Kupní smlouva

(dále jen „smlouva“)

dle § 2079 a násl. zákona č. 89/2012 Sb., občanského zákoníku,
ve znění pozdějších předpisů (dále jen „**občanský zákoník**“)

1. Smluvní strany

1.1.	**Kupující:**	**Město Benešov**
	se sídlem:	Masarykovo náměstí 100, 256 01 Benešov
	zastoupen:	Ing. Jaroslavem Hlavničkou, starostou
	Identifikační číslo:	00231401
	DIČ:	CZ00231401
	(dále jen jako „**kupující**“)	
1.2.	**Prodávající:**	**XANADU a.s.**
	se sídlem:	Žirovnická 2389, 106 00 Praha 10
	zastoupen:	Ing. Radek Nekl, předseda představenstva
	zástupce ve věcech technických:	Mgr. František Lemoch, Technický ředitel
	IČ:	14498138
	Bankovní spojení:	Unicredit Bank Czech Republic a.s., 1044153003/2700
	Telefon:	+420 283 891 154
	E-mail:	obchod@xanadu.cz
	(dále jen jako „**prodávající**“)	

Obě smluvní strany po vzájemném projednání a shodě uzavírají tuto smlouvu:

2. Předmět smlouvy

2.1. Účelem této smlouvy je dodávka zařízení včetně jeho implementace a napojení na ostatní infrastrukturu kupujícího (včetně současně budované infrastruktury) a následné předání funkčního kompletu kupujícímu, zaškolení administrátorů, uživatelů, rozvoje a podpory. Zařízení je určené pro kupujícího (město Benešov) a pro jeho organizace.

2.2. Podkladem pro uzavření této smlouvy je nabídka prodávajícího, podaná v zadávacím řízení nazvaném **„V 00669 – Dodávka IT kyberbezpečnost“, část 2: Další opatření kybernetické bezpečnosti** (dále jen „Veřejná zakázka“), zadávaném přiměřeně dle Metodického pokynu pro oblast zadávání zakázek pro programové období 2021 – 2027 vydaného Ministerstvem pro místní rozvoj (dále jen „Pravidla“) a dle § 56 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění.

2.3. Touto smlouvou se prodávající zavazuje dodat za podmínek v ní sjednaných kupujícímu zboží, uvedené v článku 3. této smlouvy a převést na něj vlastnické právo k tomuto zboží.

2.4. Kupující se zavazuje zboží převzít a zaplatit za něj sjednanou kupní cenu způsobem a v termínu stanoveném touto smlouvou.

2.5. Předmět plnění bude spolufinancován z dotačního projektu „Bezpečné centrum sdílených služeb organizací města“, registrační číslo projektu: CZ.06.01.01/00/22_004/0000143, financovaného z IROP – dále jen „Projekt“).

3. Předmět koupě

3.1. Předmětem smlouvy je dodávka **HW včetně souvisejícího infrastrukturního SW**, jehož specifikace včetně technických parametrů je uvedena v příloze č. 1 této smlouvy (dále jen „zboží“).

3.2. Součástí předmětu koupě jsou i veškeré doklady požadované právními předpisy k používání předmětu koupě - zboží. Prodávající prohlašuje, že předmět koupě splňuje veškeré podmínky stanovené právními předpisy k jeho používání, a že kupujícímu předá veškeré doklady potřebné k provozování předmětu koupě, za což kupujícímu ručí.

3.3. Předmětem koupě dle této smlouvy je dále:

- doprava do místa plnění,
- implementace, tj. veškeré nezbytné práce jejichž smyslem je zprovoznění včetně zapojení do stávajícího prostředí kupujícího tak, aby je kupující mohl užívat obvyklým způsobem (dále jen „implementace“),
- předání průvodní dokumentace,
- zaškolení kupujícího
- součinnost při penetračních testech a odstranění chyb bránící užívání dle účelu smlouvy zjištěných při testech
- nezbytná technická podpora po dobu udržitelnosti Projektu, která činí 5 let od data předání do provozu. Technická podpora zahrnuje zejména aktualizace SW firewallu, maintenance, legislativní upgrade a update (dále jen „technická podpora“).

4. Kupní cena a platební podmínky

4.1. Celková kupní cena činí:

8 699 500 Kč bez DPH

1 826 895 Kč DPH

10 526 395 Kč vč. DPH

4.2. Cena bez DPH podle čl. 4.1. této smlouvy je stanovena dle technické specifikace (Příloha č. 1 této smlouvy) jako cena nejvýše přípustná a konečná a zahrnuje celý předmět plnění dle této smlouvy (s výjimkou ceny za poskytování technické podpory, která je upravena v čl. 4.5. níže).

4.3. Sjednaná cena celkem může být změněna pouze v případě změny zákona č. 235/2004 Sb., o DPH, týkající se sazby DPH a v souvislosti s ustanoveními § 222 zákona č. 134/2016 Sb., o zadávání veřejných zakázek.

4.4. Kupující se zavazuje zaplatit kupní cenu na základě faktur, vystavených prodávajícím a doručených kupujícímu dle níže uvedeného mechanismu:

- 1. faktura ve výši 35 % z celkové kupní ceny dle čl. 4.1. výše bude vystavena po dodání zboží.
- 2. faktura ve výši 35 % z celkové kupní ceny dle čl. 4.1. výše bude vystavena po zahájení penetračního testování.
- 3. faktura ve výši 30 % z celkové kupní ceny dle čl. 4.1. výše bude vystavena po oboustranném podpisu předávacího protokolu (tj. po předání a převzetí zboží do plného provozu).

