KUPNÍ SMLOUVA

uzavřená níže uvedeného dne, měsíce a roku

dle ustanovení § 2079 a násl. a § 2085 a násl. zákona č. 89/2012 Sb., Občanského zákoníku

1. Smluvní strany

Kupující: **Město Rakovník**

Sídlo: Husovo náměstí 27, 269 01 Rakovník

IČ: 00244309

DIČ: CZ00244309

Zastoupený: PaedDr. Luďkem Štíbrem, starostou města

Kontaktní osoba: [redacted] vedoucí odboru vnitřních věcí

Bankovní spojení: Československá obchodní banka, a.s.

Číslo účtu: [redacted]

jako kupující, na straně jedné

(dále jen kupující)

a

Prodávající: **Aricoma Systems a.s.**

Sídlo: **Hornopolní 3322/34, Moravská Ostrava, 702 00 Ostrava**

IČ: **04308697**

DIČ: **CZ04308697**

Zastoupený/Jednající: **Jaroslav Dvořák**

Kontaktní osoba: [redacted]

Bankovní spojení: **Česká spořitelna a.s.**

Číslo účtu: [redacted]

Zápis v OR: **vedeném u rejstříkového soudu v Ostravě, spisová značka B 11012/KSOS**

jako prodávající na straně druhé

(dále jen prodávající)

2. Úvodní ustanovení

2.1. Tato smlouva je uzavírána v návaznosti na veřejnou zakázku s názvem „Dodávka IT infrastruktury a licencí“, zadávanou zadavatelem.

2.2. Technická specifikace kupujícího (zadavatele) k veřejné zakázce a technická specifikace z nabídky prodávajícího tvoří nedílnou součást této smlouvy jako její přílohy.

3. Vlastnické vztahy

3.1. Prodávající prohlašuje, že je výlučným vlastníkem předmětu plnění smlouvy a jeho příslušenství, které je předmětem plnění této smlouvy.

3.2. Detailní technická specifikace předmětu plnění této smlouvy a počtu kusů jednotlivého zboží a jeho příslušenství je obsažena v příloze č. 1, č. 2 a č. 3 této smlouvy a je její nedílnou součástí. V případě rozporu vzniklého mezi přílohami č. 1 a 2 této smlouvy v podobě technické specifikace platí vždy specifikace kupujícího obsažená v příloze č. 1 této smlouvy.

4. Předmět smlouvy

4.1. Předmětem této smlouvy je hmotný majetek v podobě zařízení a nehmotný majetek v podobě licencí, obojí včetně příslušenství. Předmět smlouvy je detailně specifikován v příloze č. 1 a č. 3 této smlouvy, včetně příslušenství. Prodávající je tímto povinen odevzdat kupujícímu zařízení a licence, která jsou předmětem této smlouvy a umožnit mu nabytí vlastnického práva k nim a současně závazek kupujícího zařízení převzít a zaplatit za ně prodávajícímu kupní cenu.

4.2. Součástí předmětu plnění jsou dále služby a práce prodávajícího se zařízeními přímo související a nezbytné k řádnému uvedení předmětu plnění do provozu, které jsou blíže specifikovány v příloze č. 1 této smlouvy. Bez provedení těchto služeb a prací nebude možné považovat předmět koupě za řádně dodaný.

4.3. Prodávající se zavazuje dodat předmět smlouvy kupujícímu s veškerými doklady nutnými k převzetí a zejména k užívání dodaných zařízení a software a provést všechny požadované související služby a práce.

4.4. Prodávající touto smlouvou prodává kupujícímu do výlučného vlastnictví předmět kupní smlouvy definovaný v bodě 4.1 a to včetně příslušenství.

4.5. Kupující předmět plnění této smlouvy, jímž jsou věci nové a nepoužité, kupuje za dohodnutou kupní cenu a přijímá do svého výlučného vlastnictví.

4.6. Prodávající prohlašuje, že neví ke dni podpisu této kupní smlouvy o žádných vadách prodávaných movitých věcí, na které by kupujícího upozornil.

5. Licence

5.1. Prodávající v rámci plnění předmětu této smlouvy dodává software podléhající ochraně podle zákona č. 121/2000 Sb. (autorský zákon) a ustanovení § 2358 a následující zákona č. 89/2012, občanského zákoníku, proto poskytuje kupujícímu licenci (tj. oprávnění k výkonu práva duševního vlastnictví (licenci) v ujednaném rozsahu), a to formou licenčního ujednání v této kupní smlouvě. Prodávající prohlašuje, že se jedná o licenci:

a. nevýhradní licenci k veškerým známým způsobům užití takového software, a to v rozsahu minimálně nezbytném pro řádné užívání software kupujícím;
b. licenci neomezenou územním či množstevním rozsahem (není-li v této smlouvě uvedeno jinak) a rovněž tak neomezenou způsobem nebo rozsahem užití;
c. licenci udělenou na dobu určitou, tedy po dobu držení vlastnických práv,
d. licenci převoditelnou a postupitelnou, tj. která je udělena s právem postoupení licence třetí osobě
e. licenci, kterou není kupující povinen využít.

5.2. Licence je poskytnutá v maximálním rozsahu povoleném platnými právními předpisy.

5.3. Prodávající prohlašuje, že odměna za poskytnutí licence kupujícímu je již zahrnuta v kupní ceně za poskytnuté plnění dle této kupní smlouvy.

6. Kupní cena a platební podmínky

6.1. Kupní cena je nabídkovou cenou předloženou prodávajícím v jeho nabídce na veřejnou zakázku uvedenou v článku 2.1 této smlouvy, přičemž se skládá z ceny dodávky jednotlivých zařízení a licencí.

6.2. Kupující se zavazuje zaplatit prodávajícímu za předmět spočívající v dodávce plnění uvedený v 4 této smlouvy kupní cenu ve výši

8 785 800 Kč bez DPH,

tj. 10 630 818 Kč včetně DPH,

když DPH ve výši 21 % činí 1 845 018 Kč.

6.3. Kupní cena je stanovena jako cena konečná a úplná, zahrnuje veškeré dodávky a služby s dodávkami související a veškeré jiné náklady nezbytné pro řádnou a úplnou realizaci předmětu plnění této smlouvy včetně všech rizik a vlivů s plněním předmětu této smlouvy souvisejících. Kompletní skladba kupní ceny a její rozklad je obsažen v příloze č. 3 této smlouvy.

6.4. Prodávající není oprávněn požadovat po kupujícím poskytnutí zálohy.

6.5. Prodávající na sebe bere odpovědnost za to, že sazba a výše daně z přidané hodnoty bude stanovena v souladu s platnými právními předpisy. V případě, že dojde mezi dnem podpisu kupní smlouvy a dnem uskutečnění zdanitelného plnění ke změně sazby DPH podle zákona č. 235/2004 Sb., o dani z přidané hodnoty, bude daň z přidané hodnoty připočtena ke kupní ceně ve výši dle právní úpravy platné ke dni uskutečnění zdanitelného plnění.

6.6. Kupní cenu zaplatí kupující prodávajícímu bankovním převodem na bankovní účet prodávajícího uveden v článku 1 této smlouvy na základě daňového dokladu (faktury) vystaveného prodávajícím ke dni uskutečnění zdanitelného plnění, který je dnem podepsání předávacího protokolu na předmět plnění dle této smlouvy. Daňový doklad je považován za proplacený okamžikem odepsání příslušné částky z účtu kupujícího ve prospěch účtu prodávajícího.

6.7. Prodávající na základě svého práva vystavit daňový doklad (fakturu) vystaví samostatnou fakturu za předmět koupě dle této smlouvy.

6.8. Na daňovém dokladu (faktuře) bude uveden rozklad fakturované částky na jednotlivá zařízení, tak aby byla zřejmá cena jednotlivých zařízení, a tak aby bylo kupujícímu usnadněno zavedení do majetkové evidence. Součástí daňového dokladu rovněž musí být název projektu *„Zvýšení kybernetické bezpečnosti města Rakovník“* a číslo projektu CZ.06.01.01/00/22_004/0000225.

6.9. Splatnost daňového dokladu je 30 dnů ode dne jeho doručení kupujícímu.

6.10. Daňový doklad bude obsahovat náležitosti daňového a účetního dokladu podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, bude mít náležitosti obchodní listiny dle § 435 zákona č. 89/2012 Sb., občanského zákoníku. V případě, že daňový doklad takové náležitosti nebude splňovat, bude kupujícím vrácen do dne splatnosti daňového dokladu k opravení bez jeho proplacení. V takovém případě lhůta splatnosti počíná běžet znovu ode dne doručení opraveného či nového vyhotovení daňového dokladu.

6.11. Pro případ, že prodávající je, nebo se od data uzavření smlouvy do dne uskutečnění zdanitelného plnění stane na základě rozhodnutí správce daně „nespolehlivým plátcem“ ve smyslu ustanovení § 106a zákona č. 235/2004 Sb., o DPH, ve znění pozdějších předpisů, souhlasí prodávající s tím, že mu kupující uhradí cenu plnění bez DPH a DPH v příslušné výši odvede za nespolehlivého plátce přímo příslušnému správci daně. V souvislosti s tímto ujednáním nebude prodávající vymáhat od kupujícího část z ceny plnění rovnající se výši odvedeného DPH a souhlasí s tím, že tímto bude uhrazena část jeho pohledávky, kterou má vůči kupujícímu, a to ve výši rovnající se výši odvedené DPH.

7. Předání a převzetí věci a vlastnické právo

7.1. Prodávající předá kupujícímu předmět plnění této smlouvy nejpozději do 25 týdnů od nabytí účinnosti této smlouvy, a to včetně realizace všech souvisejících služeb. Bez dodávky příslušenství a realizovaného požadovaného rozsahu služeb nebude možné ze strany kupujícího považovat předmětu plnění za realizovaný a předmět koupě nebude z jeho strany možné převzít.

7.2. Místem dodání a předání předmětu plnění této smlouvy je uvedeno v příloze č. 1 této smlouvy. Před dodávkou zařízení je prodávající povinen vyzvat kontaktní osobu kupujícího k potvrzení rozdělení jednotlivých dodávek mezi jednotlivé lokality uvedené v předmětné příloze, do kterých bude docházet k instalaci jednotlivých zařízení, přičemž předpokladu umístění zařízení do jednotlivých lokalit je již uveden v příloze č. 1 této smlouvy.

7.3. Vlastnické právo k předmětu plnění přechází na kupujícího v okamžiku jeho předání prodávajícím a převzetí kupujícím potvrzeného na předávacím protokolu.

7.4. Nebezpečí nahodilé zkázy a nahodilého zhoršení vlastností předmětu plnění včetně užitku přechází na kupujícího současně s nabytím vlastnictví.

7.5. Náklady spojené s předáním předmětu plnění, zejména dopravu, nese prodávající a náklady spojené s převzetím nese kupující.

7.6. O předání a převzetí předmětu plnění a souvisejících dokladů bude sepsán předávací protokol podepsaný zástupci obou smluvních stran. Za kupujícího je předávací protokol oprávněn podepsat a předmět plnění převzít kontaktní osoba kupujícího uvedená v článku 1. této smlouvy.

8. Součinnost

8.1. Kupující požaduje, aby maximum prací odvedl prodávající samostatně, bez zatěžování pracovníků kupujícího. Součinnost kupujícího bude omezena na nezbytnou míru a bude se vztahovat především na schvalování výstupů prodávajícího v předem definovaných kontrolních dnech a na nezbytnou IT podporu nutnou k nasazení technologií.

8.2. Rozsah součinnosti bude odsouhlasen před zahájením implementačních a instalačních služeb, včetně termínů jejího poskytování.

8.3. V případě následného požadavku prodávajícího na součinnost nad dohodnutý rámec má kupující právo součinnost odmítnout, případně ji poskytnout v termínu a rozsahu dle svých možností, a to bez dopadu na harmonogram realizace a z něj vyplývající sankce za nedodržení termínů.

8.4. Neposkytnutí součinnosti jako důvod pro posun smluvních termínů bude akceptován pouze tam, kde byla součinnost kupujícím přislíbena při zahájení implementačních a instalačních prací.

9. Projektový tým (seznam techniků)

9.1. Prodávající se zavazuje předmět plnění smlouvy realizovat prostřednictvím projektového týmu (seznamu techniků), kterým prokázal kvalifikaci ve veřejné zakázce, na jejímž základě je uzavírána tato smlouva. Projektový tým (seznam techniků) prodávajícího je odpovědný za plnění této smlouvy.

9.2. Prodávající se zavazuje realizovat předmět plnění této smlouvy prostřednictvím projektového týmu (seznamu techniků) v tomto složení na těchto pozicích:

Projektový manažer - 

Technický specialista – software Microsoft - 

Technický specialista – serverové virtualizace VMware - 

Technický specialista – zálohování - 

Technický specialista – datových úložišť - 

Technický specialista – síťových technologií - 

Technický specialista – logování - 

9.3. Změna konkrétní osoby na pozici člena projektového týmu prodávajícího je možná pouze za předpokladu prokázání potřebné kvalifikace novou osobou v rozsahu stanoveném pro danou pozici člena projektového týmu stanovenou ve veřejné zakázce, na jejímž základě je uzavřena tato smlouva. Taková změna musí být prodávajícím řádně iniciována, písemně dokladována a prokázána kvalifikace nové osoby na pozici člena projektového týmu před jeho zapojením do realizace plnění dle této smlouvy (včetně všech souvisejících požadavků na projektový tým stanovený v zadávacích podmínkách, na jejichž základě je uzavřena tato smlouva, jako např. max. počet pozic obsazených jednou osobou apod.).

10. Další práva a povinnosti smluvních stran

10.1. Prodávající se zavazuje zaslat seznam sériových čísel dodaných zařízení a MAC adres síťových karet, a to v elektronické podobě na e-mail kontaktní osoby kupujícího nejpozději do 1 týdne od realizace dodávky.

10.2. Prodávající se dále zavazuje předat kupujícímu listinné potvrzení dodaných licencí, které jsou předmětem plnění této kupní smlouvy.

10.3. Prodávající se zavazuje v rámci realizace plnění dodržovat veškeré předpisy a normy v oblasti kybernetické bezpečnosti blíže uvedené v příloze č. 1 této smlouvy a její kapitole kybernetická bezpečnost.

10.4. Prodávající je povinen zajistit i veškerá bezpečnostní opatření na ochranu osob a majetku v areálu kupujícího, jsou-li tato dotčena dodáním zboží prodávajícího.

10.5. Prodávající je povinen k náhradě újmy způsobené činností svých poddodavatelů.

10.6. Prodávající je povinen k náhradě újmy způsobné okolnostmi, které mají důvod v povaze strojů, přístrojů nebo jiných věcí, které prodávající použil.

10.7. Smluvní strany sjednávají, že prodávající není oprávněn započíst si jakoukoliv svoji peněžitou pohledávku za kupujícím, a to ani část své pohledávky, včetně pohledávek získaných postoupením, vůči jakékoliv peněžité pohledávce kupujícího za prodávajícím.

10.8. Prodávající není oprávněn postoupit jakoukoliv svoji pohledávku, a to ani část pohledávky, za kupujícím, která vznikne na základě a/nebo v souvislosti s touto smlouvou, ani k ní zřídit smluvní zástavní právo, ani postoupit svoje smluvní postavení z této smlouvy na třetí osobu.

10.9. Prodávající je povinen uchovávat veškerou dokumentaci související s realizací projektu (předmětu plnění této smlouvy) včetně účetních dokladů minimálně do konce roku 2040.

10.10. Prodávající je povinen minimálně do konce roku 2040 poskytovat požadované informace a dokumentaci související s realizací projektu (předmětu plnění této smlouvy) zaměstnancům nebo zmocněncům pověřených orgánů (CRR, MMR ČR, MF ČR, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu (předmětu plnění této smlouvy) a poskytnout jim při provádění kontroly součinnost.

10.11. Zhotovitel předloží objednateli při podpisu této smlouvy doklad o uzavření pojistné smlouvy pro případnou újmu způsobenou kupujícímu v souvislosti s plněním této smlouvy s minimálním limitem plnění z případné škodní události ve výši 5.000.000,- Kč.

11. Práva z vadného plnění a smluvní záruka

11.1. Kupující požaduje a prodávající se zavazuje držet záruku na předmět plnění této smlouvy v rozsahu definovaném v příloze č. 1 smlouvy – Technické specifikaci, kdy je pro každý typ zařízení definován odlišný typ a rozsah požadované záruky. Prodávající se dále v rámci prvních dvou let běhu této záruky zavazuje zajistit provedení zpětné montáže opraveného nebo nahrazeného zařízení z důvodu jeho vady, a to včetně

provedení jeho konfigurace, ať už nahráním konfiguračního souboru nebo jinou vhodnou cestou.

11.2. Záruka na jednotlivá zařízená, která jsou předmětem plnění této smlouvy, počíná svůj běh dnem jejich předání kupujícímu na základě řádně oběma smluvními stranami podepsaného předávacího protokolu.

11.3. Prodávajícím poskytnutá záruka v délce uvedené ve specifikaci jednotlivých zařízení obsažených v příloze č. 1 této smlouvy se vztahuje na funkčnost dodaného plnění, jakož i na jeho vlastnosti požadované kupujícím.

11.4. Na příslušenství a provedené implementační a konfigurační práce bude prodávajícím poskytována záruka v délce dvou (2) let. V případě vad takového příslušenství se prodávající zavazuje provést opravu nebo věc nahradit novou do 30 kalendářních dnů ode dne nahlášení vady kupujícím v sídle kupujícího. V případě vad provedených implementačních a konfiguračních prací se prodávající zavazuje provést opravu do 14 kalendářních dnů ode dne nahlášení vady kupujícím v místě plnění.

11.5. Po celou záruční dobu na samotná zařízení podle této smlouvy prodávající garantuje kupujícímu přijmout od něj nahlášení poruchy a dle parametrů záruky pro jednotlivé zařízení dle specifikace uvedené v příloze č. 1 této smlouvy garantuje realizaci opravy technikem v místě dodávky.

11.6. Prodávající odpovídá kupujícímu za to, že dodaný předmět smlouvy bude mít vlastnosti zabezpečující jeho řádné užívání, stanovené v minimální konfiguraci v technické specifikaci kupujícího a v konečné konfiguraci ve specifikaci obsažené v nabídce prodávajícího.

11.7. Prodávající odpovídá kupujícímu dále za to, že dodaný předmět smlouvy bude mít vlastnosti zabezpečující jeho řádné užívání a že je bez právních a faktických vad. Dále prodávající zaručuje, že na dodaném předmětu smlouvy neváznou práva třetích osob.

11.8. Prodávající se zavazuje zajistit, že veškerá komunikace na základě této kupní smlouvy bude z jeho strany vedena v českém jazyce, a to včetně uplatňování a řešení závad a reklamací jednotlivých zařízení a licencí na základě této smlouvy.

11.9. Vady musí kupující uplatnit u prodávajícího bez zbytečného odkladu poté, co se o nich dozví.

11.10. Uplatněním práv z odpovědnosti za vadné plnění není dotčeno právo kupujícího na náhradu škody.

12. Smluvní pokuty

12.1. Pro případ prodlení se zaplacením kupní ceny se kupující zavazuje uhradit prodávajícímu smluvní pokutu ve výši 0,01 % z fakturované ceny za každý den prodlení.

12.2. Nesplní-li prodávající svůj závazek vycházející z každého z dílčího termínu harmonogramu plnění, který bude připraven v rámci realizace plnění dle specifikace v příloze č. 1 této smlouvy - Technické specifikace, je oprávněn objednatel požadovat po zhotoviteli zaplacení jednorázové smluvní pokuty ve výši 5.000,- Kč za nedodržení termínu plnění každého z termínů stanoveného v harmonogramu.

