Naše zn. 122508/2026-SŽ-GŘ-O25

Vysvětlení a změna zadávací dokumentace č. 3

sektorová nadlimitní veřejná zakázka na dodávky zadávaná v otevřeném řízení podle § 56 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „***ZZVZ***"), s názvem:

„Realizace systému Zabezpečeného úložiště v prostředí Správy železnic"

Správa železnic, státní organizace (dále jen „***Zadavatel***") obdržela dne 9.7.2026 v 10:01 hodin, 9.7.2026 v 10:06 hodin, 14.7.2026 v 07:58 hodin a 14.7.2026 v 17:28 hodin žádosti o vysvětlení zadávací dokumentace. Zadavatel odpovídá na tyto žádosti doručené k veřejné zakázce následovně:

Dotaz č. 1:

Zadavatel uvádí v kap. 12.2.3 zadávací dokumentace, v rámci prokázání kvalifikace jednotlivých členů realizačního týmu, požadavek na doložení certifikace pro pozici Architekt infrastruktury (Solution Architect) následovně: *„Certifikace: platná certifikace výrobce nabízeného řešení pro návrh /deployment".*

Předmětem plnění veřejné zakázky je dodávka komplexní ICT infrastruktury sestávající z mnoha technologií a komponent více různých výrobců (servery, datová úložiště, SAN a LAN infrastruktura, bezpečnostní prvky apod.). Vzhledem k tomuto více-výrobcovému charakteru řešení není reálně možné, aby jedna osoba disponovala platnými certifikacemi výrobce „nabízeného řešení" pro všechny komponenty dodávky současně.

Vzhledem k výše uvedenému dodavatel žádá o informaci, zda je pro splnění kvalifikačního požadavku na této pozici akceptovatelné doložit:

- profesní životopis obsahující relevantní zkušenosti odborníka,
- všeobecně uznávané certifikace v požadované oblasti (např. TOGAF Practioner, ArchiMate) potvrzující znalosti a zkušenosti s návrhem /deploymentem celkové architektury řešení,
- případně další aktuální či historicky získané odborné certifikace prokazující jeho praxi, aniž by bylo nezbytné dokládat platnou certifikaci výrobce ke všem komponentám nabízeného řešení.

Odpověď č. 1:

Zadavatel k dotazu uvádí, že již s ohledem na název veřejné zakázky a zejména předmět veřejné zakázky, kterým je v souladu s čl. 4.1 zadávací dokumentace *„dodání, implementace a konfigurace technologie centralizovaného **bezpečného datového úložiště** za účelem splnění zákonných povinností Zadavatele v oblasti kybernetické a fyzické bezpečnosti"*, je zřejmé, že stěžejní součástí poptávaného plnění je dodávka **datových úložišť**, tedy položek A a B Technické specifikace, která je přílohou č. 2 Smlouvy. Ostatní položky technické specifikace jsou v tomto ohledu spíše doplňkového charakteru a ve svém souhrnu zajišťují provozní funkcionality daného řešení.

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

Zadavatel na pozici architekta infrastruktury vyžaduje osobu, která bude certifikována pro danou technologii datových úložišť, a to zejména z důvodu specifik dané technologie při zpracování návrhu celé koncepce zabezpečeného úložiště a při její následné implementaci. S ohledem na výše uvedené tedy Zadavatel uvádí, že dodavatelem navrhované alternativní varianty certifikací (např. TOGAF Practioner, ArchiMate) nepovažuje za dostatečné a trvá na svém požadavku, formulovaném v čl. 12.2.3 zadávací dokumentace, a tedy že architekt infrastruktury musí disponovat certifikací výrobce nabízeného řešení pro návrh/deployment. S ohledem na výše uvedené přitom Zadavatel uvádí, že nabízeným řešením se rozumí položky A a B, dle Technické specifikace, která je přílohou č. 2 Smlouvy. Pro vyloučení veškerých pochybností Zadavatel přistoupil k úpravě čl. 12.2.3 zadávací dokumentace.

Dotaz č. 2:

Upřesnění požadavků kapitoly 1.3.5 Technická specifikace Položky H – kabeláž a optické moduly

V souvislosti s požadavky uvedenými v kapitole **1.3.5 Technická specifikace Položky H** žádáme o upřesnění způsobu vyplnění tabulky „Nabízené řešení". Konkrétně žádáme o odpověď na následující otázky:

1. Způsob vyplnění tabulky Je správný následující přístup?

- Položky, které **jsou součástí našeho návrhu řešení** a budou použity pro propojení komponent, označíme **ANO** + uvedeme počet kusů a technické parametry.
- Položky, které **nejsou pro náš návrh řešení potřebné**, označíme **NE** s poznámkou „Nepoužito v navrženém řešení". Pokud tento přístup není správný, žádáme o upřesnění, jakým způsobem máme tabulku vyplnit.

2. Položky, které Dodavatel standardně nedodává, např. následující položky:

- Optický kabel AOC Fibre Channel SFP+/SFP28 pro rychlosti minimálně 32 Gbps
- Kabel AOC / DAC s rozhraním SFP/SFP+ pro rychlosti minimálně 1/10G
- Optický transceiver SFP/SFP+ 1/10G (variantně, dle návrhu řešení)

Tyto položky nejsou součástí našeho standardního portfolia. **Může Zadavatel upřesnit**, zda očekává jejich dodání i v případě, že nebudou pro námi navržené řešení (včetně propojení k switchům Nexus 93180YC-FX3) potřebné? Pokud ano, žádáme o sdělení, k propojení jakých konkrétních zařízení/komponentů tyto položky slouží.

3. Propojení k switchům Zadavatele.

Zadavatel uvádí, že má připravené switche **Nexus 93180YC-FX3**. Máme v návrhu řešení počítat s dodávkou kabeláže/optických modulů také pro přímé připojení našeho řešení k těmto switchům (SFP28 25 Gbps a QSFP 100 Gbps)?

Odpověď č. 2:

Zadavatel k dotazu uvádí následující:

ad. 1)

Dodavatelem uváděný přístup při vyplňování tabulek v rámci Technické specifikace (příloha č. 2 Smlouvy) je správný. Zadavatel ovšem upozorňuje na skutečnost, že Technická specifikace představuje soubor **požadavků** Zadavatele na předmět plnění a v případě jejich nesplnění se Dodavatel vystavuje riziku, že jeho nabídka bude vyloučena pro nesplnění zadávacích podmínek. Zadavatel v této souvislosti rovněž upozorňuje na následné úpravy těchto tabulek po uplynutí lhůty pro podání nabídek, jelikož takové úpravy mohou být klasifikovány jako nepřípustná (materiální) změna nabídky.

ad. 2)

Zadavatel trvá na dodání veškerých propojovacích komponent, nutných k zajištění plné provozuschopnosti, interoperability a budoucí flexibility dodávaného řešení. Konkrétní použití, počty a délky kabelů či jiných propojovacích komponent Zadavatel nestanovuje a toto ponechává

na technologickém návrhu dodavatele. V návaznosti na dotaz dodavatele bylo dále přistoupeno ke změně zadávací dokumentace, jak je blíže vymezena v příloze tohoto vysvětlení.

ad. 3)

Zadavatel v Technické specifikaci uvádí, že má ve svém prostředí pro připojení celého řešení zabezpečeného úložiště v obou lokalitách připravené switche Nexus 93180YC-FX3 s dostatečným počtem volných slotů SFP28 25 Gbps a QSFP 100 Gbps.

Po dodavateli je požadováno dodání optických modulů potřebných pro propojení řešení se síťovou infrastrukturou Zadavatele, a to včetně modulů do výše uvedených switchů Nexus. V souladu s touto informací Zadavatel upravil Technickou specifikaci ve vztahu k položce H.

Dotaz č. 3:

Kapitola 1.3.3 - Technická specifikace položky F

Požadavek: Podpora technologií LACP, MPLS, QoS, STP, SPAN, VRF, VLAN a Jumbo frame, (IEEE 802.1v, IEEE 802.1s, IEEE 802.1w, IEEE 802.1AX, IEEE 802.1p.)

Dotaz:

Protokol IEEE 802.1v je již dnes i komisí IEEE označován za „nahrazený standard" a nahrazuje jej evoluce protokolu IEEE 802.1Q (IEEE v průběhu let revidovalo hlavní standard 802.1Q (např. v edicích 2005, 2011, 2014 a novějších). Během této údržby byl standard 802.1v plně absorbován do základního textu 802.1Q. Dnes už 802.1v neexistuje jako samostatný, živý dokument, ale jako jedna z integrovaných kapitol (funkcí) v 802.1Q.

Je tedy možné považovat podporu protokolu (technologie) 802.1Q za splnění požadavku?

Odpověď č. 3:

Zadavatel v návaznosti na tento dotaz přistoupil ke změně zadávací dokumentace ve vztahu k položce F dle Technické specifikace.

Dotaz č. 4:

Požadavek: Podpora technologií LACP, MPLS, QoS, STP, SPAN, VRF, VLAN a Jumbo frame, (IEEE 802.1v, IEEE 802.1s, IEEE 802.1w, IEEE 802.1AX, IEEE 802.1p.)

Dotaz:

Pokud je technologie MPLS na nabízeném přepínači podporována v HW i SW, ale je nutné pro její aktivaci zakoupit licenci, **musí být tato licence součástí nabízené ceny**? Doplnění této licence má velký dopad na cenu zařízení.

Odpověď č. 4:

Zadavatel ve svém síťovém prostředí provozuje MPLS technologie, z tohoto důvodu Zadavatel požaduje podporu (resp. dostupnost) daných technologií na dodávaných switchích, nicméně v případě MPLS technologie netrvá na dodání licencí za účelem zprovoznění jejích funkcionalit. V návaznosti na tento dotaz Zadavatel blíže upřesnil požadavky na dodávané technologie (u Položky F) a nutnost dodání případných licencí pro jejich zprovoznění.

Dotaz č. 5:

V dokumentu Příloha č.2 smlouvy (Technická specifikace) je mimo jiné požadováno: „Technologie redukce dat (deduplikace a komprese) napříč všemi typy nabízených disků s minimálním dopadem na výkon".

Pokud uchazeč nedisponuje touto možností na točivých discích, je možné nabídnout větší kapacitu? Vzhledem k tomu, že uchazeč nezná povahu ukládaných dat, navrhujeme poměr 2:1, tzn. dodání dvojnásobné kapacity na točivých discích.

Odpověď č. 5:

Zadavatel požaduje podporu deduplikace a komprese jako funkční vlastnost nabízeného řešení, neboť z vlastní zkušenosti ví, že tyto funkce přinášejí významné úspory diskové kapacity, zejména u souborových úložišť, archivů, virtualizačních prostředí a záloh. K těmto účelům Zadavatel pořizuje technologii bezpečného úložiště.

Dodání vyšší diskové kapacity bez podpory požadované funkcionality nelze považovat za ekvivalentní řešení, neboť neřeší požadovanou funkcionalitu a současně klade zvýšené nároky na prostorové uspořádání, napájení a chlazení diskových systémů.

V návaznosti na tento dotaz Zadavatel blíže upřesnil požadavky na dodávané technologie v Technické specifikaci.

Dotaz č. 6:

V dokumentu Příloha č.2 smlouvy (Technická specifikace) je mimo jiné požadováno:
„Min. 512 GB cache paměti s možností rozšíření na 4 TB. Cache musí mít globální adresní prostor"

Žádáme zadavatele o potvrzení, že požadavek na globálně sdílenou cache nebude vykládán striktně jako požadavek na jediný společný cache prostor přístupný všem řadičům současně, ale že budou akceptována i řešení využívající distribuovanou cache architekturu, pokud zajišťují stejnou nebo vyšší úroveň dostupnosti, ochrany dat a provozní funkčnosti.

Odpověď č. 6:

Zadavatel požadavkem sledoval zajištění jednotného přístupu k datům a eliminaci omezení vyplývajících z lokální cache jednotlivých řadičů.
Zadavatel nebude trvat na implementaci konkrétního typu cache architektury. Za splnění požadavku budou považována i řešení využívající distribuovanou cache architekturu, pokud z pohledu funkčnosti, dostupnosti a přístupu k datům poskytují ekvivalent globálně sdíleného adresního prostoru. Zadavatel zároveň upravil znění technické specifikace tak, aby bylo jednoznačné, že požadavek není vázán na implementaci konkrétní cache architektury, ale na dosažení požadované funkčnosti.

Dotaz č. 7:

V dokumentu Příloha č.2 smlouvy (Technická specifikace) je mimo jiné požadováno:
„Podpora SAS disků s kapacitou alespoň 2,4 TB"

Podle názoru uchazeče se jedná o technologický požadavek vztahující se ke konkrétnímu typu a generaci diskových médií, nikoliv k požadované funkcionalitě nebo parametrům výsledného řešení. Moderní enterprise storage systémy jsou běžně osazovány vysokokapacitními SAS SSD nebo NVMe SSD disky, přičemž podpora SAS disků o kapacitě 2,4 TB sama o sobě nepředstavuje žádný měřitelný přínos z hlediska výkonu, dostupnosti ani kapacity řešení. Žádáme proto zadavatele o vysvětlení relevance tohoto požadavku ve vztahu k předmětu veřejné zakázky a o zvážení jeho odstranění, případně nahrazení požadavkem na celkovou využitelnou kapacitu, výkon či jiný objektivně měřitelný parametr řešení.

Odpověď č. 7:

Zadavatel uvádí, že účelem je zajistit, aby nabízená platforma **podporovala** vedle SSD/NVMe médií také standardní enterprise SAS disky, které mohou představovat ekonomicky výhodnou

variantu rozšíření kapacity v budoucím období. Požadovaná minimální kapacita 2,4 TB představuje běžně dostupnou enterprise kategorii SAS disků a má zajistit, aby nabízená platforma podporovala kapacitně relevantní média pro případné budoucí rozšiřování systému. Nejedná se o požadavek na konkrétní osazení dodávaného řešení, ale o požadavek na podporu této třídy diskových médií.

Současně nejsou uchazeči nijak omezeni v nabídce disků vyšších kapacit ani jiných typů médií, včetně SSD či NVMe, pokud jsou splněny všechny ostatní požadavky zadávací dokumentace. Požadavek tedy nestanovuje konkrétní konfiguraci dodávaného řešení, ale minimální technickou podporu platformy z hlediska její budoucí rozšiřitelnosti, s přihlédnutím k ekonomické stránce dalšího rozšíření a povinností jednat s péčí řádného hospodáře.

Zadavatel zároveň uvádí, že upravil znění požadavku v technické specifikaci tak, aby bylo jednoznačně zřejmé, že požadavek směřuje na podporu uvedených typů médií a neomezuje uchazeče ve volbě konkrétního typu diskových médií dodávaných v rámci nabízeného řešení.

Závěr

Zadavatel v souladu s výše uvedeným upravil zadávací podmínky veřejné zakázky.

Zadavatel se rozhodl přistoupit k úpravám dokumentu *Technická specifikace*, který je přílohou č. 2 Smlouvy, jejíž závazný vzor je přílohou č. 5 Zadávací dokumentace. Dále provedl úpravy v dokumentu *Bližší specifikace předmětu plnění*, který je přílohou č. 1 Smlouvy, jejíž závazný vzor je přílohou č. 5 Zadávací dokumentace. Úpravu provedl též v dokumentu *Zadávací dokumentace*.

Upravené verze výše zmíněných dokumentů jsou přílohou tohoto vysvětlení zadávací dokumentace, přičemž veškeré změny jsou vyznačeny formou revizí v textu dokumentu. V ostatním zůstává zadávací dokumentace nedotčena.

Současně je na profilu Zadavatele v elektronickém nástroji E-ZAK uveřejněna aktualizovaná zadávací dokumentace ve znění nyní prováděné změny. Zadavatel tímto žádá dodavatele, aby při sestavování nabídek využili příloh této aktualizované zadávací dokumentace.

Lhůta pro podání nabídek se prodlužuje a nově je stanovena na den **21. 8. 2026 do 9:00 hodin**.