4.5. Cena za technickou podporu po předání zboží do provozu je stanovena dohodnou smluvních strany na:

10 000 Kč bez DPH za 1 měsíc

2 100 Kč DPH

12 100 vč. DPH za 1 měsíc

4.6. Úhrada ceny za technickou podporu bude probíhat na základě měsíčně vystavované faktury. Datum uskutečnitelného zdanitelného plnění je sjednáno na poslední kalendářní den v měsíci.

4.7. Každá faktura musí splňovat náležitosti daňového dokladu podle § 28 zákona č. 235/2004 Sb., o DPH, bude obsahovat číslo a název dotačního projektu (konkrétně bude uveden text ve znění: *Projekt **„Bezpečné centrum sdílených služeb organizací města“**, reg. č. **CZ.06.01.01/00/22_004/0000143**, je spolufinancován z Integrovaného regionálního operačního programu“*) a bude zaslána prodávajícím na adresu kupujícího. **Splatnost faktury činí 30 kalendářních dní.**

4.8. Kupující bude oprávněn před uplynutím lhůty splatnosti vrátit prodávajícímu bez zaplacení fakturu, která nebude obsahovat některou náležitost uvedenou v této smlouvě, případně bude mít jiné závady v obsahu nebo bude uvedeno bankovní spojení a číslo účtu prodávajícího v rozporu s touto smlouvou anebo tyto náležitosti budou uvedeny chybně. U vrácené faktury musí kupující vyznačit důvod vrácení. Prodávající je povinen podle povahy nesprávnosti fakturu opravit nebo nově vyhotovit. Kupujícímu vrácením faktury přestává běžet původní lhůta splatnosti. Celá lhůta splatnosti běží znovu ode dne doručení opravené nebo nově vyhotovené faktury kupujícímu.

4.9. Platby budou zásadně probíhat bezhotovostní formou na bankovní účet prodávajícího uvedený ve smlouvě. Změnu bankovního spojení a čísla účtu prodávajícího bude možno provést pouze písemným dodatkem k této smlouvě nebo písemným sdělením prokazatelně doručeným kupujícímu, nejpozději spolu s příslušnou fakturou.

4.10. Faktura se považuje za včas uhrazenou, pokud je fakturovaná částka odepsána z účtu kupujícího.

5. Místo a doba plnění a dodací podmínky

5.1. Místem plnění je sídlo kupujícího.

5.2. Prodávající je povinen dodat zboží **nejpozději do 90 dní od účinnosti této smlouvy**.

5.3. Dodávka se považuje podle této smlouvy za dodanou, pokud bylo:

- zboží řádně dodáno včetně příslušné dokumentace (k instalaci, nastavení, zabezpečení jednotlivých komponent a včetně návrhu plánu obnovy).
- provedena instalace, implementace (případné podrobné specifické podmínky implementace jsou uvedeny u jednotlivých zařízení v příloze č. 1 smlouvy) a úspěšně vyzkoušena funkčnost,
  - činnost u níž se nepředpokládá žádný výpadek služeb lze provádět v pracovní době MÚ,
  - činnost u které se obě strany shodnou že předpokládaný výpadek bude kratší než 10 min lze provádět mimo úřední hodiny,
  - činnosti s výpadkem delší se mohou provádět pouze mimo pracovní dobu MÚ. Termín odstávky musí být znám alespoň týden předem,
  - termín školení uživatelů min. měsíc předem,
  - školení OIT může probíhat v průběhu instalace.
- součástí instalace bude následný testovací provoz provedený bez zbytečného odkladu v délce nutné pro ověření funkčnosti dodaného HW a SW. Náplň testovacího provozu bude následující:
  - zahoření a ověření funkčnosti HW zařízení
  - ověření vzájemné spolupráce jednotlivých HW zařízení
  - ověření napojení na LAN síť kupujícího
  - provedení zátěžových testů
  - ověření chování systému při výpadku některého ze zařízení (ověření vysoké dostupnosti)
  - ověření chování systému při výpadku el. energie

5.4. Po dodání zboží bude zahájena implementace plnění části 1 Veřejné zakázky v předpokládané délce trvání cca 3 měsíce. Po dokončení implementace této části Veřejné zakázky bude následovat fáze penetračního testování.

5.5. V rámci penetračního testování dojde k prověření funkčnost technických opatření a celkové bezpečnosti dodávky pomocí penetračního testu. Penetrační testování provede 3. osoba zvolená kupujícím, a to nejpozději do 14 dní od dokončení implementace plnění části 1 Veřejné zakázky, přičemž toto penetrační testování bude trvat maximálně 30 dní. V návaznosti na dokončení penetračního testování prodávající napraví nalezené chyby bránící užívání dle účelu smlouvy, a to nejpozději do 14 dní od okamžiku, kdy obdrží výsledek penetračního testování.

5.6. Po splnění dodávky zboží, tj. po prodávající napraví chyby bránící užívání dle účelu smlouvy nalezené v rámci penetračního testování, bude vyhotoven **zápis o předání a převzetí zboží**, který bude obsahovat níže uvedené náležitosti:

- název a sídlo prodávajícího a kupujícího,
- označení dodaného zboží včetně výrobního čísla,
- datum dodání,
- číslo a název dotačního projektu (konkrétně bude uveden text ve znění: *Projekt **„Bezpečné centrum sdílených služeb organizací města“**, reg. č. **CZ.06.01.01/00/22_004/0000143**, je spolufinancován z Integrovaného regionálního operačního programu“*).