12.3. Nesplní-li prodávající svůj závazek v rozsahu a čase plnění sjednaném touto smlouvou jako celku předmětu koupě, je oprávněn kupující požadovat po zhotoviteli nad rámec

nedodržení plnění dle termínů harmonogramu zaplacení jednorázové smluvní pokuty ve výši 50.000,- Kč za nedodržení termínu plnění a dále smluvní pokuty ve výši 0,1 % ze sjednané ceny plnění dle této smlouvy za každý započatý den prodlení, až do řádného dokončení a předání celého předmětu plnění a prodávající je povinen takto požadovanou smluvní pokutu zaplatit.

12.4. V případě prodlení prodávajícího s odstraněním nahlášené závady ve lhůtě uvedené v čl. 11.5 smlouvy je kupující oprávněn vyúčtovat smluvní pokutu ve výši 500,- Kč za každou, i započatou, hodinu prodlení prodávajícího s odstraněním nahlášené závady, max. však do výše 100 % pořizovací ceny daného zařízení.

12.5. V případě prodlení prodávajícího s odstraněním nahlášené závady na příslušenství se stanovuje smluvní pokuta ve výši 500,- za každý celý kalendářní týden prodlení.

12.6. V případě prodlení prodávajícího s odstraněním nahlášené závady v podobě provedených implementačních a konfiguračních prací se stanovuje smluvní pokuta ve výši 500,- za každý celý pracovní den prodlení.

12.7. Nesplní-li prodávající řádně podmínky projektového řízení dle přílohy č. 1 této smlouvy - Technické specifikace zejména v případě zápisů ze schůzek a pracovních jednání, v případě účasti odpovědné osoby prodávajícího na kontrolních dnech a v případě pravidelného reportingu, je kupující oprávněn požadovat po prodávajícím smluvní pokutu ve výši 500,- Kč za každý případ takového pochybení a to i opakovaně.

12.8. V případě realizace předmětu plnění této smlouvy projektovým týmem prodávajícího v jiném složení, než které je uvedeno v článku 9.2 této smlouvy, je objednatel oprávněn požadovat po zhotoviteli zaplacení smluvní pokuty ve výši 20.000,- Kč za každý zjištěný případ.

12.9. V případě nedodržení komunikace v českém jazyce na základě této smlouvy podle článku 11.8 smlouvy je kupující oprávněn vyúčtovat smluvní pokutu ve výši 1.000,- Kč za každý případ.

12.10. Zaplacením smluvní pokuty nezaniká povinnost druhé strany závazek splnit a není tím dotčeno právo poškozené strany na náhradu škody, které nesplněním povinnosti vznikla.

12.11. Výši smluvních pokut shodně považují obě smluvní strany za přiměřené. Smluvní pokuta je splatná do 30-ti dnů od doručení jejího vyúčtování.

13. Odstoupení od smlouvy

13.1. Odstoupení od smlouvy se řídí ustanoveními § 223 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, a dále § 2001 a násl. zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů.

13.2. Nebude-li uhrazena kupní cena do 60 dnů ode dne splatnosti daňového dokladu prodávajícímu v důsledku zavinění kupujícího a ani do dalších 15 dnů po opakovaném vyzvání prodávajícím k takové úhradě, sjednává si prodávající právo odstoupit od této kupní smlouvy.

13.3. Právo odstoupit od této kupní smlouvy má kupující tehdy, jestliže jej prodávající ujistil, že předmět plnění této smlouvy má určité vlastnosti, zejména vlastnosti kupujícím vymíněné, anebo prodávající kupujícího ujistil, že předmět plnění této smlouvy nemá žádné vady, a toto ujištění se ukáže být nepravdivým.

14. Registr smluv – doložka

14.1. Prodávající tímto uděluje souhlas kupujícímu k uveřejnění všech podkladů, údajů a informací uvedených v této smlouvě, k jejichž uveřejnění vyplývá pro kupujícího povinnost dle právních předpisů.

14.2. Prodávající je současně srozuměn s tím, že kupující je oprávněn zveřejnit obraz smlouvy a jejich případných změn (dodatků) a dalších dokumentů od této smlouvy odvozených včetně metadata požadovaných k uveřejnění dle zákona č. 340/2015 Sb., o registru smluv.

14.3. Zveřejnění smlouvy a metadata v registru smluv zajistí kupující.

15. Závěrečná ustanovení

15.1. Tato smlouva je vyhotovena v elektronickém originále, jenž po podpisu druhou ze smluvních stran obdrží obě smluvní strany. Smluvní strany se dohodly, že k podpisu smlouvy bude použit kvalifikovaný elektronický podpis ve smyslu Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 (eIDAS).

15.2. Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti uveřejněním v registru smluv.

15.3. Právní vztahy touto smlouvou výslovně neupravené a s ní související nebo z ní vyplývající se řídí ustanoveními zákona č. 89/2012 Sb., občanského zákoníku.

15.4. Jakékoli změny či doplňky této smlouvy je možné platně učinit pouze formou písemných a vzestupně číslovaných dodatků, podepsaných oprávněnými zástupci obou smluvních stran.

15.5. Přílohami této smlouvy jsou:

- Příloha č. 1 – Technická specifikace zadavatele (kupujícího)
- Příloha č. 2 – Technická specifikace účastníka zadávacího řízení (prodávajícího) z jeho vítězné nabídky, včetně jednotkových cen zařízení
- Příloha č. 3 – Cenová tabulka obsahující skladbu nabídkové ceny z nabídky prodávajícího

15.6. Strany této smlouvy berou na vědomí, že kupující jako správce osobních údajů je oprávněn zpracovávat zde uvedené osobní údaje v souladu s článkem 6 odst. 1 písm. b) Obecného nařízení (toto zpracování je nezbytné pro splnění smlouvy) a písm. c) (toto zpracování je nezbytné pro splnění právní povinnosti správce zveřejnit smlouvu na profilu zadavatele dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, v registru smluv dle zákona č. 340/2015 Sb., o registru smluv, postupy podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím nebo na své úřední desce dle zákona č. 128/2000 Sb., o obcích).

15.7. V případě, že po podpisu této smlouvy na prodávajícího anebo jeho poddodavatele budou dopadat mezinárodní sankce podle zákona upravujícího provádění mezinárodních sankcí č. 69/2006 Sb. ve smyslu zákona č. 240/2022 Sb. účinného od 1. 9. 2022, je povinen to prodávající písemně oznámit kupujícímu. V případě, že oznámení neprovede a kupující zjistí, že na prodávajícího anebo jeho poddodavatele mezinárodní sankce dopadají, vyzve prodávajícího k vysvětlení nebo nápravě formou

vyjmutí osoby ze sankčního seznamu. V případě že náprava není možná, odstoupí kupující od této smlouvy, přičemž účinnost odstoupení nastává doručením odstoupení prodávajícímu.

15.8. Smluvní strany prohlašují, že si tuto smlouvu před jejím podpisem přečetly a s celým jejím obsahem souhlasí. Dále prohlašují, že tato smlouva vyjadřuje jejich pravou a svobodnou vůli. Na důkaz toho připojují vlastnoruční podpisy na smlouvě.

15.9. Tato smlouva byla schválena usnesením rady města č. 526/24 ze dne 21. 8. 2024.

Za kupujícího

V Rakovníku

PaedDr. Luděk Štíbr

Digitálně podepsal PaedDr. Luděk Štíbr
Datum: 2024.09.20 10:56:21 +02'00'

……

PaedDr. Luděk Štíbr

starosta města

Za prodávajícího

V Praze

Ing. Jaroslav Dvořák

Digitálně podepsal Ing. Jaroslav Dvořák
Datum: 2024.09.13 09:46:12 +02'00'

……

Jaroslav Dvořák

člen představenstva

Příloha č. 1 Zadávací dokumentace – Technická specifikace zadavatele

Příloha č. 1 Kupní smlouvy – Technická specifikace kupujícího

1 Technická specifikace zadavatele (kupujícího)

Obsah

Kupující požaduje dodávku jednotlivých komponent dle této technické specifikace včetně příslušenství v níže uvedené minimální specifikaci.

Musí se jednat o zařízení nová, nepoužitá, nerepasovaná a určená pro prodej v České republice, potažmo v EU.

Součástí dodávky níže uvedených technologií budou i dále uvedené služby.

Součástí dodávky bude dále dodávka dokumentace a nezbytné zaškolení administrátorů v prostředí kupujícího k běžnému provozu a ovládání dodaných technologií včetně specifik a konfigurace provedené v prostředí kupujícího.

Nabízené zboží musí být standardní, běžně dostupné a určené k produkčnímu použití.

Není dovoleno použití beta-verzí, kódu s custom úpravami či neoficiálních verzí.

Veškeré nabízené zboží musí být pokryto oficiálním supportem, přičemž požadavek na provedení bezplatného servisního zásahu musí být možné kdykoliv vznést přímo na výrobce zařízení.

Veškeré deklarované funkce a technické parametry nabízeného zboží musí být dostupné nejpozději dnem podání nabídky.

Deklarované funkce a technické parametry nabízeného zboží musí být ověřitelné prostřednictvím oficiálních datasheetů, release notes či manuálů vydaných výrobcem.

Užité pojmy níže:

- NBD – další pracovní den, tzn. například realizace opravy zařízení nejpozději další pracovní den od nahlášení
- x BD – x pracovních dnů, tzn. například realizace opravy zařízení nejpozději poslední pracovní den dané lhůty od nahlášení
- on-site – realizace například opravy zařízení v místě dodávky

Z důvodu kompatibility se stávající infrastrukturou a proškolených správců počítačové sítě, mohou být v zadávací dokumentaci uvedeny konkrétní značky výrobků, nebo určitý výrobce. Tyto důvody jsou vždy uvedeny v konkrétní části specifikace tam, kde dochází k uvedení konkrétního produktového názvu. V souladu s § 89 odst. 6 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, zadavatel připouští možnost dodávky rovnocenného řešení, které však musí zajistit celý komplex služeb, který je kompatibilitou vyžadován, tedy komplexní řešení technologií až na úroveň elektronické podpory agend vykonávaných městem za předpokladu, že dané technologie jsou vyžadovány stávajícími platformami na nich provozovaných agendových informačních systémů.

2 Místo plnění

Předmět plnění této technické specifikace je určen pro nasazení v následujících technologických místnostech:

- Lokalita A – MěÚ Rakovník, Husovo náměstí 27
- Lokalita B – MěÚ Rakovník, Na Sekyře 166
- Lokalita C – MěÚ Rakovník, odbor dopravy, Nádražní 102

Hlavní technologická místnost (serverovna) je umístěna v 2. podlaží v lokalitě A. Záložní technologická místnost (serverovna) je umístěna v 1. podlaží v lokalitě B. Pod lokalitu A také spadá zvláštní technologická místnost pro potřeby Městské policie. V lokalitě C se v technologické místnosti nachází pouze hardware pro potřeby budovy (přepínače, UPS, laserové pojítko). Místnosti jsou vybaveny klimatizací, elektronickým a zabezpečovacím systémem. Datové rozvaděče (racky) nejsou vybaveny Rack Management Systémem.

3 Počet a typ technologií

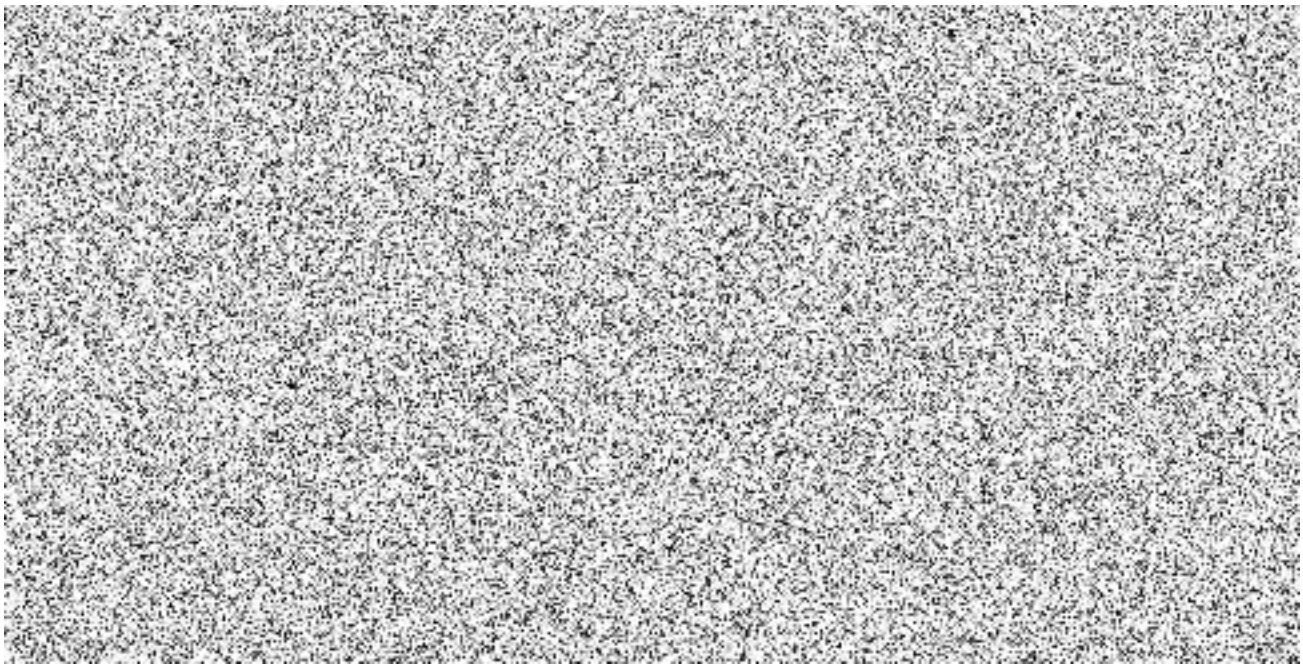
Počet a typ jednotlivých technologií, které jsou specifikovány níže, je definován v samostatné příloze zadávací dokumentace a kupní smlouvy v podobě cenové tabulky.

Cílem této tabulky je předcházet duplicitám v počtu uváděných typů kusů technologií v jednotlivých souborech jako části zadávacích podmínek nebo částech a přílohách smlouvy.

Instalační a další související práce spojené s dodávkou a nasazením jednotlivých technologií prodávající zohlední v ceně jednotlivých zařízení.

4 Zvýšení zabezpečení komunikační sítě města Rakovník

V rámci dodávky jednotlivých technologií v rámci této specifikace, dojde k jejich konfiguraci minimálně v následujícím rozsahu za účelem dosažení cílů uvedených níže.



V rámci plnění tedy bude v celé LAN implementováno řízení přístupů k mediu (síti) na základě rolí a členství v uživatelské skupině adresářové služby Active Directory s využitím technologie 802.1X.

Dále bude implementován systém centrální správy, který poskytne celkový pohled na stav a konfiguraci LAN jako celku a současně umožní centrálně provádět změny konfigurace prvků LAN a vytvořením jednotně spravovaných VLAN zavést segmentaci sítě. Součástí centrálního systému bude systém řízení přístupu zařízení a uživatelů do síťové infrastruktury založený na standardu IEEE 802.1X a systém ověření původu DNS záznamů elektronickým podpisem.

Ověřování přístupu do LAN bude realizováno protokolem 802.1X vůči adresářové službě prostřednictvím protokolů radius a P/EAP. Neověřená zařízení nezískají přístup do sítě vůbec nebo jim bude zpřístupněna pouze VLAN s omezeným přístupem (např. intranet). Spolu s ověřováním (autentizací) bude implementována i autorizace, tedy dynamické zařazení klientského zařízení nebo uživatele do určené VLAN. Součástí dodávky je vzorová konfigurace 802.1X na všech typech uživatelských koncových zařízení Zadavatele (PC, notebooky, chytré telefony, tablety, tiskárny - Windows, Linux, MacOS, Android, IOS, embedded systémy periferií) a uživatelská dokumentace pro konfiguraci koncových zařízení uživateli.

Systém musí umožňovat v budoucnu i ověřování přístupu do WiFi sítě, které bude realizováno na stejném principu jako LAN (tj. protokol 802.1X + radius). WiFi bude nabízet více SSID (např. zaměstnanci, hosté, IoT), které budou obsluhovány samostatnými VLAN a budou napojeny na radius servery. Zaměstnanci budou prostřednictvím radius serveru ověřováni v adresářové službě. Zabezpečení vnitřních sítí (BSSID) bude provedeno s využitím WPA3 (alternativně WPA2 dle podpory připojovaných zařízení) s AES šifrováním a konfigurováno shodně pro obě všechna frekvenční pásma. Řešení umožní použití autentizace prostřednictvím webového portálu (tzv. captive portál) s využitím jednorázových přístupových údajů a samostatných politik a restrikcí pro tento způsob autentizace.

Pro WiFi budou zřízeny samostatné VLAN, které budou komunikačně odděleny od ostatních vnitřních sítí organizace. Tyto VLAN budou konfigurovány na úrovní stávajícího firewallu tak, aby bylo možné komunikaci podrobit kontrole za pomoci UTM nástrojů (min. AV, IPS, kategorizace obsahu) a bude jim být přiřazen samostatný profil a/nebo virtuální kontext nakonfigurovaný ve firewallu.

Řízení provozu v LAN bude realizováno vytvořením VLAN (802.1Q), segmentací sítě s přepínáním provozu mezi VLAN na úrovni centrálního přepínače s nastavitelnými ACL. Pro řízení provozu na úrovni kvality služeb bude k dispozici technologie QoS (Quality of Services). Pro zajištění vysoké dostupnosti služeb budou klíčové aktivní prvky propojeny duálními trasami s automatickým rozkládáním zátěže a převzetím služeb v případě výpadku jedné trasy.

Součástí plnění je implementace pořízených technologií včetně osazení aktivních síťových prvků (přepínače) do připravených racků a na připravenou kabeláž (pasivní část LAN není součástí tohoto projektu).

