouvy a následně v pravidelných intervalech informovat o změnách.

20.6. Dodavatel je povinen zaslat kontaktní osobě Objednatele bez zbytečného odkladu všechna hlášení o událostech, která mají charakter Kybernetické bezpečnostní události nebo Kybernetického bezpečnostního incidentu, včetně případů porušení zabezpečení Osobních údajů, vždy bez zbytečného odkladu, nejpozději však do tří (3) hodin po jejich zjištění, a sdělit Objednateli opatření, která již provedl ve vztahu k této Kybernetické bezpečnostní události anebo Kybernetickému bezpečnostnímu incidentu, případně zvolí jinou formu dohodnutou mezi Objednatelem a Dodavatelem určenou ke včasnému hlášení Kybernetické bezpečnostní události nebo Kybernetického bezpečnostního incidentu a/nebo již učiněných opatření. Dodavatel je povinen veškeré Kybernetické bezpečnostní události a Kybernetické bezpečnostní incidenty zaznamenávat a po nezbytně dlouhou dobu uchovávat. Dodavatel je povinen poskytnout Objednateli veškerou nezbytnou součinnost k detekci, vyhodnocení či řešení Kybernetické bezpečností události nebo Kybernetického bezpečnostního incidentu, a to včetně případné realizace nutných opatření dle pokynů Objednatele. Zapříčinil-li Dodavatel Kybernetický bezpečnostní incident nebo podílel-li se na jeho vzniku, provede analýzu příčin Kybernetického bezpečnostního incidentu a navrhne opatření za účelem zamezení jeho opakování v budoucnu. Dodavatel je povinen ohlásit každou jednotlivou Kybernetickou bezpečnostní událost nebo Kybernetický bezpečnostní incident jedním z následujících způsobů:

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

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

c. ohlášením do Helpdesku Objednatele.

20.7. 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.

20.8. 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.

20.9. 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.

20.10. 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.

20.11. 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.

20.12. 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.

20.13. Dodavatel je povinen umožnit Objednateli provedení kontroly a auditu kybernetické bezpečnosti a zajistit (i smluvně) právo na provedení této kontroly a auditu kybernetické bezpečnosti u svých případných Poddodavatelů, jakož i veškerou další součinnost nezbytnou pro provedení auditu. Kontrolu a audit kybernetické bezpečnosti může rovněž provést i třetí osoba pověřená Objednatelem. Průběh takového auditu je doložen např. auditní zprávou či jiným obdobným dokumentem. Případné náklady na straně Dodavatele na provedení auditu jsou součástí Ceny za Plnění dle Smlouvy. Dodavatel je oprávněn rozporovat výsledky auditu kybernetické bezpečnosti do 7 Pracovních dnů od oznámení výsledku auditu kybernetické bezpečnosti. Dodavatel může rozporovat a) existenci vytčeného porušení či hrozby; b) že porušení či hrozba byla Dodavatelem již odstraněna. V obou případech uvede skutečnosti a důkazy k podpoře svých tvrzení. Objednatel je v takovém případě povinen takové připomínky vypořádat. V případě, že Objednatel na svém zjištění setrvá, je Dodavatel povinen se tímto auditem řídit.

20.14. 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.

20.15. 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.

20.16. 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.

20.17. 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.

20.18. 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.

20.19. Pokud Objednatel zjistí, že Dodavatel postupuje v rozporu s tímto článkem, je Objednatel v takovém případě oprávněn dožadovat se toho, aby Dodavatel odstranil vady vzniklé vadným postupem Dodavatele, zdržel se provádění postupů, které jsou v rozporu s tímto článkem, nebo konal, jak je od něj vyžadováno tímto článkem, a dále Smlouvou plnil řádným způsobem. Strany se dohodnou na podmínkách a lhůtě k odstranění nedostatků plnění Smlouvy ve smyslu tohoto odstavce, přičemž nedohodnou-li se Strany na konkrétní lhůtě, pak je Dodavatel povinen odstranit nedostatky do třiceti (30) dnů. Jestliže Dodavatel včas neodstraní nedostatky ve smyslu předchozí věty tohoto odstavce nebo se jedná o porušení povinnosti (bez ohledu na jeho závažnost), pak je Objednatel oprávněn od Smlouvy odstoupit.

20.20. 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.

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

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

a. za každý den prodlení při zavedení bezpečnostních opatření podle ZKB, VKB, těchto ZOP a Interních předpisů:

(i) ve výši 0,05 % z Ceny po dobu prvních pěti (5) dnů prodlení;

(ii) ve výši 0,1 % z Ceny po dobu od šestého (6.) dne prodlení do desátého (10.) dne prodlení; a

(iii) ve výši 0,2 % z Ceny po dobu od jedenáctého (11.) dne prodlení;

b. za každý den Objednatelem zjištěného soustavného porušování bezpečnostních opatření podle ZKB, VKB, těchto ZOP a Interních předpisů:

(i) ve výši 0,05 % z Ceny do šestého (6.) dne soustavného porušování; a

(ii) ve výši 0,1 % z Ceny od šestého (6.) dne soustavného porušování;

c. ve výši 2 % z Ceny za každý případ porušení povinnosti hlášení událostí, které mají charakter Kybernetické bezpečnostní události nebo Kybernetického bezpečnostního incidentu;

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

e. ve výši 5 % z Ceny za každý případ porušení článku 20. ZOP, přičemž toto porušení vedlo ke Kybernetickému bezpečnostnímu incidentu;

f. ve výši 0,1 % z Ceny za každý započatý den trvání porušení povinností Významného dodavatele dle článku 20. ZOP, dané porušení nebylo odstraněno a negativní následek porušení povinnosti stále trvá; a

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

21. OCHRANA OSOBNÍCH ÚDAJŮ

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

21.2. Pokud bude v rámci provádění Plnění docházet ke zpracování Osobních údajů, je rozsah zpracovávaných Osobních údajů uveden ve Smlouvě. Pokud dojde v rámci poskytování Plnění ke zpracování Osobních údajů, které Smlouva výslovně neuvádí, budou tato nová zpracování Osobních údajů prováděna za stejných podmínek.

21.3. Dodavatel bude zpracovávat Osobní údaje pro Objednatele výhradně za účelem poskytování služeb v rozsahu ujednaném podle Smlouvy. Dodavatel bude pro Objednatele zpracovávat Osobní údaje výhradně za uvedeným účelem, způsobem a na základě doložených pokynů a podmínek Objednatele a v souladu s nimi tak, jak vyplývají ze Smlouvy. Dodavatel neprodleně informuje Objednatele, pokud jsou podle jeho názoru určité pokyny Objednatele v rozporu s účinnými právními předpisy.

21.4. Dodavatel se zavazuje přijmout vhodná technická a organizační opatření podle GDPR, které se na něj jako na zpracovatele vztahují, a plnění těchto povinností na vyžádání doložit Objednateli.

21.5. Dodavatel může předávat Osobní údaje do třetí země nebo mezinárodní organizaci ve smyslu GDPR pouze na základě zvláštního pokynu Objednatele. Je-li takovéto předání založeno na povinnosti vyplývající z práva Unie nebo členského státu, které se na Objednatele vztahuje, informuje Dodavatel Objednatele o tomto právním požadavku před předáním, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu.

21.6. Dodavatel je povinen zajistit, aby se osoby oprávněné zpracovávat osobní údaje zavázaly zachovávat mlčenlivost ve vztahu ke všem Osobním údajům, které zpracovává na základě Smlouvy, a rovněž tak o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů.

21.7. Dodavatel je povinen přijmout všechna opatření dle čl. 32 GDPR tak, aby byla zajištěna odpovídající bezpečnost Osobních údajů. Dodavatel může do zpracování zapojit Poddodavatele pouze na základě předchozího písemného souhlasu Objednatele. Dodavatel se zavazuje s těmito Poddodavateli uzavřít smlouvu v souladu s GDPR zajišťující dodržování práv a povinností stanovených Smlouvou a/nebo těmito ZOP, zvláště pak povinnosti mlčenlivosti a zajištění bezpečnosti Osobních údajů a poskytnutí dostatečných záruk pro zavedení stejných technických a organizačních opatření Poddodavatelem, jakož i v souladu s dalšími aplikovatelnými právními předpisy. Dodavatel je dále povinen zohlednit povahu zpracování, být Objednateli nápomocen prostřednictvím vhodných technických a organizačních opatření pro splnění povinnosti Objednatele reagovat na žádost o výkon práv subjektu údajů dle GDPR.

21.8. Dodavatel je povinen být Objednateli nápomocen při zajišťování souladu s povinnostmi podle článku 32 až 36 GDPR, a to při zohlednění povahy zpracování informací, jež má Dodavatel k dispozici. V případech, kdy povaha věci vyžaduje informování Objednatele ze strany Dodavatele, informuje Dodavatel Objednatele bez zbytečného odkladu.

21.9. Dodavatel je povinen umožnit Objednateli a jím pověřené osobě během běžné pracovní doby Dodavatele provést v sídle Dodavatele kontrolu dodržování povinností týkajících se zpracování Osobních údajů vyplývajících ze Smlouvy, a to i po ukončení stanovené doby zpracování, tj. po ukončení této Smlouvy, a to do 3 měsíců od jejího ukončení.

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

21.11. V případě, že Dodavatel zpracuje osobní údaje nad rámec vymezený Smlouvou/doloženými pokyny Objednatele, považuje se ve vztahu k takovému zpracování za správce. Pokud tímto zpracováním nad rámec vymezený Smlouvou/doloženými pokyny Objednatele vznikne Objednateli škoda, je Dodavatel povinen škodu uhradit.

21.12. Pokud Dodavatel poruší povinnost chránit Osobní údaje v souladu s tímto článkem, vzniká Objednateli nárok na zaplacení smluvní pokuty ve výši částky sankce případně uložené z tohoto důvodu Objednateli ze strany Úřadu pro ochranu osobních údajů či jiným správním orgánem, který bude v budoucnu vykonávat působnost Úřadu pro ochranu osobních údajů. Objednatel je však za předpokladu, že mu k tomu Dodavatel poskytne nezbytnou součinnost, povinen uplatnit v příslušných řízeních veškeré přiměřené námitky, které mohl uplatnit ve svém zájmu, a v rámci řízení je povinen řádně hájit svá práva.

22. OCHRANA DŮVĚRNÝCH INFORMACÍ

22.1. Dodavatel se zavazuje zachovávat mlčenlivost o všech Důvěrných informacích, které získal nebo mu byly poskytnuty či zpřístupněny v souvislosti s plněním povinnosti dle Smlouvy, a uchovávat je v tajnosti.

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

22.3. Dodavatel nesmí bez předchozího písemného souhlasu Objednatele zpřístupnit Důvěrné informace žádné třetí osobě, a to v jakékoli formě. To neplatí u Důvěrných informací, ohledně kterých byla Dodavateli pravomocným rozhodnutím soudu, správního orgánu, či jiného příslušného státního orgánu v konkrétním případě uložena povinnost Důvěrnou informaci poskytnout nebo plyne-li taková povinnost Dodavateli z právního předpisu.

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

22.5. Dodavatel se zavazuje provést technická, organizační, právní a personální opatření, kterými zajistí dodržování povinnosti zachovat mlčenlivost o Důvěrných informacích a uchovat Důvěrné informace v tajnosti v rozsahu podle tohoto článku i ze strany svých zaměstnanců, Poddodavatelů, jakož i dalších osob, kterým budou Důvěrné informace poskytnuty či zpřístupněny.

22.6. Objednatel je oprávněn kdykoliv kontrolovat řádné plnění povinností Dodavatele uvedených v tomto článku, k čemuž se Dodavatel zavazuje bez zbytečného odkladu poskytnout Objednateli veškerou součinnost, zejména je Objednatel oprávněn kontrolovat řízení bezpečnosti Důvěrných informací Dodavatelem. V případě, že Objednatel vyzve Dodavatele na základě kontroly k nápravě, je Dodavatel povinen takové výzvě vyhovět v Objednatelem stanovené přiměřené lhůtě.

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

(a) ve výši 500 000 Kč za každé jednotlivé jednání, které představuje porušení jakékoli z povinností Dodavatele dle tohoto článku, vyjma povinností stanovených v článku 22.6. ZOP

(a) ve výši 100 000 Kč za každé jednotlivé jednání, které představuje porušení jakékoli z povinností stanovených v článku 22.6. ZOP.

