Název zakázky: Prodloužení podpory zálohovacího systému a rozšíření systému o ochranu dat proti kybernetickým hrozbám
Číslo zakázky: P24V00000121
Zadavatel: Statutární město Frýdek-Místek, se sídlem Frýdek-Místek, Radniční 1148, PSČ 738 01

1. Cena dodávky

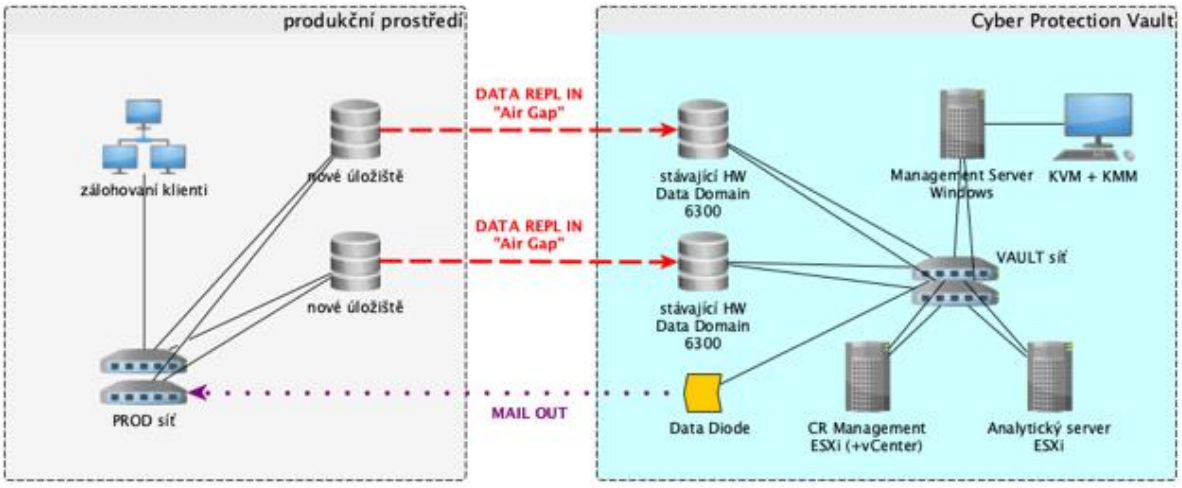
	Cena celkem bez DPH	DPH	Cena celkem včetně DPH
Celková cena řešení včetně implementace	**9 405 620**	**1 975 180,2**	**11 380 800,2**
Cena technické podpory na 5 let	**1 080 000**	**226 800**	**1 306 800**
CENA CELKEM	**10 485 620**	**2 201 980,2**	**12 687 600,2**

2. Předmět plnění

Předmětem plnění veřejné zakázky je dodávka hardware, software a služeb pro zálohování a ochranu zálohovaných dat proti ransomware a obdobným kybernetickým bezpečnostním hrozbám. Dodaná technologická platforma rozšíří současné zálohovací řešení objednavatele, které zůstane zachováno a doplní jej o offline zálohu ve zcela odděleném prostředí – datovém trezoru „Cyber Protection Vault".
Datový trezor bude v klidovém režimu plně komunikačně izolován a nebude tedy možné offline systém napadnout zevnitř komunikační sítě objednavatele. Datový trezor bude vybaven potřebnou infrastrukturou pro zajištění automatizovaného řízení procesu kopírování záloh a monitoringem, který bude napojen do monitorovacího nástroje objednavatele. Monitoring bude pouze prostřednictvím jednosměrné monitorovací komunikace směrem k dohledovému systému objednavatele.
Datový trezor bude dále vybaven zařízením pro provádění pravidelné korelační analýzy nad kopií záloh umístěných v datovém trezoru. Korelační analýza bude fungovat na principu umělé inteligence, kdy se nepracuje pouze s pravidelně obnovovanou databází vzorků již známých škodlivých kódů, ale aktivně se vyhledávají nekonzistence v datech současných a minulých a porovnávají se s očekávaným stavem. Cílem tohoto procesu je včasné odhalení útoku a uvědomění objednavatele.
Pro účely uložení dat v datovém trezoru budou použita stávající zálohovací úložiště. Pro provozní zálohování budou použita úložiště nová. Součásti implementace je uvolnění současných úložišť pro využití v datovém trezoru, tedy migrace uložených záloh ze současných úložišť na úložiště nová.
Dále je předmětem plnění rozšíření zálohovacího systému na ochranu uživatelských dat v cloudové službě Office 365.
Součástí dodávky budou i všechny potřebné instalační prvky do 19" rack skříní, propojovací kabely, potřebné komunikační transceivery, management kabely, lyžiny s možnosti vysunutí – pokud to řešení umožňuje, cable management arm apod..

Schéma zapojení dodávaného řešení:

- Součásti zapojení je i napojení na management serverů a diskových polí, které není zakresleno.



2.1. Současný technologický stav

Zálohovaná data jsou zapisovaná klienty přímo na primární deduplikační zálohovací úložiště DataDomain 6300 o kapacitě 32TB. Zálohovací systém NetWorker následně řídí klonování (zrcadlení) těchto záloh na druhou secundární DataDomain 6300 o kapacitě 32TB.
Takto klonovaná data jsou přenášena napřímo mezi úložišti DataDomain v deduplikovaném formátu, NetWorker slouží jen pro řízení.
Zálohovací systém je koncipován jako klient-server aplikace s dedikovaným zálohovacím serverem. Na zálohovacím serveru NetWorkeru jsou instalovány serverové komponenty NetWorker Server a NetWorker Management Console server.
Na vybraných klientech (zálohovaných serverech), jsou instalovány klientské programové komponenty umožňující zálohování operačního systému, Active Directory i uživatelských dat. Zálohování agentem se provádí u Active Directory řadičů, klientů s aplikačními moduly a souborových serverů s uživatelskými daty.
Tam, kde není použití zálohovacího agenta nutné, je použito zálohování na úrovni virtuálních strojů VMware. Záloha na úrovni virtuálních strojů je použitá i u agentem zálohovaných klientů, z důvodu snadné Disaster Recovery.
Objednavatel disponuje dvěma switchi JC7772A a celkem 12 Gbic 10 GB JD094B, které lze při návrhu řešení využít.

3. Technická specifikace

Objednavatel požaduje splnění následujících parametrů (včetně popisu jejich naplnění).