5.7. Zápis o předání a převzetí zboží podepíší oprávnění zástupci obou smluvních stran, přičemž podpisem zápisu o předání a převzetí dochází k převzetí a předání zboží a ke splnění předmětu koupě.

6. Odpovědnost za vady, záruka za jakost, servis

6.1. Prodávající nese odpovědnost za to, že zboží dodané a předané podle této smlouvy je ke dni dodání plně funkční a splňuje technické parametry uvedené této smlouvě. Prodávající přejímá níže uvedenou záruku za jakost zboží dodaného podle této smlouvy. Záruční doba počíná běžet dnem oboustranného podpisu zápisu o předání a převzetí zboží. **Záruční doba pro jednotlivé položky v souladu s přílohou č. 1 této smlouvy činí 60 měsíců** ode dne předání a převzetí zboží.

6.2. Záruka se nevztahuje na spotřební materiál a na vady způsobené zaviněným jednáním kupujícího anebo způsobené vyšší mocí.

6.3. Kupující se zavazuje respektovat pokyny prodávajícího v oblasti údržby a používání správných pracovních postupů.

6.4. Technická podpora a servis budou poskytovány minimálně po celou dobu udržitelnosti projektu (tj. min. 60 měsíců ode dne předání do provozu).

6.5. Technická podpora a servis budou realizovány v sídle kupujícího. Výjimku tvoří činnosti realizovatelné vzdáleným připojením.

6.6. V případě nahlášení závady prodávajícímu bude oprava provedena vzdáleně či na místě nejpozději následující pracovní den od jejího nahlášení. V případě nemožnosti opravy následující pracovní den nabídne prodávající kupujícímu alternativu (tj. náhradní řešení) na dobu trvání opravy. V případě záruční opravy (tj. pokud se nejedná o vadu způsobenou zaviněným jednáním kupujícího anebo způsobenou vyšší mocí), není kupující povinen hradit náklady na cestovné servisních techniků ke kupujícímu a zpět, tyto náklady nese prodávající.

6.7. Nahlášení závady bude provedeno prostřednictvím e-mailu zaslaného na e-mailovou adresu servis@xanadu.cz, telefonicky na tel. číslo +420 272 764 400, prostřednictvím elektronické oznamovací služby (tzv. HelpDesku) nebo prostřednictvím vzdáleného připojení na PC uživatele / server.

6.8. Telefonická, e-mailová podpora a podpora prostřednictvím vzdáleného připojení bude k dispozici minimálně v pracovních dnech od 8 do 16 hod.

6.9. Služba HelpDesk umožní příjem požadavku na servisní zásah v českém jazyce prostřednictvím webového rozhraní v režimu 7x24 hod (s výjimkou předem nahlášených servisních zásahů při správě systému HelpDesk).

6.10. Prodávající se v záruční době zavazuje zajistit dostupnost náhradních dílů a spotřebního materiálu.

6.11. Po dobu běhu záruční doby bude zajištěna udržitelnost HW a SW včetně třetích stran.

6.12. Technická podpora a servis zařízení HW a SW budou realizovány přímo prodávajícím, případně prostřednictvím autorizovaného servisního kanálu výrobce.

7. Smluvní pokuta a úrok z prodlení

7.1. Smluvními stranami bylo ujednáno, že pokud bude kupující v prodlení s úhradou ceny plnění ujednané podle této smlouvy, je kupující povinen zaplatit úrok z prodlení ve výši 0,05 % z dlužné částky za každý, byť i započatý kalendářní den prodlení.

7.2. Ocitne-li se prodávající v prodlení s plněním podle této smlouvy dle čl. 5.2, je povinen zaplatit kupujícímu smluvní pokutu ve výši 0,05 % z kupní ceny, a to za každý, byť i započatý kalendářní den prodlení se splněním dodávky.

7.3. Ocitne-li se prodávající v prodlení s plněním podle této smlouvy dle čl. 5.5 (tj. pokud nenapraví nalezené chyby bránící užívání dle účelu smlouvy zjištěné v rámci penetračního testování ve stanovené lhůtě), je povinen zaplatit kupujícímu smluvní pokutu ve výši 0,05 % z kupní ceny, a to za každý, byť i započatý kalendářní den prodlení se splněním dodávky.

7.4. Ocitne-li se prodávající v prodlení s plněním dle čl. 6.6. této smlouvy, je povinen zaplatit kupujícímu smluvní pokutu ve výši 500,- Kč za každý započatý den prodlení s dokončením servisní opravy dle čl. 6.6.

7.5. Uplatněním nároku na smluvní pokutu dle této smlouvy není dotčen nárok na náhradu škody.

7.6. Smluvní pokuta je splatná ve lhůtě 30 dnů od doručení jejího vyúčtování povinné smluvní straně z této smluvní pokuty.

8. Doba trvání smlouvy, ukončení smlouvy

8.1. Tato smlouva se uzavírá na dobu určitou, nejdéle do doby splnění závazku dle této smlouvy (tj. do okamžiku ukončení poskytování nezbytné technické podpory, resp. do doby uplynutí 5 let od data předání zboží do provozu).