4.1 Systém řízení přístupu do sítě podle standardu IEEE 802.1X (network access control)

Řešení musí splňovat následující minimální požadavky na parametry a funkcionalitu:

Systém řízení přístupu do sítě podle standardu IEEE 802.1X	
Parametr	**Minimální požadavky**
Provedení	Softwarová appliance pokročilého NAC (network access control) na bázi standardu IEEE 802.1X. Integrovaná podpora autentizace, autorizace a účtování (přístupů) uživatelů i koncových zařízení, integrovaný RADIUS

	server a databáze uživatelů a zařízení.
Nastavení přístupů	Nastavení síťového přístupu uživatelů a zařízení podle politik min. pomocí přiřazení VLAN, ACL. Atributy pro definici politik min. IP, MAC, port, VLAN, QinQ VLAN, hostname (PC name), uživatelské jméno (z Active Directory), operační systém
Autentizace	Zajištění IEEE 802.1X autentizace a autorizace pro bezdrátové sítě, Ethernet LAN sítě a VPN
Základní autentizační metody	Min. PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, MAC autentizace, certifikáty
Identity	Vestavěná databáze identit pro autentizaci, podpora standardních identitních databází - Active Directory, LDAP, ODBC
Nezávislá autentizace a autorizace	Úplné oddělení autentizace a autorizace, např. autentizace proti službě Active Directory, ale autorizace proti externí SQL databázi.
Rozšířená autentizace a autorizace	Podpora autentizace a autorizace min. LDAP, Microsoft Active Directory, generická SQL databáze, Kerberos, HTTPS web autentizace, Single Sign-On (minimálně SAML 2+ IdP a SP, OAuth, Shibboleth a Okta).
Kontextová autorizace	Autorizace zařízení a uživatelů na základě kontextových informací jako čas, typ připojení, osobní profil či členství ve skupině v Active Directory.
Externí identity	Podpora autentizace externími identitami - min. Microsoft, Google.
Komplexní autorizace	Autorizace uživatelů na základě jejich vlastních accounting informací z předchozích připojení – např. pro omezení celkového času online či objemu přenesených dat za delší časové období
Dynamická autorizace	Podpora RADIUS CoA podle RFC3576. Možnost změny autorizačního stavu zařízení bez nutnosti změny definice autorizační politiky, např. pro odpojení nebo karanténu koncových zařízení.
Izolace klientů	Zpracovávání syslog zpráv z externích zdrojů, vyhledávání definovaných událostí a automatizovaná reakce na ně. Minimálně v rozsahu příjmu zpráva ze stávajícího firewallu a izolace konkrétního klienta na základě těchto zpráv.
Zpracování syslog	Vestavěná podpora tvorby a úprav vlastních parserů, syslog zpráv pro napojení na další systémy třetích stran
Bezpečnost	Podpora okamžitého odpojení zařízení při vypršení libovolné autorizační podmínky (např. překročení objemu dat, časového intervalu, stavu zařízení apod.)
Správa	Vestavěné nástroje pro testování politik, diagnostiku chování systému i spravovaných zařízení
Portál	Captive portál pro uživatele a jejich rozšířenou autentizaci, podpora více graficky i obsahově unikátních portálů provozovaných souběžně. Integrovaná podpora úpravy vzhledu
Rychlé přihlášení	Podpora přihlášení prostřednictvím QR kódu. Zapamatování úspěšně autentizovaných/registrovaných klientů a zjednodušení opakovaných přihlášení (např. jen potvrzení uvítací/informační) stránky.
Registrace	Podpora samoobslužné registrace s ověřením SMS, e-mailem apod.
Ochrana identit	Veškeré identitní údaje v systému budou uložena ve výrobcem dodané a podporované šifrované databázi, která bude nativní součástí dodaného produktu, s minimální enkrypcí uložených dat ve standardu AES min. 128-

	bit.
Speciální zařízení	Podpora autentizace a řízení přístupů speciálních ("nepočítačových") zařízení zejména tiskárny, modality, technologické prvky, IoT.
Vysoká dostupnost	Integrovaná podpora vysoké dostupnosti v režimu active-active, tj. vytvoření clusteru min. 2 appliance. Druhá appliance je součástí dodávky.
Licence	Licence pro min. 500 konkurenčních koncových zařízení ověřovaných pomocí 802.1X bez omezení počtu uživatelů.
Automatizace a integrace	REST-API rozhraní min. pro základní funkce AAA, příjem syslog hlášení z externích zdrojů, vyhledávání klíčových událostí a automatizovaná reakce na ně. Tvorba/modifikace vlastních parserů syslog.
Kompatibilita	Appliance určena pro provoz v prostředí stávající serverové virtualizace
Podpora	Podpora výrobce software min. 60 měsíců včetně nároku na nové verze software včetně aktualizací.

4.2 Přepínače s příslušenstvím

Řešení musí splňovat následující minimální požadavky na parametry a funkcionalitu:

Přístupový přepínač	
Parametr	**Minimální požadavky**
Základní parametry	L2/3 přepínač v rackovém provedení
Porty a propustnost	min. 48x 1 GB RJ-45 PoE+ + 4x 10Gb SFP+ (nesdílené), min. 176 Gb/s
Směrování	min. statické směrování na L3 vrstvě pro IPv4 I IPv6
Propustnost	neblokovaná architektura
Automatizace VLAN	Podpora protokolu MVPR pro automatické zjišťování a přiřazení
Agregace portů	podpora LACP
Dualstack	IPv4 a IPv6 dualstack včetně podpory ACL a QoS
VLAN	VLAN 802.1Q, MAC i protocol based, podpora zařazování do VLAN a přidělení QoS a přístupových filtrů na základě 802.1X ověření
Ověřování uživatelů a zařízení	podpora 802.1X
Zrcadlení portů	Zrcadlení provozu portů pro diagnostiku a bezpečnostní monitoring, min. 4 zrcadlené skupiny
Monitoring a správa	plná podpora CLI, SSH, SNMP 1-3, syslog, sFlow, RMON, web rozhraní, podpora uložení více konfigurací a min. 2 obrazů firmware pro bezpečný a jednoduchý upgrade
Automatizace a integrace	Integrované REST API rozhraní pro ovládání síťových funkcí
Záruka a záruční servis	min. 60 měsíců, oprava/výměna do 2 pracovních dnů v místě instalace, včetně nároku na opravné verze firmware

Požadované implementační práce:

- fyzická montáž diskového úložiště do rackových skříní
- zapojení do LAN infrastruktury a nastavení politik, které bude vycházet z umístění nového prvku a stávajících konfigurací z přepínačů typu HP A5120-48G, když tyto stávající konfigurace poskytne město

- nastavení a konfigurace – aktualizace firmware na nejnovější dostupnou verzi
- konfigurace akceleračního protokolu, nastavení storage units
- otestování

5 Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů

V rámci dodávky jednotlivých technologií v rámci této specifikace, dojde k jejich konfiguraci minimálně v následujícím rozsahu za účelem dosažení cílů uvedených níže.

V současné době nevlastní město Rakovník žádný nástroj pro (centrální) zaznamenávání činnosti (logů) a navazujících systémů. Činnosti jsou v některých systémech zaznamenávány lokálně, ale bez jednotné politiky, dlouhodobého ukládání a ochrany logů před změnou, přetečením apod. Chybí tak nástroj pro podporu řešení případných kybernetických událostí a incidentů, poskytování konsolidovaných informací před vznikem a v průběhu události/incidentu. Absence nástroje také neumožňuje efektivně analyzoval chování IS a souvisejících systémů z pohledu kybernetické bezpečnosti, ale i z pohledu běžného provozu pro účely zavádění preventivních opatření předcházejících výskytu nestandardního provozního stavu a/nebo opatření k zamezené jeho opakování.

Implementací nástroje pro správu logů (tzv. log management) - zavedením komplexního systému pro správu logů je požadováno dosažení centralizovaného sjednocení různých bází bezpečnostních a provozních záznamů, které jsou poskytovány různými typy hardwarových zařízení, dále různými provozovanými operačními systémy a aplikacemi, včetně všech nástrojů implementovaných v rámci plnění dle této specifikace. Zaznamenané činnosti budou k dispozici na jednom místě ve sjednoceném formátu při zachování jejich dostupnosti, důvěrnosti a integrity. Systém zajistí uložení dat k okamžitému prohlížení a prohledávání minimálně po dobu 6 měsíců a bude umožňovat archivaci starších záznamů s možností rychlé obnovy archivu v případě potřeby. Systém musí zajistit integritu archivu.

Dodávané řešení musí být standardní Log/Event Management, který musí umožnit budoucí rozšíření o další systémy (např. systém SIEM) nebo napojení na služby SOC (Security operations center).

Řešení musí umožni sofistikovanou, transparentní a opakovatelnou pokročilou analýzu, spojenou s řešením běžných provozních i bezpečnostních událostí/incidentů a upozorňováním na ně, a to z kritických i nekritických a podpůrných systémů a aplikací. Řešení musí být schopné generovat reporty o aktivitách systémů i uživatelů, včetně auditních reportů na vyžádání, nebo se stanovenou periodicitou s definovatelným obsahem, primárně v českém jazyce a dále variantně v jazyce anglickém, bez nutnosti používat SQL (či obdobnou „programátorskou“) syntaxi pro definici či úpravu reportů.

Řešení musí zachovávat originál logů za účelem bezpečnostního auditu, a to v souladu s požadavky ISO/ČSN 27001:2013 pro pořizování auditních záznamů.

Řešení musí umožnit snadné a rychlé multikriteriální vyhledávání pro účely analýz, auditů, a podporu běžného provozu komplexního řešení ICT infrastruktury města.

Pro zajištění požadavků bezpečnosti musí řešení Log/Event Management disponovat konfigurovatelným uživatelským oddělením rolí a ochranou centralizovaných logů před neoprávněným přístupem k citlivým datům.

Reporty systému budou sloužit pro přehlednou kontrolu stavu a chování informačních systémů a uživatelů za určité období (typicky 1 měsíc) a ke kontrole dodržování compliance („jednání v souladu s pravidly") organizace.

Data uložená v systému a systémem archivovaná budou zajištěna a zabezpečena před neoprávněnou změnou i pro účely vyšetřování případného bezpečnostního incidentu.

Je požadována dodávka a implementace takového řešení, které umožní příjem a vyhodnocení všech požadovaných informací – může se jednat o jediné zařízení, softwarový nástroj či appliance nebo o řešení složené z více samostatných a vzájemně kompatibilních komponent. Řešení musí umožnit správu z jedné grafické konzole, přístupné nativně skrze https bez nutnosti instalace klienta. Ukládání všech informací bude prováděno do jedné databáze (nebo více integrovaných databází) tak, aby bylo možno realizovat multikriteriální vyhledávání napříč informacemi z různých systémů.

Mandatorní informace, která bude v systému vždy obsažena a uchována, je vazba IP-uživatel-čas. Tuto informaci bude systém čerpat ze security event-logu adresářové služby, dále z informací o probíhajících komunikacích na straně firewallu za pomoci jeho SSO agentů či logů a dalších přístupových a autentifikačních systémů (např. RADIUS logy). Dále budou získávány informace o překladu zdrojových, vnitřních IPv4 adres na externím výstupním rozhraní firewallu, kde bude prováděn NAT. Bude se tedy jednat o informace obsažené v NAT tabulce. Spolu s tím bude po stanovenou dobu možné zpětně dohledat i vnější provoz k vnitřnímu zařízení.

Řešení musí umožňovat uchování každého záznamu v jeho nezměněné podobě, ale zároveň bude schopný dávat jednotlivé události ihned do souvislostí a vyhodnocovat riziko a případné bezpečnostní události aktivně notifikovat, resp. reportovat.

Implementace řešení bude v provedena v souladu s § 23 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí Vyhlášky č.316/2014 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti.

Zadavatel může Uchazeče vyzvat k doručení funkčního vzorku. Pokud Zadavatel vyzve Uchazeče o poskytnutí funkčního vzorku (v identické konfiguraci s nabízeným systémem) pro účely testování a ověření požadovaných funkčních vlastností, Uchazeč je povinen doručit testovací vzorky na adresu sídla zadavatele do pěti (5) pracovních dnů od doručení výzvy k jejich poskytnutí. Vybraný Uchazeč poskytne testovací vzorky bezplatně a na dobu minimálně následujících 10 pracovních dnů poskytne součinnost s testováním.

5.1 Systém pro správu logů

Řešení musí splňovat následující minimální požadavky na parametry a funkcionalitu:

Systém pro správu logů	
Parametr	**Minimální požadavky**
Základní funkce	Integrovaný systém zpracování logů a událostí z definovaných zdrojů napříč výrobci aplikací, operačních systémů a síťového hardware
Architektura	Integrovaná appliance (HW se specializovaným firmware/software) nebo server se specializovaným software včetně operačního a podpůrných systémů (databáze apod.), samostatně funkční nezávislé na infrastruktuře zadavatele
Provedení	Určené pro montáž do stávajícího serverového datového rozvaděče 19", hloubka max 900 mm, včetně výsuvných kolejnic a ramene pro vedení kabelů.
Ovládání	Grafická webová konzole pro administrátory i operátory, umožňuje kompletní správu systému včetně úvodního nastavení.

Autentizace	Autentizace uživatelů vůči Active Directory nebo LDAP serveru. V případě výpadku AD/LDAP musí systém umožnit autentizaci z lokální databáze.
Uživatelské role	Podpora uživatelských rolí obsahujících přístupová práva k uloženým událostem a jednotlivým ovládacím částem systému.
Sběr dat (logů)	Je požadován bezagentový sběr logů pro uvedené zdroje logů. Pro systémy Windows je umožněn agentový i bezagentový sběr.
Windows agent	Kompletní správa a aktualizace z administrátorské konzole, sběr dat z textových i Event logů (včetně rozšířených), šifrovaná komunikace, buffer pro případ ztráty komunikace, překlad kódů na text (např. Logon type 2 => "Interactive" apod.) a textový popis události shodný s Windows Event Viewerem
Protokoly	Příjem a zpracování logy, událostí a další strojově generovaných data minimálně protokoly UDP/TCP 514 (SYSLOG), TCP 20514 (RELP, nešifrovaně) a TCP 20515 (RELP, šifrovaně).
Formáty logů	Min. RAW, Syslog, CEF, LEEF, JSON RFC7159, Windows EventLog
Třídění logů	Podpora příjmu logů na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv.
Zpracování logů	Integrované parsování a normalizace přijatých událostí/logů bez nutnosti instalovat externí aplikace nebo systémy
Ochrana logů	Zamezení mazání nebo modifikování již uložených logů. Každý log musí mít unikátní identifikátor pro jeho jednoznačnou identifikaci.
Vizualizace logů	Grafická vizualizace logů, událostí a strojových dat (grafy událostí). Dynamická vizualizace - změnou volby (např. filtru) v jednom grafu se ostatní svázané grafy upraví automaticky dle požadované volby. Integrované podpora zobrazení TOP X událostí za zvolené časové období.
Pracovní plochy	Předpřipravené pohledy (dashboardy) na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění, průběžná aktualizace pohledů výrobcem. Integrovaná podpora tvorby uživatelských dashboardů včetně ukládání
Zajištění logů	Ochrana proti ztrátě logů při přetížení systému. Ukládání nezpracovaných logů/událostí do vyrovnávací paměti o kapacitě min 25 GB, notifikace správce systému při riziku zaplnění vyrovnávací paměti
Doplňování logů	Integrovaná podpora doplňování logů dalšími údaji - zejména umístění zařízení, typ zařízení, kritičnost zařízení apod. - k jednotlivým zdrojům zejména dat, aplikacím, zařízením, IP rozsahů
Archivace	Integrovaná archivace logů včetně zajištění integrity archivů, obnova
Rozpoznávání IP, MAC	Automatické doplňování reverzních DNS záznamům k IP adresám a výrobce podle MAC adresy
Časová razítka	Podpora doplňkové značky (razítka) navíc k časovému údaji zaznamenané události/logu, sloužící jako výchozí časový údaj pro systém
Vyhledávání	Snadné multikriteriální vyhledávání událostí bez nutnosti speciálních znalosti (např. SQL dotazů apod.) napříč všemi typy dat a zařízení.
Rychlé vyhledávání	Rychlé vyhledávání i v aktuálně uložených položkách (průběžné indexování)
Geolokace	Automatické doplňování geolokačních informací k událostem a jejich grafické znázornění na mapě bez služeb třetích stran
Reporty	Integrovaný reportovací nástroj s přednastavenými obvyklými reporty a

	možností vlastních úprav a vytvoření nových pohledů bez potřeby speciálních znalostí (zejména SQL dotazů). Průběžná aktualizace přednastavených reportů výrobcem.
Integrace	Integrované REST API rozhraní pro napojené systémy, musí umožnit autorizovaný přístup ke strukturované databázi logů.
Parsery	Integrovaný grafický (vizuální) nástroj pro tvorbu vlastních parserů logů včetně testování a ladění - okamžitého zobrazení rozparsovaných testovacích dat včetně případných chyb
Konektory	Konektory (specifické parsery) pro stávající technologie - min. Active Directory, Hyper-V, VMware, Windows (vč. DNS, DHCP), Exchange, MS SQL, Fortigate, HPE/Aruba, Dell servery, Synology, Linux, Apache.
Alerty, notifikace	Předpřipravené alerty a integrovaný grafický (vizuální) nástroj pro vytváření automatických notifikací/alertů generovaných při splnění definovaných podmínek v přijatých datech. Odesílání alertů min SMTP, Syslog, TCP.
Výkon	Min. 5000 EPS (events per second), krátkodobá (min. 10 min) přetížitelnost systému až 200%
Kapacita	Využitelná diskové kapacita pro ukládání dat min. 40 TB, disky musí být chráněny min. RAID 5
Řízení diskového systému	Hardwarový řadič RAID se zálohovanou vyrovnávací pamětí (zápis i čtení) o kapacitě min 8 GB
Úložiště logů	Logy musí být ukládány do databáze (příslušná licence musí být součástí dodávky) s podporou komprese ukládaných dat.
Napájení	Systém musí mít redundantní napájení (min. 2 nezávislé zdroje)
LAN konektivita	Min. 2x LAN 1 Gb Base-T a 2x LAN 10Gb SFP+ včetně SFP+ modulů + 1x 1Gb Base-T nezávislý port pro správu hardware prostřednictvím KVM konzole s grafickým rozhraním, zabezpečeným přístupem a detailním přehledem o stavu hardware včetně okamžité a dlouhodobé spotřeby elektrické energie a stavu dílčích komponent.
Aktualizace	Integrovaná aktualizace systému prostřednictvím administrátorské konzole včetně podpory downgrade
Zálohování	Integrované zálohování a obnova konfigurace
Škálovatelnost	Systém lze propojit s dalšími systémy stejného výrobce. Spojením systémů dojde ke zvýšení kapacity, výkonu (včetně vyhledávání) a dostupnosti. Navenek se propojené systémy chovají jako jeden.
Dokumentace	Plnohodnotná (tj. shodná s originální) dokumentace v českém jazyce
Záruka a záruční servis	Min. 60 měsíců s opravou hardware do druhého pracovního dne v místě instalace, včetně nároku na nové verze firmware/software a aktualizace

6 Nástroje pro zajišťování úrovně dostupnosti informací

V rámci dodávky jednotlivých technologií v rámci této specifikace, dojde k jejich konfiguraci minimálně v následujícím rozsahu za účelem dosažení cílů uvedených níže.

Zvýšení úrovně dostupnosti informací je požadováno dosáhnout v rámci tohoto plnění následovně:

- nasazením nového diskového pole s dostatečným výkonem i kapacitou do lokality Husovo nám. 27. Kompatibilní se serverovou virtualizací ESX a dodávaných hypervisorů.
- Implementací bezpečného datového úložiště pro zálohy – požadováno je zařízení s nastavitelnou retencí ukládaných dat (záloh) tak, aby uložená data nebylo možné po určitou (nastavitelnou) dobu změnit. Z pohledu zálohovacího systému půjde o zařízení typu WORM (Write One, Read Many) do sekundární lokality Na Sekyře 166.
- Nasazením dalších dvou serverů (hypervisoru), které doplní stávající řešení a budou určeny primárně pro provoz nově nasazovaných a zvýšenou dostupnost stávajících technologií. Stávající bude v rámci plnění dle této specifikace přesunuto dodavatelem do lokality Na Sekyře 166 a bude dodavatelem konfigurováno jako Dissaster Recovery ve druhé lokalitě. Pro zalicencování serverů poskytne Zadavatel licence s platnou maintenance VMware Essential Plus pro 3 dvousocketové hosty (4 CPU licence se použijí pro zalicencování dvou nových serverů a 2 CPU licence se použijí v DR lokalitě – celkem 3 hypervisory)
- nasazením dostatečně dimenzovaného zdroje nepřerušitelného napájení s dostačenou kapacitou a dobou provozu v případě výpadku el. energie dojde k celkovému zvýšení spolehlivosti provozu a dostupnosti dat.