Přílohy:

- *Technická specifikace ve znění změny ZD č. 2*
- *Bližší specifikace předmětu plnění ve znění změny ZD č. 2*
- *Zadávací dokumentace ve znění změny ZD č. 2*

Aleš Havlín
17.07.2026 13:25
Podepsáno elektronicky

.....
Mgr. Aleš Havlín
náměstek ředitele organizační jednotky
Správa železniční telematiky
pověřený řízením organizační jednotky

Klasifikace: Veřejný dokument

SPRÁVA ŽELEZNIC

Příloha č. 2 smlouvy

Technická specifikace

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

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

Obsah

1 Technické požadavky

1.1 Technické požadavky na Datové úložiště

1.1.1 Technická specifikace Položky A

V oblasti dodávky **jednoho (1)** zařízení pro datové úložiště (primární datové úložiště v lokalitě **Praha**) definuje Zadavatel následující požadavky:

[IDENTIFIKACE MODELU - DOPLNÍ DODAVATEL]

Požadavek	**Nabízené řešení** ~~(~~doplňte **ANO~~/~~ - splňuje** nebo **NE~~,~~ – nesplňuje***, případně uveďte technické parametry, pokud lze~~)~~ **Vyplní-li dodavatel NE, jeho nabídka může být vyloučena pro nesplnění zadávacích podmínek veřejné zakázky.*
Základní vlastnosti	
Typ zařízení: Hybridní datové úložiště typu SAN~~, s podporou SSD a SAS disků~~.	[DOPLNÍ DODAVATEL]
Třída diskového pole: Enterprise.	[DOPLNÍ DODAVATEL]
Fyzické provedení do standardní rackové skříně o šířce 19 palců, výšce 42U a hloubce 120 cm.	[DOPLNÍ DODAVATEL]
Rail kit pro montáž do racku pro všechny dílčí komponenty (pokud je k danému řešení v nabídce výrobce).	[DOPLNÍ DODAVATEL]
Zcela redundantní architektura bez SPOF.	[DOPLNÍ DODAVATEL]
Napájecí zdroje: AC 230 V, redundantní, hot-swap, s minimální účinností 90%.	[DOPLNÍ DODAVATEL]
Napájecí kabely 230V IEC C13/C14 nebo C19/C20 kompatibilní s napájecím zdrojem v délce minimálně 2 metry, v barvě černé a červené (v poměru 50:50), v potřebném množství dle navrhnutého řešení (Alternativně: Napájecí kabely 230V CEE7/7 kompatibilní s napájecím zdrojem v délce minimálně 2 metry, v barvě černé a červené (v poměru 50:50), v potřebném množství dle navrhnutého řešení).	[DOPLNÍ DODAVATEL]
Maximální celkový elektrický příkon řešení: **10 kW/rack.**	[DOPLNÍ DODAVATEL]

Velikost Rack Unit (U): Max. 2x42U (celé řešení při požadované kapacitě, včetně serverů a síťových prvků).	[DOPLNÍ DODAVATEL]
~~Typ podporovaných~~Podpora nejnovějších generací disků: **NVMe/SSD~~,~~ nebo SAS/NL-SAS HDD nebo jejich kombinace**.	[DOPLNÍ DODAVATEL]
Diskové pole musí obsahovat alespoň **4 řadiče**.	[DOPLNÍ DODAVATEL]
Konfigurace musí být tolerantní k výpadku jednoho řadiče bez jakýchkoli dopadů na poskytované blokové služby. (Dodavatel během implementace pole prokáže odolnost proti selhání jednoho řadiče).	[DOPLNÍ DODAVATEL]
Podpora připojení host serverů s operačními systémy Windows Server, Solaris, HP-UX, VMware, IBM-AIX a Linux v aktuálních verzích.	[DOPLNÍ DODAVATEL]
Podpora připojení host serverů v režimu clusterů viz seznam operačních systémů zmíněných výše.	[DOPLNÍ DODAVATEL]
Podpora protokolů FC a iSCSI pro připojení externích diskových polí.	[DOPLNÍ DODAVATEL]
~~Technologie redukce dat (deduplikace a komprese) napříč všemi typy nabízených disků s minimálním dopadem na výkon.~~Řešení musí podporovat technologie datové redukce (deduplikace a komprese), které jsou aplikovatelné v rámci nabízené konfigurace úložiště. Tyto technologie musí být dostupné minimálně pro primární datovou vrstvu (např. SSD nebo akcelerační tier) a musí být implementovány způsobem zajišťujícím efektivní využití kapacity při zachování požadovaného výkonu systému.	[DOPLNÍ DODAVATEL]
Minimální konfigurace	
Celková minimální RAW kapacita diskového úložiště: **1 PB** (PetaBajt).	[DOPLNÍ DODAVATEL]
Z celkové velikosti minimálně **100 TiB** čisté užitné kapacity pomocí SSD disků.	[DOPLNÍ DODAVATEL]
Minimálně **16 FC** portů s ~~minimální~~přenosovou rychlostí minimálně **32 Gb/s** ~~FC HBA, (min.~~. Každý řadič musí být osazen nejméně 4 FC porty ~~na řadič).~~.	[DOPLNÍ DODAVATEL]
Minimálně **4 iSCSI** porty s rychlostí minimálně **10** ~~Gbps~~**Gb/s** (min. 2 porty na řadič).	[DOPLNÍ DODAVATEL]
Min. 512 GB cache paměti s možností rozšíření na 4 TB. Cache musí ~~mít globální adresní prostor~~být sdílená mezi řadiči systému tak, aby byl zajištěn konzistentní přístup k datům a	[DOPLNÍ DODAVATEL]

jejich ochrana v případě výpadku řadiče. Je přípustná jak implementace se společným (globálním) adresním prostorem cache, tak distribuovaná cache architektura, pokud zajišťuje ekvivalentní nebo vyšší úroveň dostupnosti, ochrany dat a transparentního provozu z pohledu hostitelských systémů.	
Škálovatelnost	
Škálovatelnost na minimálně 8 PB (PetaBajtů) RAW kapacity v rámci jednoho pole.	[DOPLNÍ DODAVATEL]
~~Podpora konfigurace s kombinací jak NVMe, tak standardních SAS disků.~~	~~[DOPLNÍ DODAVATEL]~~
~~Podpora nejnovějších generací SAS a NL-SAS disků pomocí vhodných řadičů.~~	~~[DOPLNÍ DODAVATEL]~~
Podpora SAS disků s kapacitou alespoň 2,4 TB~~,~~ nebo NL-SAS disků s kapacitou alespoň 8 TB~~,~~ nebo SSD Flash disků ~~a~~s kapacitou alespoň 12 TB nebo NVMe disků s kapacitou alespoň 12 TB případně jejich kombinace, dle typu nabízeného řešení.	[DOPLNÍ DODAVATEL]
Zabezpečení dat a šifrování	
Podpora minimálně Raid 1, Raid 5 a Raid 6.	[DOPLNÍ DODAVATEL]
Podpora šifrování (Data at Rest) silnými moderními algoritmy (minimálně AES 256b nebo lepší). Případná licence musí být součástí nabídky.	[DOPLNÍ DODAVATEL]
Schopnost vytvářet alespoň 2000 logických jednotek (LUN) a podporovat velikost jednoho svazku (LUN) minimálně 100 TB.	[DOPLNÍ DODAVATEL]
Podpora alespoň 10~~24~~00 ks snapshotů pro daný LUN. Podpora vytvoření snapshotu ze snapshotu (kaskádování).	[DOPLNÍ DODAVATEL]
Podpora schopnosti vytvářet nesmazatelné („immutable“) snapshoty s možností definice retenční doby.	[DOPLNÍ DODAVATEL]
Podpora synchronní replikace, asynchronní replikace, asynchronní replikace se žurnálem, replikace v 3DC (1 na 2), kaskádové replikace (1-1-1). Licence pro replikace na plnou kapacitu nabízeného diskového pole musí být součástí nabídky.	[DOPLNÍ DODAVATEL]
Automatická detekce, zaznamenávání a notifikace chyb.	[DOPLNÍ DODAVATEL]
Administrace	
Management software pro administraci z jednotného GUI (musí být součástí nabídky) i z CLI.	[DOPLNÍ DODAVATEL]
Software pro administraci musí být schopen spravovat více diskových polí z jedné konzole a je integrován s prostředím VMware v obrazovém formátu.	[DOPLNÍ DODAVATEL]

Možnost integrace s různými softwarovými nástroji pro automatizaci, monitorování a správu, jako jsou: • VMware 8.x a vyšší • Terraform • Redhat Ansible • Oracle Linux Virtualization Manager • Veeam cloud backup and recovery	[DOPLNÍ DODAVATEL]
Pro všechny činnosti související se správou diskového pole musí management software podporovat následující: • centralizovaný monitoring, konfiguraci a správu úložných komponent, • monitoring stavu, výkonu, utilizace a konfigurace, • shromažďování, ukládání a analýzu dat o výkonu diskového pole.	[DOPLNÍ DODAVATEL]
Tiering jak nad interní kapacitou, tak v rámci externích virtualizovaných diskových polí.	[DOPLNÍ DODAVATEL]
Opravy a výměny HW komponent musí být možné za běhu, bez dopadu na poskytované datové služby.	[DOPLNÍ DODAVATEL]
Upgrade firmware HW komponent diskového pole musí probíhat bez přerušení poskytované služby.	[DOPLNÍ DODAVATEL]
Správa diskového pole musí podporovat RBAC (Role-Based Access Control).	[DOPLNÍ DODAVATEL]
Správa diskového pole musí být integrovatelná na externí IdM/PAM/SIEM řešení. 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).	[DOPLNÍ DODAVATEL]
U všech disků (SSD, NVMe, SAS) a jiných datových nosičů je při poruše a/nebo reklamaci požadováno ponechání disku ~~Objednateli~~Zadavateli, z důvodu prevence úniku dat.	[DOPLNÍ DODAVATEL]
Podpora výrobce na **5 let.**	[DOPLNÍ DODAVATEL]

1.1.2 Technická specifikace Položky B

V oblasti dodávky **jednoho (1)** zařízení pro datové úložiště (sekundární datové úložiště v lokalitě **Plzeň**) definuje Zadavatel následující požadavky:

[IDENTIFIKACE MODELU - DOPLNÍ DODAVATEL]

Požadavek	Nabízené řešení ~~(~~doplňte **ANO~~/~~ - splňuje** nebo **NE~~,~~ – nesplňuje***, případně uveďte technické parametry, pokud lze~~)~~ **Vyplní-li dodavatel NE, jeho nabídka může být vyloučena pro nesplnění zadávacích podmínek veřejné zakázky.*
Základní vlastnosti	
Typ zařízení: Hybridní datové úložiště typu SAN~~, s podporou SSD a SAS disků~~.	[DOPLNÍ DODAVATEL]
Třída diskového pole: Enterprise.	[DOPLNÍ DODAVATEL]
Fyzické provedení do standardní rackové skříně o šířce 19 palců, výšce 42U a hloubce 120 cm.	[DOPLNÍ DODAVATEL]
Rail kit pro montáž do racku pro všechny dílčí komponenty (pokud je k danému řešení v nabídce výrobce).	[DOPLNÍ DODAVATEL]
Zcela redundantní architektura bez SPOF.	[DOPLNÍ DODAVATEL]
Napájecí zdroje: AC 230 V, redundantní, hot-swap, s minimální účinností 90%.	[DOPLNÍ DODAVATEL]
Napájecí kabely 230V IEC C13/C14 nebo C19/C20 kompatibilní s napájecím zdrojem v délce minimálně 2 metry, v barvě černé a červené (v poměru 50:50), v potřebném množství dle navrhnutého řešení (Alternativně: Napájecí kabely 230V CEE7/7 kompatibilní s napájecím zdrojem v délce minimálně 2 metry, v barvě černé a červené (v poměru 50:50), v potřebném množství dle navrhnutého řešení).	[DOPLNÍ DODAVATEL]
Maximální celkový elektrický příkon řešení: **10 kW/rack.**	[DOPLNÍ DODAVATEL]
Velikost Rack Unit (U): Max. 2x42U (celé řešení při požadované kapacitě, včetně serverů a síťových prvků).	[DOPLNÍ DODAVATEL]
~~Typ podporovaných~~Podpora nejnovějších generací disků: **NVMe/SSD~~,~~ nebo SAS/NL-SAS HDD nebo jejich kombinace.**	[DOPLNÍ DODAVATEL]
Diskové pole musí obsahovat alespoň **4 řadiče**	[DOPLNÍ DODAVATEL]
Konfigurace musí být tolerantní k výpadku jednoho řadiče bez jakýchkoli dopadů na poskytované blokové služby. (Dodavatel během implementace pole prokáže odolnost proti selhání jednoho řadiče).	[DOPLNÍ DODAVATEL]

Podpora připojení host serverů s operačními systémy Windows Server, Solaris, HP-UX, VMware, IBM-AIX a Linux v aktuálních verzích.	[DOPLNÍ DODAVATEL]
Podpora připojení host serverů v režimu clusterů viz seznam operačních systémů zmíněných výše.	[DOPLNÍ DODAVATEL]
Podpora protokolů FC a iSCSI pro připojení externích diskových polí.	[DOPLNÍ DODAVATEL]
~~Technologie redukce dat (deduplikace a komprese) napříč všemi typy nabízených disků s minimálním dopadem na výkon.~~ Řešení musí podporovat technologie datové redukce (deduplikace a komprese), které jsou aplikovatelné v rámci nabízené konfigurace úložiště. Tyto technologie musí být dostupné minimálně pro primární datovou vrstvu (např. SSD nebo akcelerační tier) a musí být implementovány způsobem zajišťujícím efektivní využití kapacity při zachování požadovaného výkonu systému.	[DOPLNÍ DODAVATEL]
Minimální konfigurace	
Celková minimální RAW kapacita diskového úložiště: **1 PB** (PetaBajt).	[DOPLNÍ DODAVATEL]
Minimálně **16 FC** portů s ~~minimální~~přenosovou rychlostí minimálně **32 Gb/s** ~~FC HBA, (min.~~. Každý řadič musí být osazen nejméně 4 FC porty ~~na řadič).~~ .	[DOPLNÍ DODAVATEL]
Minimálně **4 iSCSI porty** s rychlostí minimálně **10** ~~Gbps~~**Gb/s** (min. 2 porty na řadič).	[DOPLNÍ DODAVATEL]
Min. 512 GB cache paměti s možností rozšíření na 4 TB. Cache musí ~~mít globální adresní prostor~~být sdílená mezi řadiči systému tak, aby byl zajištěn konzistentní přístup k datům a jejich ochrana v případě výpadku řadiče. Je přípustná jak implementace se společným (globálním) adresním prostorem cache, tak distribuovaná cache architektura, pokud zajišťuje ekvivalentní nebo vyšší úroveň dostupnosti, ochrany dat a transparentního provozu z pohledu hostitelských systémů.	[DOPLNÍ DODAVATEL]
Škálovatelnost	
Škálovatelnost na minimálně 8 PB (PetaBajtů) RAW kapacity v rámci jednoho pole.	[DOPLNÍ DODAVATEL]
~~Podpora konfigurace s kombinací jak NVMe, tak standardních SAS disků.~~	~~[DOPLNÍ DODAVATEL]~~

~~Podpora nejnovější generace SAS a NL-SAS disků pomocí vhodných řadičů.~~	~~[DOPLNÍ DODAVATEL]~~
Podpora SAS disků s kapacitou alespoň 2,4 TB, nebo NL-SAS disk~~y~~ů s kapacitou alespoň 8 TB, nebo SSD Flash ~~disky a NVMe disky~~disků s kapacitou alespoň 12 TB, nebo NVMe disků s kapacitou alespoň 12 TB, případně jejich kombinace, dle typu nabízeného řešení.	[DOPLNÍ DODAVATEL]
Zabezpečení dat a šifrování	
Podpora minimálně Raid 1, Raid 5 a Raid 6.	[DOPLNÍ DODAVATEL]
Podpora šifrování (Data at Rest) silnými moderními algoritmy (minimáleně AES 256b nebo lepší). Případná licence musí být součástí dodávky.	[DOPLNÍ DODAVATEL]
Schopnost vytvářet alespoň 2000 logických jednotek (LUN) a podporovat velikost jednoho svazku (LUN) minimálně 100 TB	[DOPLNÍ DODAVATEL]
Podpora alespoň 10~~24~~00 ks snapshotů pro daný LUN. Podpora vytvoření snapshotu ze snapshotu (kaskádování).	[DOPLNÍ DODAVATEL]
Podpora schopnosti vytvářet nesmazatelné („immutable“) snapshoty s možností definice retenční doby.	[DOPLNÍ DODAVATEL]
Podpora synchronní replikace, asynchronní replikace, asynchronní replikace se žurnálem, replikace v 3DC (1na2), kaskádové replikace (1-1-1). Pokud je replikace podmíněná licencí, Dodavatel je povinen tuto licenci zahrnout do dodávky řešení. Licence je součástí nabídkové ceny a nenáleží Dodavateli za ni zvláštní odměna.	[DOPLNÍ DODAVATEL]
Automatická detekce, zaznamenávání a notifikace chyb.	[DOPLNÍ DODAVATEL]
Administrace	
Management software pro administraci z jednotného GUI (musí být součástí nabídky) i z CLI.	[DOPLNÍ DODAVATEL]
Software pro administraci musí být schopen spravovat více diskových polí z jedné konzole a je integrován s prostředím VMware v obrazovém formátu.	[DOPLNÍ DODAVATEL]
Možnost integrace s různými softwarovými nástroji pro automatizaci, monitorování a správu, např: • VMware 8.x a vyšší • Terraform	[DOPLNÍ DODAVATEL]

• Redhat Ansible • Oracle Linux Virtualization Manager • Veeam cloud backup and recovery	
Pro všechny činnosti související se správou diskového pole musí management software podporovat následující: • centralizovaný monitoring, konfiguraci a správu úložných komponent, • monitoring stavu, výkonu, utilizace a konfigurace, shromažďování, ukládání a analýzu dat o výkonu diskového pole.	[DOPLNÍ DODAVATEL]
Tiering jak nad interní kapacitou, tak v rámci externích virtualizovaných diskových polí.	[DOPLNÍ DODAVATEL]
Opravy a výměny HW komponent musí být možné za běhu, bez dopadu na poskytované datové služby.	[DOPLNÍ DODAVATEL]
Upgrade firmware HW komponent diskového pole musí probíhat bez přerušení poskytované služby.	[DOPLNÍ DODAVATEL]
Správa diskového pole musí podporovat RBAC (Role-Based Access Control).	[DOPLNÍ DODAVATEL]
Správa diskového pole musí být integrovatelná na externí IdM/PAM/SIEM řešení. 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).	[DOPLNÍ DODAVATEL]
U všech disků (SSD, NVMe, SAS) a jiných datových nosičů je při poruše a/nebo reklamaci požadováno ponechání disku Zadavateli, z důvodu prevence úniku dat.	[DOPLNÍ DODAVATEL]
Podpora výrobce na **5 let.**	[DOPLNÍ DODAVATEL]

1.2 Technické požadavky na servery

Součástí řešení Datových úložišť budou **2 (dvě)** serverové řešení (farmy, klastry) obsahující **8 (osm)** serverů, 4 servery v každé lokalitě. Tyto servery budou určeny pro potřebnou správu každého úložiště a bezpečnostní kontrolu uložených dat. Z důvodu škálovatelnosti a budoucího rozšíření jejich využití musí být tato serverová řešení rozšiřitelná až na plánovaný počet 12 serverů v každé z obou lokalit.

