

Klasifikace: Veřejný dokument



Příloha č. 1 smlouvy

Bližší specifikace předmětu plnění

Obsah

1	Seznam zkratk	2
2	Úvod	5
3	Záměr SŽ v oblasti bezpečného úložiště	5
3.1	Současný stav	5
3.2	Cílový stav	5
4	Předmět plnění veřejné zakázky	6
5	Požadavky na plnění	7
5.1	Datový management vybraných systémů	7
5.1.1	Analýza současného stavu data managementu	7
5.1.2	Návrh na změnu data managementu	9
5.2	Implementační plán Bezpečného úložiště	9
5.3	Technické vlastnosti Bezpečného úložiště	11
5.3.1	Specifikace technických parametrů Bezpečného úložiště	11
5.3.2	Základní vlastnosti Bezpečného úložiště	12
5.3.3	Funkční požadavky	14
5.3.4	Dodávka a implementace Bezpečného úložiště	18
5.4	Ověření funkčnosti řešení	19
5.4.1	Konfigurace Bezpečného úložiště	19
5.4.2	Napojení na vybrané systémy	19
5.4.3	Post-implementační testování	20
6	Školení, dokumentace a exit strategie	23
6.1	Školení	23
6.2	Dokumentace	24
6.3	Exit strategie	26
6.3.1	Vytvoření Exit strategie	26
6.3.2	Předání znalostí a podkladů v případě ukončení smlouvy po dokončení Fáze F5	26
6.3.3	Předání znalostí a podkladů v případě ukončení smlouvy před dokončením Fáze F5	27
7	Post-implementační a technická podpora	28
8	Konzultační služby na vyžádání	30
9	Fáze dodávky a platební milníky	30

1 Seznam zkratek

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

Přehled zkratek a pojmů:

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

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

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

2 Úvod

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

3 Záměr SŽ v oblasti bezpečného úložiště

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

3.1 Současný stav

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

3.2 Cílový stav

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

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

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

4 Předmět plnění veřejné zakázky

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

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

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

5 Požadavky na plnění

Plnění veřejné zakázky se skládá z níže uvedených částí:

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

5.1 Datový management vybraných systémů

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

5.1.1 Analýza současného stavu data managementu

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

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

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

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

Oblast	Činnost
Podklady Zadavatele	- Podklady k vybraným systémům: - Seznam vybraných 24 systémů pro projekt BÚ. - Výstupy ze současných zálohovacích nástrojů. - Základní schémata topologie sítě sloužící pro zálohování dat. - Současný zálohovací plán vybraných 24 systémů. - Určení konkrétních lokalit pro umístění BÚ v regionu Praha a Plzeň.
Výstupy Dodavatele	- Zhodnocení koncepce stávajícího zálohovacího plánu vybraných 24 systémů a návrh opatření pro optimalizaci a standardizaci dle požadavků Zadavatele a ZoKB a VoKB. - Analytický výstup popisující přístup řešení dále uvedených oblastí v prostředí SŽ (definování postupu kroků v rámci BÚ, specifikace postupu vlastní konfigurace, stanovení pořadí migrace dat jednotlivých systémů, přístup k migraci, definice rizik a jejich mitigace). Součástí analytického výstupu je i architektura systému, struktura dat, databázová technologie, objem dat, časové přírůstky, retenční politiky, současné zálohovací scénáře, řízení přístupu k datům, logování.

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

5.1.2 Návrh na změnu data managementu

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

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

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

Výstupem výše uvedených požadavků bude samostatný dokument s názvem „Koncepte Bezpečného úložiště“.

5.2 Implementační plán Bezpečného úložiště

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

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

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

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

5.3 Technické vlastnosti Bezpečného úložiště

5.3.1 Specifikace technických parametrů Bezpečného úložiště

Zadavatel ke dni zahájení zadávacího řízení provozuje nižší stovky informačních systémů, přičemž předpokládá jejich postupnou integraci do Bezpečného úložiště ve střednědobém časovém horizontu. Aktuální technické požadavky na předmět Veřejné zakázky jsou vymezeny s ohledem na pokrytí současných potřeb a zároveň na předpokládaný budoucí rozvoj navrhovaného technologického řešení,

a to zejména z hlediska kapacitních a výkonových parametrů a také v počtu napojovaných systémů.