V rámci realizace plnění bude vybudováno bezpečné úložiště pro ukládání dat, která musí být ochráněna proti jakékoli modifikaci po určenou dobu (retenční lhůtu). Jedná se zejména o zálohy databází, kritická nestrukturovaná data a kompletní zálohy virtuální serverů. Úložiště umožní konfigurovat více kategorií chráněných dat a odpovídajících retenčních lhůt. Data musí být možné ukládat pomocí běžných síťových protokolů, zejména SMB/CIFS.

Úložiště musí nativně spolupracovat se stávajícím zálohovacím systém pro možnost přímého ukládání záloh kritických dat a jejich ochrany před zničení škodlivým kódem (např. ransomware) nebo jiným způsobem.

6.1 Zálohovací úložiště s časovým zámkem

Řešení musí splňovat následující minimální požadavky na parametry a funkcionalitu:

Parametr	**Minimální požadavky**
Provedení	Umístitelné do racku, včetně montážního materiálu, maximálně 2U.
Kapacita	Řešení musí mít minimálně 54 TB využitelné (usable) lokální kapacity bez redukce dat, včetně potřebných licencí pro tuto kapacitu.
Škálovatelnost	Řešení musí umožňovat rozšíření alespoň do úrovně 1 PB čisté lokální kapacity bez redukce dat a bez nutnosti výměny jakékoliv dodávané součásti

Výkon	**Propustnost dodávaného řešení alespoň 6TB/hodinu**
Deduplikace	Zařízení musí při ukládání dat využívat princip deduplikace Uložiště nesmí vytvářet deduplikační pooly – musí disponovat globálním deduplikačním algoritmem bez ohledu na typ dat, přenosový protokol a množství zálohovacích serverů/aplikací, které na něj data ukládají.
Protokoly	Zařízení musí podporovat minimálně následující protokoly: CIFS a NFS a musí umožnit jejich současné použití
Integrace a interoperabilita	Zálohovací řešení musí být univerzální z hlediska podpory datových typů zálohovaných dat, musí podporovat všechny datové typy používané v produkčním prostředí Řešení musí umožnit komprimaci ukládaných deduplikovaných dat
Replikace	Zařízení musí obsahovat potřebné licence pro nativní funkcionalitu replikace dat do dalšího zařízení stejného výrobce. Řešení musí posílat pouze deduplikovaná zkomprimovaná data. Řešení musí podporovat alespoň následující scénáře pro replikaci: 1:1, M:1 a kaskádovou replikaci. Řešení musí umožnit funkcionalitu šifrování replikačního toku data-in-flight. Řešení musí umožnit kontrolu a správu využití pásma pro přenos dat (QoS).
Ochrana	Zařízení musí disponovat redundantními hot-swap napájecími zdroji a ventilátory. Zařízení musí zajišťovat ochranu dat alespoň na úrovni duální diskové parity. Zařízení musí zajišťovat výměnu všech disků za chodu – hot-swap. Zařízení musí obsahovat HotSpare disk. Zařízení musí obsahovat algoritmy pro kontrolu a verifikaci konzistence a čitelnosti uložených dat.
Časové zámky	Zařízení musí umožňovat nastavit ochranu dat proti nechtěnému smazání či modifikaci dat pomocí časových zámků. Po nastavenou dobu lze data číst, ale nelze je přepisovat. Tato funkce nesmí být závislá na zálohovacím software, přenosovém protokolu či typu dat. To znamená, že tato funkce musí být plně funkční s provozovaným zálohovacím SW/Veeam Backup & Replication. Časové zámky se musí aplikovat uvnitř zařízení, nikoliv pomocí externích nástrojů.
Šifrování	Zařízení musí umožňovat šifrování úložného prostoru a to bez omezení výkonu - dodání včetně potřebných licencí pro výše požadovanou kapacitu
Porty	Zařízení musí disponovat síťovými kartami min. 2x1GbE a 2x10Gb SFP+ včetně SFP+ modulů
Zabezpečení	Řešení musí umožnit vynucení přihlášení minimálně dvou typů účtů (administrátorský, bezpečnostní) pro změny spojené se změnou nastavení ochrany dat – časových zámků.
Dvoufaktorové ověřování	Řešení musí umožnit dvoufaktorové ověřování účtů pro správu díky jednorázovým heslům (Time-based One-Time Password). Pokud je potřeba externí nástroj, musí být součástí nabídky všechny potřebné licence až pro 25 uživatelů včetně potřebného hardware pro zajištění vysoké dostupnosti. Licence musí být perpetuální a instalace v místě plnění.
Správa	Řešení musí umožnit centrální správu pro všechna dodávaná zařízení prostřednictvím webového rozhraní. Řešení musí umožnit správu na principu rolí s různými typy oprávnění (Role-based Access Control).
Reporting	Řešení musí poskytovat funkcionalitu automatického reportingu, automatický call-home

Kompatibilita	Nabízený diskový úložný systém musí být plně podporován (plně kompatibilní) stávající zálohovací platformou Veeam Backup & Replication. Je požadováno aby řešení bylo uvedeno na webu výrobce zálohovacího SW mezi kompatibilními deduplikačními HW / Oficiálně podporovaná (kompatibilní) řešení se stávající platformou zálohování jsou popsána zde: https://helpcenter.veeam.com/docs/backup/vsphere/deduplicating_storage_appliances.html?ver=120
Podpora	Podpora na hardware a software musí být od jednoho výrobce, tak by byla zajištění funkčnost zařízení jako celku
Záruka a záruční servis	Požadovaná záruka a záruční servis 5 let s reakcí 8x5 NBD on-site

6.2 Produkční server s příslušenstvím

Řešení musí splňovat následující minimální požadavky na parametry a funkcionalitu:

Parametr	**Minimální požadavky**
Provedení	umístitelné do racku, včetně montážního materiálu, maximálně 1U. Barevně označené hot-plug komponenty. Pro přístup ke všem komponentám není nutné nářadí. Zásuvné ližiny s managementem kabeláže. Uzamykatelný čelní panel.
CPU	Minimálně 2x procesor 8 jádrový. Výkon serveru dle http://www.spec.org: SPECrate®2017_int_base min. 176 bodů SPECrate®2017_fp_base min. 249bodů Systém nesmí přesáhnout celkově 16 jader, z důvodu licenčních nákladů na pokrytí těchto jader licencemi software, které bude kupující na serverech provozovat.
RAM	Min. 32 slotů pro DDR5 RDIMM Min. 512GB RAM ECC, min. 4800 MT/s Počet paměťových modulů a rozmístění musí být zvoleno pro optimální výkon s CPU.
Boot Drive	Musí být zajištěn dvojicí HDD v RAID1 a kapacitou 960GB, nesmí se jednat o rotační disky. Disky pro Boot OS musí být hot-swap, přístupné z přední nebo zadní strany serveru.
Interface	Min. 3x externí USB, z toho min. 1x USB 3.0 Dedikovaný USB management port Min. 2x VGA port (jeden z každé strany serveru)
Napájecí zdroje	2x napájecí zdroj min. 600 W, redundance, min. Platinum specifikace dle 80 PLUS https://cs.wikipedia.org/wiki/80_Plus
Rozšiřující sloty	Min. 3ks PCI-e sloty x16 Gen4
Síťové porty	Min. 2x LAN 10/25GbE SFP28 s možností budoucí výměny např. za 100GbE – typ OCP, včetně SFP+ modulů
Kompatibilita	Microsoft Windows Server® Red Hat® Enterprise Linux SUSE® Linux Enterprise Server

	VMware® ESXi
HBA	Min 1x dvouportová HBA SAS 12Gb karta kompatibilní s nabízeným diskovým polem
Management a vzdálená správa	Stavové informace na čelním panelu s výraznou indikací nestandardních a chybových provozních stavů či parametrů (min. napájení, teplota, vada HDD). Aktivní indikace standardního provozního stavu. V případě závady zobrazuje její popis v textové formě. Vzdálená správa – dostupnost centrálního management prostředí serveru, nezávislého na spuštěné virtualizační platformě, či spuštěném operačním systému, vč. monitoringu, chybových hlášení emailem, vzdáleného a lokálního připojení (KVM) prostřednictvím dedikovaného LAN portu s podporou IPv4 a IPv6 Vzdálená správa musí disponovat vlastním management GUI, přístupným z běžných www prohlížečů. GUI musí být čistě v HTML5 a nesmí využívat dodatečných JAVA nebo ACTIVE-X komponent. Musí umožnit vzdálenou obrazovku s konzolí, možnost vzdáleného připojení ISO virtuální DVD a možnost vzdáleného připojení USB disku. Management serveru musí disponovat vlastním úložištěm pro firmware, ovladače a softwarové komponenty. Komponenty mohou být setříděny a organizovány do instalačních sad a mohou být použity pro obnovu či přeinstalaci vadného firmware. Centrální management serverů musí disponovat analytickou komponentou, která musí umožnit kontrolu nastavení bezpečnostních pravidel serveru oproti šabloně bezpečnostních zásad (například kontrola síly administrátorských hesel, platnosti certifikátu, zapnutí TLS pro management konzoli serveru, vypnutí USB portů a další). Tyto šablony musí být nezávislé na modelu serveru výrobce.
Bezpečnost	Z důvodu bezpečnosti musí management serveru umožňovat zakázání (a opětovné povolení) nepoužívaných USB portů, změna stavu USB portu musí být možná bez nutnosti restartu serveru. Server musí disponovat bezpečnostním systémem ověření komponent. Tento systém musí umožňovat ověřit, že mezi výrobou serveru a doručením k zákazníkovi nebyla konfigurace komponent serveru změněna ani upravena.
Compliance	Centrální management serverů musí umožňovat „server bare metal“ deployment založený na šablonách (předdefinovaných konfiguracích pravidel, jejichž součástí je kromě samotného OS i konfigurace BIOS, RAID, LAN, MAC, WWN). Z bezpečnostních důvodů musí být možné naplánovat pravidelné provedení porovnání aktuálního stavu konfigurace serveru s aplikovanou šablonou automatizovaným způsobem, s automatickým zasláním reportu o výsledku porovnání emailem. je-li tato vlastnost licencována, požadujeme plnou licenci v ceně serveru.
Automatizace	Management serveru musí umožňovat integraci do stávající virtualizační platformy VMware vCenter serveru s plnou podporou správy a updatovaní firmware serveru z prostředí vCenter serveru a s podporou vSphere Lifecycle Manager.
Záruka a technická podpora výrobce	Záruka a záruční servis min. 60 měsíců Dostupnost podpory 24 hodin denně, 365 dní v roce Reakční doba do konce následujícího pracovního dne od nahlášení na linku podpory. Servis je poskytován přímo výrobcem hardware. Oprava v místě instalace hardware. Možnost automatického generování servisního incidentu přímo u výrobce hardware

	(server musí být schopen automatizovaného předávání závad a otevírání servisních požadavku na helpdesk výrobce). Podpora musí zahrnovat i nárok na aktualizace software a firmware pro komponenty serveru. Podpora prostřednictvím Internetu musí umožňovat ověření typu a délky záruky a stahování aktuálních ovladačů, firmware, software a manuálů z internetu adresně pro konkrétní zadané sériové číslo zařízení bez nutnosti vytvoření uživatelského účtu pro danou činnost.

Jako příslušenstvím každého serveru bude dodáno PDU s následujícími parametry:

Parametr	**Minimální požadavky**
Provedení	do racku
Kapacita výstupního výkonu	max. 10A zatížení, 2300VA
Výstupní zásuvky	min. 8x zásuvka pro připojení zařízení (7x IEC320 C13 pro spotřebiče + 1x IEC320 C14 pro připojení)
Vlastnosti	možnost připojení senzorů teploty a vlhkosti (nejsou součástí dodávky) ovládání přes internetový prohlížeč na předním panelu LED diody signalizující stav zařízení LCD panel centralizovaná inteligentní správa připojených zařízení měření banku (všech zásuvek dohromady) v reálném čase napětí (V), proudu (A) a zatížení (W), spotřeby (kWh) podpora bezpečného vypnutí zařízení podpora V3 SNMP software a eco Sensors software pro vytváření reportů
Podpora	Podpora 10/100Mbit Ethernet Interface Podpora TCP/IP, UDP, HTTP, HTTPS, SSL, DHCP, SMTP, NTP, DNS, Auto Sense, Ping, SNMP V1,V2&V3 Podpora 2-level account/password security, IP/MAC filter, 128 bit SSL, RADIUS Podpora eco Sensors, Browser (IE, Firefox, Chrome, Safari)
Záruka	Min 2 roky na zařízení

6.3 Datové úložiště s příslušenstvím

Řešení musí splňovat následující minimální požadavky na parametry a funkcionalitu:

Parametr	**Minimální požadavky**
Provedení	Umístitelné do racku, včetně montážního materiálu
Parametry řadičů pole	2x hot-swap řadič, alespoň Dual-Active architektura s možností rozkládat zátěž mezi řadiči Každý řadič osazen alespoň 16GB paměti (celkem 32GB paměti) 12Gbit/s SAS připojení disků (Backend konektivita) na každém řadiči Celkem 8x 12Gb SAS ports (4x na každý řadič) 2x dedikovaný 1000baseT management port, vždy jeden na řadiči
Rozšiřitelnost pole	Rozšiřitelnost - pole v dodané konfiguraci musí být za provozu rozšiřitelné pomocí expanzních polic

	na nejméně 270 hot-plug disků SFF/LFF - možnost kombinovat SSD, rotační SAS i rotační NL_SAS disky bez omezení - SSD disky musí být konfigurovatelné jako datové nebo také v režimu minimálně read akcelerátoru (cache)
Konstrukce	Max. 2U - v rámci 2U musí být k dispozici základní jednotka pole (2x řadiče a napájení) a základní osazení disky Min. 24x 2,5" hot-plug diskových pozic v rámci základní jednotky Redundantní napájení dimenzované pro plný počet disků a řadiče (základní jednotka) Rackmount, včetně montážního kitu do standardního 19" racku.
Počet a typ disků	Osazení hot-plug disky v poptávané konfiguraci min. 6x 3,84TB SSD SAS 12Gbit/s 1DWPD, Hot Plug 6x 2,4TB SAS 10K Poptávanou konfiguraci musí být možné kdykoli rozšířit o další disky SSD, SAS i NL_SAS (připouští se doplněním příslušných expanzních jednotek)
Podpora RAID	Typy RAID: - JBOD - RAID 0,1, 5, 6, 10 - distribuovaný RAID - Možnost použít více typů RAID v rámci jednoho pole.
Funkcionalita	Software funkcionalita (licence bez omezení na počet serverů nebo kapacitu pole) - thin provisioning - distribuovaný RAID a hotsparing - standardní RAID skupiny a dedikované hotspare disky - automatický tiering (SSD, SAS a NL_SAS tier) - SSD cache - klony a snapshoty (1024 ks) - vzdálené zrcadlení mezi dvěma nebo více poli (alespoň asynchronní) - úložiště musí podporovat správu pomocí GUI z webovského prohlížeče HTML5, CLI pomocí SSH - podpora SNMP v3 - podpora notifikací pomocí emailu, SNMP trap, na vzdálený syslog server - součástí managementu úložiště musí být vestavěná funkcionalita call-home (úložiště musí být schopno automatizovaného předávání závad a otevírání servisních požadavku na helpdesk výrobce)
Kompatibilita	Nabízená technologie diskového pole musí být kompatibilní min. s: - RedHat Linux 8.2 - SuSe Linux 15.2 - MS Windows 2022, 2019, 2016 - VMware ESX 7.0, 8.0
Záruka a záruční servis	Záruka a záruční servis min. 60 měsíců Dostupnost podpory 24 hodin denně, 365 dní v roce. Reakční doba do konce následujícího pracovního dne od nahlášení na linku podpory. Servis je poskytován přímo výrobcem hardware. Oprava v místě instalace hardware. Možnost automatického generování servisního incidentu přímo u výrobce hardware (úložiště musí být schopno automatizovaného předávání závad a otevírání servisních požadavku na helpdesk výrobce).

	Podpora musí zahrnovat i nárok na aktualizace software a firmware pro komponenty úložiště. Podpora prostřednictvím Internetu musí umožňovat ověření typu a délky záruky a stahování aktuálních ovladačů, firmware, software a manuálů z internetu adresně pro konkrétní zadané sériové číslo zařízení bez nutnosti vytvoření uživatelského účtu pro danou činnost. Všechny SSD disky jsou předmětem záručních podmínek bez jakýchkoli omezení z pohledu životnosti, intenzity využití, množství zápisů a případně jiných neuvedených omezení.

6.4 UPS

Řešení musí splňovat následující minimální požadavky na parametry a funkcionalitu:

Parametr	**Minimální požadavky**
Provedení	do racku, včetně montážních ližin
Kapacita výstupního výkonu	Min. 2700 W / 3000 VA
Výstupní napětí	230V
Výstupní zásuvky	Min 8x IEC 320 C13 Min. 2x IEC 320 C19
Síťová karta	pro vzdálené monitorování a řízení UPS. Podpora SNMP v3, HTTPS Podpora IPv4 a IPv6
Stavové diody	min. indikující stavy: Napájen ze sítě, napájen z baterie, nutno vyměnit baterie, přetížení UPS
LCD display	zobrazující min. kapacitu baterie, účinnost, zatížení UPS, spotřebu energie. Možnost nastavení základních parametrů UPS včetně konfigurace výstupních zásuvek a nastavení zvukových upozornění
Battery Pack	Včetně jednoho battery packu
Rozšiřitelnost	Možnost připojení dalšího externího battery packu (není součástí dodávky)
Účinnost	98%
Záruka UPS	Min 5 let na zařízení i na baterie. U baterií akceptujeme záruku vztahující se pouze na závady, nikoliv na sníženou dobu zálohy.

6.5 Licence

Řešení musí splňovat následující minimální požadavky na parametry a funkcionalitu:

Parametr	**Minimální požadavky**
Operační systémy serverů	Windows Server v edici umožňující neomezený běh virtuálních serverů na stávající virtualizaci VMware pro všechny nabízené servery (hypervisory) pokrývající nabízené CPU
Přístupové licence na operační	250ks přístupových licencí vázaných na uživatele

systém serverů	

Je požadována dodávka licencí, jejichž pravost je garantovaná a ověřitelná u vlastníka autorských práv MICROSOFT.
Uchazeč zároveň poskytne dokumentaci, ze které bude jasný původ, resp. prodejní kanál licencí nebo zajistí zpracování smlouvy se společností Microsoft (Microsoft – SELECT Plus, Open, CSP, MPSA, EA) ve prospěch objednatele.
Vyžaduje se dodání licencí formou licenčního portálu vázaného na koncového zákazníka (objednatele), jehož součástí budou:

- Seznam nabízených licencí a jejich počet,
- Instalační médium,
- Instalační klíče,
- resp. další informace vztahujících se k licencím

Pro zdokumentování jasného původu požaduje zadavatel poskytnout dokumentaci obsahující označení prvního nabyvatele softwaru a také číslo smlouvy, pod kterou byl software pořízen, úplný řetězec vlastníků softwaru, potvrzení o odinstalaci od každého z předchozích vlastníků.
Jsou požadovány licence pro užití On-Premise.
Zdůvodnění požadavku na kompatibilitu
Zadavatel provozuje své technologické prostředí postavené na platformě OS Windows a hypervisoru VMware. Na této platformě je pak provozována majorita agendových informačních systémů zadavatele, které slouží k zajištění výkonu jeho veřejné správy a dále k zajištění interních činnosti a agend. Na této platformě jsou rovněž provozována adresářové služby a řízení uživatelských účtů a práv v nich. Z těchto důvodů je požadována kompatibilita s tímto technologickým prostředím a jako definice požadavku je uveden konkrétní produktový název.