3.1. Dodávka dvou nových deduplikačních úložišť

3.1.1. Výkon a škálovatelnost

Požadovaný parametr, vlastnost	Splněno	Popis naplnění
2 ks deduplikačních diskových úložišť	Ano	2ks deduplikačních diskových úložišť Dell PowerProtect DD6400
Každé jedno diskové úložiště musí disponovat alespoň 31TB čisté využitelné kapacity (kapacita	Ano	Každé jedno diskové úložiště disponuje 32TB čisté využitelné

před deduplikací a kompresí dat, která je dostupná pro uložení dat a lze ji zkontrolovat prostřednictvím management nástrojů).		kapacity (kapacita před deduplikací a kompresí dat, ověřitelná pomocí management nástrojů).
Diskové úložiště musí umožnit rozšiřování minimálně do 150TB čisté kapacity po max. 4TB krocích.	Ano	Každé z úložišť umožňuje licenční rozšíření kapacity po 4TB krocích až do velikosti 172TB.
Minimální propustnost pro zápis 20 TB/h	Ano	Propustnost zápisu až 27,7 TB/h.
Každé úložiště musí být osazeno minimálně: • 4x 10Gbps ETH Base-T • 4x 10Gbps SFP+ včetně 10G-SR modulů	Ano	Osazení: • 4x 10Gbps ETH Base-T • 4x 10Gbps SFP+ včetně 10G-SR modulů
Podpora min 250 konkurenčních zálohovacích úloh per úložiště.	Ano	Podpora až 270 konkurenčních vláken.
Úložiště musí při ukládání dat využívat princip in-line deduplikace na cíli na principu variabilní délky bloku.	Ano	In-line deduplikace na cíli s variabilní délkou bloku.
Architektura diskového úložiště musí pro deduplikaci využívat procesorový výkon a nesmí být závislá na počtu a typu backendových disků.	Ano	Deduplikace probíhá mezi procesorem a pamětí a není závislá na počtu a typu backendových disků.
Všechna data v rámci jednoho boxu budou deduplikována mezi sebou (žádné separátní pooly deduplikovaných dat v rámci jednoho úložiště).	Ano	Úložiště využívá tzv. globální deduplikaci. Všechna data se (nezávisle na protokolu, druhu přístupu, aplikaci, klientovi, atd.) deduplikují v rámci jednoho úložiště pro maximální efektivitu deduplikace.

3.1.2. Integrace a interoperabilita

Požadovaný parametr	**Splněno**	**Popis naplnění**
Úložiště musí podporovat minimálně následující protokoly: CIFS, NFS, VTL, FC; a musí umožnit jejich současné použití.	Ano	Podpora CIFS, NFS, VTL, NDMP a FC včetně jejich současného použití.
Úložiště musí být umožňovat přímou integraci s různými typy zálohovacích SW (minimálně Dell Data Protection Suite, Dell NetWorker, Microfocus Data Protector, IBM TSM, Veritas NetBackup, VEEAM).	Ano	Ano, přímá integrace se všemi uvedenými zálohovacími SW.
Zálohovací diskové úložiště musí být univerzální z hlediska podpory datových typů zálohovaných dat, musí podporovat všechny datové typy,	Ano	Úložiště je univerzální a nezávislé na datovém typu. Datové typy, používané v produkčním prostředí

používané v produkčním prostředí – uživatelské soubory, databáze, emaily, VMware, Oracle, MS Exchange, MS SQL.		zadavatele (soubor, databáze, emaily, VMware, Oracle a MS Exchange) jsou podporované.
Deduplikace musí být prováděna přes celé zálohovací prostředí – přes všechny aplikace, nezávisle na typu dat.	Ano	Globální deduplikace přes celé zálohovací prostředí.
Úložiště musí umožnit současnou podporu standardních aplikací, platforem a protokolů bez nutnosti změny instalované infrastruktury (např. nutnost výměny zálohovacího SW, změny topologie sítě, apod.).	Ano	Zařízení umožňuje současnou podporu standardních aplikací, platforem a protokolů bez nutnosti změny instalované infrastruktury.
Úložiště musí být kompatibilní se stávajícím zálohovacím řešením Dell DPS (NetWorker).	Ano	Zařízení je plně kompatibilní se stávajícím zálohovacím řešením Dell DPS NetWorker.
Úložiště musí umožnit ukládat data i pro archivní účely s funkcionalitou nastavení retenčních politik.	Ano	Zařízení umožňuje ukládat data i pro archivní účely s funkcionalitou Retention Lock pro nastavení retenčních politik.
Úložiště musí umožnit případnou distribuci deduplikačního algoritmu z cílového (deduplikačního úložiště) na zdrojové zařízení (backup klienta nebo backup server) z důvodu výkonu a škálovatelnosti prostředí a z důvodu úspor na slabých datových linkách.	Ano	Uložiště umožňuje deduplikaci jak na uložišti, tak na zdroji (klientovi) to je jeden ze základních principů protokolu DD Boost v nabízeném řešení.
Úložiště musí disponovat funkcí multitenancy (umožnit logické dělení diskového prostoru pro různé skupiny uživatelů s právy pouze na tyto logické jednotky s možností definice tenant administrator).	Ano	Podpora multitenancy s možností definice tenant administrator (Secure Multi Tenancy).
Úložiště musí poskytovat stejné výsledky deduplikace zálohy Oracle prostředí bez ohledu na Oracle multiplexing,	Ano	Zařízení disponuje algoritmy pro deduplikaci záloh Oracle se stejným výsledkem bez ohledu na Oracle multiplexing.

3.1.3. Replikace

V poptávaném řešení je vyžadována dodávka licencí pro replikaci a kompatibilita se stávajícím zařízením objednavatele.

Požadovaný parametr	**Splněno**	**Popis naplnění**
Úložiště musí být pro replikaci kompatibilní se stávajícím zařízením zadavatele – Dell DataDomain 6300.	Ano	Zařízení je plně kompatibilní pro replikaci kompatibilní se stávajícím

		zařízením zadavatele – Dell DataDomain 6300.
Úložiště musí obsahovat licenci pro replikaci do záložní lokality.	Ano	Replikační licence je součástí základní licence zařízení.
Úložiště musí pro replikaci posílat pouze deduplikovaná a zkomprimovaná data.	Ano	Replikují se pouze deduplikované rozdíly, replikace využívá kompresi.
Úložiště musí podporovat alespoň následující scénáře pro replikaci: 1:1, M:1 a kaskádovou replikaci.	Ano	Podpora 1:1, N:1 i kaskádové replikace.
Replikaci musí být možno spustit ve stejném čase jako zálohu bez dopadu na výkon zálohy.	Ano	Možnost spustit replikaci i v čase zálohy bez dopadu na výkon zálohy.
Úložiště musí umožnit řízení replikace v prostředí zálohovacího SW.	Ano	Uložiště umožňuje řízení replikace zálohovacím SW pomocí nativní funkce tzv. Clone Controlled Replica.
Úložiště musí umožnit funkcionalitu šifrování replikačního toku data-in-flight.	Ano	Uložiště nabízí šifrování dat inline a šifrování toku dat in-flight.
Úložiště musí podporovat replikaci dat do cloudu.	Ano	Úložiště podporuje replikaci dat do cloudu.

3.1.4. Spolehlivost, ochrana a obnova

Požadovaný parametr	**Splněno**	**Popis naplnění**
Úložiště musí disponovat interním algoritmem pro neustálou kontrolu zdraví uložených dat a v případě poškození jejich automatickou obnovu tak, aby bylo možno zálohy kdykoliv obnovit k jakémukoliv okamžiku.	Ano	Kontrola zdraví uložených dat a v případě poškození jejich automatická obnova je nativní vlastnost nabízeného systému. Tzv. „DIA" = Data Invulnerability Architecture.
Úložiště musí obnovovat data vždy z deduplikovaného a komprimovaného stavu, není přípustný mezikrok (např. externí disková cache).	Ano	Obnovuje se vždy z deduplikovaného a komprimovaného stavu, bez mezikroků.
Úložiště musí disponovat funkcionalitou pro šifrování ukládaných data metodou data-at-rest.	Ano	Uložiště disponuje funkcionalitou data-at-rest.
Úložiště je možné osadit HotSpare disky, počet hot-spare disků min. 1ks na každých 15 datových disků.	Ano	Jeden HotSpare disk na každých 12 disků v controlleru a jeden HotSpare disk na každých 15 disků v expanzních boxech.