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

5.3.2 Základní vlastnosti Bezpečného úložiště

5.3.2.1 Požadovaný typ diskového úložiště

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

5.3.2.2 Kapacita diskového úložiště

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

5.3.2.3 Očekávaný typ ukládaných dat

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

5.3.2.4 Výkon a technologie disků

- Pro primární úložiště typu bloková storage, je požadováno víceúrovňové diskové úložiště s NVMe/SSD disky nebo SAS/NL-SAS disky nebo s jejich kombinací. Zadavatel požaduje, aby součástí řešení primárního úložiště

bylo SSD úložiště o souhrnné kapacitě minimálně 100 TiB. Zadavatel rovněž připouští variantu použití výhradně NVMe/SSD disků.

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

5.3.2.5 Síťová infrastruktura

LAN/SAN

Součástí dodávky bude i potřebná síťová infrastruktura o dostatečné propustnosti dle navržené technologie úložiště, aby nevznikala úzká hrdla v rámci zápisu, čtení a redistribuce a replikace dat. Síťové řešení bude provozováno v režimu vysoké dostupnosti (HA) s využitím Ethernetové technologie 10/25GbE, 40/100GbE a SAN technologie 32/64Gb FC. K propojení obou lokalit bude využita stávající DWDM technologie o rychlosti až 100 Gb/s. Bližší technická specifikace prvků, viz samostatná Příloha č. 2 smlouvy – Technická specifikace.

Firewall

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

5.3.3 Funkční požadavky

5.3.3.1 Vysoká dostupnost a geografická redundance

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

- **Geo-redundance (dvě lokality):** Data budou uložena a zrcadlena mezi 2 fyzicky oddělenými datacentry provozovanými SŽ.
 - Primární datové úložiště bude umístěno v datovém centru CDP Praha.
 - Sekundární datové úložiště bude umístěno v datovém centru Plzeň.Technologie vzájemného propojení obou lokalit bude dle navržené technologie úložiště a technologických možností datového propojení, (propustnost, šířka přenosového pásma, latence, jitter), vždy ale s dohledem na integritu dat. Bude se jednat o georedundanci s asynchronní replikací z primární do sekundární lokality.
- **Redundantní architektura úložiště a failover:** Oba typy úložiště musí být navrženy plně redundantně (více uzlů nebo multi-controller systém), aby i lokální porucha některého zařízení neznamenal nedostupnost služby. Při poruše některého z prvků (server, kontrolér diskového pole, síťový prvek) musí jeho funkci převzít redundantní prvek.