1.2.1 Technická specifikace Položky C

Dvě (2) serverová řešení obsahující osm (8) serverů (4 servery v každé lokalitě) pro virtualizační farmu s následující konfigurací každého serveru:

[IDENTIFIKACE MODELU - DOPLNÍ DODAVATEL]

Požadavek	**Nabízené řešení** ~~(~~doplňte **ANO~~/~~ - splňuje** nebo **NE~~,~~ – nesplňuje***, případně uveďte technické parametry, pokud lze~~)~~ *Vyplní-li dodavatel NE, jeho nabídka může být vyloučena pro nesplnění zadávacích podmínek veřejné zakázky.
Provedení do 19" racku o velikosti maximálně **24U**, které bude v prvotní sestavě osazeno minimálně 4 servery a rozšiřitelné na minimálně 12 serverů v každé lokalitě.	[DOPLNÍ DODAVATEL]
2x CPU, každý minimálně **32 jader** se základní frekvencí minimálně 2,4 GHz a se spotřebou maximálně 300 W.	[DOPLNÍ DODAVATEL]
Architektura **Intel x86-64** z důvodu kompatibility současného ICT prostředí Zadavatele.	[DOPLNÍ DODAVATEL]
Operační paměť minimálně **512 GB DDR5** s použitím modulů o maximální velikosti 64 GB s možností rozšíření na dvojnásobek pomocí stejných modulů.	[DOPLNÍ DODAVATEL]
2x SSD, každý o velikosti minimálně **480 GB** v konfiguraci RAID1 (zrcadlení) pro boot a běh OS nebo virtualizační platformy.	[DOPLNÍ DODAVATEL]
Lokální úložiště v serveru • Uživatelsky použitelná čistá nekomprimovaná kapacita minimálně **2 TiB**. • Umožňuje rozšíření minimálně na 4 TiB jen přidáním disků. • Zajišťuje redundanci uložených dat minimálně na úrovni odpovídající **RAID6**. Použití výhradně **NVMe** o velikosti maximálně 2 TiB.	[DOPLNÍ DODAVATEL]
Trusted Platform Module minimálně ve verzi 2.0.	[DOPLNÍ DODAVATEL]
Minimálně **8x 25 Gbps** SFP LAN s podporou rychlosti 10 Gbps (tj. 10/25 Gbps).	[DOPLNÍ DODAVATEL]
Dedikovaný port pro HW management.	[DOPLNÍ DODAVATEL]
Minimálně **2x FC port** o rychlosti minimálně **32 Gbps.**	[DOPLNÍ DODAVATEL]
Podpora operačních systémů Windows Server, VMware a Linux v aktuálních verzích.	[DOPLNÍ DODAVATEL]
Napájecí kabely 230V IEC C13/C14 nebo C19/C20 kompatibilní s napájecím zdrojem v délce minimálně 2 metry, v barvě černé a červené (v procentuálním poměru počtu kabelů 50:50, pro	[DOPLNÍ DODAVATEL]

odlišení zálohované a nezálohované napájecí větve), v potřebném množství dle navrhnutého řešení (Alternativně: Napájecí kabely 230V CEE7/7 kompatibilní s napájecím zdrojem v délce minimálně 2 metry, v barvě černé a červené (v procentuálním poměru počtu kabelů 50:50, pro odlišení zálohované a nezálohované napájecí větve) v potřebném množství dle navrhnutého řešení).	
U všech disků (SSD, NVMe, SAS) a jiných datových nosičů je při poruše a/nebo reklamaci požadováno ponechání disku Zadavateli, z důvodu prevence úniku dat.	[DOPLNÍ DODAVATEL]
Podpora výrobce na **5 let.**	[DOPLNÍ DODAVATEL]

Zadavatel umožňuje využití technologie kombinující modulární serverové šasi a servery, která podporuje jednoduché škálování výpočetního výkonu a rychlé nasazení pouhým přidáním dalšího serverového nodu a minimalizuje zásahy do síťové infrastruktury.

1.3 Technické požadavky na síťové prvky

1.3.1 Technická specifikace Položky D

Čtyři (4) SAN switche, dva (2) do každé lokality v konfiguraci:

[IDENTIFIKACE MODELU - DOPLNÍ DODAVATEL]

Požadavek	**Nabízené řešení** {doplňte **ANO~~/~~ - splňuje** nebo **NE~~/~~ – nesplňuje***, případně uveďte technické parametry, pokud lze~~}~~ **Vyplní-li dodavatel NE, jeho nabídka může být vyloučena pro nesplnění zadávacích podmínek veřejné zakázky.*
Velikost skříně switche o maximální výšce ~~**1 RU**~~**1U** (45 mm).	[DOPLNÍ DODAVATEL]
Minimálně **24x 32 Gbps FC** portů s podporou rychlostí **64 Gbps.**	[DOPLNÍ DODAVATEL]
Dedikovaný síťový port pro oddělený management	[DOPLNÍ DODAVATEL]
2x napájecí zdroj AC/230V	[DOPLNÍ DODAVATEL]
Management switche dostupný přes CLI i GUI	[DOPLNÍ DODAVATEL]
Podpora RBAC (RADIUS / TACACS)	[DOPLNÍ DODAVATEL]

Podpora bezpečnostních protokolů Fibre Channel Security Protocols (FC-SP), SSHv2	[DOPLNÍ DODAVATEL]
Podpora SAN protokolů FCP, SCSI over FC, NVMe over FC, Inter-Switch Link, FC-NVMe	[DOPLNÍ DODAVATEL]
Podpora dalších protokolů: SPAN, Syslog, SNMP, NTP	[DOPLNÍ DODAVATEL]
Podpora výrobce na 5 let.	[DOPLNÍ DODAVATEL]
Součástí dodávky musí být licence na dobu 5 let (pokud je vyžadována) umožňující současné použití všech fyzicky osazených portů zařízení.	[DOPLNÍ DODAVATEL]
Materiál pro montáž dodaného Hardware do rackové skříně.	[DOPLNÍ DODAVATEL]

Zadavatel umožňuje integraci SAN switchů do modulárního serverového šasi z Položky C.

1.3.2 Technická specifikace Položky E:

V oblasti dodávky **dvou (2)** switchů pro oddělenou síť pro management (OOB) definuje Zadavatel následující požadavky:

[IDENTIFIKACE MODELU - DOPLNÍ DODAVATEL]

Požadavek	**Nabízené řešení** ~~(~~doplňte **ANO~~/~~ - splňuje** nebo **NE~~/~~ – nesplňuje***, případně uveďte technické parametry, pokud lze~~)~~ **Vyplní-li dodavatel NE, jeho nabídka může být vyloučena pro nesplnění zadávacích podmínek veřejné zakázky.*
Provedení switche pro instalaci do rackové skříně o hloubce **100 cm.**	[DOPLNÍ DODAVATEL]
Velikost skříně switche o maximální výšce ~~**1 RU**~~**1U** (45 mm).	[DOPLNÍ DODAVATEL]
Minimálně **48x 1G RJ45** port.	[DOPLNÍ DODAVATEL]
Minimálně **4x 1G SFP** nebo **10G SFP+** port s podporou rychlosti 1G (může být i formou vyměnitelného rozšiřujícího modulu).	[DOPLNÍ DODAVATEL]
Dedikovaný síťový port pro oddělený management.	[DOPLNÍ DODAVATEL]
2x napájecí zdroj AC/230V	[DOPLNÍ DODAVATEL]
Podpora stackování switchů (spojení v jeden virtuální switch) ~~switchů~~ a plná kompatibilita stackování se switchi v prostředí Zadavatele. Zadavatel pro oddělený management (OOB) infrastruktury používá switche Cisco řady Catalyst 9200L.	[DOPLNÍ DODAVATEL]

Podpora stackování switchů: • spojení v jeden virtuální switch, • minimálně 6 switchů ve stacku	
Podpora výrobce na 5 let.	[DOPLNÍ DODAVATEL]
Podpora protokolů IPv4 a IPv6.	[DOPLNÍ DODAVATEL]
Podpora funkce na vrstvě **L2** dle ISO/OSI modelu.	[DOPLNÍ DODAVATEL]
Minimální kapacita **15000 MAC adres.**	[DOPLNÍ DODAVATEL]
Podpora protokolů LACP a SPAN.	[DOPLNÍ DODAVATEL]
Podpora technologií VLAN, Jumbo frame~~, IEEE 802.1v, IEEE 802.1s a IEEE 802.1w~~.	[DOPLNÍ DODAVATEL]
Podpora Energy Efficient Ethernet (IEEE 802.3az).	[DOPLNÍ DODAVATEL]
Minimální výkon zpracování packetů (forwarding rate) **35 Mpps.**	[DOPLNÍ DODAVATEL]
~~Potřebné licence na dobu 5 let zahrnující funkcionality:~~ Funkcionalita, která musí být dostupná po dobu minimálně 5 let (např. pomocí licencí): • Využití všech osazených síťových portů • VLAN • LACP • SPAN.	[DOPLNÍ DODAVATEL]
Integrace se systémem Cisco ISE, který Zadavatel ve svém síťovém prostředí využívá.	[DOPLNÍ DODAVATEL]
Vzdálená správa • Vzdálená správa s dedikovaným vlastním portem 1GbE. • Možnost vzdálené aktualizace firmware. • Podpora protokolu SNMP minimálně ve verzi 2c • Podpora protokolu Syslog a předávání logů na vzdálený systém • Zapojení do centralizovaného systému vzdálené správy, který Kupující ve svém prostředí používá – ***Cisco Catalyst Center*** *(dříve Cisco DNA Center).*	[DOPLNÍ DODAVATEL]
Materiál pro montáž dodaného Hardware do rackové skříně.	[DOPLNÍ DODAVATEL]
Síťové optické moduly pro každý optický port SFP, plně kompatibilní s dodávaným switchem, originální od výrobce dodaných switchů v provedení „1/10Gbps nebo 10Gbps, Singlemode, LC, Long Range"	[DOPLNÍ DODAVATEL]

1.3.3 Technická specifikace položky F

V oblasti dodávky **čtyř (4)** datacentrových switchů pro připojení Datového úložiště definuje Zadavatel následující požadavky:

[IDENTIFIKACE MODELU - DOPLNÍ DODAVATEL]

Požadavek	Nabízené řešení ~~(~~doplňte **ANO~~/~~ - splňuje** nebo **NE~~,~~ – nesplňuje***, případně uveďte technické parametry, pokud lze~~)~~ **Vyplní-li dodavatel NE, jeho nabídka může být vyloučena pro nesplnění zadávacích podmínek veřejné zakázky.*
Provedení switche pro instalaci do rackové skříně o hloubce **100 cm.**	[DOPLNÍ DODAVATEL]
Velikost skříně switche o maximální výšce ~~**1 RU**~~**1U** (45 mm).	[DOPLNÍ DODAVATEL]
Rail kit pro montáž do racku (pokud je k danému řešení v nabídce výrobce).	[DOPLNÍ DODAVATEL]
Minimálně **48x 25G SFP~~+~~28** port s podporou rychlostí 10G a 1G.	[DOPLNÍ DODAVATEL]
Minimálně **6x 100G QSFP** port s podporou rychlosti 40G.	[DOPLNÍ DODAVATEL]
Dedikovaný síťový port pro oddělený management.	[DOPLNÍ DODAVATEL]
2x hot-swap napájecí zdroj AC/230V.	[DOPLNÍ DODAVATEL]
Směr proudu vzduchu ventilátorů: přes porty ven (Back-to-Front).	[DOPLNÍ DODAVATEL]
Podpora výrobce na **5 let.**	[DOPLNÍ DODAVATEL]
Podpora protokolů IPv4 a IPv6.	[DOPLNÍ DODAVATEL]
Podpora funkce na vrstvách **L2** i **L3** dle ISO/OSI modelu.	[DOPLNÍ DODAVATEL]
Minimální kapacita **100 000 MAC adres.**	[DOPLNÍ DODAVATEL]
Minimální kapacita **4000 aktivních VLAN** podle IEEE 802.1Q.	[DOPLNÍ DODAVATEL]
Podpora technologií a protokolů LACP, MPLS, QoS, STP, SPAN, VRF, VLAN a Jumbo frame~~, (IEEE 802.1v, IEEE 802.1s, IEEE 802.1w, IEEE 802.1AX, IEEE 802.1p.)~~.	[DOPLNÍ DODAVATEL]
Funkcionalita, která musí být dostupná po dobu minimálně 5 let (např. pomocí licencí): • Využití všech osazených síťových portů • VLAN • SPAN • LACP • VRF	[DOPLNÍ DODAVATEL]
Minimální výkon zpracování packetů (forwarding rate) **1000 Mpps.**	[DOPLNÍ DODAVATEL]
Podpora policy-based routing.	[DOPLNÍ DODAVATEL]

Dynamické směrování: OSPFv2, OSPFv3, BGP, MP-BGP včetně BGP MD5 autentizace.	[DOPLNÍ DODAVATEL]
Podpora static a dynamic VXLAN overlay architektury s využitím BGP-EVPN (RFC 7432, 8365~~)~~).	[DOPLNÍ DODAVATEL]
~~Pro propojení mezi switchi (peer-link) musí být k dispozici rozhraní s minimální agregovanou přenosovou kapacitou 2 x 100 GbE bez omezení funkčnosti VXLAN/BGP-EVPN.~~	~~[DOPLNÍ DODAVATEL]~~
Podpora ověřování TACACS+ a RADIUS.	[DOPLNÍ DODAVATEL]
Vzdálená správa • Vzdálená správa s dedikovaným vlastním portem 1GbE. • Možnost vzdálené aktualizace firmware. • Podpora protokolu SNMP minimálně ve verzi 2c. • Podpora protokolu Syslog a předávání logů na vzdálený systém.	[DOPLNÍ DODAVATEL]
Materiál pro montáž dodaného Hardware do rackové skříně.	[DOPLNÍ DODAVATEL]

1.3.4 Technická specifikace Položky G

V oblasti dodávky čtyř **(4)** kusů zařízení NGFW (**Next-Generation Firewall**) definuje Zadavatel následující požadavky pro každé z nich:

[IDENTIFIKACE MODELU - DOPLNÍ DODAVATEL]

Požadavek	**Nabízené řešení** ~~(~~doplňte **ANO**~~/~~ **- splňuje** nebo **NE**~~,~~ **– nesplňuje***, případně uveďte technické parametry, pokud lze~~)~~ **Vyplní-li dodavatel NE, jeho nabídka může být vyloučena pro nesplnění zadávacích podmínek veřejné zakázky.*
Fyzické, rack mount provedení do rozvaděče o standardní šířce 19 palců.	[DOPLNÍ DODAVATEL]
Velikost skříně o maximální výšce ~~**2 RU**~~**2U** (90 mm).	[DOPLNÍ DODAVATEL]
Minimálně **16x 25G SFP** port s podporou rychlosti 10G.	[DOPLNÍ DODAVATEL]
Minimálně **4x 100G SFP** port s podporou rychlosti 40G.	[DOPLNÍ DODAVATEL]
Dedikovaný síťový port pro oddělený management.	[DOPLNÍ DODAVATEL]
Dedikovaný konzolový port – typ RJ45 nebo USB.	[DOPLNÍ DODAVATEL]
Lokální úložiště pro logy o minimální kapacitě 500 GB v režimu RAID1.	[DOPLNÍ DODAVATEL]

Podpora nasazení v HA Clusteru pomocí dedikovaných portů.	[DOPLNÍ DODAVATEL]
2x hot-swap napájecí zdroj AC/230V	[DOPLNÍ DODAVATEL]
Interní redundantní ventilátory.	[DOPLNÍ DODAVATEL]
TPM (Trusted Platform Module) čip.	[DOPLNÍ DODAVATEL]
Celková minimální propustnost **80 Gbps.**	[DOPLNÍ DODAVATEL]
Počet souběžných TCP spojení minimálně **20 000 000.**	[DOPLNÍ DODAVATEL]
Minimální propustnost NGFW (IPS, Application control) min. **20 Gbps.**	[DOPLNÍ DODAVATEL]
Podpora bezpečnostních funkcí Antivirus, Antimalware, IPS a DLP jako nativní funkcionalita nabízeného NGFW řešení – pokud je použití bezpečnostních funkcí licencováno, musí být licence součástí nabídky.	[DOPLNÍ DODAVATEL]
Minimální propustnost SSL inspekce (IPS, HTTPS) **8 Gbps.**	[DOPLNÍ DODAVATEL]
Podpora virtuálních kontextů hardware appliance min. 3 kontexty – pokud jsou licencovány, musí být licence součástí nabídky.	[DOPLNÍ DODAVATEL]
Podpora Active-Active i Active-Passive režimů.	[DOPLNÍ DODAVATEL]
Správa všech zařízení pracujících v režimu vysoké dostupnosti musí probíhat jednotně přes společné grafické konfigurační rozhraní.	[DOPLNÍ DODAVATEL]
Grafické konfigurační rozhraní pro správu celého clusteru, dostupné pomocí webového prohlížeče (HTTPS) bez omezení na počet administrátorů a bez nutnosti instalovat dodatečnou management platformu nebo aplikaci.	[DOPLNÍ DODAVATEL]
Podpora LACP (IEEE 802.3ad).	[DOPLNÍ DODAVATEL]
Podpora TLS 1.3 i pro aplikační inspekce.	[DOPLNÍ DODAVATEL]
Podpora pravidel na základě identity uživatelů pro MS AD prostředí – nastavení bezpečnosti uživateli na základě členství v AD skupině na doménovém kontroléru.	[DOPLNÍ DODAVATEL]
Podpora Site-to-site IPsec VPN s podporou statického i dynamického routování.	[DOPLNÍ DODAVATEL]
Ověřování uživatelů proti LDAP, Radius, TACACS+.	[DOPLNÍ DODAVATEL]

Podpora výrobce na **5 let.**	[DOPLNÍ DODAVATEL]

Zařízení NGFW musí být dodány včetně veškerých potřebných licencí k provozu požadovaných služeb, viz. detailnější obecné požadavky uvedené v předchozí tabulce, s dobou platnosti a veškerými systémovými update po dobu **60 měsíců** od ukončení Fáze F2.1 pro primární lokalitu a od ukončení Fáze F2.2 pro sekundární lokalitu.