7 Další požadované implementační služby

7.1 Požadavky na zpracování prováděcí dokumentace

Prodávající před zahájením implementačních prací zpracuje prováděcí dokumentaci, která bude důsledně vycházet z předimplementační analýzy a bude zahrnovat všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění.

(Jako podklad pro zpracování prováděcí dokumentace prodávající provede předimplementační analýzu, která bude zohledňovat stávající prostředí kupujícího ve vztahu ke konkrétnímu nabízenému plnění prodávajícího, zejména pak s ohledem na prodávajícím použité technické řešení, minimálně pro následující oblasti:

(a) Analýza a vyhodnocení stávajícího stavu, identifikace slabých míst a bezpečnostních rizik, včetně vazeb na HW a SW systémy.

(b) Způsob začlenění nabízených komodit do prostředí kupujícího.

(c) Síťová infrastruktura ve vztahu k plánovanému využití.

(d) Virtualizační infrastruktura (serverová, disková) ve vztahu k plánovanému využití.

(e) Analýza možností napojení zdrojových aplikačních systémů, resp. možností získávání jejich dat.

(f) Integrace nabízených softwarových systémů.

(g) Požadavky na rekonfiguraci stávajících systémů ve vztahu k plánovanému využití jejich dat.

(h) Dopady implementace na dostupnost a funkčnost stávajících služeb.

(i) Posouzení dopadů na non-IT technologie (spotřeba energií, tepelný výkon).

(j) Požadované součinnosti kupujícího.

(k) Návrh opatření k odstranění neshod zjištěných v průběhu analýzy.

Prováděcí dokumentace musí zohlednit podmínky stávajícího stavu, požadavky cílového stavu dle zadávací dokumentace a konkrétního technického řešení nabízeného prodávajícím a musí obsahovat minimálně tyto části:

(a) Detailní popis cílového stavu včetně funkcionalit jednotlivých částí systému,

(b) Nutné a doporučené optimalizační a konfigurační změny dodávaných systému i všech navázaných systémů (ESX, LAN, VPN atd.),

(c) Způsob zajištění dodávek a služeb, včetně harmonogramu zajištění HW dodávek

(d) Způsob zajištění koordinace realizace předmětu plnění s běžným provozem,

(e) Detailní návrh a popis postupu implementace předmětu plnění,

(f) Detailní popis zajištění bezpečnosti informací,

(g) Detailní harmonogram projektu včetně uvedení kritických milníků,

(h) Vazby na stávající systémy a jejich konfigurace,

(i) Návrh akceptačních kritérií a akceptačních testů,

(j) Detailní popis navrhovaných školení.

(k) Obsah a rozsah provozní dokumentace.

Prováděcí dokumentace bude ve lhůtě do 10 pracovních dní od předání prodávajícím připomínkována kupujícím a připomínky budou ze strany prodávajícího vypořádány (tj. zapracovány, případně s jasným a konkrétním písemným zdůvodněním odmítnuty jako nevalidní). Ze strany kupujícího nebude v rámci připomínkování v případě nepravdivých, nepřesných nebo věcně nejasných informací v této dokumentaci požadováno její opravování na správné znění, bude se pouze jednat o vyznačení výše uvedených nedokonalostí a bude na prodávajícím jejich řádné zpracování.

7.2 Zvýšení zabezpečení komunikační sítě

- Analýza stávajícího síťového prostředí a návrh nové architektury LAN, WiFi, VPN
- Zavedení segmentace a IEE802.1X
- Výměna aktivních prvků
- Návrh a provedení akceptačních testů

7.3 Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů

- Analýza a detailní identifikace zdrojů dat, jejichž provozně bezpečnostní informace bude nutné, popř. vhodné sbírat, korelovat a analyzovat. Bude obsahovat i návrh způsobu zpracování získaných informací a vhodných proaktivních i reaktivních akcí

- Vybudování systému centrálního logování pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů
- Návrh a provedení akceptačních testů, musí zahrnovat i testy archivace a obnovy logů a ověření detekce jejich neoprávněně modifikace.

7.4 Nástroje pro zajišťování úrovně dostupnosti informací

- Analýza současného způsobu ukládání a zálohování dat, návrh způsobu modernizace diskového úložiště a zálohování bez významného omezení provozu města, nasazení nových a změna umístění současných Hypervisorů, zprovoznění DR lokality
- Provedení modernizace diskového úložiště v hlavní lokalitě, včetně migrace vybraných současných hypervisorů a potřebná migraci dat v souvislosti se změnami v infrastruktuře
- Rekonstrukce zálohovacího systému se začleněním bezpečného úložiště
- Návrh a provedení akceptačních testů, musí zahrnovat výkonové testy a testy vysoké dostupnosti, dále obnovení min. 1 virtuálního serveru ze zálohy z každého úložiště záloh (tj. min 2 obnovy)
- Zapojení UPS a všech prvků v hlavní lokalitě, konfigurace virtualizační vrstvy, otestování výpadku el. energie.
- Zprovoznění DR lokality, nastavení replikace virtuálních serverů do DR lokality, otestování celého řešení.

7.5 Zaškolení administrátorů

Společné zaškolení administrátorů technologií na dodané technologie v rozsahu min. 6 hodin (může proběhnout v jednom termínu pro všechny technologie nebo může být rozděleno na dva termíny s celkovou časovou alokací min. 6 hodin).

7.6 Harmonogram a časový rámec pro realizaci instalačních služeb

Do dvou týdnů od nabytí účinnosti smlouvy na předmět plnění dle této technické specifikace předloží prodávající návrh závazného harmonogramu jednotlivých dodávek a prací, včetně požadavků na součinnost osob kupujícího. Kupující do 1 týdne návrh harmonogramu odsouhlasí, nebo k němu poskytne konkrétní závazné připomínky. Následně bude harmonogram považován za závazný, včetně smluvních pokut plynoucích za jeho nedodržení zanesených v kupní smlouvě.

S ohledem na skutečnost, že městský úřad nemůže přerušit svůj provoz, a dále na skutečnost, že v prostředí města je potřeba zachovávat potřebnou míru čistoty a klidu, mohou fyzické instalační práce probíhat v pracovních dnech pouze v časech 15:00 až 05:00 hodin a o víkendech v časech 12:00 až 05:00 hodin, nebude-li v konkrétních případech dohodnuto jinak.

Konfigurační služby a služby realizované formou vzdáleného přístupu mohou být realizovány i mimo výše uvedenou dobu, za předpokladu, že budou založeny na schváleném harmonogramu.

Přípravné práce, které nebudou zasahovat do aktivního propojení sítě bude možné ze strany prodávajícího realizovat i mimo tyto časy na základě dohody s kupujícím.

S ohledem na povahu organizace kupujícího musí prodávající při realizaci konfiguračních pracích vzít v úvahu potřebu řádného provozu informačních systémů závislých na službách zajišťovaných

prostřednictvím dodávaných technologií, které budou v rámci realizace tohoto plnění nasazovány nebo rekonfigurovány a v návrhu harmonogramu a při realizaci prací toto musí prodávající zohlednit.

7.7 Zkušební provoz

V rámci realizovaného plnění je požadován zkušební provoz nově nasazených technologií jako celku.

Zkušební provoz je součástí plnění dle této technické specifikace a je i součástí plnění tak, že je potřeba jej zohlednit do harmonogramu prací ze strany prodávajícího.

Požadovaná minimální délka zkušebního provozu jsou dva kalendářní týdny.

Předmětem zkušebního provozu je ověření provedených dodávek a služeb, tedy zejména funkčnosti dodaných zařízení a správnosti provedené konfigurace.

Zahájení zkušebního provozu proto musí předcházet nasazení všech technologií a provedení všech souvisejících dodávek a služeb (zejména konfigurací).

Zahájení zkušebního provozu podléhá předložení potvrzení o instalaci a konfiguraci technologií ze strany prodávajícího a potvrzení možnosti zahájení zkušebního provozu ze strany kupujícího.

Délka zkušebního provozu je nastavena v takové délce, aby umožnila kupujícímu ověřit správnost provedené konfigurace a dále schopnosti dodaných zařízení plnit požadavky na ně stanovené. Délka zkušebního provozu byla stanovena tak, aby kupujícímu umožnila ověřit většinu procesů a situací v rámci uvažovaného užití předmětu plnění.

7.8 Kybernetická bezpečnost

Předmět plnění dle této technické specifikace vstupuje do informačního prostředí města, které podléhá na rozličné úrovni dopadům následujících právních předpisů:

- zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
- vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
- Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)

Prodávající musí jednat řádně a v kontextu výše uvedených právních předpisů v oblasti kybernetické bezpečnosti a v případě potřeby si v rámci realizace plnění vyžádat od kupujícího doplňující informace tak, aby byl připraven reflektovat své jednání a proces realizace plnění v souladu s výše uvedenými předpisy a jejich případnou formou implementace v organizaci kupujícího.

7.9 Projektové řízení

S ohledem na rozsah projektu a dopad jeho zavedení do produkčního provozu na výkon činnosti kupujícího je v rámci dodávky předmětu plnění kupujícím požadováno aplikování základních principů projektového řízení ze strany prodávajícího.

Jedná se zejména řízení projektových prací v souladu s uzavřenou smlouvu s ohledem na věcné plnění dané smlouvou – rozsah, posloupnost a hloubku projektových prací, (tj. harmonogramu) – řízení postupu prací s ohledem na závazný harmonogram projektu – dodržování termínů harmonogramu, podchycení

případných kolizí, zpoždění nebo vznikajících rizik a jejich reportování směrem ke kupujícímu, aktivní řešení výše uvedených nestandardních situací

Zápisy - Zpracování pravdivých, úplných a věcně jasných a vypovídajících zápisů z konzultačních schůzek a pracovních jednání (s cílem zaznamenání klíčových rozhodnutí, ujednání, navržených nebo dohodnutých termínů a způsobů řešení dílčích částí projektu atd.)

Kontrolní dny - Prezenční účast odpovědné osoby prodávajícího na kontrolních dnech v pravidelných min. měsíčních intervalech v sídle kupujícího, případně se souhlasem obou smluvních stran formou videokonference nebo telekonference. Termíny kontrolních dnů budou součástí harmonogramu.

Reporting - Reporting plnění na úrovni pravidelných dvoutýdenních písemných zpráv směrem k odpovědné osobě kupujícího (seznam prací, které byly vykonány pro danou část projektu, stav těchto prací (ukončeno, odloženo, v realizaci); popis vzniklých problémů a způsob jejich řešení. Kupující si vyhrazuje právo vyžádat reporting projektu i mimo dvoutýdenní interval, na takovou žádost bude prodávající povinen reagovat vždy nejpozději písemnou zprávou do 4 pracovních dnů.

Řízení rizik plnění, hodnocení pravděpodobnosti jejich výskytu a míry dopadu, návrh řešení k jejich eliminaci.

Řízení změn na plnění, v případě požadavků na změnu v plnění provedení konzultací k ověření nutnosti změny plnění; zjištění dopadu požadovaných změn směrem ke koncepci celkového řešení, harmonogramu, dotačnímu titulu, vytížení lidských zdrojů atd. V případě odsouhlasení změn spolupráce při implementaci změn do plnění, komunikace s dalšími zapojenými osobami a specialisty za dotčené technologie a informační systémy.

7.10 Požadavky na provedení akceptačních testů

Prodávající navrhne způsob a provedení akceptačních testů. Akceptační testy musí pro všechny technologie v rámci plnění vždy zahrnovat minimálně:

(a) Prokázání kompletnosti dodávky a splnění povinných i hodnocených požadavků.

(b) Prokázání vysoké dostupnosti u řešení, která jsou takto koncipována.

(c) Prokázání aktivací software i hardware aktivačními klíči či jinými prostředky, je-li aktivace potřebná.

(d) Prokázání registrace / aktivace podpory hardware a software výrobce, je-li podpora součástí dodávky a její aktivace potřebná

(e) Pro každou komoditu navrhne prodávající vhodné doplňující testy a kritéria, kterými bude prokázána bezproblémová funkčnost a stabilita dodaného řešení.

(f) Výkonové testy prokazující shodu s požadovanými výkonnostními parametry a dále výrobcem deklarovanými či s ohledem na technologii objektivně očekávatelnými parametry, např. výkon u datových úložišť (IOPS, přenosová rychlost, latence)

O provedení akceptace a jejím výsledku musí být vyhotoven písemný akceptační protokol. Šablony akceptačních protokolů budou předány kupujícím při zahájení plnění, pro zapracování prodávajícím do prováděcí dokumentace.

Podrobný popis nabízeného plnění

Komodita	Zajišťovaná oblast	Technologie
4.1	Systém řízení přístupu do sítě podle standardu IEEE 802.1X (network access control)	**Aruba Clearpass Policy Manager + licence pro 500 konkurenčních zařízení**
4.2	Přepínače s příslušenstvím	**18x Síťové přepínače Aruba 6100**
5.1	Systém pro správu logů	**1x LogManager L + 10 Gbe NIC SFP+**
6.1	Zálohovací úložiště s časovým zámkem	**1x Exagrid EX27**
6.2	Produkční server s příslušenstvím + PDU	**2x PowerEdge R660 + 2x PDU PE-5108G**
6.3	Datové úložiště s příslušenstvím	**1x Dell PowerVault ME5024 Storage Array**
6.4	UPS	**1x Eaton 9PX 3000i RT2U, battery pack, 9PX 72V RT3U, Eaton Komunikační karta - Gigabit Network Card**
6.5	Licence	**2x Windows Server Datacenter + 250 USER CAL**

Systém řízení přístupu do sítě podle standardu IEEE 802.1X (network access control)

Systém řízení přístupu do sítě podle standardu IEEE 802.1X			
Parametr	**Minimální požadavky**	**Způsob naplnění tohoto povinného parametru**	**Odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
Provedení	Softwarová appliance pokročilého NAC (network access control) na bázi standardu IEEE 802.1X. Integrovaná podpora autentizace, autorizace a účtování (přístupů) uživatelů i koncových zařízení, integrovaný RADIUS server a databáze uživatelů a zařízení.	Pokročilý systém řízení přístupu do sítě (network access control) v povedení softwarové appliance založená na IEEE 802.1X. Podporuje autentizaci, autorizaci, účtování přístupů uživatelů i libovolných síťových zařízení. Obsahuje RADIUS server i databáze uživatelů a zařízení.	Aruba ClearPass.pdf
Nastavení přístupů	Nastavení síťového přístupu uživatelů a zařízení podle politik min. pomocí přiřazení VLAN, ACL. Atributy pro definici politik min. IP, MAC, port, VLAN, QinQ VLAN, hostname (PC name), uživatelské jméno (z Active Directory), operační	Umožňuje nastavit síťový přístup uživatelů a zařízení podle politik pomocí přiřazení VLAN, ACL. Atributy pro definici politik IP, MAC, port, VLAN, Q in Q VLAN, hostname (PC name), uživatelské jméno Active Directory, operační systém	ClearPass-Wired.pdf

	systém		
Autentizace	Zajištění IEEE 802.1X autentizace a autorizace pro bezdrátové sítě, Ethernet LAN sítě a VPN	Podporuje autentizaci a autorizaci pomocí IEEE802.1X pro různé typy sítí (včetně bezdrátových, Ethernet LAN a VPN) napříč různými výrobci	Aruba ClearPass.pdf
Základní autentizační metody	Min. PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, MAC autentizace, certifikáty	Podpora EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS), PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP- Public, EAP-PWD), TTLS (EAP-MSCHAPv2, EAP-GTC, EAP- TLS, EAP-MD5, PAP, CHAP), MAC authentication, Online Certificate Status Protocol (OCSP), Admin/operator access security via CAC and TLS certificates	Aruba ClearPass.pdf
Identity	Vestavěná databáze identit pro autentizaci, podpora standardních identitních databází - Active Directory, LDAP, ODBC	Interní databáze využitelná napříč doménami, podpora Active Directory, LDAP, ODBC	Aruba ClearPass.pdf
Nezávislá autentizace a autorizace	Úplné oddělení autentizace a autorizace, např. autentizace proti službě Active Directory, ale autorizace proti externí SQL databázi.	Podpora více nezávislých zdrojů pro autentizaci a autorizaci včetně Active Directory, SQL databáze a požadovaného scénáře.	Aruba ClearPass.pdf
Rozšířená autentizace a autorizace	Podpora autentizace a autorizace min. LDAP, Microsoft Active Directory, generická SQL databáze, Kerberos, HTTPS web autentizace, Single Sign-On (minimálně SAML 2+ IdP a SP, OAuth, Shibboleth a Okta).	Pro autentizaci a autorizaci jsou podporovány LDAP, MS AD, obecná SQL databáze (vč. MySQL, PostGRES, Oracle, ODBC), Kerberos, web autentizace (https). Systém podporuje Single-Sign-On SAML2 (standardní podpora Identity Providers (IdP) a Relying Party (RP)), Oauth2, Shibboleth i Okta	Aruba ClearPass.pdf
Kontextová autorizace	Autorizace zařízení a uživatelů na základě kontextových informací jako čas, typ připojení, osobní profil či členství ve skupině v Active Directory.	Integrovaný context-based policy engine umožňuje autorizace na základě libovolných atributů z Active Directory a parametrů připojení, zařízení či uživatele včetně času, typu připojení, osobního profilu	Aruba ClearPass.pdf ClearPass-Wired.pdf
Externí identity	Podpora autentizace externími identitami - min. Microsoft, Google.	Podpora externích (cloudových identit Microsoft Azure AD a Google Workspace (dříve G Suite).	Aruba ClearPass.pdf
Komplexní autorizace	Autorizace uživatelů na základě jejich vlastních accounting informací z předchozích připojení – např. pro omezení celkového času online či objemu přenesených dat za delší časové období	Uživatele lze autorizovat podle politik s využitím účtovaných informací z předchozích připojení, např. čas, objem přenesených dat. Včetně příkladového scénáře.	ClearPass-Wired.pdf
Dynamická autorizace	Podpora RADIUS CoA podle RFC3576. Možnost změny autorizačního stavu zařízení bez	Plná podpora RADIUS CoA (Change of Authorization) podle RFC3576 pro změnu autorizačního stavu zařízení beze změny	Aruba ClearPass.pdf ClearPass User Guide.pdf

	nutnosti změny definice autorizační politiky, např. pro odpojení nebo karanténu koncových zařízení.	politiky.	
Izolace klientů	Zpracovávání syslog zpráv z externích zdrojů, vyhledávání definovaných událostí a automatizovaná reakce na ně. Minimálně v rozsahu příjmu zpráva ze stávajícího firewallu a izolace konkrétního klienta na základě těchto zpráv.	Podrobné zpracování syslog zpráv a automatizované reakce pomocí Ingress Enevt Engine. Podpora integrace firewallů Fortinet a izolace klientů.	ClearPass Ingress.pdf ClearPass Fortinet.pdf
Zpracování syslog	Vestavěná podpora tvorby a úprav vlastních parserů, syslog zpráv pro napojení na další systémy třetích stran	Tvorba vlastních parserů syslog zpráv pro napojení na 3d party systémy	ClearPass Ingress.pdf ClearPass Exchange.pdf
Bezpečnost	Podpora okamžitého odpojení zařízení při vypršení libovolné autorizační podmínky (např. překročení objemu dat, časového intervalu, stavu zařízení apod.)	Funkce RADIUS Dynamic Authorization umožňuje okamžitého odpojení zařízení při vypršení libovolné autorizační podmínky (např. překročení objemu dat, časového intervalu, stavu zařízení apod.)	ClearPass User Guide.pdf
Správa	Vestavěné nástroje pro testování politik, diagnostiku chování systému i spravovaných zařízení	Snadná správa systému integrovanými nástroji pro testování politik, diagnostiku chování systému i spravovaných zařízení	ClearPass User Guide.pdf
Portál	Captive portál pro uživatele a jejich rozšířenou autentizaci, podpora více graficky i obsahově unikátních portálů provozovaných souběžně. Integrovaná podpora úpravy vzhledu	Modifikovatelná captive portál pro rozšířenou autentizaci uživatelů s možností paralelního běhů více unikátních instancí, integrovaný nástroj pro úpravy.	Aruba ClearPass.pdf
Rychlé přihlášení	Podpora přihlášení prostřednictvím QR kódu. Zapamatování úspěšně autentizovaných/registrovaných klientů a zjednodušení opakovaných přihlášení (např. jen potvrzení uvítací/informační) stránky.	Možnost přihlašování klientů pomocí QR kódu s možností zjednodušeného opakovaného přihlášení.	ClearPass QR.pdf
Registrace	Podpora samoobslužné registrace s ověřením SMS, e-mailem apod.	Integrovaná samoobslužné registrace, ověření / distribuce údajů SMS, e-mail, tištěná vizitka. Podpora externích identit, např. Facebook, Twitter	Aruba ClearPass.pdf
Ochrana identit	Veškeré identitní údaje v systému budou uložena ve výrobcem dodané a podporované	Interní databáze (nativní součást systému) je šifrována AE2-256 a jsou v ní uloženy veškeré (interní) identitní údaje	ClearPass AES256.pdf