Úložiště musí obsahovat kompletní verifikace dat – okamžitá verifikace záloh a kontrola integrity právě ukládaných dat.	Ano	Verifikace záloh a kontrola integrity v rámci „DIA" = Data Invulnerability Architecture.

3.1.5. Pokročilá ochrana dat (ochrana proti ransomware)

Požadovaný parametr	**Splněno**	**Popis naplnění**
Úložiště musí umožňovat šifrovat data a musí disponovat i nástroji pro správu klíčů.	Ano	Podpora šifrování i správy klíčů.
Úložiště musí umožňovat nastavit retenční lhůty uložených data, granulárně podle definovaných politik řízených zálohovacím SW.	Ano	Ochranné skartační lhůty funkcí Retention Lock, řízení granulárně ze zálohovacího SW.
Retenční zámek úložiště musí ochránit data před změnou, nebo smazáním před vypršením retenční lhůty.	Ano	Retention Lock chrání data před změnou, nebo smazáním před vypršením skartační lhůty.
Úložiště musí disponovat mechanismem ochrany dat a samotného úložiště před napadením útočníkem z prostředí objednavatele i mimo toto prostředí (např. hackerský útok, ransomware, apod.).	Ano	Na několika úrovních – architektura DIA, zabezpečený operační systém DDOS oddělený od zálohovaných dat, administrace oddělená od přístupu k zálohovaným datům, Cyber Recovery Vault, spolupodpis role Security Officer pro potenciálně destruktivní operace.
Úložiště musí umožnit tzv. HW hardening – tedy takové nastavení, aby nebylo možno jedním uživatelem s dostatečnými právy manipulovat s uloženými daty nebo systémovým nastavením (např. princip čtyř očí).	Ano	Pro potenciálně destruktivní operace je nutná spoluautorizace účtem typu „security officer", odlišného od účtu, který operaci provádí Účty „security officer" nemají samy o sobě administrátorská práva, je tedy vždy zapotřebí součinnosti dvou osob (účtů), tedy „čtyř očí".
Diskové úložiště musí být možno instalovat na separátním segmentu sítě, který je určen pouze pro replikaci dat pro ochranu proti ransomware. Tento segment musí být možno automaticky zpřístupnit pouze pro potřeby replikace dat a řízení tohoto přístupu bude probíhat nezávisle na zbytku běžné infrastruktury pro zálohování a obnovu z bezpečného místa prostřednictvím speciální management konzole.	Ano	Cyber Recovery Vault, zcela izolované prostředí bez možnosti aktivního přístupu z provozního prostředí a oddělenou, na zálohování nezávislou správou. Přístup do provozní sítě lze otevřít pouze z prostředí Vaultu, pouze pro deduplikovanou replikaci nových záloh (replikační komunikace je oddělená od ukládání dat či

		managementu zařízení), a pouze po dobu replikace, pak je opět uzavřen. Data v Cyber Recovery Vault jsou před každou replikací chráněna deduplikovanými snapshoty jako ochranou proti přepsání starších verzí záloh zašifrovanými daty. Správa je možná pouze z prostředí Cyber Recovery Vault pomocí na zálohování nezávislé konzole.
Úložiště musí být certifikováno podle SEC 17a-4f nebo ekvivalentní evropské nebo české normy.	Ano	Certifikace: • SEC 17a-4(f) • CFTC Rule 1.31b • FDA 21 CFR Part 11 • Sarbanes-Oxley Act • IRS 98025 and 97-22 • ISO Standard 15489-1 • MoREQ2010

3.1.6. Správa (management)

Požadovaný parametr	**Splněno**	**Popis naplnění**
Diskové úložiště musí umožnit správu prostřednictvím jednotného webového rozhraní.	Ano	Správa úložiště prostřednictvím jednotného webového rozhraní.
Diskové úložiště musí poskytovat funkcionalitu automatického reportingu, automatický call-home.	Ano	Automatický reporting a automatický call-home jsou součástí systému.
Diskové úložiště musí umožnit správu na principu rolí s různými typy oprávnění.	Ano	Možnost správy na principu rolí s různými typy oprávnění.
Diskové úložiště musí být plně kompatibilní se stávajícím zálohovacím systémem objednatele Dell DPS (podpora jednotné správy se stávajícími prvky).	Ano	Zařízení je plně kompatibilní se stávajícím zálohovacím systémem objednatele.

3.1.7. Záruka a podpora

Požadovaný parametr	**Splněno**	**Popis naplnění**
Záruka min. 5 let na kompletní HW, přístup k technické podpoře výrobce 24x7, max. odezva 4 hodiny. - Automatický call-home integrovaný se supportem, možnost automatického generování servisního incidentu.	Ano	Záruka s parametry dle zadání.

- Jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému - Neomezený přístup k HW a SW podpoře - Možnost stažení ovladačů a management software na webových stránkách - Zdarma přístup k integrovaným aktualizačním SW a FW balíkům		

3.2. Prodloužení technické podpory stávajících zálohovacích zařízení

Požadovaný parametr	**Splněno**	**Popis naplnění**
Prodloužení záruky a podpory od výrobce pro dva kusy stávajících zálohovacích zařízení Dell DataDomain 6300, minimálně do 1.8.2027 SN: CKM00193100436, CKM00193101088	Ano	Prodloužení záruky a podpory od výrobce pro zařízení SN CKM00193100436 a CKM00193101088 do 1.8.2027.
Záruka na kompletní HW, přístup k technické podpoře výrobce 24x7, max. odezva 4 hodiny. - Automatický call-home integrovaný se supportem, možnost automatického generování servisního incidentu. - Jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému - Neomezený přístup k HW a SW podpoře - Možnost stažení ovladačů a management software na webových stránkách - Zdarma přístup k integrovaným aktualizačním SW a FW balíkům	Ano	Záruka s parametry dle zadání.

3.3. Rozšíření počtu licencí stávajícího zálohovacího software

Požadovaný parametr	**Splněno**	**Popis naplnění**
Rozšíření počtu licencí stávajícího zálohovacího software DELL Data Protection Suite (NetWorker) o 10CPU licencí	Ano	10 CPU licencí DELL Data Protection Suite (NetWorker)
Záruka min. 5 let na nové SW licence, přístup k technické podpoře výrobce 24x7, max. odezva 4 hodiny. - Neomezený přístup k HW a SW podpoře - Možnost stažení ovladačů software na webových stránkách - Zdarma přístup k integrovaným aktualizačním SW balíkům	Ano	Záruka s parametry dle zadání.