8.2. Od této smlouvy může smluvní strana dotčená porušením povinnosti jednostranně odstoupit pro podstatné porušení této smlouvy, přičemž za podstatné porušení této smlouvy se zejména považuje:

a) na straně kupujícího – nezaplacení kupní ceny podle této smlouvy ve lhůtě delší 14 dní po dni splatnosti příslušné faktury,

b) na straně prodávajícího – prodlení s dodáním zboží o více než 14 dní po termínu dodání dle čl. 5.2. či dodání nefunkčního zboží, nesplňujícího požadavky čl. 3 této smlouvy, marné uplynutí sjednané lhůty pro vyřízení záruční opravy dle čl. 6.6.

8.3. Smluvní strana porušením povinnosti dotčená je povinna odstoupení od smlouvy písemně oznámit druhé smluvní straně.

9. Ostatní ujednání

9.1. Smluvní strany se dohodly, že vlastnické právo k dodanému předmětu smlouvy nabývá kupující okamžikem převzetí zboží od prodávajícího.

9.2. Nebezpečí škody na zboží přechází z prodávajícího na kupujícího okamžikem převzetí zboží od prodávajícího či okamžikem, kdy kupujícímu bylo umožněno zboží převzít a ten jej nepřevzal.

9.3. Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých vzájemných závazků. Smluvní strany jsou povinny informovat druhou smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění této smlouvy.

9.4. Smluvními stranami bylo ujednáno, že veškeré informace, jež si navzájem poskytnou, jsou označeny jako důvěrné a žádná ze smluvních stran není oprávněna je poskytnout třetí osobě ani použít v rozporu s jejich účelem pro své potřeby.

9.5. Prodávající nesmí bez předchozího souhlasu kupujícího postoupit svá práva a povinnosti plynoucí ze smlouvy třetí osobě.

9.6. Kupující se zavazuje umožnit přístup určeným pracovníkům prodávajícího do prostoru svého objektu za účelem splnění této smlouvy (předání a převzetí zboží, servis a technická podpora).

9.7. Právní vztahy touto smlouvou neupravené, jakož i právní poměry z ní vznikající a vyplývající, se řídí příslušnými ustanoveními zákona č. 89/2012 Sb., občanského zákoníku a dalšími právními předpisy České republiky.

9.8. Ujednává se, že případné spory vzniklé z této smlouvy budou účastníci řešit především vzájemnou dohodou. Pro řízení o případných sporných nárocích se ujednává příslušnost soudů. Rozhodným právem je právo České republiky.

9.9. Za písemnou formu výzvy nebo oznámení se pro účely této smlouvy pokládají oznámení učiněná elektronickou poštou na dohodnuté elektronické adresy.

9.10. Prodávající je povinen zajistit, že veškeré vlastnosti předmětu smlouvy, včetně jeho update, legislativních update, upgrade a legislativních upgrade budou po celou dobu účinnosti této smlouvy odpovídat obecně platným právním předpisům ČR.

9.11. Prodávající prohlašuje, že bude mít po celou dobu plnění předmětu smlouvy uzavřenu pojistnou smlouvu kryjící odpovědnost za škodu způsobenou provozní činností s limitem pojistného plnění minimální výši kupní ceny zboží dle čl. 4.1., kterou se zavazuje kdykoliv na vyžádání předložit k nahlédnutí kupujícímu.

10. Závěrečná ustanovení

10.1. Prodávající je povinen umožnit všem subjektům oprávněným k výkonu kontroly projektu, z jehož prostředků je dodávka hrazena, provést kontrolu dokladů souvisejících s plněním zakázky, a to po dobu danou právními předpisy ČR k jejich archivaci (zákon č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů a zákon č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů).

10.2. Prodávající je povinen uvádět povinné prvky publicity podle podmínek strukturálních fondů EU na všech tištěných dokumentech vytvořených v souvislosti s předmětem koupě (nevztahuje se na interní účetní dokumentaci apod.). Tyto povinné prvky publicity sdělí a poskytne prodávajícímu na vyžádání kupující.

10.3. Prodávající je povinen při kontrole poskytnout na vyžádání kontrolnímu orgánu daňovou evidenci v plném rozsahu. **Prodávající je podle ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, osobou povinou spolupůsobit při výkonu finanční kontroly.**

10.4. Prodávající se zavazuje umožnit osobám oprávněným k výkonu kontroly projektu, z něhož je veřejná zakázka hrazena, provést kontrolu dokladů souvisejících s plněním zakázky, a to po dobu nejméně 10 let od ukončení financování díla způsobem, který je v souladu s platnými právními předpisy České republiky a Evropských společenství.

10.5. Prodávající je povinen minimálně do konce roku 2035 poskytovat požadované informace a dokumentaci související s realizací projektu, z něhož je Veřejná zakázka hrazena, 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 a poskytnout jim při provádění kontroly součinnost.

10.6. Prodávající bere na vědomí, že úhrada ceny za předmět plnění bude provedena s využitím dotačních prostředků, získaných kupujícím a podléhajících kontrole z hlediska vykazování účelnosti jejich čerpání. Prodávající se zavazuje, že kupujícímu nahradí veškeré škody a náklady, které mu vzniknou nebo budou muset být vynaloženy, pokud z důvodu porušení této smlouvy prodávajícím vznikne kupujícímu závazek vrátit dotaci nebo její část, poskytnutou na úhradu ceny za předmět plnění, jejímu poskytovateli, a to i včetně penále případně vyměřeného jako důsledek porušení pravidel nakládání s veřejnými prostředky. To platí obdobně, pokud prodávající znemožní řádný výkon kontroly orgánům, oprávněným ke kontrole účelnosti vynaložení dotačních prostředků, resp. nepředloží jimi požadované doklady.