SPRÁVA ŽELEZNIC

Obchodní podmínky ke Smlouvě o dílo

OBSAH OBCHODNÍCH PODMÍNEK

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

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

ČÁST 1 - ÚVODNÍ USTANOVENÍ

1. Pro účely těchto Obchodních podmínek mají následující slova význam u nich uvedený:
   - 1.1. **Občanský zákoník** – zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.
   - 1.2. **ZoDPH** – zákon č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.
   - 1.3. **ZoÚ** – zákon č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů.
   - 1.4. **SZ** – zákon č. 183/2006 Sb., o územním plánování a stavebním řádu (stavební zákon), ve znění pozdějších předpisů.
   - 1.5. **ZZVZ** – zákon č. 134/2016 Sb., o zadávání veřejných zakázkách, ve znění pozdějších předpisů.
   - 1.6. **Objednatel** – Správa železnic, státní organizace, IČO 70994234, se sídlem Praha 1 – Nové Město, Dlážděná 1003/7, PSČ 110 00, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze pod sp. zn. A 48384.
   - 1.7. **Zhotovitel** – osoba uvedená ve Smlouvě o dílo jako Zhotovitel; též všechny osoby, které jsou ve Smlouvě o dílo uvedené na straně Zhotovitele, je-li na straně Zhotovitele více než jedna osoba.
   - 1.8. **Smluvní strany** – Objednatel a Zhotovitel.
   - 1.9. **Smluvní strana** – Objednatel nebo Zhotovitel dle smyslu ujednání.
   - 1.10. **Nabídka** – souhrn dokumentů, které Zhotovitel podal jako návrh do zadávacího řízení, na jehož základě byla uzavřena Smlouva o dílo.
   - 1.11. **Smlouva o dílo** – smlouva uzavřená mezi Smluvními stranami, která odkazuje na Obchodní podmínky.
   - 1.12. **Obchodní podmínky** – tento text obchodních podmínek.
   - 1.13. **Předmět díla** – věc, která má být zhotovena, nebo činnost s jiným výsledkem, specifikovaná ve Smlouvě o dílo.
   - 1.14. **Související plnění** – další plnění (práce, dodávky, služby, činnosti a výkony), která je Zhotovitel povinen dle Smlouvy o dílo poskytnout vedle samotného provedení Předmětu díla.
   - 1.15. **Rozhodnutí Objednatele** – veškerá rozhodnutí, sdělení, souhlasy, povolení či jiné výsledky úkonů orgánů státní správy, samosprávy či jiných subjektů, které pro účely Díla nebo v souvislosti s ním získal nebo do doby dokončení Díla získá Objednatel a jež Objednatel Zhotoviteli předal nebo s nimiž se Zhotovitel jinak seznámil.
   - 1.16. **Rozhodnutí Zhotovitele** – veškerá rozhodnutí, sdělení, souhlasy, povolení či jiné výsledky úkonů orgánů státní správy, samosprávy či jiných subjektů, které je Zhotovitel povinen dle Smlouvy o dílo získat. Jakékoliv Rozhodnutí Zhotovitele, které není v českém jazyku, musí být do českého jazyka přeloženo a překlad musí být úředně ověřen.
   - 1.17. **Veřejnoprávní podklady** – souhrn Rozhodnutí Objednatele a Rozhodnutí Zhotovitele.
   - 1.18. **Doklady** – veškeré listiny, které se vztahují k Předmětu díla nebo Souvisejícímu plnění a které jsou třeba k jejich převzetí a užívání; veškerá Rozhodnutí Zhotovitele; veškeré další listiny, vyjma Výzvy k úhradě, které je Zhotovitel dle Smlouvy o dílo povinen předat Objednateli. Všechny Doklady musejí být v českém jazyku, nebo v původním jazyku s překladem do českého jazyka, není-li uvedeno jinak.
   - 1.19. **Dílo** – souhrn veškerých plnění, která je Zhotovitel povinen provést za účelem splnění Smlouvy o dílo; zahrnuje zejm. provedení Předmětu díla, poskytnutí či provedení Souvisejícího plnění a dodání Dokladů.
   - 1.20. **Cena díla** – cena za Dílo sjednaná ve Smlouvě o dílo (částka bez DPH).
   - 1.21. **Výzva k úhradě** – daňový doklad, je-li Zhotovitel povinen dle ZoDHP uhradit v souvislosti s provedením Díla nebo jeho části DPH, nebo faktura, pokud

Zhotovitel v souvislosti s provedením Díla nebo jeho části není dle ZoDPH povinen uhradit DPH.

1.22. **Vícepráce** – práce, dodávky nebo služby nad rámec Smlouvy o dílo, na jejichž provedení se Smluvní strany dohodnou po uzavření Smlouvy o dílo.

1.23. **Méněpráce** – práce, dodávky nebo služby v rámci Smlouvy o dílo, na jejichž vypuštění se Smluvní strany dohodnou po uzavření Smlouvy o dílo.

1.24. **Obalový materiál** – palety, dřevěné desky či jiné věci, které slouží pro potřeby přepravy nebo ochrany Předmětu díla. Dle kontextu Smlouvy o dílo se rozumí Obalovým materiálem též jednotlivý kus palety, dřevěné desky nebo jiné věci.

1.25. **Přejímací řízení** – proces, při kterém Zhotovitel předává a Objednatel kontroluje a přebírá Dílo, nebo je odmítá.

1.26. **Předávací protokol** – listina osvědčující předání a převzetí Díla nebo jeho části, jejíž minimální náležitosti jsou uvedeny v části Předání a převzetí Díla.

1.27. **Záruční doba** – doba, do jejíhož uplynutí je Objednatel oprávněn uplatňovat práva z vad plnění poskytnutého Zhotovitelem na základě Smlouvy o dílo; Záruční doba činí 24 měsíců.

1.28. **CTD** – Centrum telematiky a diagnostiky, organizační jednotka Objednatele.

ČÁST 2 - NÁVRH NA UZAVŘENÍ SMLOUVY O DÍLO

2. Odpověď Smluvní strany na návrh na uzavření Smlouvy o dílo učiněný druhou Smluvní stranou, která vymezuje obsah návrhu jinými slovy nebo která obsahuje jakékoliv, byť nepodstatné, dodatky, odchylky, výhrady nebo omezení není přijetím návrhu.

3. I pozdní přijetí návrhu na uzavření Smlouvy o dílo má účinky včasného přijetí, pokud navrhující Smluvní strana bez zbytečného odkladu alespoň ústně vyrozumí druhou Smluvní stranu, že přijetí považuje za včasné, nebo pokud se začne chovat ve shodě s návrhem.

4. Plyne-li z písemnosti, která vyjadřuje přijetí návrhu na uzavření Smlouvy o dílo, že byla odeslána za takových okolností, že by došla navrhující Smluvní straně včas, kdyby její přeprava probíhala obvyklým způsobem, má pozdní přijetí účinky včasného přijetí, ledaže navrhující Smluvní strana bez odkladu vyrozumí alespoň ústně druhou Smluvní stranu, že považuje návrh za zaniklý.

5. Bez ohledu na jakékoliv okolnosti nelze přijmout návrh na uzavření Smlouvy o dílo tak, že se Smluvní strana, jíž je návrh určen, podle návrhu zachová.

6. **Odkáží-li Smluvní strany v návrhu na uzavření Smlouvy o dílo i v přijetí návrhu na obchodní podmínky, které si odporují, je Smlouva o dílo přesto uzavřena s obsahem určeným v tom rozsahu, v jakém obchodní podmínky nejsou v rozporu; to platí i v případě, že to obchodní podmínky vylučují. Vyloučí-li to některá ze Smluvních stran nejpozději bez zbytečného odkladu po výměně projevů vůle, Smlouva o dílo uzavřena není.**

7. Smlouva o dílo může být uzavřena pouze v písemné podobě.

ČÁST 3 - DÍLO

8. Zhotovitel se zavazuje provést na svůj náklad a nebezpečí pro Objednatele Dílo a Objednatel se zavazuje Dílo převzít a zaplatit Zhotoviteli Cenu díla a příslušnou DPH, bude-li Zhotovitel povinen dle ZoDHP uhradit v souvislosti s provedením Díla nebo jeho části DPH.

9. Zhotovitel je povinen provést Dílo v jakosti, provedení a způsobem uvedeným ve Smlouvě o dílo a zároveň

9.1. v jakosti, provedení a způsobem, jenž odpovídá vlastnostem a způsobu, které Zhotovitel popsal nebo které Objednatel očekával s ohledem na povahu Díla, a to v rozsahu, ve kterém není v rozporu s jakostí, provedením a způsobem sjednaným ve Smlouvě o dílo,

9.2. v jakosti, provedení a způsobem, jenž se hodí k účelu vyplývajícímu ze Smlouvy o dílo a není-li v ní vyjádřen pak k účelu, ke kterému se Dílo obvykle používá, a

to v rozsahu, ve kterém není v rozporu s jakostí, provedením a způsobem sjednaným ve Smlouvě o dílo,

9.3. v souladu s Veřejnoprávními podklady,

9.4. v souladu s požadavky právních předpisů a příslušných ČSN.

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

ČÁST 4 - CENA DÍLA

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

ČÁST 5 - ZMĚNA CENY DÍLA

19. Změna ceny díla je možná pouze v případě

19.1. víceprací nebo méněprací,

19.2. zjistí-li Zhotovitel při kontrole projektové dokumentace předané mu Objednatelem vady nebo její nevhodnost či neúplnost, které mají vliv na náklady Zhotovitele,

19.3. v jiných případech jen pokud se na tom Smluvní strany dohodnou.

20. V případě víceprací i méněprací Zhotovitel provede ocenění jejich soupisu jednotkovými cenami položkového rozpočtu, je-li ve Smlouvě o dílo zahrnut.
21. Pokud práce, dodávky nebo služby nebudou v položkovém rozpočtu obsaženy nebo položkový rozpočet není ve Smlouvě o dílo zahrnut, užije se pro jejich ocenění cena obvyklá.
22. V případě vad, nevhodnosti nebo neúplnosti projektové dokumentace, kterou předal Objednatel Zhotoviteli, je-li taková projektová dokumentace součástí Smlouvy o dílo, mají-li takové vady, nevhodnosti nebo neúplnosti vliv na náklady Zhotovitele, postupují smluvní strany obdobně jako při oceňování víceprací nebo méněprací.
23. Změnu Ceny díla lze provést jen uzavřením dodatku ke Smlouvě o dílo.

ČÁST 6 - PLATEBNÍ PODMÍNKY

24. Objednatel neposkytuje zálohy.
25. Zhotovitel vyúčtuje Objednateli Cenu díla a případnou DPH Výzvou k úhradě.
26. Cenu díla a případnou DPH je Objednatel povinen uhradit Zhotoviteli do 30 dnů ode dne převzetí Díla; má-li být dle Smlouvy o dílo proveden též zkušební provoz, pak do 30 dnů ode dne úspěšného ukončení zkušebního provozu, nastane-li den skončení zkušebního provozu později než převzetí Díla Objednatelem.
27. Cena díla a případná DPH je uhrazena dnem jejich odepsání z bankovního účtu Objednatele.
28. Je-li Výzva k úhradě fakturou, musí obsahovat náležitosti účetního dokladu dle §11 ZoÚ a náležitosti stanovené v §435 Občanského zákoníku.
29. Je-li Výzva k úhradě daňovým dokladem, musí obsahovat náležitosti daňového dokladu dle §28 ZoDPH a náležitosti stanovené v §435 Občanského zákoníku.
30. Výzva k úhradě musí vždy obsahovat číslo Smlouvy o dílo, včetně uvedení uzavřených dodatků, její přílohou musí být vždy jedno vyhotovení Protokolu o převzetí potvrzeného Objednatelem. Ve výzvě k úhradě musí být vždy uvedeny jako identifikace Objednatele nejméně následující údaje:
    Správa železnic, státní organizace
    Dlážděná 1003/7, 110 00 Praha 1 – Nové Město
    IČO: 709 94 234
    Obchodní rejstřík u Městského soudu v Praze, sp. zn. A 48384
31. Výzvu k úhradě je Zhotovitel povinen doručit Objednateli **ve dvou vyhotoveních** nejpozději 15 dnů před uplynutím doby uvedené v odstavci 25 Obchodních podmínek.
32. Splatnost Výzvy k úhradě musí být stanovena tak, aby nenastala dříve, než uplyne doba stanovená v odstavci 25 Obchodních podmínek.
33. Stanoví-li Výzva k úhradě splatnost delší, než je jako minimální stanovena v předchozím odstavci, je Objednatel oprávněn uhradit Cenu díla a případnou DPH ve lhůtě splatnosti určené ve Výzvě k úhradě.
34. Stane-li se zhotovitel nespolehlivým plátcem nebo daňový doklad zhotovitele bude obsahovat číslo bankovního účtu, na který má být plněno, aniž by bylo uvedeno ve veřejném registru spolehlivých účtů, je objednatel oprávněn z finančního plnění uhradit daň z přidané hodnoty přímo místně a věcně příslušnému správci daně zhotovitele.
35. Je-li ve Smlouvě o dílo výslovně stanoveno, že Zhotovitel bude předávat Objednateli Dílo po částech, je Zhotovitel oprávněn vystavit Výzvu k úhradě předávané části Díla poté, co Objednatel převezme příslušnou část Díla. Ustanovení odstavců 26 - 33 Obchodních podmínek se užijí obdobně.
36. Ustanovení §2611, §2620–2622 a §2624 Občanského zákoníku se neužijí.