5.3.3.2 Škálovatelnost a tiering úložiště

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

5.3.3.3 Bezpečnostní technologie

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

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

- **Immutable backup / WORM Lock:** zajištění nezměnitelnosti záloh v retenční době.
- **Air-gap:** úložiště typu Datový trezor (Data Vault) musí navíc umožňovat fyzické nebo logické oddělení od provozní datové sítě.
- **Automatická detekce kybernetických hrozeb:** pokud úložiště umožňuje využití integrovaných nástrojů pro proaktivní monitoring a automatickou detekci kybernetických hrozeb typu ransomware nebo detekci neobvyklého chování, musí být tato funkcionality zapnuta, funkční a plně licencována.
- **Ochrana proti škodlivému kódu:** Data musí být chráněna proti škodlivému kódu (Malware, ransomware...) po celou dobu manipulace, a i po uložení. Řešení samostatně zajistí ochranu proti škodlivému kódu (virům) u již uložených dat. Pokud výrobce do řešení přímo integroval napojení na antivirové řešení, které hledá škodlivý kód v již uložených datech, je použita tato možnost. Jinak musí být dodána externí appliance/server (včetně software a licencí), na kterém běží antivirové řešení, které si uložená data z centrální části pole (ne Vaultu) automaticky připojuje a kontroluje na přítomnost virů, případně funkční ekvivalent. Bude zajištěn read-back / re-scan - pravidelné měsíční nebo týdenní bezpečnostní kontroly záloh tímto interním/externím nástrojem. Vždy s výstupem do SIEM a řešení nesmí být založeno na cloudové kontrole, ale očekává se možnost stahování aktualizací z internetu. Tyto kontroly jsou součástí technických a organizačních bezpečnostních opatření k řízení kybernetických rizik. Cílem je, aby uložené zálohy již neobsahovaly například „spící ransomware“.
- **Šifrování dat v klidu (at rest):** Veškerá data uložená v Bezpečném úložišti musí být šifrována pomocí šifrovacích algoritmů schválených ze strany NÚKIB s možností změny šifrovacího algoritmu v rámci konfigurace. Šifrování musí probíhat na úrovni diskových úložišť automaticky, transparentně pro aplikace. Tím se zajistí, že i v případě fyzického získání disků nebo neautorizovaného přístupu k úložišti útočník data nevyužije bez šifrovacích klíčů. Implementace musí být v souladu s požadavky a doporučeními NÚKIB (doporučení v oblasti kryptografické bezpečnosti), legislativy (ZoKB, nebo GDPR pro osobní údaje).
- **Správa šifrovacích klíčů (KMS/HSM):** Primární úložiště bude podporovat Hardware Security Module (HSM) pro generování, bezpečné ukládání a správu kryptografických klíčů. SŽ již HSM v nějaké formě používá – úložiště musí umožnit integraci s HSM (typicky prostřednictvím protokolu PKCS#11 nebo KMIP). Všechny klíče k šifrování dat úložiště budou spravovány tímto centrálním HSM modulem. Sekundární úložiště (Data Vault) musí mít vlastní dedikovaný HSM modul a vlastní TPM čip pro

ukládání a správu šifrovacích klíčů. Kopie klíčů může být uložena i na externích úložištích (typu flashdisk) pro případ kompromitace HSM.

- **Integrita a detekce změn:** Systém musí umět ověřovat integritu uložených dat (například skrze kontrolní součty, které detekují tichou korupci dat, tzv. bit rot, nebo neautorizovanou změnu).
- **Retence dat:** Systém musí podporovat různě definované retenční doby pro různé druhy dat, tak aby byla naplněna nejen provozní potřeba Zadavatele ale také legislativní požadavky na ochranu a archivaci.
- **Obnova dat:** Systém musí umožňovat, v případě kompromitace provozních dat, nejen manuální, ale i plně automatizovanou obnovu zálohovaných dat do bezpečného prostředí.
- **Cleanroom:** Zadavatel uvažuje o výstavbě cleanroomu a po dobu udržitelnosti tohoto projektu může dojít k jeho výstavbě. Výstavba Vaultu je prvním krokem před výstavbou cleanroomu, Zadavatel chce získat znalosti a kompetence pro případ vážného kybernetického incidentu. Dodavatel poskytne svoje know-how pro tento krok v rámci školení.
- **Testování dat:** Systém musí umožnit provádět automatizované zkoušky obnovy do izolovaného prostředí (cleanroom), aby SŽ měla jistotu, že zálohy jsou nekompromitované, validní a použitelné pro obnovu. Separátně, v rámci provozních procesů, bude zaveden plán periodických testů: například čtvrtletně provést obnovu vybraného kritického systému ze zálohy a také vyhodnotit, zda obnova odpovídá požadovanému RTO/RPO.