10.7. Prodávající se zavazuje k dodržování mezinárodních sankcí Evropské unie, přijatých v souvislosti s ruskou agresí na území Ukrajiny vůči Rusku a Bělorusku, zejména nařízení Rady EU č. 2022/576, nařízení Rady (EU) č. 269/2014 ve spojení s prováděcím nařízením Rady (EU) č. 2022/581, nařízení Rady (EU) č. 208/2014 a nařízení Rady (ES) č. 765/2006 nebo v jejich prospěch (dále jen „mezinárodní sankce EU“).

10.8. Prodávající se zavazuje během plnění smlouvy i po jejím ukončení smlouvy zachovávat mlčenlivost o všech skutečnostech, o kterých se dozví od kupujícího v souvislosti s plněním smlouvy

10.9. Tuto smlouvu lze měnit nebo doplnit pouze dohodou smluvních stran, a to formou písemného číslovaného dodatku.

10.10. Smluvní strany prohlašují, že si tuto smlouvu přečetly, a že byla ujednána po vzájemném projednání podle jejich svobodné vůle, určitě, vážně a srozumitelně.

10.11. Smlouva je, v souladu s podmínkami zákona č. 134/2016 Sb., podepsána elektronicky.

10.12. Rada města Benešov souhlasila s uzavřením této smlouvy na svém jednání dne 23.08.2023 usnesením č. 729-17/2023/RM.

10.13. Smlouva nabývá platnosti dnem podpisu a účinnosti dnem jejího uveřejnění v registru smluv. Uveřejnění smlouvy v registru smluv provede kupující.

10.14. Nedílnou součástí této smlouvy jsou následující přílohy:

Příloha č. 1 – Technická specifikace

Prodávající:

V Praze dne dle data el. podpisu

Ing. Radek Nekl
Digitálně podepsal Ing. Radek Nekl
Datum: 2023.10.05 07:54:10 +02'00'

……

Ing, Radek Nekl, předseda představenstva
XANADU a.s.

Kupující:

V Benešově dne dle data el. podpisu

Ing. Jaroslav Hlavnička
Digitální podpis: 04.10.2023 13:30

……

Ing. Jaroslav Hlavnička, starosta
Město Benešov

Příloha č. 1 – Technická specifikace[1]

Nástroj pro ochranu integrity komunikačních sítí

Centrální LAN přepínače – 2 ks

Z důvodu zvýšení celkové datové propustnosti, bezpečnosti a výkonosti síťové infrastruktury požadujeme dodávku dvou kusů identických centrálních LAN přepínačů.

Parametr	Minimální požadavek
Výrobce a model	Aruba 6300M 24SFP+ 4SFP56 Swch
Provedení	• montáž do racku, včetně příslušenství pro montáž, výška 1U, stohovatelný • redundantní interní hot-swap napájecí zdroje • vyměnitelné hot-swap ventilátory
Porty:	• min. 24x 10Gb SFP+ port s volitelným fyzickým rozhraním • min. 4x SFP28/SFP56 port s volitelným fyzickým rozhraním
Management:	• RJ-45 OoB management port s podporou ethernetu • USB-C konzolový port
Vlastnosti a funkce:	• podpora přímého bezdrátového připojení ke konzoli zařízení pomocí bluetooth • kapacita Routing/Switching min. 800 Gbit/s • propustnost min. 600Mpps • tabulka MAC adres min. 29k • latence přepínače max. 5µs /1Gbit/s a 1,5µs / 10Gbit/s • min. 8GB RAM • plně manageovatelný přes webové rozhraní včetně VLAN • podpora VLAN podle IEEE 802.1Q, minimálně 4000 aktivních VLAN • podpora zařazování do VLAN podle standardu 802.1v • minimálně 10 podporovaných přepínačů ve stohu pomocí standardního síťového rozhraní • stohování až do propustsnoti 200Gbps • kterýkoli prvek ve stohu může být řídícím prvkem (1:N redundance) • stoh podporuje jednotnou konfiguraci (IP adresa, správa, konfigurační soubor) • stoh se chová jako jedno L3 zařízení (router, gateway, peer), včetně podpory dynamických směrovacích protokolů, jako např. OSPF • seskupení portů IEEE 802.3ad mezi různými prvky stohu (Multichassis LAG) • dynamické směrování OSPFv2, OSPFv3 a BGP včetně podpory BFD

[1] Níže v textu je kupující označen rovněž jako „zadavatel“ a prodávající jako „dodavatel“.