3.4. Software pro zálohování Office365

Požadovaný parametr	Splněno	Popis naplnění
Výrobce a obchodní název nabízeného software	Ano	Storware Backup&Recovery for Microsoft 365.
Licence pro zálohování uživatelských dat Office 365 do on-premise.	Ano	Licence pro zálohování uživatelských dat Office 365 do on-premise.
Podpora zálohování Exchange Online (emaily, kontakty, kalendáře, eventy), OneDrive for Business (soubory), SharePoint Online a Microsoft Teams (týmové a 1:1 chaty, týmové dokumenty, knihovny, stránky – sites).	Ano	Podpora zálohování s parametry dle zadání.
Obnova dat po položkách (Item Level)	Ano	Obnova dat po položkách je podporována.
Obnova dat do Office365	Ano	Obnova dat do Office365 je podporována.
Ukládání dat na nově dodávaná deduplikační disková zálohovací úložiště.	Ano	Data ukládaná na nově dodávaná deduplikační disková zálohovací úložiště.
Záruka min. 5 let na nové SW licence, přístup k technické podpoře výrobce 24x7, max. odezva 4 hodiny. - Neomezený přístup k HW a SW podpoře - Možnost stažení ovladačů software na webových stránkách - Zdarma přístup k integrovaným aktualizačním SW balíkům	Ano	Záruka s parametry dle zadání.

3.5. Cyber Protection Management software

Cyber Protection Management software. Software, který poběží v oddělené „Cyber Protection" lokalitě, musí řídit operace v Cyber lokalitě a zajišťovat replikace bezpečných úložišť. Musí být postaven na zabezpečené architektuře a poskytovat následující funkce:

Požadovaný parametr	Splněno	Popis naplnění
Výrobce a obchodní název nabízeného software	Ano	DELL PowerProtect Cyber Recovery Manager
Cyber Protection Management Software pro správu replikačního propojení bezpečných úložišť, který povolí propojení pouze tehdy, pokud musí být přenesena/replikována nová data. Cyber Management software povolí nebo	Ano	Cyber Recovery Manager pro správu replikačního propojení bezpečných úložišť. Povolí propojení pouze tehdy, pokud musí být přenesena/replikována nová

zakáže replikační port a tedy i replikaci mezi bezpečnými úložišti.		data. Cyber Recovery Manager povolí nebo zakáže replikační port a tedy i replikaci mezi bezpečnými úložišti.
Uživatelské rozhraní založené na HTML5	Ano	Uživatelské rozhraní je založené na HTML5.
Implementace REST API	Ano	Software disponuje REST API.
Rozhraní příkazového řádku (CLI)	Ano	Je k dispozici rozhraní příkazového řádku (CLI).
Informační panely zobrazující systémové výstrahy a další důležité podrobnosti	Ano	Informační panely v administrátorském rozhraní zobrazují systémové výstrahy a další důležité podrobnosti.
Možnost přenášet výstrahy prostřednictvím SMTP do externích nástrojů nebo prostředí	Ano	Cyber Recovery Manager má možnost přenášet výstrahy prostřednictvím SMTP do externích nástrojů nebo prostředí.
Možnost vytváření a správy zásad a politik pro zacházení s daty, včetně jejich plánování	Ano	Možnost vytváření a správy zásad a politik pro zacházení s daty, včetně jejich plánování.
Pomoc při obnově a možnost snadného exportu dat do hosta pro obnovy	Ano	Pomoc při obnově a možnost snadného exportu dat do hosta pro obnovy.
Možnost automatického obnovení pro zálohovací software používaný objednavatelem (NetWorker)	Ano	Možnost automatického obnovení pro zálohovací software NetWorker.
Integrace s analytickým softwarem pro detekci kybernetických hrozeb (např. ransomware či hackerský útok), včetně plánování	Ano	Integrace s analytickým softwarem (CyberSense) pro detekci kybernetických hrozeb (např. ransomware či hackerský útok), včetně plánování.
SW licence bez omezení kapacity spravovaných dat v Cyber Protection lokalitě a podpora výrobce na celé prostředí pod dobu 5 let	Ano	Licence SW je bez omezení kapacity spravovaných dat v Cyber Protection lokalitě, je možná podpora výrobce na celé prostředí pod dobu 5 let.

3.6. Analytický Cyber Protection software

Analytický Cyber Protection software v Cyber lokalitě bude určený pro analýzu dat zálohovaných aplikací, sloužící ke kontrole, zda jsou chráněná data na bezpečném úložišti nezměněná a obnovitelná. Jakmile jsou data replikována do Cyber lokality, provede se analýza, aniž by byl

potřeba zálohovací software. Cyber Protection software provede analýzu, která by měla prozkoumat izolovaná data (soubory, databáze apod.), a aby odhalila neobvyklé chování, které by svědčilo o kybernetickém útoku. Toto chování zahrnuje poškození souborů, šifrování souborů nebo stránek v databázi nebo jejich odstranění a vytvoření.

Požadovaný parametr	**Splněno**	**Popis naplnění**
Výrobce a obchodní název nabízeného software	Ano	DELL CyberSense
Požadovaný SW musí být licenčně schopen pokrýt kontrolu 30TB zdrojových dat. Zároveň nesmí být jinak omezen např. počtem analýz apod.	Ano	Nabízená licence pokrývá kontrolu 30TB zdrojových dat. Není nijak omezena počtem analýz apod.
Schopnost prozkoumat izolovaná data (soubory, databáze apod.), aby odhalila neobvyklé chování, které by svědčilo o kybernetickém útoku. Toto chování zahrnuje poškození souborů, šifrování souborů nebo stránek v databázi nebo jejich odstranění a vytvoření.	Ano	CyberSense software má schopnost prozkoumat izolovaná data (soubory, databáze apod.), aby odhalila neobvyklé chování, které by svědčilo o kybernetickém útoku. Toto chování zahrnuje poškození souborů, šifrování souborů nebo stránek v databázi nebo jejich odstranění a vytvoření.
Schopnost opakovat zkoumání a porovnávat je s předchozími k zjištění, jak se data mění	Ano	CyberSense má schopnost opakovat zkoumání a porovnávat je s předchozími k zjištění, jak se data mění
Využívat statistik provedených analýz založených na obsahu (content-based) svědčících o poškození dat ransomwarem k rozpoznávání útoků	Ano	CyberSense umí využívat statistik provedených analýz založených na obsahu (content-based) svědčících o poškození dat ransomwarem k rozpoznávání útoků.
Využívat algoritmů strojového učení (machine learning), které byly vyškoleny na nejnovější hrozby ransomwaru, aby bylo možné učinit deterministické rozhodnutí, zda byla data napadena.	Ano	CyberSense umí využívat algoritmů strojového učení (machine learning), které byly vyškoleny na nejnovější hrozby ransomwaru, aby bylo možné učinit deterministické rozhodnutí, zda byla data napadena.
Nezávislost na databázi známých ransomware kódů dodávanou výrobcem a mít schopnost odhalit i zatím neznámé typy škodlivých útoků	Ano	CyberSense je nezávislý na databázi známých ransomware kódů dodávanou výrobcem a má schopnost odhalit i zatím neznámé typy škodlivých útoků.