ČÁST 7 - MÍSTO PLNĚNÍ

37. Zhotovitel je povinen předat Objednateli Dílo v místě, jež vyplývá ze Smlouvy o dílo. Nelze-li takto místo předání Díla zjistit, vyzve Zhotovitel Objednatele, aby sdělil, ve kterém místě má Zhotovitel Objednateli Dílo předat. Nesdělí-li Objednatel místo plnění do 5 pracovních dnů ode dne doručení výzvy Zhotovitele, je Zhotovitel povinen Dílo předat Objednateli v sídle Objednatele.

ČÁST 8 - DOBA PLNĚNÍ

38. Zhotovitel je povinen zahájit provádění Díla bez zbytečného odkladu po uzavření Smlouvy o dílo.
39. Je-li součástí povinností Zhotovitele doprava Díla po jeho zhotovení do místa plnění dle Smlouvy o dílo, je Zhotovitel povinen dopravit Dílo do místa plnění v pracovní den v době od 8 do 15 hodin. Dodá-li Zhotovitel Dílo Objednateli v jiné než uvedené době, je Objednatel oprávněn odmítnout Dílo převzít a není zároveň v prodlení s převzetím Díla. Připadne-li konec sjednané doby plnění na sobotu, neděli nebo svátek, není Zhotovitel

v prodlení, dodá-li Dílo nejblíže následující pracovní den v časovém rozmezí dle tohoto odstavce.

40. Není-li stanoveno jinak, je Zhotovitel povinen začít s plněním svých povinností vždy bez zbytečného odkladu.
41. Zjistí-li Zhotovitel jakékoliv skutečnosti, které by mohly mít vliv na dobu plnění, je Zhotovitel povinen bez zbytečného odkladu Objednatele o takových skutečnostech informovat.

ČÁST 9 - PROVÁDĚNÍ DÍLA

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

Harmonogram

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

Kontrola provádění prací

51. Objednatel je oprávněn kontrolovat provádění Díla. Zjistí-li objednatel, že Zhotovitel provádí Dílo v rozporu s povinnostmi vyplývajícími ze Smlouvy o dílo, Obchodních podmínek, Veřejnoprávních podkladů, právních předpisů nebo příslušných ČSN, je Objednatel oprávněn dožadovat se toho, aby Zhotovitel odstranil vady vzniklé vadným prováděním a Dílo prováděl řádným způsobem. Jestliže tak Zhotovitel neučiní v přiměřené lhůtě, jedná se o podstatné porušení Smlouvy o dílo.
52. Zhotovitel je povinen písemně vyzvat Objednatele ke kontrole a prověření prací, které v dalším postupu budou zakryty nebo se stanou nepřístupnými. Zhotovitel je povinen vyzvat Objednatele nejméně 3 pracovní dny před termínem, v němž budou předmětné práce zakryty nebo znepřístupněny.
53. Před zakrytím nebo znepřístupněním prací je Zhotovitel povinen pořídit podrobnou fotodokumentaci prací a předat ji Objednateli v digitální podobě na CD nebo DVD nosiči bez zbytečného odkladu po pořízení fotodokumentace.
54. Pokud se Objednatel ke kontrole přes včasné písemné vyzvání nedostaví, je Zhotovitel oprávněn předmětné práce zakrýt. Bude-li se v tomto případě Objednatel dodatečně požadovat jejich odkrytí, je Zhotovitel povinen toto odkrytí provést na náklady Objednatele. Pokud se však zjistí, že práce nebyly řádně provedeny, nese veškeré náklady spojené s odkrytím prací, opravou chybného stavu a následným zakrytím Zhotovitel.

55. Obdobně bude-li Objednatel požadovat vykonání zvláštních zkoušek nebo ověření jakékoliv části Díla z důvodu podezření, že tato část Díla neodpovídá Smlouvě o dílo, Obchodním podmínkám, Veřejnoprávním podkladům, právním předpisům nebo příslušným ČSN, a bude-li zjištěno, že podezření bylo správné, nese náklady spojené s vykonáním zkoušek nebo ověřením Zhotovitel.
56. Zhotovitel je povinen umožnit výkon technického a autorského dozoru.

Kontrolní dny

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

Dodržování zákazu požívání alkoholických nápojů a užívání jiných návykových látek

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

Dodržování podmínek stanovisek příslušných orgánů a organizací

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

Použité materiály a výrobky

68. Zhotovitel se zavazuje a odpovídá za to, že při realizaci Díla nepoužije žádný materiál, o kterém je v době jeho užití známo, že je škodlivý. Pokud tak Zhotovitel učiní, je povinen na vyzvání Objednatele provést nápravu, přičemž veškeré náklady s tím spojené nese Zhotovitel.
69. Zhotovitel se zavazuje, že k realizaci Díla nepoužije materiály, které nemají požadovanou certifikaci či předepsaný průvodní doklad, je-li to pro jejich použití nezbytné podle Smlouvy o dílo, Obchodních podmínek, Veřejnoprávních podkladů, právních předpisů nebo příslušných ČSN. Certifikace a průvodní doklady Zhotovitele použitých materiálů jsou součástí Dokladů.

Částečné plnění

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

Ostatní ujednání

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

ČÁST 10 - ZKUŠEBNÍ PROVOZ

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

ČÁST 11 - PŘEPRAVA DÍLA

86. Ustavení této části se užijí v případě, je-li Dílo po svém zhotovení za účelem předání Objednateli přepravováno.
87. Je-li dle Smlouvy o dílo nebo zvyklostí třeba Předmět díla zabalit, Zhotovitel Předmět díla zabalí dle Smlouvy o dílo; není-li ujednání o balení Předmětu díla ve Smlouvě o dílo, pak dle zvyklostí, a není-li jich, pak způsobem potřebným pro uchování Předmětu díla a jeho ochranu.
88. Jestliže Zhotovitel označí Obalový materiál nejpozději do doby převzetí Předmětu díla Objednatelem jako vratný, a to přímo na Obalovém materiálu, v Dokladech nebo jiným zřejmým způsobem, ze kterého bude zřejmé, který Obalový materiál je vratný, je Objednatel oprávněn předat Zhotoviteli při předávacím řízení (viz ČÁST 13 - Obchodních podmínek) stejné množství Obalového materiálu téhož druhu a srovnatelného nebo

nižšího stupně opotřebení. V rozsahu předání Obalového materiálu Objednatelem Zhotoviteli dle předchozí věty zaniká právo Zhotovitele na vrácení Obalového materiálu.

89. V rozsahu, v němž Objednatel nevrátí vratný Obalový materiál Zhotoviteli dle předchozího odstavce, je Zhotovitel oprávněn Objednateli vyúčtovat zálohu na vratný Obalový materiál. Výše zálohy nesmí přesáhnout dvojnásobek pořizovací ceny Obalového materiálu.
90. Doposud nevrácený vratný Obalový materiál je Objednatel povinen na vlastní náklady dopravit do sídla Zhotovitele, a to nejpozději do jednoho roku od převzetí Předmětu díla Objednatelem. Objednatel je oprávněn nahradit nevrácený vratný Obalový materiál Obalovým materiálem stejného druhu a srovnatelného nebo nižšího stupně opotřebení. Bez zbytečného odkladu po převzetí vráceného Obalového materiálu nebo jeho náhrady Zhotovitelem, je Zhotovitel povinen vrátit Objednateli zaplacenou zálohu na vratný Obalový materiál. Nevrátí-li Objednatel dosud nevrácený vratný Obalový materiál nebo Obalový materiál stejného druhu a srovnatelného nebo nižšího stupně opotřebení ani do dvou let od převzetí Předmětu díla Objednatelem, stává se nevrácený vratný Obalový materiál vlastnictvím Objednatele a složená záloha se stává vlastnictvím Zhotovitele.
91. Pokud Zhotovitel Předmět díla Objednateli odesílá prostřednictvím dopravce, umožní Zhotovitel Objednateli uplatnit práva z přepravní smlouvy vůči dopravci, pokud o to Objednatel Zhotovitele požádá.
92. Pokud Zhotovitel Předmět díla Objednateli odesílá prostřednictvím dopravce, je Zhotovitel povinen zajistit dopravu u dopravce tak, aby Předmět díla byl dodán Objednateli v době uvedené v odstavci 39 Obchodních podmínek.
93. Je-li třeba provést vyložení Předmětu díla z dopravního prostředku, je vyložení povinen provést Zhotovitel na své náklady.
94. Je-li Objednatel v prodlení s převzetím Předmětu díla, uchová jej Zhotovitel, může-li s ním nakládat, pro Objednatele způsobem přiměřeným okolnostem. Převzal-li Objednatel Předmět díla, který zamýšlí odmítnout, uchová jej způsobem přiměřeným okolnostem. Smluvní strana, která uchovává Předmět díla pro druhou Smluvní stranu, má právo na náhradu účelně vynaložených nákladů spojených s uchováním Předmětu díla, nemůže jej však za účelem zajištění svého práva na úhradu nákladů zadržet.

ČÁST 12 - PODDODAVATELÉ

95. Zhotovitel je oprávněn pověřit provedením části Díla třetí osobu – poddodavatele. Zhotovitel odpovídá za činnost poddodavatele tak, jako by činnost prováděl sám.
96. Zhotovitel je oprávněn pověřit provedením části Díla poddodavatele pouze, pokud je poddodavatel uveden v příloze Smlouvy o dílo.
97. Zhotovitel se zavazuje, že poddodavatelé splní všechny povinnosti vyplývající Zhotoviteli ze Smlouvy o dílo, a to přiměřeně k povaze a rozsahu poddodávky.
98. Zhotovitel se zavazuje, že poddodavatelé, kterými prokazoval splnění kvalifikace v zadávacím řízení, se budou podílet na provedení příslušné věcně vymezené části Díla v rozsahu dle Nabídky Zhotovitele.
99. Zhotovitel je oprávněn změnit poddodavatele pouze s předchozím písemným souhlasem Objednatele. Objednatel vydá písemný souhlas se změnou do 10 dnů od doručení žádosti Zhotovitele. Objednatel souhlas se změnou nevydá, pokud
    99.1. prostřednictvím původního poddodavatele Zhotovitel v zadávacím řízení prokazoval kvalifikaci a nový poddodavatel nebude mít stejnou či vyšší kvalifikaci jako původní nahrazovaný poddodavatel nebo
    99.2. po Objednateli nelze spravedlivě požadovat, aby s takovou změnou souhlasil.