1.3.5 Technická specifikace Položky H

V oblasti ~~dodávky~~ datové kabeláže a ~~optických modulů pro připojení Datového úložiště~~propojení, Dodavatel navrhne a dodá ~~kompletní~~veškerou kabeláž ~~(metalickou i optickou) a~~ , optické moduly ~~potřebné pro propojení~~a jiné propojovací síťové prvky, které jsou nezbytné pro plně funkční datové zapojení všech dodávaných komponent řešení~~, včetně SAN a LAN konektivity, a~~. Dodané prvky musí být ~~dimenzovány pro plný~~ součástí nabídky v rozsahu nezbytném pro kompletní provoz řešení~~. Optické moduly~~ a to bez nutnosti dalších investic ze strany Zadavatele.

Veškeré dodané síťové prvky musí být podporované výrobci dodávaných zařízení a plně s nimi kompatibilní~~ s dodanými zařízeními a certifikované výrobcem~~.

Dodavatel je povinen realizovat propojení všech komponent řešení~~, musí podporovat přenosové rychlosti dle návrhu~~ v souladu s technickou dokumentací výrobců jednotlivých zařízení tak, aby byla zajištěna plná funkčnost, maximální propustnost síťového připojení, dostupnost a redundance dodávaného řešení.

Zadavatel uvádí, že ve svém prostředí pro připojení celého řešení zabezpečeného úložiště má v obou lokalitách připravené switche **Nexus 93180YC-FX3** ~~s dostatečným počtem portů SFP28 25 Gbps, single mode, duplex a QSFP 100 Gbps, single mode, duplex~~v HA režimu (v každé lokalitě dva kusy, celkem tedy 4 kusy) s dostatečným počtem volných slotů SFP28 25 Gbps a QSFP 100 Gbps, včetně propojovací kabeláže (duplex, singlemode). Součástí plnění ze strany Dodavatele je také **dodávka optických modulů** potřebných pro propojení řešení se síťovou infrastrukturou Zadavatele a to **včetně modulů do výše uvedených switchů Nexus**.

~~**Požadavek**~~	~~**Nabízené řešení**~~ ~~**(doplňte ANO/NE, počet kusů, případně uveďte technické parametry, pokud lze)**~~
~~Kabel–AOC / DAC s rozhraním QSFP+/QSFP28 pro rychlosti minimálně **40/100G**~~	~~[DOPLNÍ DODAVATEL]~~
~~Kabel–AOC / DAC s rozhraním SFP+/SFP28 pro rychlosti minimálně **10/25G**~~	~~[DOPLNÍ DODAVATEL]~~

Optický kabel AOC Fibre channel SFP+/SFP28 pro rychlosti minimálně **32 Gbps**	[DOPLNÍ DODAVATEL]
Kabel AOC / DAC s rozhraním SFP/SFP+ pro rychlosti minimálně **1/10G**	[DOPLNÍ DODAVATEL]
Optický transceiver s rozhraním QSFP+/QSFP28 pro rychlosti minimálně **40/100G**	[DOPLNÍ DODAVATEL]
Optický transceiver s rozhraním SFP+/SFP28 pro rychlosti minimálně **10/25G**	[DOPLNÍ DODAVATEL]
Optický transceiver SFP+/SFP28 Fibre Channel **32/64 Gbps**	[DOPLNÍ DODAVATEL]
Optický transceiver SFP/SFP+ **1/10G** (variantně, dle návrhu řešení)	[DOPLNÍ DODAVATEL]
Optické kabely ve vhodné délce, s parametry odpovídajícími navrhovanému řešení (např. konektory LC-LC, MM/SM, SR/LR, OM4/OS1)	[DOPLNÍ DODAVATEL]
Ethernetový kabel **RJ45**, **S/FTP,** min. **CAT6A**	[DOPLNÍ DODAVATEL]

2 Implementační požadavky

2.1 Implementace síťových switchů

V oblasti implementace síťových switchů jsou definovány následující činnosti, resp. požadavky:

Činnost	Služba bude poskytnuta (doplňte ANO/NE, případně uveďte detailní popis služby)
Dodávka zařízení: Zadavatel požaduje dodávku a montáž zařízení do obou lokalit organizace SŽ v Praze a Plzni, v souladu s navrženým plánem rozmístění prvků.	[DOPLNÍ DODAVATEL]
Základní konfigurace: • Ověření zařízení na absenci HW vad. • Registrace zařízení. • Instalace výrobcem doporučené verze operačního systému. • Konfigurace základních parametrů (management rozhraní, hostname, DNS, NTP, STP, administrátorské přístupy, napojení na centrální uživatelský systém (LDAP/RADIUS), odesílání událostí do externího zařízení).	[DOPLNÍ DODAVATEL]
Síťová konfigurace: • Linková agregace. • IP adresace a VLAN tagy • Nasazení v režimu Stack (dle modelu switche, pokud je vyžadováno) • Nasazení v režimu peer-link (VXLAN) s rychlostí propoje alespoň 2x100Gb (dle modelu switche)	[DOPLNÍ DODAVATEL]

2.2 Implementace Next Generation Firewall

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

Činnost	Služba bude poskytnuta (doplňte ANO/NE, případně uveďte detailní popis služby)
Dodávka zařízení: Zadavatel požaduje dodávku a montáž zařízení do obou lokalit organizace SŽ v Praze a Plzni, v souladu s navrženým plánem rozmístění prvků.	[DOPLNÍ DODAVATEL]
Základní konfigurace: • Ověření zařízení na absenci HW vad. • Registrace zařízení. • Instalace výrobcem doporučené verze operačního systému. • Konfigurace základních parametrů (management rozhraní, hostname, DNS, NTP, administrátorské přístupy, napojení na centrální uživatelský systém (LDAP/RADIUS), odesílání událostí do externího zařízení).	[DOPLNÍ DODAVATEL]
Konfigurace vysoké dostupnosti (HA) Nasazení v režimu Active – Passive.	[DOPLNÍ DODAVATEL]
Síťová konfigurace • Linková agregace. • IP adresace a VLAN tagy. • Směrování. • DHCP relay (pokud bude potřeba).	[DOPLNÍ DODAVATEL]
Vytvoření objektů a bezpečnostní politiky: • Specifikace nových pravidel pro nové NGFW. • Návrh jmenné konvence pravidel a objektů dle akceptované metodiky.	[DOPLNÍ DODAVATEL]
Dodavatel definuje vzorové bezpečnostní politiky dle vzoru Zadavatele: • IPS a/nebo IDS. • Application Control.	[DOPLNÍ DODAVATEL]
SSO Autentizace: Napojení na Active Directory řízení přístupů na základě identit.	[DOPLNÍ DODAVATEL]

~~2.2.1 Nástroj centrální správy NGFW – Položka I~~

1.3.6 Technická specifikace Položky I

Zadavatel požaduje plnou kompatibilitu dodávaných firewallů s jedním z nástrojů centrální správy a managementu, které již Zadavatel ve svém prostředí provozuje. Zadavatel ve svém prostředí provozuje centrální správu firewallových technologií pomocí nástrojů **FortiManager** a **Firewall Management Center**.

Pokud nebude možné zajistit plnou kompatibilitu dodávaných NGFW Dodavatelem se současným centrálním managementem, je Dodavatel povinen v rámci své dodávky dodat a naimplementovat v prostředí Zadavatele **nový nástroj centrální správy NGFW** včetně příslušných licencí s dobou platnosti a veškerými systémovými update po dobu minimálně 60 měsíců od zprovoznění nástroje centrální správy, který bude splňovat následující požadavky.

Požadavky na nástroj centrální správy NGFW

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

[IDENTIFIKACE NABÍZENÉHO NÁSTROJE - DOPLNÍ DODAVATEL]

~~Požadavek~~Požadavek (požadováno pouze v případě, že nabízení řešení NGFW není kompatibilní se stávajícími systémy Zadavatele pro centrální správu firewallů)	**Nabízené řešení** ~~(~~doplňte **ANO**~~/~~ **- splňuje** nebo **NE – není součástí nabídky**, případně uveďte **technické** parametry, pokud lze ~~)~~
Typ nástroje: Nástroj může být realizován jako fyzický, nebo virtualizovaný, s podporou virtualizační platformy VMware, která je hlavní a jedinou virtualizační platformou provozovanou Zadavatelem.	[DOPLNÍ DODAVATEL]
Nástroj centrální správy musí umožnit správu minimálně 20 fyzických zařízení.	[DOPLNÍ DODAVATEL]
Nástroj centrální správy umožňuje příjem a uložení událostí v minimálním množství 10 GB událostí za den s možností licenčního rozšíření minimálně na 50 GB událostí za den.	[DOPLNÍ DODAVATEL]
Nástroj centrální správy umožňuje základní analýzu událostí za účelem včasné identifikace reálné či potenciální hrozby. Primárně bude pro vyhodnocování incidentů používán nástroj aktuálně využívaný v prostředí SŽ, log management a SIEM.	[DOPLNÍ DODAVATEL]

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

Činnost	~~**Služba bude poskytnuta**~~ ~~**(doplňte ANO/NE, případně uveďte detailní popis služby)**~~
Dodávka zařízení: Dodávka nástroje do lokality Praha. V případě virtualizovaného ~~zař~~řešení poskytnutí instalačních dat skrze internetovou konektivitu.	~~[DOPLNÍ DODAVATEL]~~
Základní konfigurace • Ověření zařízení na absenci HW vad (pouze u fyzického zařízení). • Registrace zařízení~~.~~ v systému podpory výrobce (pokud je vyžadováno). • Instalace výrobcem doporučené verze operačního systému. • Konfigurace základních parametrů (management rozhraní, hostname, DNS, NTP, administrátorské přístupy, napojení na centrální uživatelský systém (LDAP/RADIUS), odesílání událostí do externího zařízení).	~~[DOPLNÍ DODAVATEL]~~
Integrace dodaných NGFW do centrální správy.	~~[DOPLNÍ DODAVATEL]~~
Poskytnutí plné podpory Dodavatele při konfiguraci dodaného nástroje až po úplné spuštění nástroje pro centrální správu NGFW.	~~[DOPLNÍ DODAVATEL]~~

Odstraněné buňky

2 Implementační činnosti

V oblasti implementace technologií Zadavatel předpokládá od Dodavatele provedení následujících činností (bude-li potřeba tyto činnosti provést za účelem plného zprovoznění dodávaného řešení):

Činnost
Dodávka a instalace zařízení: Dodavatel zajistí: • dodávku veškerého HW, SW a licencí potřebných pro provoz řešení, • fyzickou instalaci zařízení do racků v obou lokalitách organizace SŽ v Praze a Plzni, v souladu s navrženým plánem rozmístění prvků, • zapojení napájecích a datových kabelů, • označení zařízení dle standardů Zadavatele, • kontrolu kompatibility všech komponent řešení, • ekologickou likvidaci obalového materiálu.
Základní konfigurace: Dodavatel zajistí: • ověření bezvadnosti dodaného HW, • aktualizaci firmware a operačních systémů na výrobcem doporučené verze, • registraci zařízení u výrobce, • konfiguraci management rozhraní, • konfiguraci IP adresace, • konfiguraci DNS, NTP, • vytvoření administrátorských účtů, • konfiguraci RBAC/role-based access control, • napojení na centrální autentizační infrastrukturu zadavatele (LDAP, Active Directory, RADIUS, TACACS+), • konfiguraci logování a auditu do nástroje SIEM, • konfiguraci SNMP, Syslog, SMTP notifikací, • vytvoření záloh konfigurace zařízení, • jiné konfigurace, dle doporučení dodavatele/výrobce.
Konfigurace diskového pole Dodavatel zajistí: • napojení na HSM, • vytvoření storage poolů, • vytvoření diskových skupin dle návrhu, • konfiguraci RAID nebo ekvivalentní ochrany dat, • vytvoření LUN/Volume, • konfiguraci snapshotů, • konfiguraci replikace mezi lokalitami (je-li požadována), • konfiguraci tieringu, deduplikace a komprese (pokud je podporováno), • konfiguraci monitoringu kapacity a výkonu, • konfiguraci multipath přístupu ze serverů, • konfiguraci prostředků kybernetické ochrany, • jiné konfigurace, dle doporučení dodavatele/výrobce.

Konfigurace serverů

Dodavatel zajistí:

- instalace aktuálních (nebo doporučených) firmware,
- konfigurace BIOS/UEFI,
- konfigurace RAID řadičů,
- konfigurace síťových adaptérů (LAN,SAN),
- instalace hypervizoru nebo operačního systému,
- vytvoření připojení k diskovému poli,
- ověření vysoké dostupnosti,
- jiné konfigurace, dle doporučení dodavatele/výrobce.

Konfigurace aktivních síťových prvků

Dodavatel zajistí konfiguraci síťové infrastruktury nezbytnou pro provoz řešení, zejména:

- VLAN,
- MTU/Jumbo Frames,
- Linková agregace (LACP), je-li využíváno,
- konfiguraci SAN provozu,
- implementaci redundance síťových cest,
- konfiguraci VXLAN/EVPN (pokud je součástí architektury),
- bezpečnostní konfiguraci management rozhraní,
- redundantní propojení síťových prvků v rámci lokality s minimální agregovanou kapacitou 100 Gb/s,
- jiné konfigurace, dle doporučení dodavatele/výrobce.

Konfigurace NGFW

Dodavatel zajistí:

- připojení firewallů do navržené síťové architektury,
- konfiguraci fyzických a logických rozhraní,
- konfiguraci VLAN,
- konfiguraci linkové agregace (LACP), je-li navržena,
- konfiguraci směrování,
- integraci s LAN a serverovou infrastrukturou,
- nasazení firewallů v HA clusteru dle návrhu řešení,
- konfiguraci monitoringu stavu clusteru,
- ověření funkčnosti přepnutí při výpadku jednoho zařízení.
- specifikaci nových pravidel pro nové NGFW,
- návrh jmenné konvence pravidel a objektů dle akceptované metodiky,
- vytvoření bezpečnostních zón,
- implementaci bezpečnostní politiky,
- konfiguraci IPS funkcionalit, pokud jsou součástí dodávky,
- konfiguraci aplikační kontroly, pokud je součástí dodávky,
- jiné konfigurace, dle doporučení dodavatele/výrobce.

3 Obecná ustanovení

Dodavatel je povinen dodat Hardware v takovém rozsahu, včetně jeho příslušenství, v jakém bude tento Hardware schopen řádně sloužit účelu vymezenému ve Smlouvě a jejích přílohách. Skutečnost, že takové příslušenství není výslovně uvedeno v této příloze Smlouvy, neznamená, že jej Dodavatel není povinen dodat. Cena za takové příslušenství musí být součástí nabídkové ceny Dodavatele.

Dodavatel se zavazuje dodat Hardware nový, nepoužitý, nerepasovaný a určený pro EU trh. V opačném případě se jedná o podstatné porušení Smlouvy.

Klasifikace: Veřejný dokument

SPRÁVA ŽELEZNIC

Příloha č. 1 smlouvy

Bližší specifikace předmětu plnění

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

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

Obsah

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	*(Active Directory)* 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	*(Domain Name System)* je distribuovaný hierarchický jmenný systém používaný v síti Internet. Překládá názvy domén na číselné IP adresy a zpět, obsahuje informace o tom, které stroje poskytují příslušnou službu.
DR	*(Disaster Recovery)* 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	*(End of Sale)* Datum ukončení prodeje.
EOL	*(End of Life)* Datum konce životnosti produktu.
Failover	Failover představuje proces, kdy v případě výpadku primárního prvku dochází k přesměrování provozu na záložní prvek.
GDPR	*(General Data Protection Regulation)* 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	*(High Availability)* je vysoká dostupnost služeb. Předpokladem řešení je použití dvou a více nezávislých zařízení s cílem zajistit funkčnost v případě výpadku.

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

SW	*Software* – 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	*(Transport Layer Security)* 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	*(Virtual Private Network)* 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	*(Zvláštní obchodní podmínky pro Zakázky v oblasti ICT)* - 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 regulatorní 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 regulatorních požadavků ZoKB (dle relevance). • Návrh automatizace práce s daty, automatizace obnovy.

Výstupem výše uvedených požadavků bude samostatný dokument s názvem „Koncepce 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 ~~– Hybrid Storage s NVMe/SSD a SAS/NL-SAS disky~~ 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.

- ~~Požadovaný poměr mezi NVMe/SSD a SAS/NL-SAS disky je procentuálně 10:90~~
  - ~~SSD minimálně 100 TB~~
  - ~~SAS minimálně 900 TB~~
- 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.
- ~~Zadavatel rovněž připouští variantu použití výhradně NVMe/SSD disků.~~

- 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 přistupovaná 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 neznamenala 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 detekcí neobvyklého chování, musí být tato funkcionalita 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. ~~Na vstupu do úložiště (při zápisu dat ze systémů) budou nasazeny bezpečnostní nástroje zadavatele na detekci známého malware (antivirové skeny záloh atd.), pokud to bude technicky možné.~~ ~~Cílem je, aby uložené zálohy již neobsahovaly například „spící ransomware".~~ 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 umožnovat, 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 granulární 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 prostupů • 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 připraveno pro ukládání, obnovu a kontrolu dat v souladu s definovanými technickými a bezpečnostními pravidly.