	šifrované databázi, která bude nativní součástí dodaného produktu, s minimální enkrypcí uložených dat ve standardu AES min. 128-bit.		
Speciální zařízení	Podpora autentizace a řízení přístupů speciálních ("nepočítačových") zařízení zejména tiskárny, modality, technologické prvky, IoT.	Integrovaná podpora autentizace a autorizece libovolných i speciálních / nepočítačových síťových zařízení min. s využitím MAC	Aruba ClearPass.pdf ClearPass User Guide.pdf
Vysoká dostupnost	Integrovaná podpora vysoké dostupnosti v režimu active-active, tj. vytvoření clusteru min. 2 appliance. Druhá appliance je součástí dodávky.	Systém podporuje vysokou dostupnost a (High Availability) a rozkládání zátěže (load balancing) ze 2 uzlů (cluster) doplnění o další appliance je součástí nabídky	ClearPass User Guide.pdf
Licence	Licence pro min. 500 konkurenčních koncových zařízení ověřovaných pomocí 802.1X bez omezení počtu uživatelů.	Licence pro 500 konkurenčních koncových zařízení ověřovaných pomocí 802.1X bez omezení počtu uživatelů.	Součást nabídkové ceny
Automatizace a integrace	REST-API rozhraní min. pro základní funkce AAA, příjem syslog hlášení z externích zdrojů, vyhledávání klíčových událostí a automatizovaná reakce na ně. Tvorba/modifikace vlastních parserů syslog.	Integrované RESTful API pro autentizaci/autorizaci/účtování. Příjem syslog událostí, prohledávání a automatické reakce. Vlastí parsery syslog.	Aruba ClearPass.pdf ClearPass User Guide.pdf ClearPass Ingress.pdf ClearPass Exchange.pdf
Kompatibilita	Appliance určena pro provoz v prostředí stávající serverové virtualizace	Podpora ESX	Aruba ClearPass.pdf
Podpora	Podpora výrobce software min. 60 měsíců včetně nároku na nové verze software včetně aktualizací.	Záruka 60 měsíců v místě instalace, včetně podpory výrobce a nároku na nové verze software včetně aktualizací.	Součást nabídkové ceny

Přepínače s příslušenstvím

Přístupový přepínač			
Parametr	**Minimální požadavky**	**Způsob naplnění tohoto povinného parametru**	**Odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
Základní parametry	L2/3 přepínač v rackovém provedení	Aruba 6100 L3/L2 switch v rackovém provedení	Aruba 6100.pdf

Porty a propustnost	min. 48x 1 GB RJ-45 PoE+ + 4x 10Gb SFP+ (nesdílené), min. 176 Gb/s	48x 1Gb Base-T POE+ + 4x 10Gb SFP+ nesdílené, propustnost 176 Gb/s	Aruba 6100.pdf
Směrování	min. statické směrování na L3 vrstvě pro IPv4 I IPv6	Switch umožňuje statické směřování na L3 pro IPv4 a IPv6	Aruba 6100.pdf
Propustnost	neblokovaná architektura	Definovaná propustnost switche je v non-blocking architektuře	Aruba 6100.pdf
Automatizace VLAN	Podpora protokolu MVPR pro automatické zjišťování a přiřazení	Switch podporuje protokol Multiple VLAN Registration Protocol pro automatické zjišťování a přiřazení	Aruba 6100.pdf
Agregace portů	podpora LACP	Switch podporuje agregaci portů LACP	Aruba 6100.pdf
Dualstack	IPv4 a IPv6 dualstack včetně podpory ACL a QoS	Switch podporuje DualStack IPv4 a IPv6 dualstack včetně podpory ACL a QoS	Aruba 6100.pdf
VLAN	VLAN 802.1Q, MAC i protocol based, podpora zařazování do VLAN a přidělení QoS a přístupových filtrů na základě 802.1X ověření	Switch umožňuje VLAN 802.1Q, MAC i protocol based, podpora zařazování do VLAN a přidělení QoS a přístupových filtrů na základě 802.1X ověření	Aruba 6100.pdf
Ověřování uživatelů a zařízení	podpora 802.1X	Switch podporuje 802.1x	Aruba 6100.pdf
Zrcadlení portů	Zrcadlení provozu portů pro diagnostiku a bezpečnostní monitoring, min. 4 zrcadlené skupiny	Switch podporuje zrcadlení provozu portů pro diagnostiku a bezpečnostní monitoring, min. 4 zrcadlené skupiny	Aruba 6100.pdf
Monitoring a správa	plná podpora CLI, SSH, SNMP 1-3, syslog, sFlow, RMON, web rozhraní, podpora uložení více konfigurací a min. 2 obrazů firmware pro bezpečný a jednoduchý upgrade	Switch plně podporuje CLI, SSH, SNMP 1-3, syslog, sFlow, RMON, web rozhraní, podporuje uložení více konfigurací a min. 2 obrazů firmware pro bezpečný a jednoduchý upgrade	Aruba AOS-CX 6100.pdf
Automatizace a integrace	Integrované REST API rozhraní pro ovládání síťových funkcí	Switch má integrované REST API rozhraní pro ovládání síťových funkcí	Aruba 6100.pdf
Záruka a záruční servis	min. 60 měsíců, oprava/výměna do 2 pracovních dnů v místě instalace, včetně nároku na opravné verze firmware	Záruka min. 60 měsíců, oprava do 2 pracovních dnů v místě instalace, včetně nároku na opravné verze firmware	Součást nabídkové ceny

Systém pro správu logů

Systém pro správu logů			
Parametr	**Minimální požadavky**	**Způsob naplnění tohoto povinného parametru**	**Odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
Základní funkce	Integrovaný systém zpracování logů a událostí z definovaných zdrojů napříč výrobci aplikací, operačních systémů a síťového hardware	LOGmanager je systém pro zpracování logů a událostí z definovaných zdrojů napříč výrobci aplikací, operačních systémů a síťového hardware	Logmanager Datasheet.pdf
Architektura	Integrovaná appliance (HW se specializovaným firmware/software) nebo server se specializovaným software včetně operačního a podpůrných systémů (databáze apod.), samostatně funkční nezávislé na infrastruktuře zadavatele	Systém bude dodán ve formě hardwarové appliance (hw se specializovaným firmware/software) a bude samostatně funkční nezávisle na infrastruktuře Objednatele	Logmanager Datasheet.pdf
Provedení	Určené pro montáž do stávajícího serverového datového rozvaděče 19", hloubka max 900 mm, včetně výsuvných kolejnic a ramene pro vedení kabelů.	Systém je určen pro montáž do 19“ datového rozvaděče, hloubka je menší než 800 mm a součástí dodávky budou výsuvné kolejnice a rameno pro vedení kabelů. Pro Logmanager L je jako HW platforma využitý server Dell PowerEdge R7525	Logmanager Datasheet.pdf Logmanager_L-PowerEdge R7525.pdf
Ovládání	Grafická webová konzole pro administrátory i operátory, umožňuje kompletní správu systému včetně úvodního nastavení.	Systém je ovládán prostřednictvím grafická webová konzole pro administrátory I operátory, konzole umožňuje kompletní správu systému včetně úvodního nastavení.	Logmanager Datasheet.pdf Logmanager Dokumentace.pdf
Autentizace	Autentizace uživatelů vůči Active Directory nebo LDAP serveru. V případě výpadku AD/LDAP musí systém umožnit autentizaci z lokální databáze.	Systém podporuje autentizace uživatelů vůči Active Directory nebo LDAP serveru. V případě výpadku AD/LDAP systém umožňuje autentizaci z lokální databáze.	Logmanager Dokumentace.pdf
Uživatelské role	Podpora uživatelských rolí obsahujících přístupová práva k uloženým událostem	Systém obsahuje podpora uživatelských rolí, které obsahují přístupová práva k uloženým událostem a jednotlivým ovládacím částem	Logmanager Dokumentace.pdf

	a jednotlivým ovládacím částem systému.	systému.	
Sběr dat (logů)	Je požadován bezagentový sběr logů pro uvedené zdroje logů. Pro systémy Windows je umožněn agentový i bezagentový sběr.	Systém zajišťuje bezagentový sběr logů z podporovaných systém s výjimkou Windows OS. Pro detailní logování OS Windows je vhodné do OS instalovat agenty, které jsou součástí dodávky.	Logmanager Dokumentace.pdf
Windows agent	Kompletní správa a aktualizace z administrátorské konzole, sběr dat z textových i Event logů (včetně rozšířených), šifrovaná komunikace, buffer pro případ ztráty komunikace, překlad kódů na text (např. Logon type 2 => "Interactive" apod.) a textový popis události shodný s Windows Event Viewerem	Agenty OS Windows je možné spravovat a aktualizovat z administrátorské konzole systému. Agent se systémem komunikuje šifrovaně, obsahuje lokální buffer pro případ ztráty komunikace, provádí překlad kódů na text poskytuje textový popis události shodný s Windows Event Viewerem	Logmanager Dokumentace.pdf
Protokoly	Příjem a zpracování logy, událostí a další strojově generovaných data minimálně protokoly UDP/TCP 514 (SYSLOG), TCP 20514 (RELP, nešifrovaně) a TCP 20515 (RELP, šifrovaně).	Systém podporuje příjem a zpracování logů, událostí i dalších strojově generovaných dat protokoly UDP/TCP 514 (SYSLOG), TCP 20514 (RELP, nešifrovaně) a TCP 20515 (RELP, šifrovaně).	Logmanager Dokumentace.pdf
Formáty logů	Min. RAW, Syslog, CEF, LEEF, JSON RFC7159, Windows EventLog	Systém podporuje formáty logů RAW, Syslog, CEF, LEEF, JSON RFC7159, Windows EventLog a další, včetně vlastních parserů.	Logmanager Dokumentace.pdf
Třídění logů	Podpora příjmu logů na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv.	Systém podporuje příjem logů na rozsahu více než 50 TCP a UDP portů pro zjednodušené třídění vstupních zpráv	Logmanager Dokumentace.pdf
Zpracování logů	Integrované parsování a normalizace přijatých událostí/logů bez nutnosti instalovat externí aplikace nebo systémy	Systém obsahuje parsování a normalizaci přijatých událostí/logů. Není nutné instalovat externí aplikace nebo systémy	Logmanager Dokumentace.pdf
Ochrana logů	Zamezení mazání nebo modifikování již uložených logů. Každý log musí mít unikátní identifikátor pro jeho jednoznačnou identifikaci.	Systém zamezuje mazání nebo modifikování již uložených logů. Každý log má unikátní identifikátor pro jeho jednoznačnou identifikaci.	Logmanager Dokumentace.pdf
Vizualizace logů	Grafická vizualizace logů, událostí a	Systém obsahuje grafická vizualizaci logů,	Logmanager Datasheet.pdf

	strojových dat (grafy událostí). Dynamická vizualizace - změnou volby (např. filtru) v jednom grafu se ostatní svázané grafy upraví automaticky dle požadované volby. Integrované podpora zobrazení TOP X událostí za zvolené časové období.	událostí a strojových dat (grafy událostí) včetně dynamická vizualizace – změnou volby (filtru apod.) v jednom grafu se ostatní svázané grafy upraví automaticky dle požadované volby. Systém mám Integrovánu podporu zobrazení TOP X událostí za zvolené časové období.	Logmanager Dokumentace.pdf
Pracovní plochy	Předpřipravené pohledy (dashboardy) na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění, průběžná aktualizace pohledů výrobcem. Integrovaná podpora tvorby uživatelských dashboardů včetně ukládání	Systém obsahuje předpřipravené dashboardy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění. Dashboardy jsou průběžné aktualizovány výrobcem. Systém má integrovánu podporu tvorby uživatelských dashboardů včetně ukládání.	Logmanager Dokumentace.pdf
Zajištění logů	Ochrana proti ztrátě logů při přetížení systému. Ukládání nezpracovaných logů/událostí do vyrovnávací paměti o kapacitě min 25 GB, notifikace správce systému při riziku zaplnění vyrovnávací paměti	Systém poskytuje ochranu proti ztrátě logů při přetížení systému. Ukládá nezpracované logy/události do vyrovnávací paměti o kapacitě větší než 25 GB a notifikuje správce systému při riziku zaplnění vyrovnávací paměti	Logmanager Dokumentace.pdf
Doplňování logů	Integrovaná podpora doplňování logů dalšími údaji - zejména umístění zařízení, typ zařízení, kritičnost zařízení apod. - k jednotlivým zdrojům zejména dat, aplikacím, zařízením, IP rozsahů	Systém má vestavěnu podporu doplňování logů dalšími údaji včetně umístění zařízení, typu zařízení, kritičnost zařízení a dalších k jednotlivým zdrojům dat, aplikacím, zařízením i IP rozsahů.	Logmanager Dokumentace.pdf
Archivace	Integrovaná archivace logů včetně zajištění integrity archivů, obnova	Systém obsahuje archivaci logů včetně zajištění integrity archivů a umožňuje jejich obnovu	Logmanager Dokumentace.pdf
Rozpoznávání IP, MAC	Automatické doplňování reverzních DNS záznamům k IP adresám a výrobce podle MAC adresy	Systém automaticky doplňuje reverzní DNS záznamy k IP adresám a výrobce podle MAC adresy	Logmanager Dokumentace.pdf
Časová razítka	Podpora doplňkové značky (razítka) navíc k časovému údaji zaznamenané události/logu, sloužící jako výchozí	Systém mám integrovánu podporu doplňkové značky (razítka) navíc k časovému údaji zaznamenané události/logu a tato značka slouží jako výchozí časový údaj pro systém	Logmanager Dokumentace.pdf

	časový údaj pro systém		
Vyhledávání	Snadné multikriteriální vyhledávání událostí bez nutnosti speciálních znalosti (např. SQL dotazů apod.) napříč všemi typy dat a zařízení.	Systém poskytuje jednoduché multikriteriální vyhledávání událostí bez nutnosti speciálních znalosti (např. SQL dotazů apod.) napříč všemi typy dat a zařízení.	Logmanager Dokumentace.pdf
Rychlé vyhledávání	Rychlé vyhledávání i v aktuálně uložených položkách (průběžné indexování)	Systém průběžně indexuje ukládané položky a poskytuje rychlé vyhledávání i v aktuálně uložených položkách	Logmanager Dokumentace.pdf
Geolokace	Automatické doplňování geolokačních informací k událostem a jejich grafické znázornění na mapě bez služeb třetích stran	Systém automaticky doplňuje geolokační informace k událostem z interní databáze a umožňuje jejich grafické znázornění na mapě bez služeb třetích stran	Logmanager Dokumentace.pdf
Reporty	Integrovaný reportovací nástroj s přednastavenými obvyklými reporty a možností vlastních úprav a vytvoření nových pohledů bez potřeby speciálních znalostí (zejména SQL dotazů). Průběžná aktualizace přednastavených reportů výrobcem.	Systém obsahuje integrovaný reportovací nástroj s přednastavenými obvyklými reporty a možností vlastních úprav a vytvoření nových pohledů bez potřeby speciálních znalostí (např. SQL dotazů apod.). Výrobce průběžně aktualizuje přednastavené reporty.	Logmanager Dokumentace.pdf
Integrace	Integrované REST API rozhraní pro napojené systémy, musí umožnit autorizovaný přístup ke strukturované databázi logů.	Systém obsahuje integrované REST API rozhraní pro napojené systémy, které umožňuje autorizovaný přístup ke strukturované databázi logů. Přístup k API je součástí dodávky.	Logmanager Dokumentace.pdf
Parsery	Integrovaný grafický (vizuální) nástroj pro tvorbu vlastních parserů logů včetně testování a ladění - okamžitého zobrazení rozparsovaných testovacích dat včetně případných chyb	Systém obsahuje integrovaný grafický vizuální nástroj pro tvorbu vlastních parserů logů. Nástroj umožňuje testování a ladění parserů formou okamžitého zobrazení rozparsovaných testovacích dat včetně případných chyb	Logmanager Dokumentace.pdf
Konektory	Konektory (specifické parsery) pro stávající technologie - min. Active Directory, Hyper-V, VMware, Windows (vč. DNS, DHCP), Exchange, MS SQL, Fortigate, HPE/Aruba, Dell servery,	Systém obsahuje specifické parsery Active Directory, Vmware, Windows (vč. DNS, DHCP), Exchange, MS SQL, Fortinet, HPE/Aruba, Dell servery, Synology, Linux, Apache i nabízený Systém pro analýzu síťového provozu GreyCortex	Logmanager Dokumentace.pdf