ČÁST 13 - PŘEDÁNÍ A PŘEVZETÍ DÍLA

100. Závazek Zhotovitele provést Dílo je splněn jeho dokončením a převzetím Díla Objednatelem, včetně převzetí veškerých Dokladů.
101. Součástí Dokladů je dle povahy a charakteru Díla též
    101.1. dodavatelská výrobní a dílenská dokumentace,

101.2. atesty, záruční listy, prohlášení o shodě všech věcí, jež byly použity při provádění Díla,
101.3. zápisy a osvědčení o všech předepsaných zkouškách, měřeních,
101.4. dokumenty osvědčující průběh zkušebního provozu,
101.5. servisní plán, návod k obsluze a návod k použití částí Díla,
101.6. doklady o zabezpečení likvidace odpadů v souladu s právními předpisy,
101.7. fotodokumentace z průběhu provádění Díla, zejména fotodokumentace prací a konstrukcí, které byly dalším postupem prací zakryté nebo jinak znepřístupněné,

102. V případě, že Smlouva o dílo, Obchodní podmínky, Veřejnoprávní podklady, právní předpisy nebo příslušné ČSN předepisují provedení zkoušek, revizí, atestů a měření či zajištění prohlášení o shodě týkajících se Díla, je Zhotovitel povinen zajistit jejich úspěšné provedení před předáním Díla Objednateli.
103. Objednatel Dílo převezme za předpokladu, že provedení Díla odpovídá Smlouvě o dílo, Obchodním podmínkám, Veřejnoprávním podkladům, právním předpisům a příslušným ČSN, je dokončeno (plně funkční), a je prosté vad s výjimkou ojedinělých drobných vad, které samy o sobě ani ve spojení s jinými nebrání užívání Díla funkčně nebo esteticky, ani jeho užívání podstatným způsobem neomezují.
104. Splnění podmínek pro předání Díla bude ověřeno v rámci přejímacího řízení. Zhotovitel je povinen písemně vyzvat Objednatele k převzetí Díla (zahájení přejímacího řízení). Přejímací řízení bude Objednatelem zahájeno do 5 pracovních dnů po obdržení písemné výzvy Zhotovitele.
105. Objednatel je oprávněn přizvat k účasti v přejímacím řízení i jiné osoby, jejichž účast pokládá za nezbytnou.
106. O průběhu přejímacího řízení bude Zhotovitelem pořízen zápis s identifikací vad Díla, pokud budou v průběhu přejímacího řízení zjištěny. Zápis bude použit jako podklad pro zpracování Předávacího protokolu. Zpracování návrhu Předávacího protokolu zajistí Zhotovitel.
107. Předávací protokol obsahuje
107.1. výslovný souhlas Objednatele s převzetím Díla
107.2. datum převzetí Díla,
107.3. prohlášení Objednatele, zda přebírá Dílo bez výhrad, nebo s výhradami,
107.4. soupis zjištěných vad nebránících řádnému užívání Díla,
107.5. dohodnuté lhůty k odstranění zjištěných vad nebo jiná opatření (byla-li dohodnuta),
107.6. soupis Dokladů předaných Zhotovitelem Objednateli.
108. Objednatel převezme Dílo bez výhrad, je-li v předávacím řízení zjištěno, že Dílo je prosté vad.
109. Převezme-li Objednatel Dílo s výhradami, postupují Smluvní strany dále obdobně dle ustanovení odstavců 138 - 152 Obchodních podmínek, přičemž pro odstranění vad platí doba sjednaná v Předávacím protokolu, jinak doba 15 dní od oboustranného podpisu Předávacího protokolu a za reklamaci se považuje identifikace vad uvedená v Předávacím protokolu podepsaném Objednatelem.
110. V případě, že Objednatel Dílo nepřevezme, bude mezi Smluvními stranami sepsán záznam s uvedením důvodu nepřevzetí Díla a s uvedením stanovisek Smluvních stran. Zpracování záznamu zajistí Zhotovitel.
111. V případě nepřevzetí Díla Smluvní strany sjednají lhůtu pro odstranění zjištěných vad. Nebude-li vada odstraněna ve lhůtě sjednané, jinak do 15 dní, je Objednatel oprávněn zajistit odstranění vady jinou odborně způsobilou osobou na náklady Zhotovitele. Veškeré náklady vzniklé Objednateli v souvislosti s odstraněním vady způsobem dle předchozí věty je Zhotovitel povinen Objednateli uhradit. Zhotovitel je povinen ve stanovené lhůtě odstranit vady i v případě, kdy podle jeho názoru za vady neodpovídá. Náklady na odstranění v těchto sporných případech nese až do vyjasnění nebo do vyřešení rozporu Zhotovitel. Po odstranění vad vyzve Zhotovitel Objednatele k zahájení náhradního přejímacího řízení, které Objednatel zahájí bezodkladně, nejpozději do 2 pracovních dnů od obdržení výzvy Zhotovitele.

112. Podpisem Předávacího protokolu nebo záznamu o nepřevzetí Díla je přejímací řízení ukončeno.
113. Pro průběh náhradního přejímacího řízení se užijí ustanovení odstavců 103 - 112 Obchodních podmínek obdobně.
114. Připouští-li to povaha Předmětu díla, a není-li sjednán zkušební provoz, má Objednatel právo, aby byl Předmět díla před ním překontrolován nebo aby byly předvedeny jeho funkce.
115. Ustanovení §1921, §2112, §2605 odst. 2, §2606, §2609, §2618 a §2629 Občanského zákoníku se neužijí.

ČÁST 14 - VLASTNICKÉ PRÁVO A NEBEZPEČÍ ŠKODY

116. Vlastnické právo k Dílu náleží od počátku Objednateli.
117. Vlastnické právo k dodávkám materiálu a jiných hmotných movitých věcí nabývá Objednatel okamžikem jejich zapracování do Díla, učiněním součástí Díla nebo jakýmkoliv funkčním, estetickým či jiným spojením s Dílem.
118. Vlastnické právo k jakékoli dokumentaci vztahující se k Dílu, která není autorským dílem, nabývá Objednatel okamžikem jejího vyhotovení.
119. Je-li vlastníkem Díla nebo jeho části v souladu s §1083 a §1084 Občanského zákoníku vlastník pozemku, užijí se ustanovení odstavců 116 a 117 přiměřeně.
120. Nebezpečí škody na Díle nese Zhotovitel, na Objednatele přechází okamžikem oboustranného podpisu Předávacího protokolu. Pokud nebyly s Předmětem díla předány zároveň též všechny Doklady, nese Zhotovitel nebezpečí škody na dosud nepředaných Dokladech až do jejich převzetí Objednatelem.
121. Náklady nutné k odstranění škody na Díle vzniklé v době, kdy nebezpečí škody nese Zhotovitele, hradí Zhotovitel v plném rozsahu a tyto náklady nemají vliv na Cenu díla.
122. Škody na Díle vzniklé v době, kdy nebezpečí škody nese Zhotovitele, je povinen Zhotovitel odstranit v součinnosti s Objednatelem jako vlastníkem poškozené věci a dle jeho pokynů.
123. Ustanovení §2599 Občanského zákoníku se neužijí.

ČÁST 15 - VADY PLNĚNÍ A ZÁRUKA

124. Zhotovitel se zavazuje, že Dílo bude v okamžiku jeho převzetí Objednatelem vyhovovat všem požadavkům na dílo stanoveným Smlouvou o dílo, Obchodními podmínkami, Veřejnoprávními podklady, právními předpisy a příslušnými ČSN.
125. Zhotovitel se zavazuje, že Dílo bude vyhovovat též plnění nabídnutému Zhotovitelem v Nabídce.
126. Dílo musí být prosté všech faktických a právních vad. Plnění má právní vadu, pokud k němu uplatňuje právo třetí osoba.
127. Zhotovitel se zavazuje (poskytuje Objednateli záruku), že Dílo a veškeré jeho části si po celou dobu od okamžiku jeho převzetí Objednatelem, až do uplynutí Záruční doby zachová vlastnosti stanovené v odstavcích 124 - 126 Obchodních podmínek.
128. Záruční doba začíná běžet dnem převzetí Díla Objednatelem, nebo jeho poslední části, je-li Dílo dodáváno po částech, nebo ode dne úspěšného ukončení zkušebního provozu, je-li dle Smlouvy o dílo vyžadován a nastane-li okamžik úspěšného ukončení zkušebního provozu později než okamžik převzetí Díla, resp. jeho poslední části.
129. Dílo má vady (Zhotovitel plnil vadně), jestliže při převzetí Objednatelem nebo kdykoliv od převzetí Objednatelem do konce Záruční doby nebude mít vlastnosti stanovené v odstavcích 124 - 126 Obchodních podmínek.
130. Objednatel má práva z vadného plnění i v případě, jedná-li se o vadu, kterou musel s vynaložením obvyklé pozornosti poznat již při uzavření Smlouvy o dílo.
131. Objednatel nemá práva z vadného plnění, způsobila-li vadu po přechodu nebezpečí škody na věci na Objednatele vnější událost. To neplatí, způsobil-li vadu Zhotovitel nebo jakákoliv třetí osoba, jejímž prostřednictvím plnil své povinnosti vyplývající ze Smlouvy o dílo.

132. Zhotovitel neodpovídá za vady spočívající v opotřebení Předmětu díla, které je obvyklé u věcí stejného nebo obdobného druhu jako Předmět díla.
133. Zhotovitel odpovídá za vady spočívající v opotřebení Předmětu díla, ke kterému do konce Záruční doby vzhledem k požadavkům Smlouvy o dílo, Obchodních podmínek, Veřejnoprávních podkladů, právních předpisů a příslušných ČSN na jakost a provedení Předmětu díla nemělo dojít.
134. Zhotovitel nenese odpovědnost za vady způsobené Objednatelem nebo třetími osobami, ledaže Objednatel nebo takové osoby postupovaly v souladu s Doklady nebo pokyny, které obdrželi od Zhotovitele.

ČÁST 16 - UPLATNĚNÍ PRÁV Z VADNÉHO PLNĚNÍ

135. Odpovídá-li Zhotovitel za vady Díla, má Objednatel práva z vadného plnění.
136. Objednatel je oprávněn vady reklamovat u Zhotovitele jakýmkoliv způsobem, preferovaná je písemná forma. Zhotovitel je povinen přijetí reklamace bez zbytečného odkladu písemně potvrdit. V reklamaci Objednatel uvede popis vady nebo uvede, jak se vada projevuje.
137. Vada je uplatněna včas, je-li písemná forma reklamace odeslána Zhotoviteli nejpozději v poslední den Záruční doby. Připadne-li konec Záruční doby na sobotu, neděli nebo svátek, je vada včas uplatněna, je-li písemná forma reklamace odeslána Zhotoviteli nejblíže následující pracovní den.
138. Má-li Předmět díla vady, za které Zhotovitel odpovídá, má Objednatel právo
    138.1. na odstranění vady dodáním nového Předmětu díla nebo jeho části bez vady, pokud to není vzhledem k povaze vady zcela zřejmě nepřiměřené, nebo dodání chybějící části Předmětu díla,
    138.2. na odstranění vady opravou Předmětu díla nebo jeho části,
    138.3. na přiměřenou slevu z Ceny díla, nebo
    138.4. odstoupit od Smlouvy o dílo.
139. Objednatel je oprávněn požadovat odstranění vad dodáním nového Předmětu díla nebo jeho části bez vady, vyskytla-li se stejná vada po její opravě opětovně, nebo nemůže-li Objednatel řádně užívat Předmět díla nebo jeho část pro větší počet vad.
140. Objednatel je oprávněn nároky dle odstavce 138 kombinovat, je-li to vzhledem k okolnostem možné. Objednatel není oprávněn kombinovat nároky, které si navzájem odporují (např. dodání nové části Předmětu díla a zároveň slevy z Ceny díla na tutéž část Předmětu díla).
141. Objednatel sdělí Zhotoviteli volbu nároku z vady v reklamaci, nebo bez zbytečného odkladu po reklamaci. Provedenou volbu nemůže Objednatel změnit bez souhlasu Zhotovitele; to neplatí, žádal-li Objednatel opravu vady, která se ukáže jako neopravitelná.
142. Nesdělí-li Objednatel Zhotoviteli, jaké právo si zvolil ani bez zbytečného odkladu poté, co jej k tomu Zhotovitel vyzval, může Zhotovitel odstranit vady podle své volby opravou nebo dodáním nového Předmětu díla nebo jeho části; volba nesmí Objednateli způsobit nepřiměřené náklady.
143. Objednatel má nárok na náhradu nákladů účelně vynaložených v souvislosti s oznámením vad Zhotoviteli.