Toto navazuje na dokumenty „Koncepce 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-implementačních 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 • nákres 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 uživatelům, pokud systémy nedisponují 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 do 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-implementační podpora Dodavatele	Dodavatel zajistí Post-implementační 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-implementační 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 zapracování 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 fáze, 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 – Koncepce 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

Platební milník	Fáze	Popis	Způsob akceptace fáze	Kapitola obsahující požadavky
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: • Dokument – Závěrečná zpráva z testování funkčních a bezpečnostních parametrů Bezpečného úložiště	5.4.3
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	F6.1A	Technická podpora – primární lokalita	Fáze F6.1A bude vykazována na základě pravidelných měsíčních výkazů	7

Platební milník	Fáze	Popis	Způsob akceptace fáze	Kapitola obsahující požadavky
měsíčních výkazů.				
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 skutečného čerpání ze strany Zadavatele.	F7	Konzultační služby na vyžádání	Akceptační protokol s ohledem na obsah požadovaných Konzultačních služeb	8

Naše zn. 90890/2026-SŽ-GŘ-O25

ZADÁVACÍ DOKUMENTACE

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

„Realizace systému Zabezpečeného úložiště v prostředí Správy železnic"

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

Identifikační údaje Zadavatele a osoby zastupující Zadavatele:

Název:	Správa železnic, státní organizace
Sídlo:	Dlážděná 1003/7, Praha 1 – Nové Město, PSČ 110 00
IČO:	709 94 234
DIČ:	CZ 70994234

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

Zastoupen:	Ing. Tomášem Tóthem, generálním ředitelem
Profil Zadavatele:	https://zakazky.spravazeleznic.cz/

1. Informace o osobě, která zpracovala část Zadávací dokumentace

Zadavatel označuje následující části Zadávací dokumentace, na jejichž zpracování se podílela osoba odlišná od Zadavatele:

Část Zadávací dokumentace	Identifikace osoby
Přílohy č. 1, 2, 3, 9 a 10 Přílohy č. 5 Zadávací dokumentace - *Závazný vzor smlouvy*	s-boost s.r.o., IČO: 23037539, se sídlem Senovážné náměstí 978/23, Nové Město, 110 00 Praha 1
Příloha č. 1, 2, 3, 4, 5, 6, 7 a 8 Zadávací dokumentace Přílohy č. 5 a 8 Přílohy č. 5 Zadávací dokumentace – *Závazný vzor smlouvy*	PORTOS s.r.o., advokátní kancelář, IČO: 481 18 753, se sídlem Hvězdova 1716/2b, 140 00 Praha 4

2. Informace o předběžné tržní konzultaci:

2.1. Zadavatel v souladu s § 33 ZZVZ realizoval před zahájením zadávacího řízení předběžnou tržní konzultaci (dále jen „**PTK**") s dodavateli, a to písemnou formou (informace o konání PTK byla uveřejněna na profilu zadavatele – viz Přehled - E-ZAK Správa železnic, https://zakazky.spravazeleznic.cz/contract_display_17444.html). Zadavatel v této souvislosti obeznámil neomezený okruh potenciálních dodavatelů se svým záměrem a potřebami prostřednictvím dokumentu Pozvánka k předběžné tržní konzultaci ve věci přípravy zadávacích podmínek pro veřejné zakázky s názvy „Mobilní kontejnerové datové centrum" a "Realizace systému zabezpečeného úložiště v prostředí Správy železnic", případně pro jinou veřejnou zakázku shodnou s předmětem těchto dvou zakázek (dále jen „**Pozvánka**") a zároveň zaslal Pozvánku 11 vybraným dodavatelům přímo prostřednictvím e-mailu. Dodavatelé, kteří projevili zájem účastnit se PTK, měli Zadavateli v rámci dotazovacího kola PTK zaslat odpovědi na otázky uvedené v Příloze č. 4 Pozvánky – *Otázky k zodpovězení PTK*, a to na e-mailovou adresu: cnitptk@spravazeleznic.cz.

2.2. Předběžné tržní konzultace se účastnili následující dodavatelé:

- ALTRON, a.s., se sídlem Novodvorská 994/138, Braník, 142 00 Praha 4, IČO: 64948251,
- GAPP System, spol. s r.o., se sídlem Petržílkova 2565/23, Stodůlky, 158 00 Praha 5, IČO: 60487291,
- Conteg, spol. s r.o., se sídlem Štětkova 1638/18, Nusle, 140 00 Praha 4, IČO: 25701843,
- ALTEPRO solutions a.s., se sídlem Na Maninách 1092/20, Holešovice, 170 00 Praha 7, IČO: 03665496,
- Aricoma Systems a.s., se sídlem Hornopolní 3322/34, Moravská Ostrava, 702 00 Ostrava, IČO: 04308697,
- HEWLETT-PACKARD s.r.o., se sídlem Za Brumlovkou 1559/5, Michle, 140 00 Praha 4, IČO: 17048851,
- AŽD Praha s.r.o., se sídlem Žirovnická 3146/2, Záběhlice, 106 00 Praha 10, IČO: 48029483,
- O2 IT Services s.r.o., se sídlem Za Brumlovkou 266/2, Michle, 140 00 Praha 4, IČO: 02819678,
- KABEL TRADE PRAHA s.r.o., se sídlem Praha 4 - Kunratice, Dobronická 1257, PSČ 14800, IČO: 256 13 383,
- Power Tech spol. s r.o., se sídlem Na Šutce 391/32, Troja, 182 00 Praha 8, IČO: 26196930.

2.3. Informace o předmětu a výsledku předběžné tržní konzultace:

Zadavatel seznámil dodavatele se svým záměrem realizovat veřejnou zakázku a s cílem, jehož má být prostřednictvím plnění veřejné zakázky dosaženo.

V rámci předběžné tržní konzultace Zadavatel ověřil:

a) formu dodávky, spolupráci na dokumentaci a testování řešení,

b) soulad s právními předpisy a zkušenosti dodavatelů s veřejnými zakázkami,

c) možnosti financování, rámcové ceny a výpočet celkových nákladů vlastnictví,

d) předchozí realizace, technické kompetence a schopnost provozní podpory.

Na základě informací sdělených v rámci předběžné tržní konzultace Zadavatel:

a) ověřil, že trh je připraven dodat požadované řešení v plném rozsahu a většina

dodavatelů má relevantní zkušenosti, avšak že pro přesné návrhy, ceny a srovnatelnost nabídek je nezbytné upřesnit technickou specifikaci. Zadavatel proto rozpracoval dokumenty Bližší specifikace předmětu plnění a Technická specifikace, které tvoří přílohu Závazného vzoru smlouvy. Konkrétně Zadavatel na základě PTK definoval požadavky na vhodnou technologii pro Bezpečné úložiště, stanovil nižší velikost úložiště a změnil poměr rychlých a pomalých disků oproti původnímu předpokladu,

b) stanovil požadavky na významné zakázky v rámci technické kvalifikace dle čl. 12.1 této Zadávací dokumentace,

c) stanovil časový Harmonogram plnění, který tvoří Přílohu č. 9 Přílohy č. 5 této zadávací dokumentace – Závazný vzor smlouvy,

d) upravil údaj o předpokládané hodnotě veřejné zakázky,

e) rozhodl nezahrnout do této Veřejné zakázky dodávku Mobilního kontejnerového datového centra a tuto realizovat jako samostatnou veřejnou zakázku.

2.4. Shrnutí výsledku předběžné tržní konzultace tvoří Přílohu č. 9 této Zadávací dokumentace.

3. Druh veřejné zakázky a zadávacího řízení:

3.1. Hlavní předmět veřejné zakázky ve smyslu § 15 ZZVZ odpovídá veřejné zakázce na dodávky.

3.2. Zadavatel zadává veřejnou zakázku v souvislosti s výkonem své relevantní činnosti ve smyslu § 153 odst. 1. písm. f) ZZVZ. Jedná se proto o sektorovou veřejnou zakázku.

3.3. Veřejná zakázka je v souladu s § 56 a násl. ZZVZ zadávána v **otevřeném řízení** ve smyslu § 3 písm. b) ZZVZ.

4. Účel a předmět veřejné zakázky:

4.1. Předmětem veřejné zakázky je dodání, implementace a konfigurace technologie centralizovaného bezpečného datového úložiště za účelem splnění zákonných povinností Zadavatele v oblasti kybernetické a fyzické bezpečnosti. Součástí plnění je zpracování analytické části, vytvoření koncepce Bezpečného úložiště, návrh detailního implementačního postupu pro vybrané systémy, dodání HW, implementace a konfigurace technologie a napojení na vybrané systémy Zadavatele.

4.2. Podrobné vymezení předmětu veřejné zakázky je uvedeno v Příloze č. 5 Zadávací dokumentace – Závazný vzor smlouvy (dále tak jen „**smlouva**").

4.3. Klasifikace předmětu veřejné zakázky (CPV) :

Hlavní kód CPV: 30210000-4 | Stroje na zpracování dat (technické vybavení)

Doplňkové kódy CPV:

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

Kód CPV: 72224000-1 | Poradenské služby v oblasti řízení projektů

Kód CPV: 72263000-6 | Implementace programového vybavení

Kód CPV: 72253200-5 | Systémová podpora

Kód CPV: 72245000-4 | Smluvní analýza systémů a programování

Kód CPV: 80533000-9 | Seznamovací počítačové kurzy pro uživatele

Kód CPV: 32415000-5 | Ethernetové sítě

Kód CPV: 72511000-0 | Programové vybavení pro správu sítě

Kód CPV: 50312310-1 | Údržba zařízení datové sítě

Kód CPV: 50324100-3 | Údržba systémů

Kód CPV: 72000000-5 | Informační technologie: poradenství, vývoj programového vybavení, internet a podpora

Kód CPV: 72263000-6 | Implementace programového vybavení

Kód CPV: 72261000-2 | Podpora programového vybavení.

4.4. Předmět plnění veřejné zakázky bude spolufinancován z Evropských strukturálních a investičních fondů prostřednictvím Integrovaného regionálního operačního programu (IROP) v rámci projektu „Dohled a řízení bezpečnosti", reg. č. "CZ.06.01.01/00/22_005/0000104".

4.5. 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 k varování ze dne 17. prosince 2018 (dále jen „**metodika**"), která stanoví mimo jiné postupy pro provádění a aktualizaci analýzy rizik v oblasti kybernetické bezpečnosti.

V souladu s touto metodikou a v návaznosti na povinnosti vyplývající ze zákona č. 264/2025 Sb., o kybernetické bezpečnosti, a z vyhlášky č. 409/2025 Sb., *o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností*, provedl Zadavatel analýzu rizik související s předmětnou veřejnou zakázkou. Na základě provedené analýzy rizik Zadavatel identifikoval rizika spojená s výše uvedenými technickými a programovými prostředky jako neakceptovatelná a současně stanovil opatření k jejich zvládání, spočívající v nepřipuštění použití těchto prostředků v rámci plnění veřejné zakázky, za účelem zajištění odpovídající úrovně kybernetické bezpečnosti.

Zadavatel tak na základě vydaného varování NÚKIB, navazující metodiky a provedené analýzy rizik, v souladu s povinnostmi vyplývajícími ze zákona č. 264/2025 Sb., o kybernetické bezpečnosti, nepřipouští v rámci plnění veřejné zakázky použití technických nebo programových prostředků společností (výrobců), které jsou uvedeny v aktuálně platném varování NÚKIB jako hrozba v oblasti kybernetické bezpečnosti.

Pokud by některý z dodavatelů ve své nabídce nerespektoval zákaz, resp. zadávací podmínku uvedenou v tomto čl. 4.5 Zadávací dokumentace, tzn. že by pro plnění veřejné zakázky navrhl použití technických nebo programových prostředků výše uvedených společností (výrobců), Zadavatel bude postupovat podle § 48 odst. 2 písm. a) ZZVZ ve spojení s § 48 odst. 8 ZZVZ a přistoupí k vyloučení takového dodavatele ze zadávacího řízení.

5. Předpokládaná hodnota

5.1. Předpokládaná hodnota veřejné zakázky se nezveřejňuje.

6. Doba plnění a místo plnění veřejné zakázky, prohlídka místa plnění:

6.1. Doba plnění veřejné zakázky

Termín zahájení plnění: Od okamžiku účinnosti smlouvy.

Termín ukončení plnění: do skončení Fáze F6.2 (Post-implementační podpora), přičemž

Fáze F6.2 nebude ukončena dříve než za 60 měsíců od skončení fáze F3.3.

Podrobnosti ohledně doby plnění veřejné zakázky stanoví Harmonogram plnění, který tvoří Přílohu č. 9 smlouvy.

6.2. Místo plnění veřejné zakázky

Plnění veřejné zakázky bude probíhat na dvou místech:

- V Trianglu 2474, 190 00 Praha 9 – Libeň, a
- Cvokařská 2834/2, 301 00 Plzeň – Slovany.

6.3. Prohlídka místa plnění

Zadavatel neprovádí prohlídku místa plnění ve smyslu ustanovení § 97 ZZVZ, neboť její uskutečnění není pro účely průběhu zadávacího řízení či plnění veřejné zakázky nezbytné.

7. Sociálně a environmentálně odpovědné zadávání, inovace

7.1. Zadavatel při vytváření zadávacích podmínek, včetně pravidel pro hodnocení nabídek, a výběru dodavatele, postupoval tak, aby v co nejvyšší možné míře naplnil zásady sociálně odpovědného zadávání, environmentálně odpovědného zadávání a inovací tak jak jsou definovány v § 28 odst. 1 písm. p) až r) ZZVZ (dále jen „***odpovědné zadávání***"). Vzhledem k tomu, že jednotlivé postupy odpovědného zadávání nebyly v ZZVZ ani v jiném zákoně taxativně vymezeny a současně je odpovědné zadávání stále se velmi dynamicky vyvíjejícím institutem veřejného zadávání, Zadavatel při vytváření podmínek zvažoval použití zejména těch prvků odpovědného zadávání, které byly v době vytváření zadávacích podmínek jednoznačně vymezitelné a vymahatelné, a současně byla u nich vysoká míra jistoty, že Zadavatel jejich aplikací neporuší ostatní zásady uvedené v § 6 ZZVZ a také principy 3E vyplývající ze zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole).

7.2. Zadavatel aplikuje v zadávacím řízení prvky odpovědného zadávání podle čl. 7.3 a 7.4 této Zadávací dokumentace. Použití jiných prvků odpovědného zadávání, které byly Zadavateli známy při vytváření této Zadávací dokumentace, není vzhledem k povaze a smyslu zakázky možné z těchto důvodů:

7.2.1. V oblasti environmentálního odpovědného zadávání Zadavatel neshledal potřebu použití dílčích aspektů odpovědného zadávání, neboť činnosti, které jsou předmětem této veřejné zakázky, nezatěžují životní prostředí nad rámec běžného života a spotřeba energií, vody, surovin a produkce znečišťujících látek je minimální či žádná.

7.2.2. V oblasti inovací Zadavatel nestanovil dílčí kritéria odpovědného zadávání s ohledem na skutečnost, že v rámci předmětu plnění veřejné zakázky neidentifikoval žádná možná inovativní řešení. Z těchto důvodů jsou inovace u daného předmětu plnění fakticky vyloučeny.

7.2.3. V oblasti sociálně odpovědného zadávání Zadavatel neshledal potřebu použití dalších dílčích aspektů odpovědného zadávání, kromě těch, které jsou uvedeny v čl. 7.3 a 7.4 této Zadávací dokumentace, s ohledem na specifičnost těchto služeb, kdy předmětem služeb je specializované plnění. Vzhledem k těmto důvodům je nutné, aby se na plnění veřejné zakázky podílely osoby s vysokou kvalifikací. Nejedná se tedy o vhodnou příležitost k zaměstnání osob znevýhodněných na trhu práce.

7.3. Rovnocenné platební podmínky v rámci dodavatelského řetězce:

7.3.1. Zadavatel realizuje zakázku s ohledem na ochranu malých a středních podniků v případném postavení poddodavatelů, a to formou:

a. umožnění přímých plateb případným poddodavatelům a

b. zajištění stejné doby splatnosti faktur pro poddodavatele jako pro vybraného dodavatele.

7.4. Dodržování pracovněprávních předpisů:

7.4.1. Zadavatel stanovuje, že vybraný dodavatel je při plnění veřejné zakázky povinen dodržovat pracovněprávní předpisy, a to zejména, nikoliv však výlučně, předpisy upravující mzdy zaměstnanců, pracovní dobu, dobu odpočinku mezi směnami, placené přesčasy, bezpečnost práce apod. Zadavatel dále vyžaduje zajistit férové pracovní podmínky a odpovídající úroveň bezpečnosti práce pro všechny osoby podílející se na plnění veřejné zakázky. Vybraný dodavatel je povinen zajistit splnění tohoto požadavku Zadavatele i u svých poddodavatelů.

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

8. Požadavky Zadavatele na kvalifikaci dodavatelů

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

8.2. Kritéria kvalifikace

Zadavatel požaduje, aby dodavatelé prokázali následující:

a) svou základní způsobilost dle § 74 a § 75 ZZVZ;

b) svou profesní způsobilost dle § 77 ZZVZ;

c) svou ekonomickou kvalifikaci dle § 78 ZZVZ;

d) svou technickou kvalifikaci dle § 79 ZZVZ.

8.3. Forma prokazování splnění kvalifikace

8.3.1. Dodavatel prokáže splnění kvalifikace ve všech případech příslušnými doklady.

8.3.2. Za účelem prokázání kvalifikace Zadavatel přednostně vyžaduje doklady evidované v systému, který identifikuje doklady k prokázání splnění kvalifikace (systém e-Certis).