Využívat forenzních nástrojů pro nalezení poškozených souborů a diagnostiku vektoru útoku	Ano	CyberSense umí využívat forenzních nástrojů pro nalezení poškozených souborů a diagnostiku vektoru útoku.
Poskytovat hlášení o uživatelském účtu, který poškození způsobil, aby bylo možné tento účet uzamknout, a také podat zprávu o aplikaci, která provedla změny v souboru.	Ano	CyberSense umí poskytovat hlášení o uživatelském účtu, který poškození způsobil, aby bylo možné tento účet uzamknout, a také podat zprávu o aplikaci, která provedla změny v souboru.
Schopnost určit poslední dobrou-čistou zálohu	Ano	CyberSense má schopnost určit poslední dobrou-čistou zálohu.
Schopnost obnovit a nahradit poškozené soubory poslední dobrou kopií.	Ano	CyberSense má schopnost obnovit a nahradit poškozené soubory poslední dobrou kopií.
Plná podpora a integrace se zálohovacím software používaný objednavatelem (NetWorker)	Ano	CyberSense má plnou podporu integrace se zálohovacím software NetWorker.
Podpora Backup clienta pro: OS Windows a Linux	Ano	Backup client pro OS Windows a Linux je podporovaný.
Podpora Backup clienta pro: Aplikace: Sharepoint, Exchange, MS-SQL, MySQL, Oracle, SAP HANA	Ano	Podpora backup clienta pro Sharepoint, Exchange, MS-SQL, MySQL a Oracle.
Podpora Backup clienta pro hypervizor: VMware	Ano	Podpora pro hypervisor VMware.
Podpora File System zálohy nativní Backup to disk (B2D) SQL, Oracle. Nestrukturované soubory, AD, LDAP, DNS.	Ano	Podpora filesystém zálohy backup to disk SQL, Oracle, nestrukturované soubory, AD, LDAP, DNS.
Požadovaný SW musí být schopen min. po dobu 5let aktualizace na nové verze, statistik, forenzních nástrojů, a zároveň musí mít zajištěnu podporu výrobcem.	Ano	CyberSense je schopen po dobu 5let aktualizace na nové verze, statistik, forenzních nástrojů, a mít zajištěnu podporu výrobcem.

3.7. Server pro správu Cyber Recovery Management

Požadovaný parametr	Splněno	Popis naplnění
Server pro správu Cyber Recovery Management – 1 ks		
Výrobce a obchodní název nabízeného zařízení	Ano	Dell PowerEdge R660
Provedení RACK – šíře 19”, 1U, 2CPU, 10x hot-swap HDD slot.	Ano	Provedení RACK – šíře 19”, 1U, 2CPU, 10x hot-swap HDD slot.

Příslušenství pro montáž do racku, vč. kabelového managementu umožňujícího vysunutí serveru za chodu, bez nutnosti odpojování napájecích a datových kabelů.	Ano	Příslušenství pro montáž do racku, vč. kabelového managementu umožňujícího vysunutí serveru za chodu, bez nutnosti odpojování napájecích a datových kabelů.
Operační paměť 128GB (4x 32GB RDIMM 5600MT/s)	Ano	Operační paměť 128GB (4x 32GB RDIMM 5600MT/s)
1x CPU 8C/16T min 2.6GHz, min. 23M Cache	Ano	1x CPU 8C/16T min 2.6GHz, 23M Cache
Disky pro OS 2x M.2 480GB SSD, v RAID 1 na dedikovaném řadiči (tyto disky nezabírají žádnou z požadovaných hot-swap pozic).	Ano	Disky pro OS 2x M.2 480GB SSD, v RAID 1 na dedikovaném řadiči (tyto disky nezabírají žádnou z požadovaných hot-swap pozic).
Disky pro data min. 3x 960GB SSD hot-swap, 3 DWPD, v RAID 5 na dedikovaném řadiči s 8GB cache.	Ano	Disky pro data 3x 960GB SSD hot-swap, 3 DWPD, v RAID 5 na dedikovaném řadiči s 8GB cache.
I/O Porty: - 2x 10/25GbE osazené SFP+ moduly - 2x 1GbE Base-T	Ano	I/O Porty: - 2x 10/25GbE osazené SFP+ moduly - 2x 1GbE Base-T
TPM 2.0	Ano	TPM 2.0
Napájecí zdroje v redundantní konfiguraci 1+1, hot-plug min. 1100W Titanium	Ano	Napájecí zdroje v redundantní konfiguraci 1+1, hot-plug 1100W Titanium
OOB management: - Server musí disponovat kompletním out-of-band managementem s dedikovaným LAN portem 1GbE RJ-45. - Interní web-GUI managementu pouze v HTML5, možnost ovládání pomocí CLI. - Management serveru nepožaduje instalaci agenta jak pro monitoring, tak pro update SW/FW/BIOS v jednotlivých HW komponentech serveru. - Podpora HW profilů. Podpora IPv6. - Podpora hromadné konfigurace více serverů pomocí XML souborů (z USB, nebo síťovým PXE bootem), hesla v takovém souboru musí být hashovaná proti zneužití (zero touch deployment). - Server musí umožňovat „lock-out" BIOSu a firmware jednotlivých komponent tak aby bylo zabráněno přepisu závadnou aktualizací.	Ano	OOB management s parametry dle zadání.

- Je požadována funkcionalita secure-erase (zabezpečené smazání veškerých dat na serveru a jeho komponentách po jeho vyřazení) - Základní deska či management serveru musí být vybaveny vlastním dedikovaným úložištěm pro umístění ovladačů potřebných pro instalaci OS, diagnostických nástrojů a také konfiguračních parametrů jednotlivých komponent pro případ výměny HW, aby nebylo nutné použití CD/DVD nebo jiných asistenčních médií. - Možnost nastavení parametrů a odečet stavu serverů a logů pomocí mobilního telefonu (Android, iOS), bez nutnosti kabelového připojení. - Součástí managementu serveru musí být vestavěná funkcionalita call-home (server musí být schopen automatizovaného předávání závad a otevírání servisních požadavku na helpdesk výrobce)		
Předinstalovaná image ESXi min. 8.0 na OS discích	Ano	Na serveru bude předinstalovaná image ESXi min. 8.0 na OS discích.
Součástí dodávky serveru budou licence VMware vSphere Standard, licencované dle dodaného CPU – s podporou na 5 let	Ano	Součástí dodávky serveru budou licence VMware vSphere Standard, licencované dle dodaného CPU, s podporou na 5 let.
Záruka min. 5 let na kompletní HW, přístup k technické podpoře výrobce 24x7, max. odezva 4 hodiny. - Automatický call-home integrovaný se supportem, možnost automatického generování servisního incidentu. - Jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému - Neomezený přístup k HW a SW podpoře - možnost stažení ovladačů a management software na webových stránkách - Zdarma přístup k integrovaným aktualizačním SW a FW balíkům	Ano	Záruka s parametry dle zadání.