ČÁST 17 - PODMÍNKY ODSTRANĚNÍ VAD

144. Pokud Objednatel požaduje v reklamaci odstranění vady, je Zhotovitel povinen neprodleně po obdržení reklamace zahájit činnosti vedoucí k odstranění reklamované vady. Pokud Objednatel v reklamaci uvede, že se jedná o havárii, je Zhotovitel povinen zahájit odstraňování vady nejpozději do 48 hodin po obdržení reklamace.
145. Zhotovitel je povinen odstranit Objednatelem reklamovanou vadu nejpozději do 30 dnů ode dne oznámení vady Zhotoviteli. Jde-li o vadu označenou Objednatelem v reklamaci jako havarijní, je Zhotovitel povinen odstranit vadu nejpozději do 5 dnů.

146. Nezahájí-li Zhotovitel činnosti vedoucí k odstranění vady do 10 dnů od oznámení vady Zhotoviteli, nebo nebude-li vada odstraněna ve lhůtě dle předcházejícího odstavce, je Objednatel oprávněn
    146.1. zajistit odstranění vady jinou odborně způsobilou právnickou nebo fyzickou osobou na účet Zhotovitele,
    146.2. požadovat slevu z Ceny díla, nebo
    146.3. od Smlouvy o dílo odstoupit.
147. Veškeré náklady vzniklé Objednateli v souvislosti s odstranění vady způsobem dle předchozího odstavce je Zhotovitel povinen Objednateli uhradit.
148. Zhotovitel je povinen odstranit vadu bez ohledu na to, zda je uplatnění vady oprávněné či nikoli. Prokáže-li se však kdykoli později, že uplatnění vady Objednatelem nebylo oprávněné, tj. že Zhotovitel za vadu neodpovídal, je Objednatel povinen uhradit Zhotoviteli veškeré jím účelně vynaložené náklady v souvislosti s odstraněním vady.
149. Objednatel je povinen poskytnout Zhotoviteli součinnost nezbytnou k odstranění vady.
150. Do odstranění vady nemusí Objednatel platit dosud nezaplacenou část Ceny díla a případnou příslušnou DPH odhadem přiměřeně odpovídající jeho právu na slevu.
151. Při dodání nového Předmětu díla nebo jeho části vrátí Objednatel Zhotoviteli na náklady Zhotovitele Předmět díla nebo jeho část původně dodanou.
152. Týká-li se vada Dokladů nebo jiného plnění poskytnutého Zhotovitelem dle Smlouvy o dílo než Předmětu díla, užijí se ustanovení odstavců 135 – 151 obdobně.
153. Ustanovení §1917–1924, §2099–2101, §2103 – 2117, §2165 – 2172, §2618 a §2629 Občanského zákoníku se neužijí.

ČÁST 18 - POJIŠTĚNÍ

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

ČÁST 19 - DUŠEVNÍ VLASTNICTVÍ

160. Zhotovitel je povinen při provádění Díla postupovat tak, aby při provádění Díla ani následným užíváním Díla Objednatelem nedošlo k porušení práv duševního vlastnictví. Bude-li v souvislosti s Dílem, jakkoliv dotčeno právo k duševnímu vlastnictví, je Zhotovitel povinen upravit veškeré právní vztahy s osobami, kterým taková práva náležejí nebo jež jsou oprávněny je vykonávat, tak, aby zamezil vznášení jakýchkoli oprávněných nároků těchto osob ve vztahu k Objednateli.
161. Zhotovitel tímto poskytuje Objednateli oprávnění k výkonu práva duševního vlastnictví (licenci nebo podlicenci) ke všem plněním poskytnutým Objednateli při provádění Díla,

které jsou nebo budou předmětem duševního vlastnictví a ke kterým je oprávněn takové oprávnění poskytnout. Oprávnění Zhotovitel poskytuje

161.1. bezúplatně,
161.2. jako nevýhradní,
161.3. z hlediska časového a územního v rozsahu neomezeném,
161.4. z hlediska věcného rozsahu (způsobu užití) tak, že opravňuje Objednatele ke všem známým způsobům užití,
161.5. bez množstevního omezení.

162. Objednatel není povinen oprávnění využít.
163. Objednatel je oprávněn oprávnění tvořící součást licence nebo podlicence poskytnout nebo též postoupit třetí osobě zcela nebo zčásti.
164. Zhotovitel se zavazuje, že na žádost Objednatele autor nebo autoři autorského díla, jež je součástí nebo příslušenstvím Díla, udělí Objednateli bez zbytečného odkladu bezúplatně právo

164.1. upravit či jinak změnit označení autora,
164.2. autorské dílo nebo jeho název upravit či jinak měnit,
164.3. autorské dílo s jakýmkoliv jiným autorským dílem spojit či zařadit do díla souborného.

165. Žádný výsledek činnosti provedené na základě Smlouvy o dílo nebo v souvislosti s ní, který je předmětem duševního vlastnictví, není Zhotovitel oprávněn bez předchozího písemného svolení Objednatele užít k jiným účelům, než je provedení Díla, zejména je nesmí poskytnout třetím osobám.

ČÁST 20 - SANKCE

166. Poruší-li Zhotovitel povinnost provést Dílo ve sjednané době, je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 0,5 % z Ceny díla za každý den prodlení.
167. Poruší-li Objednatel povinnost zaplatit Cenu díla ve sjednané době, je povinen uhradit Zhotoviteli zákonný úrok z prodlení ve výši dle právních předpisů.
168. Poruší-li Zhotovitel povinnost odstranit vadu Díla ve sjednané době, je povinen uhradit Objednateli smluvní pokutu ve výši 0,5 % z Ceny díla za každý den prodlení až do odstranění vady. Jde-li o vadu, kterou Objednatel označil v reklamaci jako havárii, je Zhotovitel povinen uhradit smluvní pokutu ve dvojnásobné výši.
169. Poruší-li Zhotovitel povinnost nepostoupit žádnou svou pohledávku za Objednatelem vyplývající ze Smlouvy o dílo a/nebo poruší zákaz zřídit zástavní právo k pohledávce, byť by takové postoupení a/nebo zřízení zástavního práva bylo neplatné či neúčinné, je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 10 % z nominální hodnoty postoupené a/nebo zastavené pohledávky, včetně hodnoty případného příslušenství ke dni účinnosti postoupení vůči postupníkovi.
170. Poruší-li Zhotovitel jakékoliv jiné povinnosti vyplývající ze Smlouvy o dílo, Obchodních podmínek nebo Veřejnoprávních podkladů než povinnosti, na které se vztahuje smluvní pokuta dle této části, je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 5% z Ceny díla za každý jednotlivý případ porušení povinnosti.
171. Poruší-li Zhotovitel nebo osoba, kterou Zhotovitel používá při provádění díla jakoukoliv povinnost stanovenou Směrnicí SŽDC č. 120 Dodržování zákazu kouření, požívání alkoholických nápojů a užívání jiných návykových látek, č.j. 36503/2017-SŽDC-GŘ-O10 ze dne 3.11.2017, účinnou od 7.1.1.2017 v rámci Objednatelem prováděné kontroly na základě výše uvedené směrnice je Objednatel oprávněn na základě posouzení souvisejících okolností, uplatnit vůči Zhotoviteli sankci ve výši 5 000,- Kč za každý jednotlivý případ.
172. Zaplacení smluvní pokuty nezbavuje Zhotovitele povinnosti splnit dluh smluvní pokutou utvrzený.
173. Objednatel je oprávněn požadovat náhradu škody a nemajetkové újmy způsobené porušením povinnosti, na kterou se vztahuje smluvní pokuta, v plné výši.

ČÁST 21 - OBECNÁ ODPOVĚDNOST ZHOTOVITELE

174. Zhotovitel je povinen po dobu plnění povinností ze Smlouvy o dílo chránit majetek Objednatele i třetích osob před jeho poškozením, znehodnocením, zničením a ztrátou a postupovat tak, aby neomezoval práva osob nad míru nezbytnou k provádění Díla.
175. Způsobí-li Zhotovitel v souvislosti s Dílem nebo porušením svých povinností vyplývajících ze Smlouvy o dílo, Obchodních podmínek, Veřejnoprávních podkladů, právních předpisů a příslušných ČSN jakoukoli újmu Objednateli nebo třetím osobám, je povinen nahradit Objednateli škodu a nemajetkovou újmu, včetně případných sankcí udělených Objednateli orgány státní správy, jejichž příčinou bylo porušení smluvních povinností Zhotovitele, a jde-li o újmu způsobenou třetím osobám, je povinen způsobenou újmu na vlastní náklady bezodkladně odčinit.
176. Újmou se pro účely Obchodních podmínek rozumí zejm. jakékoliv poškození, znehodnocení, či znečištění věcí nebo prostor nebo jejich jiná nežádoucí změna a jakékoliv neoprávněné omezení práv Objednatele nebo třetích osob.
177. Zhotovitel odpovídá za jakékoli porušení svých povinností stanovených Smlouvou o dílo, Obchodními podmínkami, Veřejnoprávními podklady, právními předpisy a příslušnými ČSN a je povinen uhradit veškeré pokuty udělené mu příslušnými orgány státní správy v souvislosti s prováděním Díla ze svého, ledaže mu byla pokuta udělena v souvislosti s respektováním příkazu Objednatele, proti kterému uplatnil písemnou výhradu a na jehož splnění Objednatel trval anebo v souvislosti s užitím Objednatelem opatřené věci, na jejíž nevhodnost Objednatele písemně upozornil a Objednatel na jejím užití trval.
178. Povinnosti k náhradě újmy způsobené porušením svých povinností ze Smlouvy o dílo, Obchodních podmínek, Veřejnoprávních podkladů, právních předpisů a příslušných ČSN se Zhotovitel vůči Objednateli zprostí, prokáže-li, že mu ve splnění povinnosti zabránila mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na jeho vůli. Překážka vzniklá z osobních poměrů Zhotovitele nebo vzniklá až v době, kdy byl Zhotovitel s plněním povinnosti v prodlení, ani překážka, kterou byl Zhotovitel povinen překonat, jej však povinnosti k náhradě nezprostí.

ČÁST 22 - ODSTOUPENÍ OD SMLOUVY O DÍLO

179. Poruší-li Smluvní strana Smlouvu o dílo podstatným způsobem, může druhá Smluvní strana písemnou formou od Smlouvy o dílo odstoupit.
180. Podstatné je takové porušení povinnosti, o němž Smluvní strana porušující Smlouvu o dílo již při uzavření Smlouvy o dílo věděla nebo musela vědět, že by druhá Smluvní strana Smlouvu o dílo neuzavřela, pokud by toto porušení předvídala, nebo je-li porušení povinnosti ve Smlouvě o dílo nebo v Obchodních podmínkách jako podstatné označeno; v ostatních případech se má za to, že porušení podstatné není.
181. Podstatným porušením Smlouvy o dílo je též prodlení Zhotovitele a Objednatele s plněním povinností vyplývajících Zhotoviteli a Objednateli ze Smlouvy o dílo o více než 30 dní.
182. Objednatel je oprávněn od Smlouvy o dílo odstoupit též
    182.1. z důvodů uvedených v části Předání a převzetí Díla (viz ČÁST 13 - Obchodních podmínek),
    182.2. nabylo-li právní moci rozhodnutí o nařízení exekuce vůči Zhotoviteli jako povinnému,
    182.3. ocitne-li se Zhotovitel ve stavu úpadku nebo hrozícího úpadku,
    182.4. jestliže Zhotovitel nebo jeho poddodavatel, nebo z jejich pokynu jakákoliv osoba, nabídne nebo poskytne jakékoliv osobě úplatek nebo jiný majetkový či jiný prospěch za účelem získání neoprávněného prospěchu nebo výhody v souvislosti s Dílem nebo jeho prováděním,
    182.5. uvedl-li Zhotovitel v Nabídce informace nebo doklady, které neodpovídají skutečnosti a měly nebo mohly mít vliv na výsledek řízení,
    182.6. stanoví-li tak Smlouvy o dílo.