8.3.3. Zadavatel vylučuje možnost, aby dodavatelé pro účely podání nabídky požadované doklady o kvalifikaci dle čl. 8 této ZD nahradili písemným čestným prohlášením dle § 86 ZZVZ. Tím není dotčen bod 8.3.10 ZD.

8.3.4. Dodavatel může nahradit požadované doklady jednotným evropským osvědčením pro veřejné zakázky ve smyslu § 87 ZZVZ. Vzor jednotného evropského osvědčení je stanoven prováděcím nařízením Komise (EU) 2016/7 ze dne 5. ledna 2016, kterým se zavádí standardní formulář jednotného evropského osvědčení pro veřejné zakázky (dostupný např. na internetové adrese: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0007&from=cs).

8.3.5. Dodavatel není povinen předložit Zadavateli doklady osvědčující skutečnosti obsažené v jednotném evropském osvědčení pro veřejné zakázky, pokud Zadavateli sdělí, ve kterém jiném zadávacím řízení mu je již předložil.

8.3.6. Povinnost předložit doklad může dodavatel splnit odkazem na odpovídající informace vedené v informačním systému veřejné správy ve smyslu *zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů,* nebo v obdobném systému vedeném v jiném členském státu, který umožňuje neomezený dálkový přístup. Takový odkaz musí obsahovat internetovou adresu a údaje pro přihlášení a vyhledání požadované informace, jsou-li takové údaje nezbytné. V ČR jde zejména o výpis z obchodního rejstříku, výpis z veřejné části živnostenského rejstříku nebo výpis ze seznamu kvalifikovaných dodavatelů.

8.3.7. Dodavatel předkládá doklady prokazující splnění kvalifikace ve formě prosté kopie. Tímto není dotčeno oprávnění Zadavatele dle bodu 22.2.2 ZD a právo požadovat předložení

originálu nebo úředně ověřené kopie dokladu postupem dle § 46 odst. 1 ZZVZ.

8.3.8. Doklady prokazující základní způsobilost podle § 74 ZZVZ musí prokazovat splnění požadovaného kritéria způsobilosti nejpozději v době 3 měsíců přede dnem zahájení zadávacího řízení.

8.3.9. V případech, kdy Zadavatel v rámci prokázání splnění kvalifikace požaduje předložení čestného prohlášení dodavatele, musí takové čestné prohlášení obsahovat Zadavatelem požadované údaje.

8.3.10. Pokud ZZVZ nebo Zadavatel požaduje předložení dokladu podle právního řádu České republiky, může dodavatel předložit obdobný doklad podle právního řádu státu, ve kterém se tento doklad vydává. Doklad, který je vyhotoven v jiném jazyce, než který Zadavatel určil pro podání nabídky, se předkládá s překladem do jazyka určeného Zadavatelem pro podání nabídky. Není-li v zadávacích podmínkách výslovně stanoveno jinak, platí, že Zadavatel určil pro podání nabídky český jazyk. Bude-li mít Zadavatel pochybnosti o správnosti překladu, je oprávněn si vyžádat předložení úředně ověřeného překladu dokladu tlumočníkem zapsaným do seznamu soudních tlumočníků a soudních překladatelů podle zákona č. 354/2019 Sb., o soudních tlumočnících a soudních překladatelích, ve znění pozdějších předpisů. Doklad v českém nebo slovenském jazyce a doklad o vzdělání v latinském jazyce se předkládají bez překladu; Zadavatel může povinnost předložit překlad prominout i u jiných dokladů. Pokud se podle příslušného právního řádu požadovaný doklad nevydává, může být nahrazen písemným čestným prohlášením.

8.4. **Prokázání kvalifikace prostřednictvím jiných osob dle § 83 ZZVZ**

8.4.1. Dodavatel může ekonomickou kvalifikaci, technickou kvalifikaci nebo profesní způsobilost s výjimkou kritéria podle § 77 odst. 1 ZZVZ prokázat prostřednictvím jiných osob. Dodavatel je v takovém případě povinen Zadavateli předložit:

a) doklady prokazující splnění profesní způsobilosti podle § 77 odst. 1 ZZVZ jinou osobou,

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

c) doklady o splnění základní způsobilosti podle § 74 ZZVZ jinou osobou a

d) smlouvu nebo jinou osobou podepsané potvrzení o její existenci, jejímž obsahem je závazek jiné osoby k poskytnutí plnění určeného k plnění veřejné zakázky nebo k poskytnutí věcí nebo práv, s nimiž bude dodavatel oprávněn disponovat při plnění veřejné zakázky, a to alespoň v rozsahu, v jakém jiná osoba prokázala kvalifikaci za dodavatele.

8.4.2. Nejedná-li se o situaci dle bodu 8.4.3 ZD, má se za to, že požadavek podle písm. d) je splněn, pokud z obsahu smlouvy nebo potvrzení o její existenci podle písm. d) vyplývá závazek jiné osoby plnit veřejnou zakázku společně a nerozdílně s dodavatelem.

8.4.3. Prokazuje-li dodavatel prostřednictvím jiné osoby kvalifikaci a předkládá doklady podle § 79 odst. 2 písm. a), b) nebo d) ZZVZ vztahující se k takové osobě, musí ze smlouvy nebo potvrzení o její existenci podle písm. d) vyplývat závazek, že jiná osoba bude vykonávat služby, ke kterým se prokazované kritérium kvalifikace vztahuje.

8.4.4. Dodavatelé a jiné osoby prokazují (mohou prokázat) kvalifikaci společně.

8.4.5. Dodavatel a jiná osoba, jejímž prostřednictvím dodavatel prokazuje ekonomickou kvalifikaci podle § 78 ZZVZ, nesou společnou a nerozdílnou odpovědnost za plnění veřejné zakázky.

8.4.6. Zadavatel upozorňuje, že povinnost doložit veškeré doklady uvedené výše v tomto článku platí i v případě, kdy je část kvalifikace prokazována poddodavatelem poddodavatele (pod-poddodavatelem).

8.5. **Prokazování kvalifikace v případě společné účasti dodavatelů dle § 82 ZZVZ**

8.5.1. V případě společné účasti dodavatelů prokazuje základní způsobilost dle § 74 a § 75 ZZVZ a profesní způsobilost podle § 77 odst. 1 ZZVZ každý dodavatel samostatně.

8.6. **Prokazování kvalifikace získané v zahraničí dle § 81 ZZVZ**

8.6.1. V případě, že byla kvalifikace získána v zahraničí, prokazuje se doklady vydanými podle právního řádu země, ve které byla získána, a to v rozsahu požadovaném Zadavatelem.

8.6.2. Potvrzení pro daňové nedoplatky zahraničních dodavatelů v ČR vydává Finanční úřad pro Prahu 1 a potvrzení pro nedoplatky zahraničních dodavatelů v ČR na pojistném a na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti vydává Pražská správa sociálního zabezpečení.

8.7. **Změny kvalifikace účastníka zadávacího řízení dle § 88 ZZVZ**

8.7.1. Pokud po předložení dokladů nebo prohlášení o kvalifikaci dojde v průběhu zadávacího řízení ke změně kvalifikace účastníka zadávacího řízení, je účastník zadávacího řízení povinen tuto změnu Zadavateli do 5 pracovních dnů oznámit a do 10 pracovních dnů od oznámení této změny předložit nové doklady nebo prohlášení ke kvalifikaci. Zadavatel může tyto lhůty prodloužit nebo prominout jejich zmeškání. Povinnost podle věty první účastníku zadávacího řízení nevzniká, pokud je kvalifikace změněna takovým způsobem, že:

a) podmínky kvalifikace jsou nadále splněny,

b) nedošlo k ovlivnění kritérií hodnocení nabídek.

8.7.2. Zadavatel může vyloučit účastníka zadávacího řízení, pokud prokáže, že účastník nesplnil shora uvedenou povinnost.

8.8. **Výpis ze seznamu kvalifikovaných dodavatelů dle § 228 ZZVZ**

8.8.1. Předložení dokladu o zapsání dodavatele do seznamu kvalifikovaných dodavatelů vedeného Ministerstvem pro místní rozvoj dle § 226 až § 232 ZZVZ nahrazuje v souladu s § 228 ZZVZ doklad prokazující profesní způsobilost podle § 77 ZZVZ v tom rozsahu, v jakém údaje ve výpisu ze seznamu kvalifikovaných dodavatelů prokazují splnění kritérií profesní způsobilosti, a základní způsobilost podle § 74 ZZVZ v plném rozsahu. Výpis ze seznamu kvalifikovaných dodavatelů nesmí být k poslednímu dni, ke kterému má být prokázána základní způsobilost nebo profesní způsobilost, starší než tři měsíce.

8.9. **Předložení certifikátu dle § 234 ZZVZ**

8.9.1. Platným certifikátem vydaným v rámci schváleného systému certifikovaných dodavatelů lze podle § 234 ZZVZ prokázat kvalifikaci v zadávacím řízení. Má se za to, že dodavatel je kvalifikovaný v rozsahu uvedeném na certifikátu.

8.10. **Důsledek nesplnění kvalifikace**

8.10.1. Dodavatel, který nesplní kvalifikaci v rozsahu požadovaném ZZVZ a touto zadávací dokumentací, může být Zadavatelem z účasti v zadávacím řízení vyloučen. Vybraný dodavatel, který nesplní kvalifikaci v rozsahu požadovaném ZZVZ a touto zadávací dokumentací, bude Zadavatelem z účasti v zadávacím řízení vyloučen.

9. Základní způsobilost dle § 74 a § 75 ZZVZ

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

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

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

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

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

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

Dodavatel prokazuje splnění podmínek základní způsobilosti v tomto kritériu ve vztahu k České republice a k zemi svého sídla předložením **písemného čestného prohlášení**. K prokázání uvedeného kritéria je dodavatel oprávněn využít vzor čestného prohlášení uvedeného jako Příloha č. 1 této Zadávací dokumentace.

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

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

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

Dodavatel prokazuje splnění podmínek základní způsobilosti v tomto kritériu ve vztahu k České republice předložením **výpisu z obchodního rejstříku, nebo předložením písemného čestného prohlášení v případě, že není v obchodním rejstříku zapsán**. V případě, že dodavatel není zapsán v obchodním rejstříku, je k prokázání uvedeného kritéria oprávněn využít vzor čestného prohlášení uvedeného jako Příloha č. 1 Zadávací dokumentace.

9.2. Je-li dodavatelem právnická osoba, musí podmínku uvedenou v odstavci 9.1 písm. a) splňovat tato právnická osoba a zároveň každý člen statutárního orgánu. Je-li členem statutárního orgánu dodavatele právnická osoba, musí podmínku uvedenou shora pod písm. a) splňovat:

a) tato právnická osoba,

b) každý člen statutárního orgánu této právnické osoby a

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

9.3. Účastní-li se zadávacího řízení pobočka závodu:

9.3.1. zahraniční právnické osoby, musí podmínku uvedenou v odstavci 9.1 písm. a) splňovat tato právnická osoba a vedoucí pobočky závodu

9.3.2. české právnické osoby, musí podmínku uvedenou shora pod písm. a) splňovat:

a) tato právnická osoba,

b) každý člen statutárního orgánu této právnické osoby a

c) osoba zastupující tuto právnickou osobu v statutárním orgánu dodavatele

d) vedoucí pobočky závodu.

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

a) by vyloučení účastníka znemožnilo zadání veřejné zakázky v tomto zadávacím řízení a

b) naléhavý veřejný zájem, zejména veřejné zdraví nebo ochrana životního prostředí, vyžaduje plnění veřejné zakázky.

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

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

10. Profesní způsobilost dle § 77 ZZVZ

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

10.1.1. Dodavatel prokazuje splnění profesní způsobilosti dle § 77 odst. 1 ZZVZ ve vztahu k České republice předložením výpisu z obchodního rejstříku nebo jiné obdobné evidence, pokud jiný právní předpis zápis do takové evidence vyžaduje.

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

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

11. Ekonomická kvalifikace dle § 78 ZZVZ

11.1. Zadavatel požaduje, aby minimální obrat dodavatele dosahoval za každé ze 3 bezprostředně předcházejících účetních období minimální úrovně 100 mil. Kč.

11.2. Jestliže dodavatel vznikl později, postačí, předloží-li údaj o svém obratu v požadované výši za všechna účetní období od svého vzniku.

11.3. Dodavatel prokazuje splnění tohoto kritéria ekonomické kvalifikace předložením **výkazu zisku a ztrát dodavatele nebo obdobného dokladu podle právního řádu země sídla dodavatele**.

11.4. V případě, že dodavatel prokazuje ekonomickou kvalifikaci podle § 78 ZZVZ prostřednictvím jiné osoby ve smyslu § 83 ZZVZ, požaduje Zadavatel, aby dodavatel a jiná osoba nesli společnou a nerozdílnou odpovědnost za plnění veřejné zakázky. V takovém případě dodavatel v nabídce doloží doklad o příslušném závazku, tj. společné a nerozdílné odpovědnosti za plnění veřejné zakázky.

12. Technická kvalifikace dle § 79 ZZVZ

12.1. Seznam významných zakázek

12.1.1. K prokázání kritéria technické kvalifikace požaduje Zadavatel doložení **Seznamu významných zakázek poskytnutých za posledních 5 let před zahájením zadávacího řízení**.

Ze seznamu významných zakázek musí vyplývat alespoň následující údaje:

a) název objednatele,

b) předmět plnění významné zakázky,

c) doba realizace významné zakázky,

d) finanční objem významné zakázky, je-li dále požadován,

e) kontaktní osoba objednatele, u které bude možné realizaci významné zakázky ověřit, vč. kontaktního e-mailu a telefonu.

Za účelem zpracování seznamu významných zakázek je dodavatel oprávněn využít dokument Příloha č. 3 této Zadávací dokumentace.

12.1.2. Ze Seznamu významných zakázek musí vyplývat, že dodavatel v uvedeném období realizoval minimálně:

- **1 významnou zakázku**, jejímž předmětem byla dodávka HW infrastruktury, zahrnující minimálně:
  - servery
  - disková pole
  - síťové prvky
  - konfigurace a implementace bezpečnostních pravidel,

  přičemž tato významná zakázka musí kumulativně zahrnovat **všechny** z uvedených položek servery/disková pole/síťové prvky/konfigurace a implementace bezpečnostních pravidel, a
- **2 významné zakázky**, jejichž předmětem byla dodávka HW infrastruktury, zahrnující:
  - servery
  - disková pole
  - síťové prvky
  - konfigurace a implementace bezpečnostních pravidel,

  přičemž každá z těchto 2 významných zakázek musí kumulativně zahrnovat **alespoň 2** z uvedených položek servery/disková pole/síťové prvky/konfigurace a implementace bezpečnostních pravidel,

a to v objemu min. 10 mil. Kč bez DPH za každou významnou zakázku.

12.1.3. Ze Seznamu významných zakázek musí dále vyplývat, že ze zakázek splňujících požadavky dle předchozího odstavce:

- alespoň jedna zakázka byla v objemu 20 mil. Kč bez DPH,
- alespoň jedna zakázka zahrnovala dvě geograficky oddělené lokality nebo primární / sekundární lokalitu,
- alespoň jedna zakázka zahrnovala analýzu data managementu.

12.1.4. Doba „za posledních 5 let před zahájením zadávacího řízení" se pro účely tohoto zadávacího řízení považuje za splněnou, pokud významná zakázka byla v průběhu této doby dokončena alespoň v rozsahu odpovídajícímu požadavkům Zadavatele uvedeným výše. Významná zakázka může být uznána výhradně tehdy, pokud subjekt dokládající poskytnutí příslušné významné zakázky v jejím rámci realizoval činnosti relevantní z hlediska požadavků uplatněných Zadavatelem, přičemž tyto relevantní činnosti nebyly realizovány (ukončeny) dříve, než v posledních 5 letech před zahájením zadávacího řízení veřejné zakázky. Doba „za posledních 5 let před zahájením zadávacího řízení" se považuje za splněnou i v případě, že se jedná o významné zakázky, které probíhaly i po zahájení zadávacího řízení, nebo pokud stále probíhají, za předpokladu splnění výše uvedených parametrů ke dni konce lhůty pro prokázání kvalifikace (tj. řádné dokončení příslušné části významné zakázky, která naplňuje požadavky Zadavatele na významné zakázky). Z předložených údajů a dokladů vztahujících se k příslušné významné zakázce musí být zcela jednoznačně zřejmé, jaké činnosti, v jakém rozsahu a v jakém časovém

období příslušný subjekt při plnění příslušné zakázky realizoval.

12.2. **Seznam techniků nebo technických útvarů, kteří se budou podílet na plnění veřejné zakázky (bez ohledu na to, zda jde o zaměstnance dodavatele nebo osoby v jiném vztahu k dodavateli) a osvědčení o vzdělání a odborné kvalifikaci těchto osob (realizační tým)**

12.2.1. K prokázání kritéria technické kvalifikace požaduje Zadavatel **doložit jmenný seznam členů realizačního týmu** a dále ve vztahu ke každému členovi realizačního týmu:

a) strukturovaný profesní životopis, z něhož bude vyplývat splnění požadavků Zadavatele (je-li požadována referenční zkušenost s projektem, uvede dodavatel rovněž údaje, z nichž bude ověřitelné splnění požadavku, včetně kontaktních údajů na objednatele příslušného projektu), jehož vzor je Přílohou č. 2 této Zadávací dokumentace,

b) údaj o tom, zda je člen realizačního týmu v pracovněprávním či jiném vztahu k dodavateli (v takovém případě uvede v jakém),

c) doklady, z nichž bude vyplývat splnění požadavků Zadavatele na vzdělání či odbornou způsobilost, je-li požadováno (vysokoškolský diplom, autorizace, osvědčení, certifikát, apod.).