3.8. Management server pro práci uvnitř Izolovaného prostředí

Požadovaný parametr	Splněno	Popis řešení požadavku
Management server pro práci uvnitř Izolovaného prostředí – 1 ks		
Výrobce a obchodní název nabízeného zařízení	Ano	Dell PowerEdge R660xs

Provedení RACK – šíře 19", 1U, 1CPU	Ano	Provedení RACK – šíře 19", 1U, 1CPU
Příslušenství pro montáž do racku, vč. kabelového managementu umožňujícího vysunutí serveru za chodu, bez nutnosti odpojování napájecích a datových kabelů.	Ano	Příslušenství pro montáž do racku, vč. kabelového managementu umožňujícího vysunutí serveru za chodu, bez nutnosti odpojování napájecích a datových kabelů.
Operační paměť 32GB (2x 16GB RDIMM 4800MT/s)	Ano	Operační paměť 32GB (2x 16GB RDIMM 4800MT/s)
1x CPU 8C/8T @ 1,8GHz, min. 22M Cache	Ano	1x CPU 8C/8T @ 1,8GHz, 22M Cache
Disky pro OS 2x 480 GB SSD, 3 DWPD, v RAID 1 na dedikovaném řadiči.	Ano	Disky pro OS 2x 480 GB SSD, 3 DWPD, v RAID 1 na dedikovaném řadiči.
I/O Porty: - 2x 10/25GbE osazené SFP+ moduly - 2x 1GbE Base-T	Ano	I/O Porty: - 2x 10/25GbE osazené SFP+ moduly - 2x 1GbE Base-T
TPM 2.0	Ano	TPM 2.0
Napájecí zdroje v redundantní konfiguraci 1+1, hot-plug. Min. 1100W Titanium	Ano	Napájecí zdroje v redundantní konfiguraci 1+1, hot-plug. 1100W Titanium
OOB management: - Server musí disponovat kompletním out-of-band managementem s dedikovaným LAN portem 1GbE RJ-45. - Interní web-GUI managementu pouze v HTML5, možnost ovládání pomocí CLI. - Management serveru nepožaduje instalaci agenta jak pro monitoring, tak pro update SW/FW/BIOS v jednotlivých HW komponentech serveru. - Podpora HW profilů. Podpora IPv6. - Podpora hromadné konfigurace více serverů pomocí XML souborů (z USB, nebo síťovým PXE bootem), hesla v takovém souboru musí být hashovaná proti zneužití (zero touch deployment). - Server musí umožňovat „lock-out" BIOSu a firmware jednotlivých komponent tak aby bylo zabráněno přepisu závadnou aktualizací. - Je požadována funkcionalita secure-erase (zabezpečené smazání veškerých dat na serveru a jeho komponentách po jeho vyřazení)	Ano	OOB management s parametry dle zadání.

- Základní deska či management serveru musí být vybaveny vlastním dedikovaným úložištěm pro umístění ovladačů potřebných pro instalaci OS, diagnostických nástrojů a také konfiguračních parametrů jednotlivých komponent pro případ výměny HW, aby nebylo nutné použití CD/DVD nebo jiných asistenčních médií. - Možnost nastavení parametrů a odečet stavu serverů a logů pomocí mobilního telefonu (Android, iOS), bez nutnosti kabelového připojení. - Součástí managementu serveru musí být vestavěná funkcionalita call-home (server musí být schopen automatizovaného předávání závad a otevírání servisních požadavku na helpdesk výrobce)		
Součástí serveru bude OS Windows Server 2022 Standard, 16CORE včetně medií + předinstalovaná image	Ano	Součástí serveru bude OS Windows Server 2022 Standard, 16CORE včetně medií + předinstalovaná image
Záruka min. 5 let na kompletní HW, přístup k technické podpoře výrobce 24x7, max. odezva 4 hodiny. - Automatický call-home integrovaný se supportem, možnost automatického generování servisního incidentu. - Jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému - Neomezený přístup k HW a SW podpoře - možnost stažení ovladačů a management software na webových stránkách - Zdarma přístup k integrovaným aktualizačním SW a FW balíkům	Ano	Záruka s parametry dle zadání.

3.9. Server pro automatizovanou analýzu záloh

Požadovaný parametr	Splněno	Popis řešení požadavku
Server pro automatizovanou analýzu záloh – 1 ks		
Výrobce a obchodní název nabízeného zařízení	Ano	DELL PowerEdge R660
Provedení RACK – šíře 19”, 1U, 2CPU, 10x hot-swap HDD slot.	Ano	Provedení RACK – šíře 19”, 1U, 2CPU, 10x hot-swap HDD slot.
Příslušenství pro montáž do racku, vč. kabelového managementu umožňujícího vysunutí serveru za chodu, bez nutnosti odpojování napájecích a datových kabelů.	Ano	Příslušenství pro montáž do racku, vč. kabelového managementu umožňujícího vysunutí serveru za

		chodu, bez nutnosti odpojování napájecích a datových kabelů.
Operační paměť 256GB (min. 16x16GB RDIMM 5600MTMT/s)	Ano	Operační paměť 256GB (16x16GB RDIMM 5600MTMT/s)
2x CPU 12C/24T @ 2,4GHz, min. 30M Cache	Ano	2x CPU 12C/24T @ 2,4GHz, 30M Cache
Disky pro OS 2x M.2 480GB SSD, v RAID 1 na dedikovaném řadiči (tyto disky nezabírají žádnou z požadovaných hot-swap pozic).	Ano	Disky pro OS 2x M.2 480GB SSD, v RAID 1 na dedikovaném řadiči (tyto disky nezabírají žádnou z požadovaných hot-swap pozic).
Disky pro data min. 5x 3.2TB SSD hot-swap, v RAID 5 na dedikovaném řadiči s 8GB cache.	Ano	Disky pro data 5x 3.2TB SSD hot-swap, v RAID 5 na dedikovaném řadiči s 8GB cache.
I/O Porty: - 2x 10/25GbE osazené SFP+ moduly - 2x 10GbE Base-T	Ano	I/O Porty: - 2x 10/25GbE osazené SFP+ moduly - 2x 10GbE Base-T
TPM 2.0	Ano	TPM 2.0
Napájecí zdroje v redundantní konfiguraci 1+1, hot-plug min. 1800W Titanium	Ano	Napájecí zdroje v redundantní konfiguraci 1+1, hot-plug. 1800W Titanium
OOB management: - Server musí disponovat kompletním out-of-band managementem s dedikovaným LAN portem 1GbE RJ-45. - Interní web-GUI managementu pouze v HTML5, možnost ovládání pomocí CLI. - Management serveru nepožaduje instalaci agenta jak pro monitoring, tak pro update SW/FW/BIOS v jednotlivých HW komponentech serveru. - Podpora HW profilů. Podpora IPv6. - Podpora hromadné konfigurace více serverů pomocí XML souborů (z USB, nebo síťovým PXE bootem), hesla v takovém souboru musí být hashovaná proti zneužití (zero touch deployment). - Server musí umožňovat „lock-out" BIOSu a firmware jednotlivých komponent tak aby bylo zabráněno přepisu závadnou aktualizací. - Je požadována funkcionalita secure-erase (zabezpečené smazání veškerých dat na	Ano	OOB management s parametry dle zadání.

serveru a jeho komponentách po jeho vyřazení) - Základní deska či management serveru musí být vybaveny vlastním dedikovaným úložištěm pro umístění ovladačů potřebných pro instalaci OS, diagnostických nástrojů a také konfiguračních parametrů jednotlivých komponent pro případ výměny HW, aby nebylo nutné použití CD/DVD nebo jiných asistenčních médií. - Možnost nastavení parametrů a odečet stavu serverů a logů pomocí mobilního telefonu (Android, iOS), bez nutnosti kabelového připojení. - Součástí managementu serveru musí být vestavěná funkcionalita call-home (server musí být schopen automatizovaného předávání závad a otevírání servisních požadavku na helpdesk výrobce)		
Předinstalovaná image ESXi na OS discích	Ano	Na serveru bude předinstalovaná image ESXi (v8.0) na OS discích.
Součástí dodávky serveru budou licence VMware vSphere Standard, licencované dle dodaného CPU – s podporou na 5 let	Ano	Součástí dodávky serveru budou licence VMware vSphere Standard, licencované dle dodaného CPU, s podporou na 5 let.
Záruka min. 5 let na kompletní HW, přístup k technické podpoře výrobce 24x7, max. odezva 4 hodiny. - Automatický call-home integrovaný se supportem, možnost automatického generování servisního incidentu. - Jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému - Neomezený přístup k HW a SW podpoře - možnost stažení ovladačů a management software na webových stránkách - Zdarma přístup k integrovaným aktualizačním SW a FW balíkům	Ano	Záruka s parametry dle zadání.