183. Smluvní strana může od Smlouvy o dílo odstoupit, pokud z chování druhé Smluvní strany nepochybně vyplyne, že poruší Smlouvu o dílo podstatným způsobem, a nedá-li na výzvu oprávněné Smluvní strany přiměřenou jistotu.
184. Jakmile Smluvní strana oprávněná odstoupit od Smlouvy o dílo oznámí druhé Smluvní straně, že od Smlouvy o dílo odstupuje, nebo že na Smlouvě o dílo setrvává, nemůže volbu již sama změnit.
185. Zakládá-li prodlení Smluvní strany nepodstatné porušení její povinnosti ze Smlouvy o dílo, může druhá Smluvní strana od Smlouvy o dílo odstoupit poté, co prodlévající Smluvní strana svoji povinnost nesplní ani v dodatečné přiměřené lhůtě, kterou jí druhá Smluvní strana poskytla výslovně nebo mlčky.
186. Oznámí-li Smluvní strana Smluvní straně prodlévající, že jí určuje dodatečnou lhůtu k plnění a že jí lhůtu již neprodlouží, platí, že marným uplynutím této lhůty od Smlouvy o dílo odstoupila.
187. Poskytla-li Smluvní strana Smluvní straně prodlévající nepřiměřeně krátkou dodatečnou lhůtu k plnění a odstoupí-li od Smlouvy o dílo po jejím uplynutí, nastávají účinky odstoupení teprve po marném uplynutí doby, která měla být prodlévající Smluvní straně poskytnuta jako přiměřená. To platí i tehdy, odstoupila-li Smluvní strana od Smlouvy o dílo, aniž by prodlévající Smluvní straně dodatečnou lhůtu k plnění poskytla.
188. Plnil-li Zhotovitel zčásti, může Smluvní strana od Smlouvy o dílo odstoupit jen ohledně nesplněného zbytku plnění. Nemá-li však částečné plnění pro Objednatele význam, může Objednatel od Smlouvy o dílo odstoupit ohledně celého plnění. Odstoupil-li od nesplněného zbytku plnění Zhotovitel, je Objednatel oprávněn odstoupit od splněné části Smlouvy o dílo, nemá-li částečně plnění pro Objednatele význam.
189. Zavazuje-li Smlouva o dílo Zhotovitele k opakované činnosti nebo k postupnému dílčímu plnění, může Objednatel od Smlouvy o dílo odstoupit jen s účinky do budoucna. To neplatí, nemají-li již přijatá dílčí plnění sama o sobě pro Objednatele význam.
190. Smluvní strany se dohodly, že dojde-li k odstoupení od Smlouvy o dílo jen ohledně nesplněného zbytku plnění, užijí se na splněnou část plnění obdobně všechna ustanovení Smlouvy o dílo a Obchodních podmínek týkající se předání a převzetí Díla, přičemž přejímací řízení Smluvní strany zahájí nejpozději do 3 pracovních dnů ode dne odstoupení od Smlouvy o dílo, a dále všechna ustanovení Smlouvy o dílo a Obchodních podmínek o právech a povinnostech Smluvních stran, které jsou Smluvní stany povinny plnit v době ode dne převzetí Díla Objednatelem, tedy zejm. ustanovení o vadách Díla.
191. Ustanovení §1977, §2002–2003 Občanského zákoníku se neužijí.

ČÁST 23 - OSTATNÍ UJEDNÁNÍ

Částečné plnění

192. Ustanovení Smlouvy o dílo a Obchodních podmínek platí obdobně též pro části Díla, provádí-li Zhotovitel Dílo v souladu se Smlouvou o dílo po částech, není-li uvedeno jinak.

Postoupení, započtení

193. Zhotovitel není oprávněn postoupit žádnou svou pohledávku za Objednatelem vyplývající ze Smlouvy o dílo nebo vzniklou v souvislosti se Smlouvou o dílo.
194. K pohledávce za Objednatelem vyplývající se Smlouvy o dílo nebo vzniklé v souvislosti se Smlouvou o dílo nesmí být zřízeno zástavní právo.
195. Zhotovitel není oprávněn provést jednostranné započtení žádné své pohledávky za Objednatelem vyplývající ze Smlouvy o dílo nebo vzniklé v souvislosti se Smlouvou o dílo na jakoukoliv pohledávku Objednatele za Zhotovitelem.
196. Objednatel je oprávněn provést jednostranné započtení jakékoliv své splatné i nesplatné pohledávky za Zhotovitelem vyplývající ze Smlouvy o dílo nebo vzniklé v souvislosti se Smlouvou o dílo (zejm. smluvní pokutu) na jakoukoliv splatnou či nesplatnou pohledávku Zhotovitele za Objednatelem.

Mlčenlivost

197. Zhotovitel je povinen zachovávat mlčenlivost o všech skutečnostech a informacích, které jsou obsažené ve Smlouvě o dílo a dále o všech skutečnostech a informacích, které mu byly v souvislosti se Smlouvou o dílo nebo jejím plněním, jakkoliv zpřístupněny, předány

či sděleny, nebo o nichž se jakkoliv dozvěděl, vyjma těch, které jsou v okamžiku, kdy se s nimi Zhotovitel seznámil, prokazatelně veřejně přístupné, nebo těch, které se bez zavinění Zhotovitele veřejně přístupnými stanou. Zhotovitel nesmí takové skutečnosti a informace použít v rozporu s jejich účelem, nesmí je použít ve prospěch svůj nebo třetích osob a nesmí je použít ani v neprospěch Objednatele. Povinnosti dle tohoto odstavce je Zhotovitel povinen zachovávat i po zániku závazku ze Smlouvy o dílo, vyjma případů, kdy se takové skutečnosti a informace stanou prokazatelně veřejně přístupné bez zavinění Zhotovitele. Povinnosti dle tohoto odstavce se nevztahují na případy, kdy je Zhotovitel povinen zveřejnit takové skutečnosti nebo informace na základě povinnosti uložené mu právním předpisem nebo rozhodnutím orgánu veřejné moci.

Poskytování informací

198. Vzhledem k veřejnoprávnímu charakteru Objednatele Zhotovitel výslovně prohlašuje, že je s touto skutečností obeznámen a souhlasí se zveřejněním Smlouvy o dílo včetně Obchodních podmínek v rozsahu a za podmínek vyplývajících z příslušných právních předpisů.

Kontrola

199. Zhotovitel si je vědom, že je ve smyslu §2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů, povinen spolupůsobit při výkonu finanční kontroly a zavazuje se finanční kontrolu strpět.
200. Je-li Dílo z jakékoliv části financováno z prostředků Evropské unie, je Zhotovitel povinen
    200.1. strpět veškeré kontroly vyplývající z režimu financování Díla z prostředků Evropské unie,
    200.2. poskytnout při takových kontrolách veškerou nezbytnou součinnost,
    200.3. archivovat veškerou dokumentaci týkající se Smlouvy o dílo po dobu stanovenou pravidly, jimiž se řídí financování Díla z prostředků Evropské unie.

Jazyk

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

Forma, označení času

202. Písemnou formou (podobou) se rozumí listina podepsaná oprávněnou osobou Smluvní strany nebo email podepsaný zaručeným elektronickým podpisem oprávněné osoby Smluvní strany.
203. Je-li ve Smlouvě o dílo nebo Obchodních podmínkách uvedena lhůta nebo doba počítané podle dnů, měsíců nebo let, rozumí se tím vždy kalendářní den, měsíc nebo rok, není-li uvedeno jinak.

Reference

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

Salvatorní klauzule

205. Je-li nebo stane-li se některé oddělitelné ustanovení Smlouvy o dílo nebo Obchodních podmínek neplatné, neúčinné či nevymahatelné, nedotýká se tato skutečnost ostatních ustanovení. Smluvní strany se zavazují nahradit takové ustanovení jiným ustanovením, které svým obsahem a smyslem bude nejvíce odpovídat obsahu a smyslu ustanovení nahrazovaného.

SPRÁVA ŽELEZNIC

Příloha č. 9 Smlouvy

Realizační tým

Účastník:

Obchodní firma/jméno	ALEF NULA, a.s.
Sídlo/místo podnikání	Pernerova 691/42, 186 00 Praha 8
IČO	61858579
Zastoupen	Ing. Milanem Zinkem, předsedou představenstva

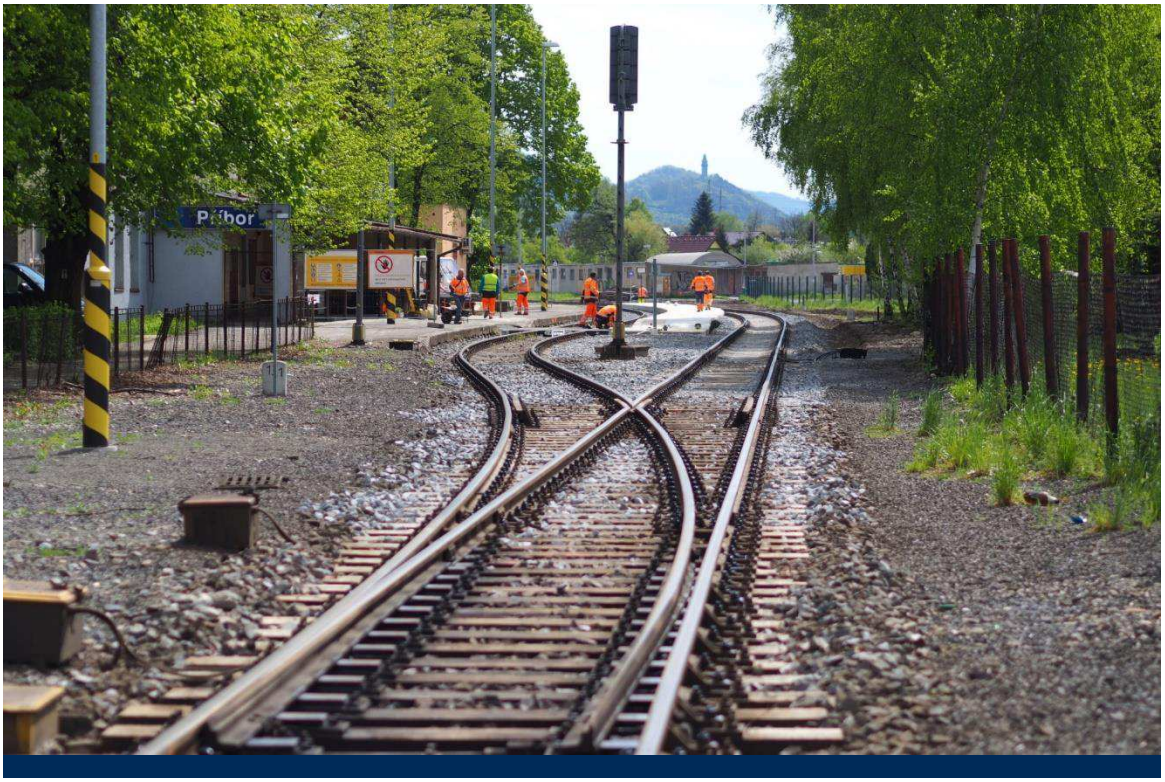
který podává nabídku na nadlimitní sektorovou veřejnou zakázku s názvem **„Log management a SIEM", č.j. 61441/2023-SŽ-GŘ-O8**, tímto níže předkládá seznam členů realizačního týmu, kteří se budou na plnění předmětu veřejné zakázky podílet:

Pozice člena realizačního týmu	Jméno a příjmení
Bezpečnostní architekt	xxx
SIEM architekt	xxx
Administrátor SIEM	xxx
Administrátor SIEM	xxx
Administrátor SIEM	xxx
Projektový manažer	xxx

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

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

SPRÁVA ŽELEZNIC



Platforma SŽ 2.0: Vymezení služeb

Březen 2022

SPRÁVA ŽELEZNIC

Historie verzí

Verze	Popis	Platnost od	Předchozí verze
1.0	Úvodní verze Platformy SŽ	27.01.2020	
2.0	Aktualizace Platformy SŽ s názvem „Platforma SŽ 2.0: Vymezení služeb“	01.04.2022	

Obsah

Seznam zkratek

APP	Aplikační vrstva
AS	Aplikační server
AU	Archivní úložiště
DB	Databáze
DR	Disaster Recovery
HW	Hardware označuje veškeré fyzicky existující technické vybavení počítače
OS	Operační systém
SW	Software je sada všech počítačových programů používaných v počítači, které provádějí nějakou činnost
SŽ	Správa železnic, státní organizace
SŽT	Správa železničních informačních technologií
VM	*z angl. „Virtual Machine".* Virtuální stroj
WLS	WebLogic Server
WS	Webový server
ZZVZ	Zákon o zadávání veřejných zakázek

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 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. Primárním cílem Platformy SŽ je poskytnout potenciálním dodavatelům přehled o prostředí SŽ a současně umožnit organizaci SŽ zajištění efektivního vytváření a provozování ICT řešení při dodržení vysoké kvality a bezpečnosti služeb.