5.3.3.4 Řízení přístupu a správa identit

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

- **Centralizovaná autentizace a autorizace:** Primární úložiště se plně začlení do stávajícího systému pro správu identit Identity Management (IdM) a do stávajícího systému pro vzdálený přístup Privileged Access Management (PAM). Uživatelé (nebo služby) přistupující k datům úložiště budou ověřováni proti centrální databázi účtů (např. Active Directory/ADFS). Přístupová práva k datům pak budou udělována na základě rolí definovaných v IdM a řízena členstvím ve skupinách v AD (případně v několika na sobě nezávislých AD) – například administrátoři záloh, auditní role, běžní uživatelé konkrétní aplikace apod. Tím se zajistí jednotné přihlašování (Single Sign-On) a především efektivní a přehledná správa přístupových oprávnění.
- **Role-Based Access Control:** Systém musí podporovat RBAC – přiřazování oprávnění podle role. Např. administrátor úložiště může spravovat infrastrukturu, ale nedostane se k obsahu záloh konkrétní aplikace, pokud k tomu není důvod. Naopak správce dané aplikace může mít právo obnovit její data ze zálohy, ale nevidí jiné části úložiště. Tato granulózní oprávnění lze spravovat přes IdM/PAM nebo lokálně v úložišti, ale preferujeme centralizaci. Privilegované účty (správci systému) by měly

být spravovány právě přes PAM s minimem trvalých přístupů a případně vyžadovat víceúrovňové schválení pro nejcitlivější operace.

- **Důsledná autentizace:** Pro administrativní přístupy vyžadujeme vícefaktorovou autentizaci (MFA). Ať už přes integraci s existující MFA SŽ, nebo vlastnostmi PAM.
- **Audit a záznamy přístupů:** Systém musí logovat veškeré přístupy k datům i administrativní akce minimálně v rozsahu požadovaném ZoKB/VoKB. Každé přečtení či obnova záložního souboru, každá změna nastavení, přidání uživatele apod. Tyto logy budou dlouhodobě uchovávány pro potřeby auditu a v souladu s legislativou (např. zákon o KB vyžaduje určitou dobu uchování záznamů o událostech). Mimo interního logování budou údaje předávány i do centrálního log managementu a SIEM. Systém musí podporovat běžné formáty log souborů (např. CLF, ELF, SysLog, JSON...).
- **Oddělení prostředí a tenantů:** Úložiště může sloužit více různým agendám (více systémům). Je žádoucí, aby bylo možné logicky oddělit data jednotlivých skupin systémů či útvarů (tzv. multitenancy). Například data provozních technologických systémů mohou být ve vyhrazeném oddílu, logicky odděleném od dat ekonomických systémů, pokud to správu zjednoduší a zvýší přehlednost přístupů. Oddělení by však nemělo bránit centrální správě – je to logická vrstva navíc pro případnou granularitu oprávnění.

5.3.3.5 Integrace, monitorování a dohled

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

- **Kompatibilita s IT prostředím SŽ:** Navržené úložiště bude plně kompatibilní s existujícími systémy a technologiemi, které jej budou využívat. To zahrnuje podporu běžných standardních protokolů pro přístup k datům – např. CIFS/SMB v3, NFS, SFTP, FTPS pro souborové sdílení, příp. blokové protokoly (iSCSI, Fibre Channel) pro připojení databázových serverů. V případě, že řešení nějaký z protokolů nepodporuje, je možné v rámci před-implementační analýzy navrhnout napojení jiným protokolem v rámci pracnosti a dodávky Dodavatele. Úložiště by mělo umožnit snadnou integraci do virtualizační platformy (VMware vSphere) a do clusterových prostředí, pokud některé systémy používají sdílená datová úložiště.
- **Napojení na monitorovací systémy:** Infrastruktura bude připojena k centrálnímu monitorovacímu systému Zabbix, provozovaný SŽ tak, aby stav hardware (disky, zdroje, teploty), služby replikací a záloh byly neustále sledovány operátory. Výpadky, pokles výkonu nebo poruchy komponent budou automaticky hlášeny. Dále bude systém poskytovat telemetrii výkonu – využití kapacity, IO, síťové přenosy – pro účely kapacitního plánování. Budou podporovány běžné protokoly pro monitoring – SNMPv3, ICMP, HTTPS, IPMI, Storage Insights. Úložiště typu Data Vault bude monitorováno pouze jednosměrným kanálem typu SNMP trap.