3.10. Síťový jednosměrný komunikační prvek (typu DataDiode)

Požadovaný parametr	Splněno	Popis řešení požadavku
Jednosměrný komunikační prvek typu DataDiode – 1 ks		
Výrobce a obchodní název nabízeného zařízení	Ano	DELL/Owl Cyber Defence OPDS-1000
Jednosměrný komunikační prvek (DataDiode), určený pro bezpečné přenášení stavových	Ano	Jednosměrný komunikační prvek typu DataDiode, určený pro

informací a logů do systému centrálního dohledu o minimální kapacitě portů 1GbE		bezpečné přenášení stavových informací a logů do systému centrálního dohledu. Kapacita portů 1GbE.
Požadované protokoly: Email (SMTP), SNMP Traps, Syslog	Ano	Email (SMTP), SNMP Traps, Syslog
Interní zabezpečení: RBAC – podpora pro dlouhá hesla Zabezpečení proti neoprávněné manipulaci – pravidelná kontrola, zda systém neobsahuje žádné změny souborů, pokud dojde k neoprávněné manipulaci, automaticky se vypne. Systém interních logů a varování pro sledování a audit veškeré aktivity. Management porty oddělené od portů pro přenos dat	Ano	Zabezpečení dle zadání. - RBAC - Kontrola integrity - Interní logy a audit - Oddělené management porty
max. 1U včetně příslušenství pro snadnou montáž do standardního 19" racku	Ano	Výška 1U včetně příslušenství do 19" racku.
Min. 2x 1GbE RJ-45 datové I/O porty	Ano	2x 1GbE RJ-45 datové I/O porty
Min. 2x 1GbE RJ-45 admin I/O porty	Ano	2x 1GbE RJ-45 admin I/O porty
Administrace možná pouze přes admin I/O porty rozdílné od datových portů.	Ano	Administrace je možná pouze přes oddělené admin I/O porty, rozdílné od datových portů.
Technická podpora a servis na 5 let s reakční dobou NBD, jediné kontaktní místo pro hlášení poruch pro všechny komponenty dodávaného systému včetně SW dodávaného se zařízením od výrobce Technická podpora a servis je poskytován výrobcem HW. Dostupnost technické podpory na telefonu min. v pracovní dny. Možnost nahlášení požadavku podpory 24x7.	Ano	Technická podpora a servis s parametry dle zadání.

Zdarma možnost stažení ovladačů a Firmware ze stránek výrobce pro konkrétní HW, po zadání jedinečného identifikátoru		

3.11. Příslušenství

Požadovaný parametr	Splněno	Popis řešení požadavku
KVM přepínač – 1ks		
Výrobce a obchodní název nabízeného zařízení	Ano	DELL KVM/KMM
Digitální KVM přepínač, 8 portů, vč. 19" KMM LCD a zabudované klávesnice	Ano	Digitální KVM přepínač, 8 portů, vč. 19" KMM LCD a zabudované klávesnice.
Provedení RACK – šíře 19", 1U	Ano	Provedení RACK – šíře 19", 1U
Kompatibilita I/O portů s Cyber Recovery servery	Ano	Kompatibilita I/O portů s Cyber Recovery servery.
Příslušenství: - 4ks SIP kabel - 1ks SIP kabel pro přístup k rozhraní sériových konzolí aktivních prvků	Ano	Příslušenství: - 4ks SIP kabel - 1ks SIP kabel pro přístup k rozhraní sériových konzolí aktivních prvků
Záruka min. 5let s reakční dobou NBD na kompletní HW, přístup k technické podpoře výrobce 24x7. Servis/výměna následující pracovní den. Možnost stažení ovladačů a management software na webových stránkách Zdarma přístup k integrovaným aktualizačním SW a FW balíkům.	Ano	Záruka s parametry dle zadání.

4. Společné obecné požadavky

Požadovaný parametr	Hodnota	Popis řešení požadavku
Obecné požadavky		
Veškeré nabízené zboží, i jeho části, musí být originální, nově vyrobené, nepoužité, určené pro český trh a Objednavatele. V databázi výrobce, pokud taková existuje, musí být Objednavatel veden jako první uživatel zboží.	Ano	Veškeré nabízené zboží, i jeho části, bude originální, nově vyrobené, nepoužité, určené pro český trh a Objednavatele. Zboží bude v databázi výrobce registrované na Objednatele jako na prvního uživatele.

Je-li součástí produktů SW či FW, pak se musí jednat o verze, které jsou standardní, běžně dostupné a určené k produkčnímu použití. Není dovoleno použití beta verzí, neoficiálních verzí ani SW/FW se zákaznickými úpravami.	Ano	Verze SW a FW, jsou standardní, běžně dostupné a určené k produkčnímu použití. Nebude použito beta verzí, neoficiálních verzí ani SW/FW se zákaznickými úpravami.
Pro dodávané HW komponenty uchazeč v nabídce doloží, že komponenty obsahují software výrobce s platnou licencí a dodávané komponenty splňují podmínky servisní podpory výrobce	Ano	Software pro HW komponenty bude předán s platnou licencí a dodávané komponenty budou ověřitelně splňovat podmínky servisní podpory výrobce.
Nabízené zboží musí být pokryto oficiální podporou výrobce tak, aby v případě závady, kterou není Dodavatel schopen odstranit, mohl Objednavatel tuto závadu eskalovat přímo k technické podpoře výrobce zařízení. Objednavatel musí mít možnost si sám legálně stahovat bezpečnostní záplaty i nové verze SW/FW přímo ze stránek výrobce, na základě zaregistrování čísla aktivovaného servisního kontraktu.	Ano	Podpora výrobce pro Objednatele dle zadání.
Soulad s výše uvedenými skutečnostmi Dodavatel doloží prohlášením, které bude potvrzeno oficiálním zastoupením výrobce v ČR či EU.	Ano	Bude doloženo v době podpisu smlouvy (výrobce potvrdí konkrétní zboží z objednávky registrované na Objednatele). Případně čestným prohlášením zástupce výrobce před objednáním.
Dodávané komponenty budou licencované jménem objednavatele tak, aby bylo možné eskalovat případné závady na technickou podporu výrobce.	Ano	Dodávané komponenty budou licencované jménem objednavatele tak, aby bylo možné eskalovat případné závady na technickou podporu výrobce.
Akceptační testy budou provedeny před předáním díla do rutinního provozu	Ano	Akceptační testy budou provedeny před předáním díla do rutinního provozu.
Testy provede dodavatel ve spolupráci s pracovníky objednavatele za stejných podmínek, za jakých bude pracovat dílo v rutinním provozu	Ano	Testy provede dodavatel ve spolupráci s pracovníky objednavatele za stejných podmínek, za jakých bude pracovat dílo v rutinním provozu.