	Synology, Linux, Apache.		
Alerty, notifikace	Předpřipravené alerty a integrovaný grafický (vizuální) nástroj pro vytváření automatických notifikací/alertů generovaných při splnění definovaných podmínek v přijatých datech. Odesílání alertů min SMTP, Syslog, TCP.	Systém obsahuje předpřipravené alerty a integrovaný grafický vizuální nástroj pro uživatelské vytváření automatických notifikací/alertů generovaných při splnění definovaných podmínek v přijatých datech. Systém podporuje odesílání alertů SMTP, Syslog, TCP protokoly	Logamanager Datasheet.pdf Logmanager Dokumentace.pdf
Výkon	Min. 5000 EPS (events per second), krátkodobá (min. 10 min) přetížitelnost systému až 200%	Trvalý výkon systému je 5000 EPS, s krátkodobou přetížitelností 200% po dobu 10 min.	Logamanager Datasheet.pdf Logmanager Dokumentace.pdf
Kapacita	Využitelná diskové kapacita pro ukládání dat min. 40 TB, disky musí být chráněny min. RAID 5	Čistá využitelná diskové kapacita pro ukládání data je 40 TB, disky jsou chráněny RAID 6	Logmanager Dokumentace.pdf
Řízení diskového systému	Hardwarový řadič RAID se zálohovanou vyrovnávací pamětí (zápis i čtení) o kapacitě min 8 GB	Systém obsahuje hardwarový řadič RAID s vyrovnávací paměti read/write 8 GB (součást serveru DELL, který je základem appliance)	Logmanager_L-PowerEdge R7525.pdf Dell-perc11.pdf
Úložiště logů	Logy musí být ukládány do databáze (příslušná licence musí být součástí dodávky) s podporou komprese ukládaných dat.	Logy jsou ukládány do interní databáze systému jejíž licence je součástí licence systému, databáze podporuje kompresi ukládaných dat.	Logmanager Dokumentace.pdf
Napájení	Systém musí mít redundantní napájení (min. 2 nezávislé zdroje)	Systém obsahuje 2 nezávislé zdroj, konfigurované pro redundanci napájení (součást serveru DELL, který je základem appliance)	Logmanager datasheet.pdf Logmanager Dokumentace.pdf
LAN konektivita	Min. 2x LAN 1 Gb Base-T a 2x LAN 10Gb SFP+ včetně SFP+ modulů + 1x 1Gb Base-T nezávislý port pro správu hardware prostřednictvím KVM konzole s grafickým rozhraním, zabezpečeným přístupem a detailním přehledem o stavu hardware včetně okamžité a dlouhodobé spotřeby elektrické energie a stavu dílčích komponent.	Systém obsahuje 2x LAN 1 Gb port + 2x 10Gb SFP+ , včetně modulů,1 nezávislý port (1Gbe) pro správu hardware prostřednictvím KVM konzole s grafickým rozhraním, zabezpečeným přístupem a detailním přehledem o stavu hardware včetně okamžité a dlouhodobé spotřeby elektrické energie a stavu dílčích komponent (součást serveru DELL, který je základem appliance).	Logmanager Datasheet.pdf Logmanager Dokumentace.pdf
Aktualizace	Integrovaná aktualizace systému prostřednictvím administrátorské	Systém obsahuje integrované zálohování a obnova konfigurace.	Logmanager Dokumentace.pdf

	konzole včetně podpory downgrade		
Zálohování	Integrované zálohování a obnova konfigurace	Systém obsahuje integrované zálohování a obnova konfigurace.	Logmanager Dokumentace.pdf
Škálovatelnost	Systém lze propojit s dalšími systémy stejného výrobce. Spojením systémů dojde ke zvýšení kapacity, výkonu (včetně vyhledávání) a dostupnosti. Navenek se propojené systémy chovají jako jeden.	Systém podporuje škálovatelnost propojením s dalšími systémy stejného výrobce. Spojením systémů dojde ke zvýšení kapacity, celkového výkonu včetně vyhledávání a dostupnosti. Navenek se propojené systémy chovají jako jeden.	Logmanager Dokumentace.pdf
Dokumentace	Plnohodnotná (tj. shodná s originální) dokumentace v českém jazyce	Součástí dodávky a podpory systému je plnohodnotná dokumentace v českém jazyce (výrobcem je česká společnost). Anglická dokumentace je obsahově totožná s českou.	Logmanager Dokumentace.pdf
Záruka a záruční servis	Min. 60 měsíců s opravou hardware do druhého pracovního dne v místě instalace, včetně nároku na nové verze firmware/software a aktualizace	60 měsíců s opravou hardware do druhého pracovního dne v místě instalace, včetně nároku na nové verze firmware/software a aktualizace	Součástí cenové nabídky

Zálohovací úložiště s časovým zámkem

Parametr	**Minimální požadavky**	**Způsob naplnění tohoto povinného parametru**	**Odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
Provedení	Umístitelné do racku, včetně montážního materiálu, maximálně 2U.	Exagrid EX27, v rackovém provedení 2U včetně ližin do racku	ExaGrid-Datasheet.pdf
Kapacita	Řešení musí mít minimálně 54 TB využitelné (usable) lokální kapacity bez redukce dat, včetně potřebných licencí pro tuto kapacitu.	Exagrid EX27 má využitelnou kapacitu 54TB bez redukce dat, včetně potřebných licencí pro tuto kapacitu.	ExaGrid-Datasheet.pdf
Škálovatelnost	Řešení musí umožňovat rozšíření alespoň do úrovně 1 PB čisté lokální kapacity bez redukce dat a bez nutnosti	Zařízení lze škálovat až na kapacitu 1,7PB čisté lokální	ExaGrid-Datasheet.pdf

	výměny jakékoliv dodávané součásti	kapacity bez redukce dat a bez nutnosti výměny jakékoliv dodávané součásti	
Výkon	Propustnost dodávaného řešení alespoň 6TB/hodinu	Propustnost EX27 je 6,09TB/h	ExaGrid-Datasheet.pdf
Deduplikace	Zařízení musí při ukládání dat využívat princip deduplikace Uložiště nesmí vytvářet deduplikační pooly – musí disponovat globálním deduplikačním algoritmem bez ohledu na typ dat, přenosový protokol a množství zálohovacích serverů/aplikací, které na něj data ukládají.	Zařízení při ukládání dat využívá princip deduplikace. Zařízení nevytváří deduplikační pooly, ale používá globální deduplikační algoritmus bez ohledu na typ dat, přenosový protokol a množství zálohovacích serverů/aplikací, které na něj data ukládají.	ExaGrid-Datasheet.pdf
Protokoly	Zařízení musí podporovat minimálně následující protokoly: CIFS a NFS a musí umožnit jejich současné použití	Zařízení podporuje CIFS a NFS, oba protokoly je možné provozovat současně	ExaGrid-Datasheet.pdf
Integrace a interoperabilita	Zálohovací řešení musí být univerzální z hlediska podpory datových typů zálohovaných dat, musí podporovat všechny datové typy používané v produkčním prostředí Řešení musí umožnit komprimaci ukládaných deduplikovaných dat	Zařízení musí je univerzální z hlediska podpory datových typů zálohovaných dat, musí podporovat všechny datové typy používané v produkčním prostředí a umožňuje komprimaci ukládaných deduplikovaných dat	ExaGrid-Datasheet.pdf
Replikace	Zařízení musí obsahovat potřebné licence pro nativní funkcionalitu replikace dat do dalšího zařízení stejného výrobce. Řešení musí posílat pouze deduplikovaná zkomprimovaná data. Řešení musí podporovat alespoň následující scénáře pro replikaci: 1:1, M:1 a kaskádovou replikaci. Řešení musí umožnit funkcionalitu šifrování replikačního toku data-in-flight. Řešení musí umožnit kontrolu a správu využití pásma pro přenos dat (QoS).	Zařízení obsahuje funkce pro replikaci dat do dalšího zařízení nativně. Přenos dat je optimalizován pro WAN, přenášejí se pouze deduplikovaná zkomprimovaná data. Zařízení podporuje následující scénáře pro replikaci: 1:1, M:1 a kaskádovou replikaci. Řešení umožňuje funkcionalitu šifrování replikačního toku data-in-flight.	ExaGrid-Datasheet.pdf

		Řešení umožňuje kontrolu a správu využití pásma pro přenos dat Quality o Service (QoS).	
Ochrana	Zařízení musí disponovat redundantními hot-swap napájecími zdroji a ventilátory. Zařízení musí zajišťovat ochranu dat alespoň na úrovni duální diskové parity. Zařízení musí zajišťovat výměnu všech disků za chodu – hot-swap. Zařízení musí obsahovat HotSpare disk. Zařízení musí obsahovat algoritmy pro kontrolu a verifikaci konzistence a čitelnosti uložených dat.	Systém má dvojité redundantní zdroje a ventilátory. Zařízení využívá RAID6, disky vyměnitelné za chodu (hot-swap) a hot-spare disk (hot swappable spare). Řešení obsahuje algoritmy pro kontrolu a verifikaci konzistence a čitelnosti uložených dat.	ExaGrid-Datasheet.pdf ExaGrid-Technical_Specifications.pdf
Časové zámky	Zařízení musí umožňovat nastavit ochranu dat proti nechtěnému smazání či modifikaci dat pomocí časových zámků. Po nastavenou dobu lze data číst, ale nelze je přepisovat. Tato funkce nesmí být závislá na zálohovacím software, přenosovém protokolu či typu dat. To znamená, že tato funkce musí být plně funkční s provozovaným zálohovacím SW/Veeam Backup & Replication. Časové zámky se musí aplikovat uvnitř zařízení, nikoliv pomocí externích nástrojů.	Řešení využívá unikátní technologii Retention Time-Lock umožňuje nastavit ochranu dat proti nechtěnému smazání či modifikaci dat pomocí časových zámků. Po nastavenou dobu lze data číst, ale nelze je přepisovat. Tato funkce není být závislá na zálohovacím software, přenosovém protokolu či typu dat. Tato funkce je tedy plně funkční s provozovaným zálohovacím SW/Veeam Backup & Replication. Časové zámky se aplikují uvnitř zařízení, nikoliv pomocí externích nástrojů.	ExaGrid-Datasheet.pdf
Šifrování	Zařízení musí umožňovat šifrování úložného prostoru a to bez omezení výkonu - dodání včetně potřebných licencí	Řešení je osazené tzv. self-encrypted disky, které nemají	ExaGrid-Datasheet.pdf

	pro výše požadovanou kapacitu	dopad na výkon, funkce není licencována	
Porty	Zařízení musí disponovat síťovými kartami min. 2x1GbE a 2x10Gb SFP+ včetně SFP+ modulů	Zařízení je osazené 2x1GbE a 2x10Gb SFP+ včetně SFP+ modulů	ExaGrid-Technical_Specifications.pdf
Zabezpečení	Řešení musí umožnit vynucení přihlášení minimálně dvou typů účtů (administrátorský, bezpečnostní) pro změny spojené se změnou nastavení ochrany dat – časových zámků.	Řešení vyžaduje pro některé činnosti např. spojené se změnou nastavení ochrany dat – časových zámků vynucení přihlášení dvou účtů, administrátorského a tzv. security účtu	ExaGrid-Datasheet.pdf
Dvoufaktorové ověřování	Řešení musí umožnit dvoufaktorové ověřování účtů pro správu díky jednorázovým heslům (Time-based One-Time Password). Pokud je potřeba externí nástroj, musí být součástí nabídky všechny potřebné licence až pro 25 uživatelů včetně potřebného hardware pro zajištění vysoké dostupnosti. Licence musí být perpetuální a instalace v místě plnění.	Řešení umožnuje nativně dvoufaktorové ověřování účtů pro správu díky jednorázovým heslům (Time-based One-Time Password).	ExaGrid-Datasheet.pdf
Správa	Řešení musí umožnit centrální správu pro všechna dodávaná zařízení prostřednictvím webového rozhraní. Řešení musí umožnit správu na principu rolí s různými typy oprávnění (Role-based Access Control).	Řešení umožňuje centrální správu pro všechny zařízené prostřednictvím webového rozhraní a umožňuje správu na principu rolí s různými typy oprávnění (Role-based Access Control).	ExaGrid-Datasheet.pdf
Reporting	Řešení musí poskytovat funkcionalitu automatického reportingu, automatický call-home	Management zařízení poskytuje funkcionalitu call to repair a automatického monitoringu zdraví zařízení.	ExaGrid-Security_Reliablity_and_Redundancy_DS.pdf
Kompatibilita	Nabízený diskový úložný systém musí být plně podporován (plně kompatibilní) stávající zálohovací platformou Veeam Backup & Replication. Je požadováno aby řešení bylo uvedeno na webu výrobce zálohovacího SW mezi kompatibilními deduplikačními HW / Oficiálně	Řešení je plně podporováno stávající zálohovací platformou Veeam Backup & Replication a je uvedeno na webu výrobce	ExaGrid-Datasheet.pdf

	podporovaná (kompatibilní) řešení se stávající platformou zálohování jsou popsána zde: https://helpcenter.veeam.com/docs/backup/vsphere/deduplicating_storage_appliances.html?ver=120		
Podpora	Podpora na hardware a software musí být od jednoho výrobce, tak by byla zajištění funkčnost zařízení jako celku	Zařízení jeho HW i SW část je od jednoho výrobce. Záruka je tak poskytována od jednoho výrobce	ExaGrid-Datasheet.pdf
Záruka a záruční servis	Požadovaná záruka a záruční servis 5 let s reakcí 8x5 NBD on-site	Zařízení je pokryto zárukou 5 let 8x5 NBD on-site	Součástí nabídkové ceny

Produkční server s příslušenstvím + PDU

Parametr	**Minimální požadavky**	**Způsob naplnění tohoto povinného parametru**	**Odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
Provedení	umístitelné do racku, včetně montážního materiálu, maximálně 1U. Barevně označené hot-plug komponenty. Pro přístup ke všem komponentám není nutné nářadí. Zásuvné ližiny s managementem kabeláže. Uzamykatelný čelní panel.	Server optimalizovaný pro umístění do racku. Server má barevně označené hot-plug komponenty, zásuvné ližiny s managementem kabeláže a uzamykatelný čelní panel	Poweredge-r660.pdf Poweredge-r660-technical-guide.pdf
CPU	Minimálně 2x procesor 8 jádrový. Výkon serveru dle http://www.spec.org: SPECrate®2017_int_base min. 176 bodů SPECrate®2017_fp_base min. 249bodů Systém nesmí přesáhnout celkově 16 jader, z důvodu licenčních nákladů na pokrytí těchto jader licencemi software, které bude kupující na serverech provozovat.	2x Intel Xeon Gold 5415+ 8C/16C SPECrate®2017_int_base min. 176 bodů SPECrate®2017_fp_base min. 249bodů	http://www.spec.org
RAM	Min. 32 slotů pro DDR5 RDIMM Min. 512GB RAM ECC, min. 4800 MT/s Počet paměťových modulů a rozmístění musí být zvoleno pro optimální výkon s CPU.	Server obsahuje 32 DDR5 DIMM slots, server je osazen 8 moduly 64GB RDIMM, 4800MT/s Dual Rank	Poweredge-r660.pdf Poweredge-r660-technical-guide.pdf

Boot Drive	Musí být zajištěn dvojicí HDD v RAID1 a kapacitou 960GB, nesmí se jednat o rotační disky. Disky pro Boot OS musí být hot-swap, přístupné z přední nebo zadní strany serveru.	Server je osazen BOSS-N1 controller card + with 2 M.2 960GB (RAID 1) hot-swap přístupné ze zadní strany serveru	Poweredge-r660.pdf Poweredge-r660-technical-guide.pdf
Interface	Min. 3x externí USB, z toho min. 1x USB 3.0 Dedikovaný USB management port Min. 2x VGA port (jeden z každé strany serveru)	Server je osazen 3x USB konektory (2x USB 2.0 a 1x USB 3.0) z toho jeden je na čelním panelu s podporou bootování. Server má dedikovaný USB management port - 1x iDRAC Direct (Micro-AB USB) port. Server má VGA z přední a zadní strany serveru.	Poweredge-r660.pdf Poweredge-r660-technical-guide.pdf
Napájecí zdroje	2x napájecí zdroj min. 600 W, redundance, min. Platinum specifikace dle 80 PLUS https://cs.wikipedia.org/wiki/80_Plus	Dual, Fully Redundant(1+1), Hot-Plug Power Supply,1100W MM(100-240Vac) Titanium	Poweredge-r660.pdf Poweredge-r660-technical-guide.pdf
Rozšiřující sloty	Min. 3ks PCI-e sloty x16 Gen4	Server je osazen Riser 3x16 LP Slots (Gen4)	Poweredge-r660.pdf Poweredge-r660-technical-guide.pdf
Síťové porty	Min. 2x LAN 10/25GbE SFP28 s možností budoucí výměny např. za 100GbE – typ OCP, včetně SFP+ modulů	Server je osazen Broadcom 57414 Dual Port 10/25GbE SFP28, OCP NIC 3.0. Kartu je možné vyměnit za model s rychlostí 100GbE	Poweredge-r660.pdf Poweredge-r660-technical-guide.pdf
Kompatibilita	Microsoft Windows Server® Red Hat® Enterprise Linux SUSE® Linux Enterprise Server VMware® ESXi	Microsoft Windows Server with Hyper-V Red Hat Enterprise Linux SUSE Linux Enterprise Server VMware ESXi Canonical Ubuntu Server LTS	Poweredge-r660.pdf Poweredge-r660-technical-guide.pdf
HBA	Min 1x dvouportová HBA SAS 12Gb karta kompatibilní s nabízeným diskovým polem	Server je osazen HBA355e Adapter FH & LP, DIB, která je kompatibilní s nabízeným diskovým polem	Poweredge-r660.pdf Poweredge-r660-technical-guide.pdf
Management a vzdálená správa	Stavové informace na čelním panelu s výraznou indikací nestandardních a chybových provozních stavů či parametrů (min. napájení, teplota, vada HDD). Aktivní indikace standardního provozního stavu. V případě závady zobrazuje její popis v textové formě. Vzdálená správa – dostupnost centrálního management prostředí serveru, nezávislého na spuštěné virtualizační platformě, či spuštěném operačním systému, vč. monitoringu, chybových hlášení emailem, vzdáleného a lokálního připojení (KVM) prostřednictvím dedikovaného LAN portu s podporou IPv4 a IPv6	Na čelním panelu se nachází LCD panel zobrazující požadované informace. Server nabízí Integrovaný řadič Integrated Dell Remote Access Controller (iDrac) v edici Enterprise, který disponuje požadovanými funkcemi v kombinaci s centrálním managementem Dell OpenManage	Poweredge-r760xs-technical-guide.pdf iDrac9-User-Guide.pdf Dell-Openmanage.pdf

	Vzdálená správa musí disponovat vlastním management GUI, přístupným z běžných www prohlížečů. GUI musí být čistě v HTML5 a nesmí využívat dodatečných JAVA nebo ACTIVE-X komponent. Musí umožnit vzdálenou obrazovku s konzolí, možnost vzdáleného připojení ISO virtuální DVD a možnost vzdáleného připojení USB disku. Management serveru musí disponovat vlastním úložištěm pro firmware, ovladače a softwarové komponenty. Komponenty mohou být setříděny a organizovány do instalačních sad a mohou být použity pro obnovu či přeinstalaci vadného firmware. Centrální management serverů musí disponovat analytickou komponentou, která musí umožnit kontrolu nastavení bezpečnostních pravidel serveru oproti šabloně bezpečnostních zásad (například kontrola síly administrátorských hesel, platnosti certifikátu, zapnutí TLS pro management konzoli serveru, vypnutí USB portů a další). Tyto šablony musí být nezávislé na modelu serveru výrobce.		
Bezpečnost	Z důvodu bezpečnosti musí management serveru umožňovat zakázání (a opětovné povolení) nepoužívaných USB portů, změna stavu USB portu musí být možná bez nutnosti restartu serveru. Server musí disponovat bezpečnostním systémem ověření komponent. Tento systém musí umožňovat ověřit, že mezi výrobou serveru a doručením k zákazníkovi nebyla konfigurace komponent serveru změněna ani upravena.	Server obsahuje iDrac v edici umožňující zakázání (a opětovné povolení) nepoužívaných USB portů, změna stavu USB portu musí být možná bez nutnosti restartu serveru. Server disponuje Server Secured Component Verification	iDrac9-security-configuration-guide.pdf Poweredge-Secured Component Verification.pdf
Compliance	Centrální management serverů musí umožňovat „server bare metal“ deployment založený na šablonách	Centrální management Dell OpenManage serverů Dell OpenManage umožňuje „server bare metal“ deployment založený na	Dell-Openmanage.pdf