Dokument je udržován a pravidelně aktualizován jednotkou SŽT.

Platforma SŽ obsahuje:

- Architektonické principy SŽ
- Katalog služeb Platformy SŽ
- Katalog technologií Platformy SŽ

Při plánování a rozšiřování ICT řešení je nutné respektovat všechny části Platformy SŽ.

Navíc v případech zakázkového vývoje software pro SŽ musí dodavatel splnit požadavky definované v dokumentu Standardy vývoje informačních systémů SŽ, který je přílohou tohoto dokumentu.

3 Motivace Platformy SŽ

Cílem Správy železnic je zajistit, že:

- Uchazeči výběrových řízení na ICT řešení budou hodnoceni na základě jejich celkové ekonomické efektivity, a nikoliv pouze na základě nabídkové ceny,
- 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 prostředí SŽ bude:
    - na jednu stranu dostatečně široká, aby neúměrně neomezovala soutěž potenciálních dodavatelů, a
    - na druhou stranu dostatečně ohraničená, aby umožnila efektivní správu systémů zaměstnanci a dodavateli 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].

Očekává se, že tento dokument pomůže s nastavením jasných povinných parametrů pro nové uchazeče v oblasti technologických standardů SŽ.

Mezi přínosy dokumentu Platformy SŽ 2.0 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.
- Zajištění možnosti bezpečného převzetí systémů do provozu a zajištění provozu interními silami SŽ.

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

4 Architektonické principy

Kapitola stanovuje základní rámec pravidel a principů, které je nutné respektovat při návrhu a realizaci ICT řešení podle Platformy SŽ.

P01: Bezpečnost a soulad s vnitropodnikovými předpisy

- Navrhované řešení a procesy jím podporované musí být v souladu s legislativními a regulatorními nároky a vnitropodnikovými předpisy Správy železnic.
- Řešení musí umožnit monitorování akcí uživatelů, zejména jejich práce s daty a dokumenty.
- Musí být zajištěna administrovatelnost a auditovatelnost integračních vazeb.
- Vývoj a test není 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 je zajištěn na všech vrstvách řešení (HW, OS, DB, AS, aplikace, koncový uživatel).
- Musí být zajištěno napojení na centrální dohledovou konzoli.
- Služby poskytované do prostředí internetu budou procházet penetračním testem.

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 Vyhláškou č. 82/2018 Sb.o Kybernetické bezpečnosti.

P02: 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.

P03: 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 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.

P04: Nezávislost na dodavatelích

- Řešení je navrhované s ohledem na omezení či eliminaci rizika vendor-lock.

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

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

P05: 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 nového zákaznického řešení.
- Vzájemné integrace musí být realizované přes aplikační middleware. Integrační scénáře zajišťují, aby implementace nových funkcí v řídící aplikaci minimalizovala vyvolané změny na straně návazných aplikací.
- Preferujeme přírůstkovou integraci před přenosem kompletních informací.
- Preferujeme řešení v min. třívrstvé či vícevrstvé architektuře s min. 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 a uživatelské.
- Případné zdrojové kódy jsou verzovány a ověřeny, že z nich je možno vytvořit interními týmy Správy železnic build aplikace. Zdrojové kódy a dokumentace jsou ukládány na standardizované úložiště Správy železnic.
- Návrh prostředí reflektuje trendy technologií a zároveň business potřeby.

Zdůvodnění: Regulace nákupu a 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.

P06: Business kontinuita jako zásadní činnost

- 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 a „disaster recovery" postupy.

Zdůvodnění: Správa železnic jakožto správce železniční dopravní cesty, 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

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.

ICT služby Platformy jsou rozděleny do následujících skupin (kategorií):

- **Infrastrukturní**
  Infrastrukturní službou je míněno poskytování IT infrastruktury na úrovni HW, virtualizace, operačních systémů a diskových úložišť.
- **Platformní**
  Platformní služba poskytuje databázovou platformu či portálové řešení, které integruje webové aplikace a služby do jednoho spolupracujícího celku. Podporuje standardizované komunikační protokoly a formáty dat.
- **Podpůrné**
  Podpůrné služby zajišťují komplexní správu a provoz IT infrastruktury. Například monitorovací systémy, zálohování, reporting. Podpůrné služby jsou povinné k využití dodavatelem, pokud není jinak určeno SŽ.

5.1 Infrastrukturní služby

5.1.1 Služba virtuálních strojů

Služba virtuálních strojů (dále jen „VM“) je provozována na vysoce dostupné virtualizační technologii VMware a hardware s procesory Intel Xeon E5-26XX, Intel Silver 4215. Všechna VM s operačním systémem Windows Server mají nainstalován balík VMware Open Tool.

Parametry služby jako sizing virtuálních strojů, výběr OS podporovaných Platformou SŽ 2.0, počet a konfigurace síťových karet jsou konfigurovány individuálně na základě požadavků projektu, resp. dodávaného řešení.

SŽ zajišťuje vysokou dostupnost služby virtuálních strojů na úrovni vi, a to v rámci jednoho datového centra. Pokud služby dodávaného řešení vyžadují zajištění vysoké dostupnosti, tato musí být zajištěna dodavatelem v rámci dodávky včetně služby loadbalancingu.

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
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

5.1.2 Služba datového uložiště

Služba datového úložiště je provozována na datových úložištích typu SAN, která jsou osazena 10K SAS disky v RAID5 (+hotspare disk) případně RAID 6, nebo disky SSD v RAID5 (+hotspare disk) pro aplikace vyžadující vyšší výkon, typicky databáze. V rámci služby datového uložiště není poskytována služba replikace mezi SAN úložišti, ani služba tieringu. V primárním datovém centru CDP je dále provozováno škálovatelné, výkonné, softwarově-definované datové uložiště postavené na technologii VMware vSAN, využívající prostředků fyzických serverů x86 a jejich komponent (cpu, ram, nic a disk). VMware vSAN je nativně integrované s hypervisorem VMware ESXi.

Služba	Popis
Lokální datový disk 10K	Služba datového uložiště, provozovaného na SAN storage a 10K discích v RAID 5 (+hotspare) případně RAID 6 poli, pro systémové a datové disky.
Lokální datový disk SSD	Služba datového uložiště, provozovaného na SAN storage osazeného SSD disky v poli RAID5 (+hotspare).

5.2 Platformní služby

Platformní služba (PaaS – Platform as a Service) poskytuje databázovou či integrační platformu (middleware). Tato integruje aplikace a služby do jednoho spolupracujícího celku. Podporuje standardizované komunikační protokoly a formáty dat.

V rámci platformy Správy železnic jsou poskytovány tyto platformní služby:

5.2.1 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.

5.2.2 Služby zabezpečených webových serverů

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

5.2.3 Služby zabezpečených aplikačních serverů

Služba	Popis
.NET na Win.VMware.x86_64	Aplikační server Microsoft .NET prostředí pro vývoj a provoz aplikací založených na .NET frameworku
JBOSS na Win.VMware.x86_64	Služba virtuálního aplikačního serveru JBOSS provozovaná na serverech s operačním systémem Windows Server s virtualizací VMware.
Oracle WebLogic na RHEL.VMware.x86_64	Služba virtuálního aplikačního Oracle WebLogic Serveru (WLS), pro provoz aplikací postavených na standardu JAVA EE na serverech s operačním systémem RHEL s virtualizací VMware.
Oracle WebLogic na SLES.VMware.x86_64	Služba virtuálního aplikačního Oracle WebLogic Serveru (WLS), pro provoz aplikací postavených na standardu JAVA EE na serverech s operačním systémem SLES s virtualizací VMware.
Oracle WebLogic na Win.VMware.x86_64	Služba virtuálního aplikačního Oracle WebLogic Serveru (WLS), pro provoz aplikací postavených na standardu JAVA EE na serverech s operačním systémem Windows Server s virtualizací VMware.

5.2.4 Služby zabezpečených 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.

5.3 Podpůrné služby

Podpůrné služby standardně poskytované k využití pro dodávaná ICT řešení.

5.3.1 Bezpečnost

Služby zabezpečení infrastruktury.

Služba	Popis
Antivirus	Antivirové řešení fSecure, provozované jako virtualní 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 fSecure. Nasazením antivirového řešení fSecure jako virtuální appliance, jsou minimalizovány konzumované výpočetní zdroje a dopad na výkon virtualizační infrastruktury.
PAM	Privileged Access Management (PAM) je řešení které pomáhá kontrolovat, monitorovat, zabezpečit a auditovat privilegované identity před jejich zneužitím. Omezení: Aktuálně v pilotním provozu
IDM	Identity Management (IDM) je řešení umožňující řízení uživatelských účtů a jejich oprávnění napříč systémy. IDM umožňuje lepší přehlednost, bezpečnost a automatizaci. V prostředí Správy žželeznic bylo implementováno open-source řešení MidPoint společnosti Evolveum, jenž nevyžaduje nákup licencí. Toto řešení má otevřenou a rozšiřitelnou architekturu založenou na standardech Java, XML a REST.
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.

5.3.2 Monitoring, alerting

Služba	Popis
Monitoring	
Zabbix	Služba dohledu infrastruktury je zajištěna pomocí dohledových agentů instalovaných na provozovaném prostředí nebo bez-agentově se vzdáleným dohledem, sledování standardními protokoly SNMP, HTTP, HTTPS apod. Dodavatelé ve spolupráci s jednotkou SŽT zajistí napojení dodávaných řešení na monitoring Zadavatele. Tím není dotčena případná povinnost dodavatele řešení monitorovat kvalitu a dostupnost dodávaného řešení v rámci vlastního monitoringu.

5.3.3 Aktualizace systémů, Distribuce aplikací

Služba	Popis
Aktualizace	
Distribuce SW a aktualizace koncových stanic	Technologií System Center Configuration Manager (SCCM) je zajištěna distribuce softwarových balíčků a aktualizace koncových stanic. Patchování klientských stanic probíhá 1 x měsíčně a je plně v gesci Správy železnic.
Aktualizace serverových operačních systémů	Aktualizace serverových operačních systému Windows Server je řešena skriptovacím jazykem Powershell. Patchování serverových operačních systémů probíhá 1 x měsíčně a je zajištěno Správou železnic, pokud není s dodavatelem řešení dohodnuto jinak. Aktualizace serverových operačních systémů založených na linuxové distribuci je prováděna manuálně, na vyžádání správce aplikace, nebo v reakci na kybernetické hrozby.

5.3.4 Zálohování

Služba	Popis
Zálohování a obnova	Služba zálohování prostředí je zajištěna technologií IBM Spectrum Protect (TSM – Tivoli Storage Manager) komplexním řešením pro fyzické fileservery, virtualizované prostředí a širokou škálu aplikací. IBM Spectrum Protect zálohuje data s využitím technologie VMware snapshot. 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

Služba	Popis
	virtualizovaného serveru. Záloha probíhá jednou denně a retence je nastavena na 30 posledních verzí. Záloha datových svazků připojených k jednotlivým serverům, pro dosažení max. 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 Oracle nebo SQL databází 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.

5.3.5 Komunikační infrastruktura

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	Firewall soustava je velmi důležitým uzlem veškeré komunikace v síti SŽ, jenž pomocí pravidel filtruje síťový provoz a chrání prostředky v síti Správy železnic.
Proxy	Proxy soustava zajišťuje přístup uživatelů a serverů k internetu. Naprostá většina komunikace uživatelů do internetu 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 k prostředkům datových center Správy železnic.
VPN S2S	Služba virtuální privátní sítě Site-to-Site.

6 Technologie Platformy SŽ

Tato kapitola popisuje technologie, jež tvoří základ k výše uvedeným infrastrukturním a platformním službám.