5. Implementace

Součástí implementace bude dodávka a zapojení řešení dle schématu v kapitole Předmět plnění, a kompletní zprovoznění nabízeného řešení do plně funkčního a provozuschopného stavu.
Jedná se zejména o kompletní sestavení, montáž, instalaci, zahoření, propojení a konfiguraci všech HW prvků, včetně jejich propojení se stávající HW infrastrukturou objednavatele. Dále instalaci, implementaci a konfiguraci veškerých dodávaných SW, včetně jeho propojení se stávající SW infrastrukturou objednatele, pokud bude potřeba. Vše dle doporučení a standardů výrobců dodaného HW a SW, dále odzkoušení bezchybného propojení a komunikace nového HW a SW. Ověření plné funkčnosti celého řešení formou 1měsíčního zkušebního provozu a řádné proškolení administrátorů.

Implementace bude dále zahrnovat tyto činnosti:

- provedení akceptačních testů, předání do zkušebního provozu a následně předání infrastruktury do ostrého provozu (obě předání proběhnou oproti akceptačního protokolu)

- zpracování a poskytnutí dokumentace skutečného stavu včetně schématu zapojení, dokumentace parametrů, konfigurací a nastavení hodnot a poskytnutí všech hesel a přístupů ve standardním editovatelném formátu (docx, rtf, apod.). V dokumentaci bude uveden stručný návod na aktualizaci firmware, postupy pro obnovení dat z nově dodaného řešení a manipulaci s analýzou záloh nově dodávaného řešení, včetně portálů a servisních účtů, přes který lze získat jednotlivé firmware. Dále kontakty pro případné reklamační a servisní požadavky.

- veškerá dokumentace a příručky se po předání zadavateli stávají jeho majetkem a může s nimi nakládat dle svých potřeb.

- školení bude probíhat v místě plnění nebo online pomocí videokonference v rozsahu min. 2x4 hodiny potřebném pro provoz a údržbu systému (ukázka, popis a vysvětlení jednotlivých částí systémů, vysvětlení stávající konfigurace atd.). Školení se dle předpokladu zúčastní 3 zaměstnanci zadavatele (k dispozici je školící místnost s prezentační technikou v místě plnění).

- náklady na implementaci musí být zahrnuty v nabídkové ceně

5.1. Realizační projekt

Dodavatel zpracuje a předloží ke schválení Realizační projekt, který bude podrobně popisovat kroky nutné pro implementaci navrženého řešení. Součástí projektu bude návrh akceptačních testů pro ověření funkčnosti dodaného řešení. Akceptace Realizačního projektu Objednavatelem je podmínkou pro realizaci dalších etap projektu.

5.2. Rozsah implementace

Součástí dodávky musí být kompletní instalace všech dodaných komponent. Jedná se zejména o:

Požadovaný parametr	Splněno	Popis řešení požadavku
Vytvoření realizačního projektu	Ano	Ano, nabídka obsahuje tuto službu.
Doprava zboží, likvidace obalů	Ano	Ano, nabídka obsahuje tuto službu.
Instalace HW do racků	Ano	Ano, nabídka obsahuje tuto službu.
Oživení, aktualizace firmware	Ano	Ano, nabídka obsahuje tuto službu.
Konfigurace sítí, konfigurace OOB managementu	Ano	Ano, nabídka obsahuje tuto službu.

Instalace a konfigurace nových datových úložišť	Ano	Ano, nabídka obsahuje tuto službu.
Migrace záloh ze stávajících zálohovacích úložišť na nově dodávaná úložiště	Ano	Ano, nabídka obsahuje tuto službu.
Rekonfigurace stávajících zálohovacích úložišť pro použití v „Cyber Protection" lokalitě, nastavení replikací mezi „Produkční" a „Cyber Protection" lokalitou	Ano	Ano, nabídka obsahuje tuto službu.
Instalace a konfigurace veškerého dodaného SW v produkční lokalitě: • Software pro zálohování Office365	Ano	Ano, nabídka obsahuje tuto službu.
Vytvoření politik pro zálohování Office365	Ano	Ano, nabídka obsahuje tuto službu.
Instalace a konfigurace veškerého dodaného SW • VMware vSphere (vCenter + ESXi) • Windows Server • Cyber Protection Management Software • Analytický Cyber Protection software	Ano	Ano, nabídka obsahuje tuto službu.
Vygenerování/registrace licencí veškerého dodaného software	Ano	Ano, nabídka obsahuje tuto službu.
Vytvoření politik v Cyber Protection Management software	Ano	Ano, nabídka obsahuje tuto službu.
Integrace Cyber Protection Management software a Analytického Cyber Protection software	Ano	Ano, nabídka obsahuje tuto službu.
Nastavení DataDiode pro odesílání notifikací z „Cyber Protection" prostředí	Ano	Ano, nabídka obsahuje tuto službu.
Nastavení odesílání notifikací na všech komponentech	Ano	Ano, nabídka obsahuje tuto službu.
Pilotní provoz	Ano	Ano, nabídka obsahuje tuto službu.
Akceptační testy	Ano	Ano, nabídka obsahuje tuto službu.
Zaškolení obsluhy pro všechny dodávané komponenty	Ano	Ano, nabídka obsahuje tuto službu.

Zpracování technické dokumentace v českém jazyce	Ano	Ano, nabídka obsahuje tuto službu.

6. Technická podpora řešení

Součástí dodávky bude technická podpora Dodavatele, poskytovaná po dobu pěti let.

6.1. Předmět podpory

Dodané zálohovací řešení včetně "Cyber Protection" části.

- podpora bude poskytovaná v českém jazyce
- 2x ročně profylaktická kontrola a opatchování dodaného řešení na základě zaslaných požadavků objednavatele (upgrade v rámci stejné verze)
- 6 člověkodnů za rok na konzultační činnosti
- administrace a správa prostředí v jednotkách požadavků měsíčně (max. 10 objednávek/měsíc)
- řešení chyb na vyžádání objednavatele
- SLA 5x9 NBD (dostupnost v pracovní dny a pracovní hodiny 8-17 hod.)

7. Plán implementace a odstávek, termíny

Všechny části navrhovaného řešení musí být dodány nejpozději do 3. měsíců od data zveřejnění smlouvy v registru smluv. Implementační práce musí být dokončeny nejpozději 1 měsíc po dodání navrhovaného řešení. Po měsíční implementační době začne měsíční pilotní provoz, po kterém dojde k podepsání akceptačních protokolů.

Bezodstávkové instalace a konfigurace můžou probíhat za provozu. Práce, které vyžadují odstávku je možno provádět po pracovní době. Veškeré práce musí probíhat po předešlé domluvě.

Odstávky je možno provádět po domluvě v těchto časech:

- pondělí a středa od 17:00 do 19:00
- úterý a pátek od 14:00 do 19:00
- čtvrtek od 15:00 do 19:00
- odstávky po 19 hod. a o víkendu je možno realizovat po individuální domluvě