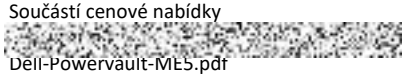
	(předdefinovaných konfiguracích pravidel, jejichž součástí je kromě samotného OS i konfigurace BIOS, RAID, LAN, MAC, WWN). Z bezpečnostních důvodů musí být možné naplánovat pravidelné provedení porovnání aktuálního stavu konfigurace serveru s aplikovanou šablonou automatizovaným způsobem, s automatickým zasláním reportu o výsledku porovnání emailem. je-li tato vlastnost licencována, požadujeme plnou licenci v ceně serveru.	šablonách. Zároveň management umožnuje pravidelné provedení porovnání aktuálního stavu konfigurace serveru s aplikovanou šablonou automatizovaným způsobem, s automatickým zasláním reportu o výsledku porovnání emailem.	
Automatizace	Management serveru musí umožňovat integraci do stávající virtualizační platformy VMware vCenter serveru s plnou podporou správy a updatovaní firmware serveru z prostředí vCenter serveru a s podporou vSphere Lifecycle Manager.	Součástí řešení je i licence OpenManage Enterprise Advanced Plus	Dell-Openmanage.pdf
Záruka a technická podpora výrobce	Záruka a záruční servis min. 60 měsíců Dostupnost podpory 24 hodin denně, 365 dní v roce Reakční doba do konce následujícího pracovního dne od nahlášení na linku podpory. Servis je poskytován přímo výrobcem hardware. Oprava v místě instalace hardware. Možnost automatického generování servisního incidentu přímo u výrobce hardware (server musí být schopen automatizovaného předávání závad a otevírání servisních požadavku na helpdesk výrobce). Podpora musí zahrnovat i nárok na aktualizace software a firmware pro komponenty serveru. Podpora prostřednictvím Internetu musí umožňovat ověření typu a délky záruky a stahování aktuálních ovladačů, firmware, software a manuálů z internetu adresně pro konkrétní zadané sériové číslo zařízení bez nutnosti vytvoření uživatelského účtu pro danou činnost.	Záruka 60 měsíců, oprava druhý pracovní den v místě instalace, nárok na podporu výrobce a nové verze software a firmware. Zařízení umožňuje automatického generování servisního incidentu přímo u výrobce hardware (zařízení je schopno automatizovaného předávání závad a otevírání servisních požadavku na helpdesk výrobce), díky záruce ProSupport, dostupnost podpory je 24 hodin denně, 365 dní v roce. Reakční doba do konce následujícího pracovního dne od nahlášení na linku podpory. Servis je poskytován přímo výrobcem hardware. Oprava v místě instalace hardware. Prostřednictvím Internetu je možné ověření typu a délky záruky a stahování aktuálních ovladačů, firmware, software a manuálů z internetu adresně pro konkrétní zadané sériové číslo zařízení bez nutnosti vytvoření uživatelského účtu pro danou činnost.	Součástí cenové nabídky  Poweredge-r760xs.pdf Poweredge-r760xs-technical-guide.pdf Dell-SupportAssist.PDF Dell-prosupport-brochure.PDF

Parametr	Minimální požadavky	Způsob naplnění tohoto povinného parametru	Odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
Provedení	do racku	ATEN napájecí jednotka 8xIEC320 C13+ 1xC14, overIP v provedení do racku	ATEN-pe5108G.pdf
Kapacita výstupního výkonu	max. 10A zatížení, 2300VA	max. 10A zatížení, 2300VA	ATEN-pe5108G.pdf
Výstupní zásuvky	min. 8x zásuvka pro připojení zařízení (7x IEC320 C13 pro spotřebiče + 1x IEC320 C14 pro připojení)	8x zásuvka pro připojení zařízení (7x IEC320 C13 pro spotřebiče + 1x IEC320 C14 pro připojení) + 1x zástrčka IEC C14 10A pro připojení zařízení do sítě 230V	ATEN-pe5108G.pdf
Vlastnosti	možnost připojení senzorů teploty a vlhkosti (nejsou součástí dodávky) ovládání přes internetový prohlížeč na předním panelu LED diody signalizující stav zařízení LCD panel centralizovaná inteligentní správa připojených zařízení měření banku (všech zásuvek dohromady) v reálném čase napětí (V), proudu (A) a zatížení (W), spotřeby (kWh) podpora bezpečného vypnutí zařízení podpora V3 SNMP software a eco Sensors software pro vytváření reportů	Zařízení umožňuje připojení senzorů teploty a vlhkosti (nejsou součástí dodávky). Ovládání zařízení je přes internetový prohlížeč, na předním panelu má LED diody signalizující stav zařízení a LCD panel. Management obsahuje centralizovanou inteligentní správu připojených zařízení, měření banku (všech zásuvek dohromady) v reálném čase napětí (V), proudu (A) a zatížení (W), spotřeby (kWh) podpora bezpečného vypnutí zařízení podpora V3 SNMP software a eco Sensors software pro vytváření reportů	ATEN-pe5108G.pdf
Podpora	Podpora 10/100Mbit Ethernet Interface Podpora TCP/IP, UDP, HTTP, HTTPS, SSL, DHCP, SMTP, NTP, DNS, Auto Sense, Ping, SNMP V1,V2&V3 Podpora 2-level account/password security, IP/MAC filter, 128 bit SSL, RADIUS Podpora eco Sensors, Browser (IE, Firefox, Chrome, Safari)	Podpora 10/100Mbit Ethernet Interface Podpora TCP/IP, UDP, HTTP, HTTPS, SSL, DHCP, SMTP, NTP, DNS, Auto Sense, Ping, SNMP V1,V2&V3 Podpora 2-level account/password security, IP/MAC filter, 128 bit SSL, RADIUS Podpora eco Sensors, Browser (IE, Firefox, Chrome, Safari)	ATEN-pe5108G.pdf
Záruka	Min 2 roky na zařízení	Záruka 24 měs. záruka poskytovaná výrobcem	Součástí nabídkové ceny

Datové úložiště s příslušenstvím

Parametr	Minimální požadavky	Způsob naplnění tohoto povinného parametru	Odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
Provedení	Umístitelné do racku, včetně montážního materiálu	Dell PowerVault ME5024 2U včetně montážního kitu do racku	Dell-Powervault-ME5.pdf
Parametry řadičů pole	2x hot-swap řadič, alespoň Dual-Active architektura s možností rozkládat zátěž mezi řadiči Každý řadič osazen alespoň 16GB paměti (celkem 32GB paměti) 12Gbit/s SAS připojení disků (Backend konektivita) na každém řadiči Celkem 8x 12Gb SAS ports (4x na každý řadič) 2x dedikovaný 1000baseT management port, vždy jeden na řadiči	Diskové pole Dell PowerVault ME5024 je osazené dual-active kontroléry s možností rozkládat zátěž mezi řadiči a backend konektivitou 12 Gb SAS. Každý řadič je osazen celkem 24GB paměti (celkem tedy 48GB). Celkem je k dispozici 8 12Gb SAS portů (4+) a 2x dedikovaná management 1Gbe	Dell-Powervault-ME5.pdf
Rozšiřitelnost pole	Rozšiřitelnost - pole v dodané konfiguraci musí být za provozu rozšiřitelné pomocí expanzních polic na nejméně 270 hot-plug disků SFF/LFF - možnost kombinovat SSD, rotační SAS i rotační NL_SAS disky bez omezení - SSD disky musí být konfigurovatelné jako datové nebo také v režimu minimálně read akcelerátoru (cache)	Rozšiřitelnost diskové pole je až 276 hot-plug disků SFF/LFF. Diskové pole umožňuje libovolnou kombinaci jak SSD, rotačních SAS, tak NLSAS disků. Diskové pole má zalicencovanou funkci Auto-tiering	Dell-Powervault-ME5.pdf
Konstrukce	Max. 2U - v rámci 2U musí být k dispozici základní jednotka pole (2x řadiče a napájení) a základní osazení disky Min. 24x 2,5" hot-plug diskových pozic v rámci základní jednotky Redundantní napájení dimenzované pro plný počet disků a řadiče (základní jednotka)	Diskové pole ME5024 je 2U zařízení (2x řadiče a napájení) a základní osazení disky 24x 2,5" hot-plug diskových pozic, včetně montážního kitu do racku. Diskové pole má redundantní napájení i pro plný počet disků.	Dell-Powervault-ME5.pdf

	Rackmount, včetně montážního kitu do standardního 19" racku.		
Počet a typ disků	Osazení hot-plug disky v poptávané konfiguraci min. 6x 3,84TB SSD SAS 12Gbit/s 1DWPD, Hot Plug 6x 2,4TB SAS 10K Poptávanou konfiguraci musí být možné kdykoli rozšířit o další disky SSD, SAS i NL_SAS (připouští se doplněním příslušných expanzních jednotek)	Osazení hot-plug HDD 6x 3.84TB SSD SAS Read Intensive up to 24Gbps 512e 2.5in Hot-Plug a 6x 2.4TB 10K RPM SAS 12Gbps 512e 2.5in Hot-plug Hard Drive. Konfiguraci je možné doplňovat o další disky či expanzní police.	Dell-Powervault-ME5.pdf
Podpora RAID	Typy RAID: - JBOD - RAID 0,1, 5, 6, 10 - distribuovaný RAID - Možnost použít více typů RAID v rámci jednoho pole.	JBOD, RAID 1, 5, 6, 10, nebo ADAPT RAID, v rámci pole je možné použít více typů RAID.	Dell-Powervault-ME5.pdf
Funkcionalita	Software funkcionalita (licence bez omezení na počet serverů nebo kapacitu pole) - thin provisioning - distribuovaný RAID a hotsparing - standardní RAID skupiny a dedikované hotspare disky - automatický tiering (SSD, SAS a NL_SAS tier) - SSD cache - klony a snapshoty (1024 ks) - vzdálené zrcadlení mezi dvěma nebo více poli (alespoň asynchronní) - úložiště musí podporovat správu pomocí GUI z webovského prohlížeče HTML5, CLI pomocí SSH - podpora SNMP v3 - podpora notifikací pomocí emailu, SNMP trap, na vzdálený syslog server - součástí managementu úložiště musí být vestavěná funkcionalita call-home (úložiště musí být schopno automatizovaného předávání závad a otevírání servisních požadavku na helpdesk výrobce)	Diskové pole obsahuje licenci bez omezení na počet serverů nebo kapacitu pole pro: - thin provisioning - distribuovaný RAID a hotsparing - standardní RAID skupiny a dedikované hotspare disky - automatický tiering (SSD, SAS a NLSAS tier) - SSD cache - klony a snapshoty (1024 ks) - vzdálené zrcadlení mezi dvěma nebo více poli (alespoň asynchronní) Diskové pole se menežuje pomocí HTML5, případně CLI pomocí SSH. Diskové pole podporuje SNMP v3, notifikaci pomocí emailu, SNMP trap, na vzdálený syslog server. Součástí managementu je fce call-home úložiště je schopno automatizovaného předávání závad a otevírání servisních požadavku na helpdesk výrobce	Dell-Powervault-ME5.pdf Dell-Powervault-ME5-Administrators-guide.pdf
Kompatibilita	Nabízená technologie diskového pole musí být	Podpora: - RedHat Linux 9.2, 8.8, 8.2 and 7.8	Dell-Powervault-ME5.pdf

	kompatibilní min. s: - RedHat Linux 8.2 - SuSe Linux 15.2 - MS Windows 2022, 2019, 2016 - VMware ESX 7.0, 8.0	- SuSe Linux 15.2 and 12.5 - MS Windows 2022, 2019, 2016 - VMware ESX 7.0, 8.0 a 6.7 - Citrix XenServer 8.x and 7.x	
Záruka a záruční servis	Záruka a záruční servis min. 60 měsíců Dostupnost podpory 24 hodin denně, 365 dní v roce. Reakční doba do konce následujícího pracovního dne od nahlášení na linku podpory. Servis je poskytován přímo výrobcem hardware. Oprava v místě instalace hardware. Možnost automatického generování servisního incidentu přímo u výrobce hardware (úložiště musí být schopno automatizovaného předávání závad a otevírání servisních požadavku na helpdesk výrobce). Podpora musí zahrnovat i nárok na aktualizace software a firmware pro komponenty úložiště. Podpora prostřednictvím Internetu musí umožňovat ověření typu a délky záruky a stahování aktuálních ovladačů, firmware, software a manuálů z internetu adresně pro konkrétní zadané sériové číslo zařízení bez nutnosti vytvoření uživatelského účtu pro danou činnost. Všechny SSD disky jsou předmětem záručních podmínek bez jakýchkoli omezení z pohledu životnosti, intenzity využití, množství zápisů a případně jiných neuvedených omezení.	Záruka Dell PoSupport 60 měsíců, dostupnost podpory 24 hodin denně, 365 dní v roce, NBD. Servis je poskytován přímo výrobcem HW, oprava v místě instalace. Zařízení umožňuje automatického generování servisního incidentu přímo u výrobce hardware (zařízení je schopno automatizovaného předávání závad a otevírání servisních požadavku na helpdesk výrobce).Záruka zahrnuje i nárok na aktualizace software a firmware pro komponenty úložiště. Prostřednictvím Internetu je možné ověření typu a délky záruky a stahování aktuálních ovladačů, firmware, software a manuálů z internetu adresně pro konkrétní zadané sériové číslo zařízení bez nutnosti vytvoření uživatelského účtu pro danou činnost. Všechny SSD disky jsou předmětem záručních podmínek bez jakýchkoli omezení z pohledu životnosti, intenzity využití, množství zápisů a případně jiných neuvedených omezení.	Součástí cenové nabídky  Dell-Powervault-ME5.pdf Dell-SupportAssist.PDF Dell-prosupport-brochure.PDF

UPS

Parametr	**Minimální požadavky**	**Způsob naplnění tohoto povinného parametru**	**Odkaz na přiloženou část nabídky, kde je možné**

			ověřit naplnění parametru
Provedení	do racku, včetně montážních ližin	Eaton 9PX 3000i Rack2U, včetně montážního kitu do racku.	Eaton-9px-3000.pdf
Kapacita výstupního výkonu	Min. 2700 W / 3000 VA	Provedení 3000 VA/3000W	Eaton-9px-3000.pdf
Výstupní napětí	230V	Výstupní napětí je 230V	Eaton-9px-3000.pdf
Výstupní zásuvky	Min 8x IEC 320 C13 Min. 2x IEC 320 C19	Výstupní přípojky: -(8) IEC-320-C13 -(2) IEC-320-C19	Eaton-9px-3000.pdf
Síťová karta	pro vzdálené monitorování a řízení UPS. Podpora SNMP v3, HTTPS Podpora IPv4 a IPv6	Eaton Komunikační karta M3 - Gigabit Network Card s podporou protokolů HTTPS1.1, MQTTS, TLS1.2, SNMPv1, SNMP v3, NTP, SMTPS, BOOTP/DHCP, CLI, SSH, ARP and Syslog a IPv4/v6, TLSv1.2, HTTP(S)v1.1, NTP, SMTP(S), BOOTP/DHCP, SSH, SysLog(S), LDAP, AD, RADIUS	Eaton-Gigabit-Management-Card.pdf
Stavové diody	min. indikující stavy: Napájen ze sítě, napájen z baterie, nutno vyměnit baterie, přetížení UPS	Na předním panelu jsou stavové diody indikující stavy: Napájen ze sítě, napájen z baterie, nutno vyměnit baterie, přetížení UPS atd.	Eaton-9px-3000.pdf
LCD display	zobrazující min. kapacitu baterie, účinnost, zatížení UPS, spotřebu energie. Možnost nastavení základních parametrů UPS včetně konfigurace výstupních zásuvek a nastavení zvukových upozornění	Na předním panelu je grafický LCD zobrazující min. kapacitu baterie, účinnost, zatížení UPS, spotřebu energie. Možnost nastavení základních parametrů UPS včetně konfigurace výstupních zásuvek a nastavení zvukových upozornění	Eaton-9px-3000.pdf
Battery Pack	Včetně jednoho battery packu	Konfigurace je včetně Eaton Externí baterie pro 9PX 72V RT3U	Eaton-BatteryPack.pdf
Rozšiřitelnost	Možnost připojení dalšího externího battery packu (není součástí dodávky)	Až 4 EBM	Eaton-9px-3000.pdf
Účinnost	98%	Účinnost 98%	Eaton-9px-3000.pdf
Záruka UPS	Min 5 let na zařízení i na baterie. U baterií akceptujeme záruku vztahující se pouze na závady, nikoliv na sníženou dobu zálohy.	Záruka na 5 let na zařízení i na baterie.	Součástí nabídkové ceny

Licence

Parametr	Minimální požadavky	Způsob naplnění tohoto

		povinného parametru
Operační systémy serverů	Windows Server v edici umožňující neomezený běh virtuálních serverů na stávající virtualizaci VMware pro všechny nabízené servery (hypervisory) pokrývající nabízené CPU	2x (1x pro každý fyzický server) 9EA-01290 - Microsoft® Win Server Datacenter Core 2022 Single Language 16 Licenses – licenční program Microsoft Select Plus GOV
Přístupové licence na operační systém serverů	250ks přístupových licencí vázaných na uživatele	250x R18-06495 - Microsoft® Win Server CAL 2022 Single Language User CAL – licenční program Microsoft Select Plus GOV

Cenová tabulka veřejné zakázky s názvem Dodávka IT infrastruktury a licencí

1. Účastník zadávacího řízení cenou tabulku vyplní a cenu vypočte pouze v buňkách označených

2. Účastník vyplní do tabulky jednotlivé ceny dodávek a služeb včetně jejich příslušenství

3. Pro stanovení nabídkové ceny do ceny zařízení dodavatele zanese cenu standardní záruky, která je k zařízení dodávána. Nadstandardní záruku, záruční servis a podporu dodavatel nacení samostatně do příslušné položky k zařízení v tabulce níže. Podpora zařízení a podpora software za předpokladu, že první rok podpory je součástí dodávky licence nebo zařízení může být součástí ceny zařízení a licence, každý další rok musí být naceněn samostatně ve sloupečku E této tabulky, jako samostatná podpora, není-li v technické dokumentaci uvedeno jinak.

4. Náklady na implementační služby budou zohledněny v ceně dodávek zařízení.

Název dodavatele:	**Aricoma Systems a.s.**

Položka	Počet	Celková cena za uvedený Počet [Kč bez DPH]	Cena za prodlouženou záruku a záruční servis k zařízení dle specifikace [Kč bez DPH]	Tech. podpora po dobu 5 let (maintenance, bezpečnostní update, patche, subskribce, nároky na aktualizační balíčky dat atd.) [Kč bez DPH]
Systém řízení přístupu do sítě podle standardu IEEE802.1x (licence network access control)	1	772 483 Kč	x	129 000 Kč
Přepínače s příslušenstvím	18	1 420 978 Kč	71 200 Kč	x
Systém pro správu logů	1	1 007 730 Kč	187 995 Kč	746 415 Kč
Zálohovací úložiště s časovým zámkem	1	1 217 583 Kč	578 700 Kč	x
Produkční server s příslušenstvím	2	769 759 Kč	255 879 Kč	x
Datové úložiště s příslušenstvím	1	679 083 Kč	252 158 Kč	x
Licence serverových operačních systémů	2	265 659 Kč	x	x
Klientské přístupové licence na serverové OS	250	248 976 Kč	x	x
UPS	1	138 792 Kč	43 410 Kč	x
		Nabídková cena celkem v Kč bez DPH		8 785 800 Kč
		DPH ve výši 21 %		1 845 018 Kč
		Nabídková cena celkem v Kč včetně DPH		10 630 818 Kč

V Praze dne dle el. podpisu

Ing. Jaroslav Dvořák

Digitálně podepsal Ing. Jaroslav Dvořák
Datum: 2024.07.18 23:33:02 +02'00'

Podpis osoby oprávněné za účastníka zadávacího řízení