12.2.2. Členové realizačního týmu budou odpovědní za činnosti, které bude dodavatel provádět v průběhu realizace veřejné zakázky. Každá osoba v realizačním týmu může zastávat i více pozic, splňuje-li požadavky na každou z těchto pozic.

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

Pracovní pozice	**Popis role a minimální požadavky na kvalifikaci člena realizačního týmu**
Architekt infrastruktury (Solution Architect)	**Popis role:** Architekt infrastruktury je odpovědný za návrh a architektonické zpracování komplexních řešení ICT infrastruktury se zaměřením na oblast síťových technologií, serverových platforem a datových úložišť dodávaného technického řešení. V rámci výkonu této role zajišťuje návrh technické koncepce infrastruktury, včetně řešení vysoké dostupnosti, bezpečnosti, škálovatelnosti a kontinuity provozu. Odpovídá za zpracování architektonické a technické dokumentace, za návrh řešení pro prostředí s více lokalitami včetně geograficky oddělených datových center a za návrh mechanismů replikace dat, zálohování a disaster recovery. **Popis minimálních požadavků na kvalifikaci člena realizačního týmu:** • Minimálně **3 roky** praxe na uvedené pozici (či obdobné), přičemž obsahem této praxe bylo: o návrh ICT infrastruktury v oblasti sítí a datových úložišť. • Certifikace: platná certifikace výrobce nabízeného řešení pro návrh/deployment *(nabízeným řešením se pro účely tohoto kritéria technické kvalifikace rozumí Položky A a B Technické specifikace, která je přílohou č. 2 závazného vzoru smlouvy).*
Síťový specialista	**Popis role:** Síťový specialista je odpovědný za praktickou realizaci a implementaci dodávaného řešení na základě architektonického návrhu zpracovaného Architektem infrastruktury. V rámci výkonu této role přebírá schválené technické řešení a zajišťuje jeho detailní

	rozpracování do úrovně implementační dokumentace, následnou konfiguraci, nasazení a uvedení do provozu. Odpovídá za instalaci, konfiguraci a optimalizaci aktivních síťových prvků, včetně OOB přepínačů, L3 směrovačů, bezpečnostních prvků FW a dalších komponent tvořících síťovou infrastrukturu.
	
	Jeho činností je realizace řešení pro prostředí Zadavatele s vysokými nároky na dostupnost, bezpečnost a výkon, včetně implementace redundance, segmentace sítě, vysoké dostupnosti a propojení geograficky oddělených lokalit. Zajišťuje implementaci mechanismů pro bezpečný přenos dat, monitoring síťového provozu, optimalizaci výkonu a řešení incidentů vzniklých v průběhu nasazení i převzetí do ostrého provozu.
	
	Odpovídá za provádění funkčních a zátěžových testů, spolupracuje při akceptačních řízeních a zajišťuje předání řešení do provozu včetně zpracování provozní a technické dokumentace.
	
	Popis minimálních požadavků na kvalifikaci člena realizačního týmu:
	
	• Minimálně **3 roky** praxe na uvedené pozici (či obdobné), přičemž obsahem této praxe bylo:
	  ○ návrh nebo správa sítí.
	
	• Certifikace:
	  ○ platná certifikace na úrovni professional/experta v oblasti síťových technologií, ať již se zaměřením na oblast implementace a správy datových center či v oblasti podnikových sítích. Zadavatel pro účely této certifikace uzná jak relevantní, technologicky neutrální certifikace, tak certifikace související s konkrétními technologiemi jako např.: Cisco Certified Network Professional Enterprise (CCNP Enterprise), Juniper Networks Certified Internet Professional – Enterprise Routing and Switching (JNCIP-ENT), Cisco Certified Network Professional Data Center (CCNP Data Center), Juniper Networks Certified Internet Professional – Data Center (JNCIP-DC) nebo jiné ekvivalentní či vyšší certifikace prokazující odpovídající odborné znalosti,
	  ○ platná certifikace na úrovni professional/experta v oblasti síťové bezpečnosti zahrnující firewall. Zadavatel pro účely této certifikace uzná relevantní technologicky neutrální certifikace, tak certifikace související s konkrétními technologiemi jako např.: Fortinet Certified Solution Specialist (FCSS) – Network Security, Cisco Certified Network Professional Security (CCNP Security), Juniper Networks Certified Internet Professional – Security (JNCIP-SEC), Palo Alto Networks Certified Network Security Engineer (PCNSE) nebo jiné ekvivalentní či vyšší certifikace prokazující odpovídající odborné znalosti.

Bezpečnostní specialista	**Popis role:** Tato role bude vykonávat funkci architekta kybernetické bezpečnosti dle zákona č. 264/2025 Sb., o kybernetické bezpečnosti, v platném znění, resp. vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, v platném znění. Bezpečnostní specialista bude odpovědný za návrh, implementaci a dohled nad bezpečnostními opatřeními v oblasti dodávaného řešení

	s cílem zajistit důvěrnost, integritu a dostupnost informačních a komunikačních systémů na technické řešení provozovaném. V rámci své role vychází z architektonického návrhu infrastruktury a bezpečnostní koncepce organizace, které dále rozpracovává do konkrétních bezpečnostních mechanismů, technických konfigurací a provozních pravidel. Bezpečnostní specialista úzce spolupracuje s architektem infrastruktury i síťovým specialistou. Bezpečnostní specialista odpovídá za implementaci a konfiguraci bezpečnostních technologií, zejména v oblasti firewallů nové generace (NGFW), systémů pro detekci a prevenci průniků komunikace, systémů pro řízení přístupu, segmentaci sítí dle koncepce organizace, šifrování komunikace a napojení dohledových nástrojů. Podílí se na návrhu bezpečnostní architektury pro projekt bezpečného úložiště s vysokými nároky na dostupnost a odolnost, včetně řešení pro geograficky oddělené lokality a prostředí kritické infrastruktury Zadavatele. **Popis minimálních požadavků na kvalifikaci člena realizačního týmu:** • Minimálně **3 roky** praxe na uvedené pozici (či obdobné), přičemž obsahem této praxe byl: o návrh implementace bezpečnostních opatření a zajišťování bezpečné architektury v oblasti informační nebo kybernetické bezpečnosti. • Certifikace: o platná certifikace vztahující se ke kybernetické bezpečnosti informačních systémů např. Certified Ethical Hacker Practical (CEH practical), Offensive Security Certified Professional (OSCP), Comptia Pentest+, Certified Information Systems Security Professional (CISSP), CompTIA CySA+ nebo jiná ekvivalentní či vyšší certifikace prokazující odpovídající odborné znalosti, **NEBO** o platná certifikace vztahující se k bezpečnostním řešením např. Cisco Certified Specialist – Network Security Firepower (CCNP Security), Fortinet Certified Professional (FCP)- Network Security, Fortinet Certified Solution Specialist (FCSS) - Network Security, Palo Alto Networks Certified Network Security Administrator (PCNSA) nebo Engineer (PCNSE), nebo jiná ekvivalentní či vyšší certifikace prokazující odpovídající odborné znalosti.
Datový analytik pro data storage	**Popis role:** Datový analytik pro data storage je role zaměřená na systematické zpracování, analýzu a interpretaci dat souvisejících s provozem bezpečného úložiště. Systém práce s daty je v kontextu bezpečnostních událostí a výkonnostních ukazatelů klíčových informačních systémů na daném úložišti. V rámci své role zajišťuje transformaci provozních, technických a bezpečnostních dat do strukturované podoby umožňující jejich další vyhodnocování, identifikaci trendů, rizik a optimalizačních či výkonových příležitostí. Datový analytik pro data storage odpovídá za návrh metodiky sběru dat, jejich konsolidaci z různých zdrojů relevantních pro organizaci. Provádí pokročilé analýzy zaměřené na výkonnost, dostupnost, kapacitní plánování, bezpečnostní události a efektivitu

	provozu úložiště. Výstupy svých analýz zpracovává do přehledných reportů, dashboardů a analytických podkladů a dokumentace. **Popis minimálních požadavků na kvalifikaci člena realizačního týmu:** • Minimálně **1 rok** praxe na uvedené pozici (či obdobné), přičemž obsahem této praxe bylo: o analýza korporátních dat, mapování životního cyklu dat a potřeb jednotlivých stakeholderů.
Projektový manažer	**Popis role:** Projektový manažer je odpovědný za komplexní řízení všech složek dodavatele v projektu Bezpečného úložiště, a to od návrhu řešení, přes jeho dodávku a implementaci až po akceptaci a předání do provozu Zadavatele. Odpovídá za plánování a koordinaci kapacit dodavatele, řízení úkolů a milníků projektu, věcnou kontrolu jednotlivých fází a včasnou identifikaci a řízení součinnosti potřebné pro řádné dokončení díla. Současně dohlíží na plnění smluvních podmínek, dodržování harmonogramu a požadovanou kvalitu plnění. V rámci své role zajišťuje vedení projektové dokumentace. Koordinuje činnost realizačního týmu dodavatele, zejména architekta, síťových a bezpečnostních specialistů a dalších odborných rolí, a zajišťuje efektivní komunikaci mezi všemi zapojenými stranami. Odpovídá za řízení rizik projektu, včasnou identifikaci problémů a návrh nápravných opatření předkládaných projektovému výboru a managementu SŽ, včetně pravidelného reportingu a organizace kontrolních dnů. Projektový manažer zároveň odpovídá za přípravu podkladů pro akceptační řízení, za soulad akceptačních protokolů se smlouvou a Zvláštními obchodními podmínkami pro Zakázky v oblasti ICT. **Popis minimálních požadavků na kvalifikaci člena realizačního týmu:** • Minimálně **3 roky** praxe na uvedené pozici (či obdobné), přičemž obsahem této praxe bylo: o řízení IT/ICT projektů. • Certifikace: platná certifikace PRINCE2 Foundation nebo jiná obdobná či vyšší certifikace.

13. Požadavky Zadavatele na způsob zpracování nabídkové ceny:

13.1. Zadavatel požaduje, aby účastník uvedl nabídkovou cenu za plnění předmětu této veřejné zakázky, v české měně (Koruna česká), v členění bez daně z přidané hodnoty (DPH).

13.2. Za účelem výpočtu nabídkové ceny v Kč bez DPH vyplní účastník dokument Ceník, který tvoří Přílohu č. 3 smlouvy. Za správnost provedení výpočtu nabídkové ceny odpovídá účastník.

13.3. Zadavatel požaduje, aby účastník uvedl také dílčí ceny za části předmětu Veřejné zakázky (jednotlivé položky) v souladu s dokumentem Ceník, který tvoří Přílohu č. 3 smlouvy.

13.4. Účastník je povinen vyplnit všechna požadovaná pole v dokumentu Ceník, který tvoří Přílohu č. 3 smlouvy, která jsou označena k vyplnění dodavatelem.

13.5. Celková nabídková cena jakož i nabídková cena doplněná účastníkem do jednotlivých buněk v dokumentu Ceník, který tvoří Přílohu č. 3 smlouvy, představuje maximální výši úhrady za plnění dle Smlouvy, jakož i za jednotlivé položky a je stanovena jako cena „nejvýše přípustná" a pevná. V této ceně musí být zahrnuty veškeré náklady spojené s realizací předmětu veřejné zakázky, tj. veškeré náklady související. Zadavatel připouští

překročení celkové nabídkové ceny a/nebo jednotkových cen dodavatele pouze za podmínek stanovených ve smlouvě.

14. Jiné požadavky Zadavatele na plnění veřejné zakázky:

14.1. Využití poddodavatele

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

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

b) předložil seznam poddodavatelů, pokud jsou dodavateli známi a uvedl, kterou část veřejné zakázky bude každý z poddodavatelů plnit.

14.1.2. Seznam poddodavatelů učiní dodavatel přílohou Smlouvy.

15. Varianty nabídky

15.1. Zadavatel nepřipouští varianty nabídky.

16. Závazný vzor smlouvy

16.1. Dodavatel je povinen využít Závazný vzor smlouvy, který tvoří dokument Příloha č. 5 Zadávací dokumentace.

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

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

17. Způsob hodnocení nabídek:

17.1. Kritéria hodnocení

17.1.1. Hodnocení nabídek bude provedeno v souladu s § 114 a násl. ZZVZ podle kritéria nejnižší nabídkové ceny.

17.1.2. Celková nabídková cena musí být zpracována v souladu s čl. 13 a dokumentem Ceník, který tvoří Přílohu č. 3 smlouvy.

17.1.3. Jako ekonomicky nejvýhodnější bude vyhodnocena nabídka s nejnižší Celkovou nabídkovou cenou v Kč bez DPH.

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

18. Zadávací dokumentace:

18.1. Uveřejnění zadávací dokumentace

18.1.1. V souladu s § 96 odst. 1 a 2 ZZVZ je Zadávací dokumentace s výjimkou formulářů dle § 212 ZZVZ zveřejněna na profilu Zadavatele na internetové adrese: https://zakazky.spravazeleznic.cz/. Tamtéž budou uveřejňovány i vysvětlení, změny nebo doplnění zadávací dokumentace této veřejné zakázky.

18.2. Námitky proti zadávacím podmínkám

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

18.3. Vysvětlení, změna nebo doplnění zadávací dokumentace

18.3.1. Zadavatel může zadávací dokumentaci vysvětlit, doplnit či změnit za podmínek podrobně stanovených v § 98, § 99 a souvisejících ustanoveních ZZVZ.

18.3.2. Požádá-li o vysvětlení zadávací dokumentace dodavatel, Zadavatel při vyřízení žádosti postupuje v souladu s § 98 a souvisejícími ustanoveními ZZVZ.

19. Závaznost pokynů Zadavatele

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

20. Komunikace mezi Zadavatelem a dodavatelem:

20.1. Veškerá komunikace mezi Zadavatelem a dodavatelem musí být v souladu s § 211 ZZVZ vedena pouze písemnou formou, a to elektronicky, s výjimkou případů vymezených v ustanovení § 211 odst. 5 ZZVZ. Nestanoví-li tato Zadávací dokumentace jinak, bude veškerá komunikace mezi Zadavatelem a dodavatelem probíhat v českém jazyce. Doručování písemností a komunikace mezi Zadavatelem a dodavatelem bude ze strany Zadavatele probíhat prostřednictvím elektronického nástroje E-ZAK (na adrese: https://zakazky.spravazeleznic.cz/), který splňuje podmínky vyhlášky č. 260/2016 Sb., o stanovení podrobnějších podmínek týkajících se elektronických nástrojů, elektronických úkonů při zadávání veřejných zakázek a certifikátu shody. Na komunikaci ze strany dodavatelů učiněnou elektronicky, avšak nikoliv prostřednictvím elektronického nástroje E-ZAK, bude tedy Zadavatel vždy odpovídat prostřednictvím elektronického nástroje.

20.2. Zpracování osobních údajů včetně jejich zvláštních kategorií případně poskytnutých v průběhu zadávacího řízení je Zadavatelem prováděno pouze za účelem zadání Veřejné zakázky, přičemž Zadavatel v celém procesu ochrany osobních údajů postupuje v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES, obecně závaznými právními předpisy a vnitřními předpisy zadavatele, které agendu ochrany osobních údajů upravují.

21. Požadavky Zadavatele na zpracování nabídky, způsob podání nabídek

21.1. Účastník předloží nabídku v elektronické podobě, a to s využitím elektronického nástroje E-ZAK. Způsob správného podání nabídky v elektronické podobě na veřejnou zakázku je uveden v uživatelské příručce elektronického nástroje E-ZAK pro dodavatele, která je k dispozici na internetové stránce profilu Zadavatele: https://zakazky.spravazeleznic.cz/manual.html.

21.2. Pro tyto účely a v souladu se ZZVZ systém vyžaduje registraci účastníků a elektronický podpis založený na kvalifikovaném certifikátu. Podáním nabídky účastník se stanovenou formou komunikace a doručování souhlasí a zavazuje se poskytnout veškerou nezbytnou součinnost, zejména provést registraci v elektronickém nástroji E-ZAK a pravidelně kontrolovat doručené zprávy.

21.3. Účastník je povinen přiložit ke své nabídce čestné prohlášení o tom, že v souvislosti se zadávacím řízením na předmětnou veřejnou zakázku neuzavřel a neuzavře s jinými osobami zakázanou dohodu ve smyslu zákona č. 143/2001 Sb., o ochraně hospodářské soutěže a o změně některých zákonů (zákon o ochraně hospodářské soutěže), ve znění pozdějších předpisů a že nepostupoval ve vzájemné shodě s jiným účastníkem zadávacího řízení, s nímž je spojenou osobou podle zákona č. 586/1992 Sb., o daních z příjmů, ve znění pozdějších předpisů, při přípravě částí nabídek, které mají být hodnoceny podle kritérií hodnocení. Vzor čestného prohlášení je upraven jako Příloha č. 4 této Zadávací dokumentace.

21.4. Speciální požadavky Zadavatele na zpracování nabídek:

21.4.1. Podává-li nabídku více osob společně, zejména jako společnost ve smyslu ustanovení § 2716 a násl. zákona č. 89/2012 Sb., občanský zákoník, případně jako jiné sdružení či seskupení dodavatelů (dále v textu této Zadávací dokumentace je takové seskupení dodavatelů obecně označováno zejména jako „***společnost***" dodavatelů a člen takového seskupení jako „***společník***"), musí předložit informace o takové společnosti.