- **SIEM a log management:** Všechny relevantní logy budou odesílány do centrálního Security Information and Event Management (SIEM) systému. Úložiště musí umět exportovat logy standardním způsobem (syslog, případně API integrace) a obsahovat dostatečné informace (uživatelská ID, IP adresy, kódy událostí). Odesílané logy musí být ve standardizovaném formátu JSON, CEF, LEEF atd. Pro úložiště typu Data Vault musí být logy aktivně odesílány z úložiště (push).
- **Provozní dohled a správa:** Dodané řešení musí zahrnovat nástroj pro správu konfigurace a diagnostiku, např. v podobě centrální management konzole (Unified storage manager) pro veškerá úložiště, s možností skriptování rutinních úloh (Infrastructure as a Code).
- Integrace úložiště typu Data Vault na vnější prostředí musí být provedena skrze datovou diodu, která zajistí jednosměrnost komunikace na fyzikální úrovni.

5.3.4 Dodávka a implementace Bezpečného úložiště

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

Oblast	Činnost
Dodání technologií BÚ	Výstup Dodavatele • Dodávka technologií BÚ do dvou lokalit dle přílohy č. 2 smlouvy – Technická specifikace, Základních vlastností (kapitola 5.3.2) a Funkčních požadavků (kapitola 5.3.3)
Montáž technologií BÚ	Výstup Dodavatele • Montáž a zapojení prvků BÚ (úložiště, servery) • Montáž a zapojení síťových prvků (přepínače, firewally) • Kompletní kabelové propojení (napájecí, datové) • Kompletní vyvázání kabelových rezerv • Zapnutí všech HW komponent • Odvoz a ekologická likvidace obalových materiálů.

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

5.4 Ověření funkčnosti řešení

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

5.4.1 Konfigurace Bezpečného úložiště

Konfigurace dodaných HW komponent pro Bezpečné úložiště zahrnuje všechny kroky nutné pro oživení všech fyzických prvků, požadovaných serverů, diskových polí, síťových prvků a záložních zdrojů. Konfigurace musí reflektovat požadavky na vysokou dostupnost, bezpečnost a škálovatelnost systému a musí být v souladu s akceptovaným dokumentem „Implementační plán Bezpečného úložiště“, který je výstupem kapitoly 5.2 Příprava implementačního plánu pro realizaci Bezpečného úložiště. Změny a odchylky od schválené implementace musí být schváleny ze strany zadavatele a musí být zaneseny v rámci konfigurační dokumentace.

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

Oblast	Činnost
Síťová konfigurace	Výstup Dodavatele • Zprovoznění a napojení Out-of-band sítě dle požadavků Zadavatele. • Konfigurace portů • Konfigurace síťových protokolů • Konfigurace síťových přístupů • Konfigurace HA
Aplikační konfigurace	Výstup Dodavatele • Zprovoznění a napojení Out-of-band sítě dle požadavků Zadavatele. • Konfigurace aplikačních síťových protokolů • Konfigurace software a aplikací pro splnění Funkčních požadavků uvedených v kapitole 5.3.3

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

5.4.2 Napojení na vybrané systémy

Napojení vybraných systémů Zadavatele na BÚ zahrnuje veškeré kroky nutné k zajištění správného, bezpečného a funkčního přenosu dat mezi systémy a úložištěm. Cílem této části je zajistit, aby všech 24 vybraných systémů bylo

přípravě pro ukládání, obnovu a kontrolu dat v souladu s definovanými technickými a bezpečnostními pravidly.

Toto navazuje na dokumenty „Koncepte Bezpečného úložiště“ a „Implementační plán Bezpečného úložiště“.

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

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

5.4.3 Post-implementační testování

Tyto testy ověřují, že je zařízení správně zapojené a fyzicky funkční a zda řešení dosahuje očekávaných výkonnostních parametrů (viz. kapitola 5.2 tohoto

dokumentu - Kontrolní a testovací scénáře). Na základě testovacího scénáře, může Dodavatel vyžadovat spolupráci Zadavatele a naopak. Dodavatel poskytne plnou podporu při identifikaci a odstranění nálezů z testování a návrh nápravných opatření.