Tyto softwarové a hardwarové prostředky nesmějí být přímo použity v návrhu řešení. Jejich použití je možné pouze prostřednictvím výše uvedených infrastrukturních nebo platformních služeb.

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 či bezpečnostní zajištění.

Při použití zapouzdřených technologií je nutné danou technologii identifikovat nejméně v následujícím rozsahu:

- Název
- Verze
- Výrobce
- Licence
- Termín a úroveň podpory

Technologie	Popis
Integrace	
LifeRay	Bezplatný open-source podnikový portál založený na jazyce Java, umožňující správu dat, aplikací a procesů.
Aplikační servery	
Microsoft Internet Information Services (IIS)	Framework pro běh třívrstvých podnikových aplikací s kolekcí rozšiřujících modulů provozovaný nad operačními systémy Windows, vytvořený společností Microsoft.
Oracle WebLogic Server	Aplikační server Oracle WebLogic Server (WLS) pro provoz aplikací na platformě J2EE
JBoss	Aplikační server JBoss pro provoz platformy J2EE pro řešení s potřebou autonomního prostředí, nebo pro aplikace nepožadující vysokou dostupnost
Webové servery	
Apache HTTP Server	Webový server postavený na open-source technologii Apache.
MS IIS	Webový server s kolekcí rozšiřujících modulů provozovaný nad operačními systémy Windows, vytvořený společností Microsoft.
Databázové systémy	
Oracle Database	Relační databázový systém společnosti Oracle určený pro mission critical aplikace.
Microsoft SQL	Relační a analytický databázový systém Microsoft SQL Server.
Serverové operační systémy	
Windows Server	Operační systém, na němž jsou provozovány aplikační či webové služby a databázové stroje založené zejména na technologiích společnosti Microsoft.
RHEL	Operační systém RedHat Enterprise Linux (RHEL) je linuxová distribuce společnosti RedHat určená pro komerční sféru. Použití pro aplikační servery.
SLES	Operační systém SUSE Linux Enterprise Server (SLES) je linuxová distribuce společnosti SUSE určená pro komerční sféru. Použití pro aplikační servery.
Virtualizační platformy	
VMware	Primární virtualizační platforma pro virtualizaci hardwarové platformy x86_64. Tato zajišťuje business kontinuitu, škálovatelnost a flexibilitu provozu pro operační systémy. Platforma je primárně určena pro virtualizaci operačních systému Windows, případně Linux.
Oracle VM	Virtualizační platforma Oracle, pro virtualizaci hardwarové platformy x86_64 založena na technologii Citrix Xen Hypervisor. Omezené využití: Primárně určena pro provoz Oracle DB.
Hardware	
x86_64	Servery postavené na architektuře x86_64 – 64bitové procesory, provozovány na platformě Intel 2-socketových serverech typu rack a blade.
SAN datová uložiště	Uložiště dat s podporou vysoké dostupnosti, škálování a vysokou úrovní zabezpečení. Podporuje vytváření snapshotů, replikaci dat a automatický tiering datových uložišť.
Network and Security	
VPN	Zabezpečený vzdálený přístup do sítě SŽ je řešen pomocí technologie Cisco ASA.
Firewall	Zabezpečení pomocí firewall pravidel je zabezpečeno technologií Cisco.

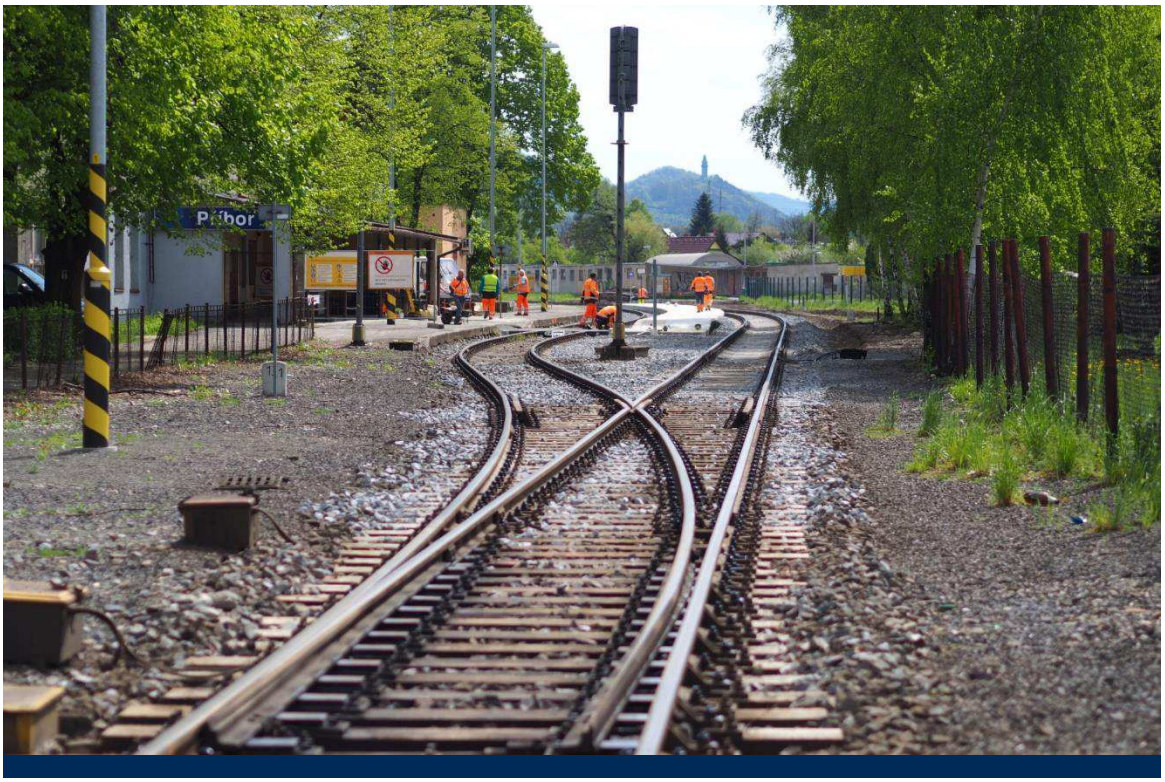
7 Přílohy

Příloha 1 – Standardy vývoje informačních systémů Správy železnic

Správa železnic, státní organizace
Název organizační jednotky
Dlážděná 1003/7
110 00 Praha 1

Datum tisku
2022-04-2931

SPRÁVA ŽELEZNIC



Standardy vývoje informačních systémů Správy železnic

Březen 2022

Historie verzí

Verze	Popis	Platnost od	Předchozí verze
0.1	Draft	22. 3. 2022	
1.0	První verze dokumentu	31. 3. 2022	

Obsah

Seznam zkratek a pojmů

3NF	Třetí normální forma
API	*z angl. Application Programming Inteface*, rozhraní pro programování aplikací
APP	Aplikační vrstva
AS	Aplikační server
DB	Databáze
DBMS	*z angl. Database Management System*, Systém řízení databáze
DC	Datové centrum
DDL	*z angl. Data Definition Language*
DR	*z angl. Disaster Recovery*, Obnova po havárii
HA	*z angl. High Availability,* Vysoká dostupnost
HW	Hardware označuje veškeré fyzicky existující technické vybavení počítače
JSON	*z angl. JavaScript Object* Notation, JavaScriptový objektový zápis
OS	Operační systém
SQL	Structured Query Language, standardizovaný dotazovací jazyk pro práci v relačních databázích
SW	Software je sada všech počítačových programů používaných v počítači, které provádějí nějakou činnost
SŽ	Správa železnic, státní organizace
WS	Webový server
XML	*z angl. Extensible Markup Language*, obecný značkovací jazyk

1 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.

1.1 Dvouvrstvá architektura

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

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

1.1.1 Datová vrstva

Realizace datové vrstvy je požadována prostřednictví preferované relační databáze (dle služeb Platformy) 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.

1.1.2 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 1.4.

1.2 Třívrstvá a vícevrstvá architektura

Třívrstvá a vícevrstvá architektura je požadována při vývoji software ve všech případech mimo výjimky definované v kap. 1.1. 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

1.2.1 Datová vrstva

Realizace datové vrstvy je požadována prostřednictvím preferované relační databáze (dle služeb Platformy) a respektováním metodiky 3NF. Je požadován jednoznačný datový model s minimální redundancí dat, 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 třívrstvé a vícevrstvé architektury není umožněno, aby logika byla rozprostřena částečně v databázi a částečně v aplikační vrstvě. Aplikační logika je tak striktně pouze v aplikační vrstvě.

1.2.2 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 1.4.

1.2.3 Prezentační vrstva

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

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

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

1.2.4 Integrační vrstva

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

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

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

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

1.3 Požadavky na prezentační vrstvu

1.3.1 Uživatelské rozhraní (User Interface, UI)

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
- 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)
- responzivní design webových aplikací

1.3.2 Uživatelský prožitek (User Experience, UX)

UX je to, co uživatel pocítí a pamatuje si v důsledku použití aplikace, systému nebo webu. 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 mít následující vlastnosti:

- cílem je efektivní uživatel
- návodné ovládání
- ergonomie
- jednoduché, intuitivní
- pravidla přístupnosti, tam kde je požadováno
- zobrazování relativních a požadovaných dat
- rychlost odezvy (doba zpracování požadavku od uživatele by na serveru neměla přesáhnout 0,5s, tak aby celková doba odezvy uživatelský ovládacích prvků byla kratší než 0,8s. V případě, že je předpokládaný čas odezvy delší než 0,8s, ale kratší než 2s

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

bude uživateli zobrazen wait cursor a pokud bude předpokládaný čas odezvy delší než 2s bude pro informaci uživatele použit progress bar zobrazující průběh operace.)
- použití lazy loading v odůvodněných případech
- jednotná terminologie v celém systému
- ne všechno na jedné obrazovce
- ne všechno v rozbalovacím menu (příliš mnoho položek)
- navigace, kde se uživatel v aplikaci nachází
- minimalizace použití dlouhých textů
- vhodné využití grafických a obrazových prvků
- nepoužívat drobný text
- pečlivé plánování dialogů (logické skupiny)
- ne překrývající se dialogy
- jednotné, stejné ovládací prvky v dialozích na stejných místech s popisky s jednotnou terminologií

1.4 Bezpečnost

Všechny vyvíjené aplikace musejí splňovat požadavky kladené platnou legislativou a interními předpisy Správy železnic.

Klíčovým dokumentem z pohledu požadavků na vyvíjený software je „Provozní politika prvků v působnosti systému řízení bezpečnosti informací", který specifikuje požadavky pro následující oblasti:

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

1.4.1 Zabezpečení aplikací

Je požadováno, aby jednotlivé vrstvy splňovaly minimálně tyto požadavky:

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

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

1.4.2 Autentizace a autorizace

1.4.2.1 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
- Manuální přihlášení, autentizaci pomocí vyvíjeného software, tzn. Uživatelská jména a hesla jsou uložena v databázi v šifrované podobě.
- Autentizaci pomocí protokolu LDAP, proti Active Directory
- 2FA

1.4.2.2 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

V rámci naplnění povinností vyplývajících ze zákona č. 181/2014 Sb. a vyhlášky č. 82/2018 Sb. je požadováno, aby vyvíjený software umožňoval správu uživatelů a rolí pomocí externího nástroje na řízení identit, tj. Identity managementem implementovaným ve Správě železnic. Integrace mezi vyvíjeným softwarem a Identity management bude realizována prostřednictvím integrační vrstvy vyvíjeného software.

1.4.3 GDPR

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

1.5 Dokumentace

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

1.5.1 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.

1.5.2 E-R modely databáze

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

1.5.3 Objektový model pro aplikace

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

1.5.4 Procesní diagramy, schémata toků dat

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

1.5.5 Komunikační rozhraní

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

1.5.6 Drátové modely všech obrazovek uživatelského rozhraní aplikací

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

1.5.7 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.)

1.5.8 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.

1.5.9 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.

1.6 Předávání vývoje do provozu

Pokud nebude určeno jinak, veškeré výstupy (zdrojové kódy, konfigurační soubory, testovací data, dokumentace atp.) musejí být předávány prostřednictvím určeného repositáře.