	• podpora ověřování MAC adres, minimálně 1000 ověřených MAC adres • ověřování pomocí 802.1X, minimálně 2000 ověřených uživatelů • 802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port • dynamické zařazování do VLAN a přidělení QoS podle RFC 4675 • podpora ověřování pomocí RADIUS serveru, včetně RADIUS CoA (RFC3576) • podpora TACACS+ • podpora uživatelských rolí definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely. • podpora NTPv4 pro IPv4 a IPv6 včetně VRF a MD5 autentizace • upgrade OS přepínače bez narušení provozu (ISSU) • podpora "jumbo rámců", včetně velikosti 9k Byte • podpora skriptování v jazyce Python – lokální interpret jazyka v přepínači • CE (Conformité Européene), RoHS, EN 60950-1
Kabeláž a optické moduly	• 1x 0,65m 50Gb SFP56 kabel • 3x 3m 10Gb SFP+ DA kabel • kabely budou dodání originální od výrobce switchů (použití OEM se nepovoluje)
Záruka	• min. 5 LET, max. odezva NBD on-site po nahlášení problému • servis je poskytován certifikovaným servisním partnerem případně přímo výrobcem • podpora musí zahrnovat jak HW, tak SW a musí být poskytována v českém jazyce • jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému • servisní zásahy budou prováděny vždy v místě instalace zařízení. Nabízené zařízení musí být pokryto oficiální podporou výrobce tak, aby v případě závady, kterou není Dodavatel schopen odstranit, mohl Zadavatel tuto závadu eskalovat přímo k technické podpoře výrobce zařízení • zadavatel musí mít možnost si sám legálně stahovat bezpečnostní záplaty i nové verze Software/Firmware pro nabízené zařízení přímo ze stránek výrobce zařízení
Certifikace dodavatele, původ zboží	• Jsou splněny „Požadavky na certifikaci dodavatele HW a původ zboží“

LAN přepínače klientské – 9 ks

Z důvodu zvýšení celkové datové propustnosti, bezpečnosti a výkonosti síťové infrastruktury požadujeme dodávku 9 kusů identických LAN přepínačů.

Parametr	Minimální požadavek
Výrobce a model	Cisco Catalyst 9200L 48-port PoE+, 4 x 10G, Network Essentials
Provedení	• montáž do racku, včetně příslušenství pro montáž, výška 1U, stohovatelný • možnost instalovat interní redundantní napájecí zdroj
Porty:	• min. 48 portů 10/100/1000 Base-TX s PoE+ napájením • min. 2 dedikované stohovací porty s kapacitou 80 Gb/s • min. 4x 1/10Gb SFP+ uplink portů
Vlastnosti:	• minimálně 8 podporovaných přepínačů ve stohu přes dedikované porty, bez snížení počtu použitelných ethernetových portů • možnost osazení redundantních napájecích zdrojů • PoE 740W, vč. schopnosti poskytovat PoE napájení připojeným zřízením i během restartu přepínače • kapacita Routing/Switching min. 176 Gbit/s • propustnost min. 130 Mpps • tabulka MAC adres min. 16k • buffer min. 6MB • počet IPv4 routes min. 3000; IPv6 min. 1500 • IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis • min. 8 linek jako součást Link Aggregation Group trunku • min. počet konfigurovatelných Link Aggregation Group trunků 48 • IEEE 802.1Q • min. počet aktivních VLAN 512 • IEEE 802.1x • konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací) • integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication) • možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů • RADIUS CoA • podpora instance spanning-tree protokolu per VLAN • IEEE 802.1w - Rapid Spanning Tree Protocol • protokol MVRP nebo VTP pro definici a správu VLAN sítí • podpora ju MBo rámců (min. 9198 bytes) • detekce protilehlého zařízení (např. CDP nebo LLDP) • směrování protokolů IPv4 a IPv6 v hardware • RIP, EIGRP Stub, OSPFv2; OSPFv3 - minimálně 1000 Routes • VRRP • Reverse path check (uRPF) pro IPv4 i IPv6 • IGMPv2, IGMPv3 • IGMP snooping

	• MLD snooping • min. počet HW QoS front 8 • QoS classification – ACL, DSCP, CoS based • QoS marking - DSCP, CoS • automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní) • QoS Policing • IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard) • možnost definovat povolené MAC adresy na portu • PACL, VACL • paketové filtry (ACL) jsou stále aplikovány a filtrují v případě, že jsou na nich prováděny změny • IEEE 802.1ae na uplink portech • bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy • bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru • bezpečnostní funkce umožňující inspekci provozu protokolu ARP • ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů • HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů • IEEE 802.3az • automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu • SSHv2 • CLI rozhraní • vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu • model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG • interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení • aplikace softwarových záplat, nikoli povyšování celého firmware • streaming telemetrie prostřednictvím NETCONF/XML • SNMPv2/v3 • oodpora network boot (iPXE) • inventarizovatelnost komponent integrovanou RFID identifikací • TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)
Záruka	• min. 5 LET, max. odezva NBD on-site po nahlášení problému • servis je poskytován certifikovaným servisním partnerem případně přímo výrobcem

	• servisní zásahy budou prováděny vždy v místě instalace zařízení. Nabízené zařízení musí být pokryto oficiální podporou výrobce tak, aby v případě závady, kterou není Dodavatel schopen odstranit, mohl Zadavatel tuto závadu eskalovat přímo k technické podpoře výrobce zařízení • zadavatel musí mít možnost si sám legálně stahovat bezpečnostní záplaty i nové verze Software/Firmware pro nabízené zařízení přímo ze stránek výrobce zařízení

Management LAN přepínač – 1 ks

Z důvodu zvýšení celkové bezpečnosti a výkonosti síťové infrastruktury, segmentace sítě a odděleného managementu požadujeme dodávku managment LAN přepínače.