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

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

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

6 Školení, dokumentace a exit strategie

6.1 Školení

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

V oblasti odborného školení je požadováno následující plnění:

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

dodaných technologií pro forenzní šetření), se zaměřením na:

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

Obecné požadavky na školení:

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

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

6.2 Dokumentace

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

Typ dokumentace	Popis
-----------------	-------

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

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

6.3 Exit strategie

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

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

6.3.1 Vytvoření Exit strategie

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

Obsah Exit strategie

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

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

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

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

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

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

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

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

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

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

Dodavatel je povinen dodat následující dokumenty a provést následující činnosti:

Oblast	Výstup
Dokumentace	Dodavatel provede a předá Zadavateli: • export všech konfigurací • aktuální dokumentaci skutečného provedení • bezpečnostní dokumentaci.
Přístupová oprávnění a uživatelské účty	Dodavatel předá Zadavateli: • Přístupové údaje k root uživateli, pokud systém nedisponuje základním uživatelem s plnými oprávněními, dodavatel vytvoří pro zadavatele uživatelský účet/účty s plnými oprávněními, které mu předá.

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

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

7 Post-implementační a technická podpora

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

Oblast	Požadavky
Technická podpora výrobce	Zařízení nesmí mít k datu podání nabídky oznámené EOS (End Of Sale) dříve než za 2 roky, oznámené EOL (End Of Life) a EOS (End Of Support) dříve než za 5 let od dodání. Dodavatel zajistí oficiální podporu výrobce po dobu 60 měsíců od ukončení fáze F2.1 pro primární lokalitu a po dobu 60 měsíců od ukončení fáze F2.2 pro sekundární lokalitu. Tato podpora zahrnuje minimálně: • Režim podpory 8x5 – dostupnost podpory 8 hodin denně v rámci pracovních dní (pondělí až pátek), s reakční dobou technického týmu výrobce do 4 hodin.

	• Přístup k aktualizacím software/firmware – možnost stažení nových verzí firmware nebo operačního systému pro HW. • Možnost kontaktovat technický tým výrobce – při řešení bugů, anomálií a konfiguračních problémů. • Dostupnost podpory – prostřednictvím webového portálu výrobce, e-mailu a telefonu. • Přístup do supportního portálu – pro sledování stavu požadavků. • Přístup do licenčního portálu – s přehledem o zakoupených licencích, jsou-li součástí dodávky. • V rámci podpory výrobce k dodávaným serverům (Položka C) Zadavatel požaduje (nad rámec výše uvedeného) režim podpory: ○ 24x7 s reakční dobou technického týmu výrobce do 4 hodin. ○ Výměna vadného HW v režimu NBD (Next Business Day) on-site – doručení náhradního dílu následující pracovní den po nahlášení závady. • V rámci podpory výrobce k dodávaným datovým úložištím, switchům a firewallům (Položka A, B, D, E, F, G) Zadavatel požaduje (nad rámec výše uvedeného) režim podpory: ○ 8x5 s reakční dobou technického týmu výrobce do 4 hodin. ○ Výměna vadného HW v režimu NBD (Next Business Day) on-site – doručení náhradního dílu následující pracovní den po nahlášení závady.
Post-implemenční podpora Dodavatele	Dodavatel zajistí Post-implemenční podporu v rozsahu: 1) Poskytování expertních služeb, které budou využívány zejména pro podporu činností SŽ v případě řešení nestandardních stavů a pro profylaxi, aby se předcházelo omezením jeho správné funkčnosti. 2) Konzultace při konfiguracích a změnách dodaných komponent a v rámci bezpečnostní strategie napojovaných systémů řešení definovaných výstupů této Veřejné zakázky. 3) Post-implemenční podpora bude poskytována po dobu 60 měsíců od ukončení fáze F3.3.