21.4.2. Podává-li nabídku více osob společně, jsou povinni doložit v nabídce, že všichni tito dodavatelé budou vůči Zadavateli a jakýmkoliv třetím osobám z jakýchkoliv závazků vzniklých v souvislosti s veřejnou zakázkou, plněním předmětu veřejné zakázky či vzniklých v důsledku prodlení či jiného porušení smluvních nebo jiných povinností v souvislosti s plněním předmětu veřejné zakázky, zavázáni společně a nerozdílně. Účastník řízení tento požadavek doloží kopií smlouvy či jiného dokumentu, ze kterého bude daná skutečnost vyplývat.

21.4.3. Jeden ze společníků bude ve výše uvedené smlouvě či jiném dokumentu uveden jako vedoucí společník. Komunikace mezi Zadavatelem a společníky, kteří podávají společnou nabídku, potom bude v takovém případě probíhat prostřednictvím tohoto vedoucího společníka. Veškerá právní jednání budou považována za doručená, resp. odeslaná, okamžikem doručení, resp. odeslání, vedoucímu společníkovi.

21.5. Pro zpracování nabídky Zadavatel doporučuje níže uvedené řazení dokladů a dokumentů:

a) Obsah nabídky (včetně nabídkové ceny),

b) Čestné prohlášení ve vztahu k zakázaným dohodám - Vzor čestného prohlášení je upraven jako Příloha č. 4 této Zadávací dokumentace,

c) Čestné prohlášení o střetu zájmů - Vzor čestného prohlášení je upraven jako Příloha č. 7 této Zadávací dokumentace,

d) Čestné prohlášení o splnění podmínek v návaznosti na mezinárodní sankce - Vzor čestného prohlášení je upraven jako Příloha č. 8 této Zadávací dokumentace,

e) Čestné prohlášení k ve vztahu k zákonu o registru smluv - Vzor čestného prohlášení je upraven jako Příloha č. 6 této Zadávací dokumentace,

f) Doklady prokazující splnění základní způsobilosti,

g) Doklady prokazující splnění profesní způsobilosti,

h) Doklady prokazující splnění ekonomické kvalifikace,

i) Doklady prokazující splnění technické kvalifikace,

j) Závazný vzor smlouvy doplněný dle pokynů v této Zadávací dokumentaci – Závazný vzor smlouvy je upraven jako Příloha č. 5 této Zadávací dokumentace,

k) Jiné informace a doklady, je-li to potřebné.

21.6. Požaduje-li Zadavatel v nabídce pro účely posouzení splnění kvalifikace anebo hodnocení nabídek dle kritéria kvality předložení dokladů o rozhodné finanční hodnotě (např. finanční hodnota referenční zakázky, výše obratu) a v účastníkem předložených dokladech bude tato hodnota uvedena v jiné měně než CZK, bude částka přepočtena Zadavatelem dle posledního čtvrtletního průměrného kurzu devizového trhu příslušné měny k CZK stanoveného a zveřejněného ČNB ke dni zahájení zadávacího řízení. Postup dle předchozí věty se neuplatní pro hodnocení dle kritéria nejnižší nabídkové ceny. Nabídková cena musí být vždy uvedena v Zadavatelem požadované měně.

21.7. Nabídka musí být podána v českém jazyce nebo v souladu s ustanovením § 45 odst. 3 ZZVZ. Zadavatel nepřipouští podání nabídky v listinné podobě ani v jiné elektronické formě mimo elektronický nástroj E-ZAK. Povinnost překládat nabídku v českém jazyce se nevztahuje na certifikáty členů realizačního týmu či datasheety, tyto dokumenty mohou být předkládány rovněž v jazyce anglickém, avšak Zadavatel je oprávněn si vyžádat jejich překlad po dodavateli, bude-li to požadovat za potřebné.

21.8. Nabídky podávané v elektronické podobě účastník doručí do konce níže uvedené lhůty pro podání nabídek.

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

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

22. Informace pro dodavatele a podmínky pro uzavření smlouvy:

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

22.2. **Požadavky Zadavatele pro uzavření smlouvy**

22.2.1. Vybraný dodavatel je povinen Zadavateli na písemnou výzvu učiněnou dle § 122 odst. 3 ZZVZ předložit doklady či vzorky, pokud je Zadavatel požadoval a nemá je k dispozici.

22.2.2. Zadavatel je oprávněn v písemné výzvě určit další doklady, které je vybraný dodavatel povinen předložit v souladu s § 122 odst. 4 ZZVZ, tj. například originály nebo úředně ověřené kopie dokladů.

22.2.3. U vybraného dodavatele, je-li českou právnickou osobou, Zadavatel zjistí údaje o

jeho skutečném majiteli podle zákona upravujícího evidenci skutečných majitelů (dále jen „***skutečný majitel***") z evidence skutečných majitelů podle téhož zákona (dále jen „***evidence skutečných majitelů***"). Vybraného dodavatele, je-li zahraniční právnickou osobou, Zadavatel vyzve k předložení výpisu ze zahraniční evidence obdobné evidenci skutečných majitelů nebo, není-li takové evidence,

a) ke sdělení identifikačních údajů všech osob, které jsou jeho skutečným majitelem,

a

b) k předložení dokladů, z nichž vyplývá vztah všech osob podle předchozího písmene a) k dodavateli; těmito doklady jsou zejména:

- výpis ze zahraniční evidence obdobné veřejnému rejstříku,
- seznam akcionářů,
- rozhodnutí statutárního orgánu o vyplacení podílu na zisku,
- společenská smlouva, zakladatelská listina nebo stanovy.

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

22.2.5. Zadavatel upozorňuje, že preferuje uzavírání smluv v elektronické podobě prostřednictvím některého druhu zaručených elektronických podpisů. V případě, že dodavatel není schopen k takovému postupu zajistit Zadavateli součinnost, žádáme, aby Zadavatele o této skutečnosti bezodkladně informoval.

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

22.3.1. Vybraný dodavatel je povinen Zadavateli na písemnou výzvu učiněnou dle § 122 odst. 3 písm. b) ZZVZ předložit:

a) doklady a informace dle čl. 24.3 a čl. 25.7 Zadávací dokumentace;

b) kopii dokladu o pojištění odpovědnosti za škodu sjednané v rozsahu podrobně stanoveném v čl. 22. smlouvy, např. pojistná smlouva, pojistný certifikát,

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

23. Registr smluv

23.1. Zadavatel je povinen uveřejňovat uzavřené smlouvy v registru smluv na základě ustanovení zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (dále jen „***ZRS***").

23.2. Zadavatel na základě výše uvedeného požaduje, aby účastník pro účely uveřejnění smlouvy v registru smluv ve smlouvě, která bude nedílnou součástí nabídky, označil její části, které jsou předmětem obchodního tajemství nebo ty části, ve kterých jsou obsaženy informace, které nemohou být v registru smluv uveřejněny na základě ustanovení § 3 odst. 1 ZRS.

23.3. Dodavatel podáním nabídky akceptuje, že nabídková cena, která je předmětem hodnocení, bude vždy uveřejněna postupem dle ZRS. Zadavatel upozorňuje, že v případě jednotkových nabídkových cen, které nejsou předmětem hodnocení, se zpravidla nebude jednat o obchodní tajemství. V případě, že dodavatel tyto jednotkové ceny označí jako obchodní tajemství, je zadavatel oprávněn přezkoumat, zda jím označené jednotkové ceny naplňují veškeré znaky obchodního tajemství, a tyto jednotkové ceny případně uveřejnit. Dodavatel je v takovém případě zadavateli povinen poskytnout součinnost, zejména je povinen k výzvě zadavatele blíže odůvodnit naplnění všech znaků obchodního tajemství ve vztahu k jím označeným jednotkovým cenám. Dodavatel podáním nabídky dále akceptuje, že i v případě, že jednotkové ceny naplní všechny znaky obchodního tajemství, je zadavatel oprávněn uveřejnit jednotkové ceny dle ZRS, je-li to nezbytné pro účely § 9 odst. 2 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

23.4. Pokud účastník ve smlouvě, která bude nedílnou součástí nabídky, označí její části nebo určité informace dle čl. 23.2 této Zadávací dokumentace, je účastník povinen předložit Čestné prohlášení. Vzor čestného prohlášení je zpracován jako Příloha č. 6 této Zadávací dokumentace. Tímto čestným prohlášením účastník prohlašuje, že jím uvedené údaje a skutečnosti kumulativně naplňují všechny definiční znaky obchodního tajemství tak, jak je vymezeno v ustanovení § 504 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „***obchodní tajemství***") a pro případ, že by takto označené údaje a skutečnosti nenaplňovaly znaky obchodního tajemství, nese účastník veškerou odpovědnost za skutečnost, že takto znečitelněná smlouva, či rámcová dohoda byla uveřejněna způsobem odporujícím ZRS. Odpovědnost dodavatele dle předchozí věty není dotčena postupem zadavatele dle čl. 23.3 této Zadávací dokumentace

23.5. Výše uvedené čestné prohlášení dle čl. 23.4 této Zadávací dokumentace účastník nedokládá v případě, že neoznačí ve smlouvě, která bude nedílnou součástí nabídky, žádné takové části nebo informace ve smyslu čl. 23.2 této Zadávací dokumentace**.**

23.6. Účastník odpovídá za správnost a pravdivost veškerých údajů a skutečností, které jím budou uvedeny ve výše uvedeném čestném prohlášení.

23.7. Výjimkou z povinnosti uveřejnění smlouvy v registru smluv jsou důvody uvedené v ustanovení § 3 odst. 2 ZRS. Je-li účastník subjektem uvedeným v ustanovení § 3 odst. 2 písm. k) ZRS (případně je subjektem uvedeným v ustanovení § 3 odst. 2 ZRS dle jiného písmene, než je zde uvedeno), doporučuje Zadavatel, aby účastník tuto skutečnost uvedl v nabídce. V případě, že tak účastník neučiní, bude Zadavatel postupovat, jako by na smlouvu nedopadala výjimka uvedená v ustanovení § 3 odst. 2 písm. k) ZRS (případně jiná výjimka dle ustanovení § 3 odst. 2 ZRS dle jiného písmene, než je zde uvedeno) a Zadavatel neodpovídá za škodu nebo jakoukoliv jinou újmu tímto postupem vzniklou.

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

24.1. Dle § 4b zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů (dále jen „***Zákon o střetu zájmů***"), se nesmí účastnit zadávacích řízení dle ZZVZ jako účastník zadávacího řízení nebo jako poddodavatel, prostřednictvím kterého účastník zadávacího řízení prokazuje kvalifikaci, obchodní společnost, ve které veřejný funkcionář uvedený v § 2 odst. 1 písm. c) Zákona o střetu zájmů nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti.

24.2. Zadavatel požaduje, aby dodavatel a jeho poddodavatel, prostřednictvím kterého prokazuje kvalifikaci, nebyli ve střetu zájmů dle § 4b Zákona o střetu zájmů. Skutečnost, že dodavatel a jeho poddodavatel, prostřednictvím kterého prokazuje část kvalifikace, nejsou ve střetu zájmů dle § 4b Zákona o střetu zájmů, prokáže dodavatel předložením čestného prohlášení, jehož vzorové znění je Příloha č. 7 Zadávací dokumentace, ve své nabídce.

24.3. Zadavatel je oprávněn ověřovat si splnění zadávacích podmínek dle tohoto článku. Vybraný dodavatel je povinen předložit k výzvě Zadavatele dle § 122 odst. 3 písm. b) ZZVZ doklady a informace, z nichž nepochybně vyplyne, že vybraný dodavatel i všichni poddodavatelé, jimiž vybraný dodavatel prokazuje kvalifikaci, splňují podmínku neexistence střetu zájmů ve smyslu § 4b Zákona o střetu zájmů a tohoto čl. 24 Zadávací dokumentace. V případě vybraného dodavatele nebo jeho poddodavatele, prostřednictvím kterého vybraný dodavatel prokazoval část kvalifikace, je-li zahraniční právnickou osobou, je vybraný dodavatel povinen předložit zejména doklady ve smyslu § 122 odst. 6 ZZVZ, a to i ve vztahu k příslušnému poddodavateli, prostřednictvím kterého vybraný dodavatel prokazoval část kvalifikace.

24.4. V případě postupu účastníka v rozporu s čl. 24 Zadávací dokumentace bude účastník vyloučen ze zadávacího řízení.

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

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

25.2. Dle článku 5k nařízení Rady (EU) č. 833/2014 ze dne 31. července 2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, ve znění pozdějších předpisů[1] (dále jen „***Nařízení č. 833/2014***") se zakazuje se zadat jakoukoli veřejnou zakázku nebo koncesní smlouvu spadající do oblasti působnosti směrnic o zadávání veřejných zakázek, jakož i čl. 10 odst. 1, 3, odst. 6 písm. a) až e), odst. 8, 9 a 10, článků 11, 12, 13 a 14 směrnice 2014/23/EU, čl. 7 písm. a) až d), článku 8 a čl. 10 písm. b) až f) a h) až j) směrnice 2014/24/EU, článku 18, čl. 21 písm. b) až e) a g až i) a článků 29 a 30 směrnice 2014/25/EU a čl. 13 písm. a) až d), f) až h) a j) směrnice 2009/81/ES a hlavy VII nařízení Evropského parlamentu a Rady (EU, Euratom) 2018/1046 následujícím osobám, subjektům nebo orgánům, nebo pokračovat v jejich plnění s následujícími osobami, subjekty a orgány:

a) jakýkoli ruský státní příslušník, fyzická osoba s bydlištěm v Rusku nebo právnická osoba, subjekt či orgán usazené v Rusku;

b) právnická osoba, subjekt nebo orgán, které jsou z více než 50 % přímo či nepřímo vlastněny některým ze subjektů uvedených v písmeni a) tohoto odstavce, nebo

c) fyzická nebo právnická osoba, subjekt nebo orgán, které jednají jménem nebo na pokyn některého ze subjektů uvedených v písmeni a) nebo b) tohoto odstavce,

včetně subdodavatelů, dodavatelů nebo subjektů, jejichž způsobilost je využívána ve

[1] Zejm. Nařízení Rady (EU) 2022/576 ze dne 8. dubna 2022, kterým se mění nařízení (EU) č. 833/2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině

smyslu směrnic o zadávání veřejných zakázek, pokud představují více než 10 % hodnoty zakázky.

25.3. Zadavatel požaduje, aby účastník sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti v zadávacím řízení, ani žádný z jeho poddodavatelů nebo jiných osob, jejichž způsobilost je využívána ve smyslu směrnic o zadávání veřejných zakázek, **nebyli** osobami dle odst. 2 tohoto článku a Nařízení č. 833/2014.

25.4. Dle čl. 2 nařízení Rady (EU) č. 269/2014 ze dne 17. března 2014, o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, ve znění pozdějších předpisů (dále jen „***Nařízení č. 269/2014***"), a dalších prováděcích předpisů k tomuto Nařízení č. 269/2014[2], nesmějí být žádné finanční prostředky ani hospodářské zdroje přímo ani nepřímo zpřístupněny fyzickým nebo právnickým osobám, subjektům či orgánům nebo fyzickým nebo právnickým osobám, subjektům či orgánům s nimi spojeným uvedeným v příloze I Nařízení nebo v jejich prospěch; dle čl. 2 **nařízení Rady (ES) č. 765/2006** ze dne 18. května 2006 o omezujících opatřeních vzhledem k situaci v Bělorusku a k zapojení Běloruska do ruské agrese proti Ukrajině, ve znění pozdějších předpisů, nesmějí být fyzickým nebo právnickým osobám nebo subjektům uvedeným v příloze I tohoto nařízení nebo v jejich prospěch přímo ani nepřímo zpřístupněny žádné finanční prostředky ani hospodářské zdroje; dle čl. 2 **nařízení Rady (EU) č. 208/2014** ze dne 5. března 2014 o omezujících opatřeních vůči některým osobám, subjektům a orgánům vzhledem k situaci na Ukrajině nesmějí být žádné finanční prostředky ani hospodářské zdroje přímo ani nepřímo zpřístupněny fyzickým nebo právnickým osobám, subjektům či orgánům uvedeným v příloze I tohoto nařízení nebo v jejich prospěch (dále společně jen „***Osoby vedené na sankčních seznamech***").

25.5. Zadavatel dále požaduje, aby účastník sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti v zadávacím řízení, ani žádný z jeho poddodavatelů nebo jiných osob, jejichž způsobilost je využívána ve smyslu směrnic o zadávání veřejných zakázek, **nebyli** Osobami vedenými na sankčních seznamech.

25.6. Splnění zadávacích podmínek stanovených Zadavatelem dle tohoto článku prokáže účastník předložením čestného prohlášení, jehož vzorové znění je Příloha č. 8 této Zadávací dokumentace, ve své nabídce.

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

25.8. V případě postupu účastníka v rozporu s čl. 25 Zadávací dokumentace bude účastník vyloučen ze zadávacího řízení.

Přílohy Zadávací dokumentace

Příloha č. 1. Čestné prohlášení k základní způsobilosti

Příloha č. 2. Vzor profesního životopisu

Příloha č. 3. Vzor seznamu významných zakázek

[2] Zejm, Prováděcí nařízení Rady (EU) 2022/581 ze dne 8. dubna 2022, kterým se provádí nařízení (EU) č. 269/2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny a prováděcí nařízení Rady (EU) 2022/658 ze dne 21. dubna 2022, kterým se provádí nařízení (EU) č. 269/2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny.

Příloha č. 4.	Čestné prohlášení ve vztahu k zakázaným dohodám
Příloha č. 5.	Závazný vzor smlouvy
Příloha č. 6.	Čestné prohlášení ve vztahu k zákonu o registru smluv
Příloha č. 7.	Čestné prohlášení o střetu zájmů
Příloha č. 8.	Čestné prohlášení o splnění podmínek v návaznosti na mezinárodní sankce
Příloha č. 9.	Výstupy z PTK

……

Ing. Tomáš Tóth
generální ředitel