Parametr	**Minimální požadavek**
Výrobce a model	Aruba 6100 24G 4SFP+ Swch
Provedení	• montáž do racku, včetně příslušenství pro montáž, výška 1U
Porty:	• min. 24x 1Gb RJ-45 port s volitelným fyzickým rozhraním • min. 4x 1Gb SFP+ port s volitelným fyzickým rozhraním
Management:	• plně manageovatelný přes webové rozhraní včetně VLAN
Vlastnosti a funkce:	• kapacita Routing/Switching min. 128Gbit/s • propustnost min. 95Mpps • tabulka MAC adres min. 8k • latence přepínače max. 1,5µs /1Gbit/s a 1,8µs /10Gbit/s • min. 4GB RAM • podpora VLAN podle IEEE 802.1Q, minimálně 4000 VLAN; min. 500 VLAN současně • podpora ověřování MAC adres, minimálně 8000 ověřených MAC adres • ověřování pomocí 802.1X • podpora ověřování pomocí RADIUS serveru • podpora TACACS+ • podpora uživatelských rolí definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely • podpora "jumbo rámců", včetně velikosti 9k Byte • CE (Conformité Européene), RoHS, EN 60950-1
Záruka	• min. 5 LET, max. odezva NBD on-site po nahlášení problému • servis je poskytován certifikovaným servisním partnerem případně přímo výrobcem • podpora musí zahrnovat jak HW, tak SW a musí být poskytována v českém jazyce • servisní zásahy budou prováděny vždy v místě instalace zařízení. Nabízené zařízení musí být pokryto oficiální podporou výrobce tak, aby v případě závady, kterou není Dodavatel schopen

	odstranit, mohl Zadavatel tuto závadu eskalovat přímo k technické podpoře výrobce zařízení • zadavatel musí mít možnost si sám legálně stahovat bezpečnostní záplaty i nové verze Software/Firmware pro nabízené zařízení přímo ze stránek výrobce zařízení
Certifikace dodavatele, původ zboží	• Jsou splněny „Požadavky na certifikaci dodavatele HW a původ zboží“

Nástroj pro sběr a vyhodnocování kybernetických bezpečnostních událostí

Parametr	**Minimální požadavek**
Výrobce, název, verze a licenční program	ESET PROTECT Enterprise On-prem + ESET PROTECT Mail Plus
Ochrana před škodlivým SW	• Podpora operačních systémů MS: o Windows 7 a vyšší o Windows Server 2008 R2 a vyšší • Antivirový klient pro systémy: o Windows o Linux o macOS o Android • Real-Time ochrana před všemi typy PUA a malwaru: o viry o červy o trojskými koňmi (backdoor, adware, spyware, rootkit, bootkit, ransomware…) • Správa zařízení pro Windows, macOS a Linux umožňující blokaci externích zařízení a médií s podporou whitelistování dle: o výrobce, modelu nebo sériového čísla, o uživatelů nebo skupin (např. administrátorů) v AD, o lokálního času. • Schopnost blokace přístupu na definované weby nebo skupiny webů dle kategorií s možností whitelistování dle přihlášeného uživatele / skupiny v AD nebo času. • Lokální anti-spam s úspěšností detekce 99 % a vyšší. • Lokální anti-spam s možností definování důvěryhodných a spamových adres. • Nativní 64-bitové jádro. • Ochrana komunikace e-mailovými protokoly: o POP3, o POP3S, o IMAP, o IMAPS,

	○ HTTP, ○ MAPI. • Antivirus, antispyware a anti-phishing pro aktivní ochranu před všemi typy hrozeb. • Personální firewall pro zabránění neautorizovanému přístupu k zařízení se schopností automatického přebrání pravidel z brány Windows Firewall. • HIPS (Host-based Intrusion Prevention System) pro ochranu operačního systému a eliminaci aktivit ohrožující bezpečnost zařízení. • Aktivní i pasivní heuristická analýza pro detekci dosud neznámých hrozeb. • Systém pro blokaci exploitů zneužívajících zero-day zranitelností, jenž pokrývá nejpoužívanější vektory útoku: ○ síťové protokoly, ○ Flash Player, ○ Javu, ○ Microsoft Office, ○ webové prohlížeče, ○ e-mailové klienty, ○ PDF čtečky… • Systém pro detekci malwaru již na síťové úrovni poskytující ochranu i před zneužitím zranitelností na síťové vrstvě. • Anti-phishing se schopností detekce homoglyph útoků. • Kontrola RAM paměti pro lepší detekci malwaru využívající silnou obfuskaci a šifrování. • Možnost jednotlivého zapnutí detekcí: ○ potenciálně nechtěných aplikací, ○ zneužitelných aplikací, ○ podezřelých aplikací. • Cloud kontrola souborů pro urychlení skenování fungující na základě reputace souborů. • Kontrola souborů v průběhu stahování pro snížení celkového času kontroly. • Detekce s využitím strojového učení. • Funkce ochrany proti zapojení do botnetu pracující s detekcí síťových signatur. • Ochrana před síťovými útoky skenující síťovou komunikaci a blokující pokusy o zneužití zranitelností na síťové úrovni. • Kontrola s podporou cloudu pro odesílání a online vyhodnocování neznámých a potenciálně škodlivých aplikací. • Lokální sandbox.