- 4) Post-implementační podpora bude poskytována v souladu s ustanoveními ZOP podle servisního modelu C2. Nad rámec ZOP platí, že budou plánované změny či významné změny (aktualizace, patch atd.) ze strany Dodavatele poskytnuty (uvolněny) SŽ vždy v pracovních dnech, a to konkrétně v pondělí a ve středu. V případě, že plánovaná změna či významná změna a její poskytnutí vychází na státní svátek, vyzve Dodavatel SŽ k upřesnění poskytnutí (uvolnění).
- 5) Poskytování služeb ServiceDesk ze strany Dodavatele bude realizováno v souladu s ustanoveními ZOP v Režimu 4 (8×5, tj. v pracovních dnech v době od 7:00 do 15:00 na telefonním čísle určeném Dodavatelem).
- 6) (6) Součinnost při auditech řešení, opravu a zpracování identifikovaných nedostatků.

8 Konzultační služby na vyžádání

V oblasti konzultačních služeb jsou definovány následující požadavky:

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

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

9 Fáze dodávky a platební milníky

Plnění musí být dodáno v níže uvedených fázích. Každá z níže uvedených fází F1.1 až F5 je součástí jednoho z uvedených platebních milníků (A nebo B) a musí být Zadavatelem akceptována nejpozději v termínu uvedeném v Harmonogramu.

Zadavatel akceptuje výstupy dané akceptační fází, jestliže je Dodavatel provedl v šíři a kvalitě požadované v zadávací dokumentaci této veřejné zakázky. V opačném případě je Dodavatel povinen napravit nedostatky plnění.

Platební milník	Fáze	Popis	Způsob akceptace fáze	Kapitola obsahující požadavky
A	F1.1	Datový management vybraných systémů	Akceptační protokol: Dokument – Konceptce Bezpečného úložiště	5.1
A	F1.2	Implementační plán Bezpečného úložiště	Akceptační protokol Dokument – Implementační plán Bezpečného úložiště (vč. Exit strategie)	5.2
A	F2.1	Dodávka a implementace Bezpečného úložiště do primární lokality	Akceptační protokol: - Dodávka HW, SW a licencí, dle specifikace ZD - Dodací list - Montážní protokol	5.3 5.3.4
A	F2.2	Dodávka a implementace Bezpečného úložiště do sekundární lokality	Akceptační protokol: - Dodávka HW, SW a licencí dle specifikace ZD - Dodací list - Montážní protokol	5.3 5.3.4
B	F3.1 A	Konfigurace primární lokality	Akceptační protokol: Dokument - Konfigurační dokumentace	5.4.1
B	F3.1 B	Konfigurace sekundární lokality	Akceptační protokol: Dokument - Konfigurační dokumentace	5.4.1
B	F3.2	Napojení na vybrané systémy	Akceptační protokol: Dokument – Zpráva o napojení vybraných informačních systémů na Bezpečné úložiště	5.4.2
B	F3.3	Post-implementační testování	Akceptační protokol:	5.4.3

Platební milník	Fáze	Popis	Způsob akceptace fáze	Kapitola obsahující požadavky
			Dokument – Závěrečná zpráva z testování funkčních a bezpečnostních parametrů Bezpečného úložiště	
C	F4	Školení	Akceptační protokol: Dokument - Zpráva o školení zaměstnanců Správy železnic včetně prezenční listiny	6.1
C	F5	Dokumentace	Akceptační protokol: Dokumentace skutečného provedení	6.2
Plnění bude hrazeno na základě potvrzených pravidelných měsíčních výkazů.	F6.1A	Technická podpora – primární lokalita	Fáze F6.1A bude vykazována na základě pravidelných měsíčních výkazů	7
Plnění bude hrazeno na základě potvrzených pravidelných měsíčních výkazů.	F6.1B	Technická podpora – sekundární lokalita	Fáze F6.1B bude vykazována na základě pravidelných měsíčních výkazů	7
Plnění bude hrazeno na základě potvrzených pravidelných měsíčních výkazů.	F6.2	Post-implementační podpora	Fáze F6.2 bude vykazována na základě pravidelných měsíčních výkazů	7
Plnění bude hrazeno na základě	F7	Konzultační služby na vyžádání	Akceptační protokol s ohledem na obsah požadovaných Konzultačních služeb	8

Platební milník	Fáze	Popis	Způsob akceptace fáze	Kapitola obsahující požadavky
skutečného čerpání ze strany Zadavatele.				