	• Speciální modul behaviorální analýzy pro detekce nových typů ransomwaru. • Systém reputace pro získání informací o závadnosti souborů a URL adres. • Cloudový systém pro detekci nového malwaru ještě nezaneseného v aktualizacích signatur. • Technologie pro detekci rootktitů obvykle se maskujících za součásti operačního systému. • Skenr firmwaru BIOSu a UEFI. • Skenování souborů v cloudu OneDrive. • Šetření baterie notebooku – možnost odložení kontroly / provádění aktualizací, pokud je zařízení napájeno z baterie. • Podpora dotykového ovládání. • Ovládání bezpečnostního programu pomocí Příkazového řádku. • Podpora ochrany na IPv6. • Možnost řízení šířky pásma pro stahování aktualizací. • HIPS s možností definovat pravidla pro systémové registry, procesy, aplikace a soubory. • Možnost vrácení i odložení aktualizací signatur. • Možnost instalovat plnohodnotné antivirové řešení na virtuální stanici/server. • Modulární instalace. • Automatická synchronizace bezpečnostních produktů v clusteru. • Bezagentové zabezpečení pro VMware vShield a NSX. • Možnost importu/exportu nastavení. • Prezentační režim umožňující potlačení méně důležitých upozornění při práci v celoobrazovkovém režimu aplikace. • Možnost tvorby výjimek na procesy. • Ochrana před neautorizovanou změnou nastavení / vyřazení z provozu / odinstalací antimalware řešení a kritických nastavení a souborů operačního systému. • Možnost vzdáleného definování akce při připojení výměnných médií (kontrolovat, nekontrolovat, nechat na uživateli). • Možnost využití sdílené cache v rámci lokální sítě (umožňuje přeskočení skenování stejných souborů, které již byly zkontrolované na jiném zařízeních a tím výrazně zrychlit kontrolu). • Duální aktualizační profil pro možnost stahování aktualizací z mirroru v lokální síti a zároveň vzdálených serverů při nedostupnosti lokálního mirroru (pro cestující uživatele s notebooky). • Kontrola šifrovaných spojení (SSL, TLS, HTTPS, IMAPS…).

	• Možnost odesílání e-mailových upozornění a událostí přímo z klienta.
	• Integrovaný komplexní diagnostický nástroj umožňující řešit problémy s infiltrací, jakožto i jiné softwarové a hardwarové nekorektní chování (obsahuje informace procesech, službách, síťových připojeních, ovladačích a problémových položkách v registrech).
	• Upozornění při připojení k nezabezpečené bezdrátové síti nebo síti se slabým zabezpečením, jejíž šifrování lze snadno prolomit.
	• Využití Microsoft Antimalware Scan Interface (AMSI) pro kontrolu skriptů (PowerShell, wscript.exe a cscript.exe).
	• Podpora Protected Services – službu produktu je možné chránit proti nechtěné modifikaci standardní součástí operačního systému.
	• Podpora odečítače obrazovky pro zrakově postižené.
	• Podpora SNMP Trap, Syslogu a qRadar SIEM.
	• Podpora instalace skriptem - *.bat, *.sh, *.ini (GPO, SSCM…).
	• Rychlé připojení na klienta pomocí RDP z konzole pro vzdálenou správu.
	• Reportování stavu klientů chráněných jinými bezpečnostními programy.
	• Schopnost zaslat reporty a upozornění na e-mail.
	• Přidání zařízení do vzdálené správy pomocí:
	  o synchronizace s Active Directory,
	  o ruční přidání pomocí dle IP adresy nebo názvu zařízení,
	• pomocí síťového skenu nechráněných zařízení v síti.
	• platnost licence min. 60 měsíců, včetně nároku na opravné a nové verze software, vč. technické podpory výrobce.

SW pro sandboxing	• Sandbox umožňující spuštění vzorků malwaru pro:
	  o Windows,
	  o macOS,
	  o Linux,
	  o Android.
	• Možnost využití na koncových bodech a Exchange serveru pro aktivní detekci škodlivých souborů v e-mailech.
	• Řešení zajišťuje neodesílání duplicitních souborů nalezených různými endpointy.
	• Analýza neznámých vzorků v řádu jednotek minut.
	• Schopnost ochrany klientů mimo firemní síť.
	• Optimalizace pro znemožnění obejití anti-sandbox mechanismy.
	• Schopnost analýzy rootkitů a ransomwaru.
	• Schopnost detekce a zastavení zneužití nebo pokusu o zneužití zero day zranitelnosti.

	• Řešení pracuje s behaviorální analýzou.
	• Manuální odeslání vzorku do sandboxu.
	• Funkce cloudového sandboxu je integrována do antimalware produktu (cloudový sandbox nemá vlastního agenta).
	• Možnost proaktivní ochrany, kdy je potenciální hrozba blokována, dokud není znám výsledek analýzy ze sandboxu.
	• Neomezené množství odesílaných souborů.
	• Veškerá komunikace probíhá šifrovaným kanálem.
	• Webová konzole.
	• Administrace v nejpoužívanějších jazycích včetně češtiny.
	• Možnost nastavení typů odesílaných souborů:
	  o spustitelné soubory,
	  o skripty,
	  o spam,
	  o dokumenty.
	• Přehled o veškerých odeslaných souborech ve správcovské konzoli.
	• Nastavení per zařízení & per skupina.
	• Možnost nastavit na výsledek sandboxu výjimku.
	• Zaslání e-mailové notifikace v případě nalezení škodlivého kódu.
	• Správa karantény s možností vzdáleného vymazání / obnovení / obnovení a vyloučení objektu z detekce.
	• Server/proxy architektura pro síťovou pružnost – snížení zátěže.
	• platnost licence min. 60 měsíců, včetně nároku na opravné a nové verze software, vč. technické podpory výrobce

SW pro odhalení škodlivé, či podezřelé aktivity včetně analýzy	• Podpora Windows a macOS.
	• Indicators of Compromise (IOCs):
	  o MD5 hodnoty souborů,
	  o IP adresy a URL,
	  o Nesoulad názvů souborů/procesů,
	  o Neobvyklé využití aplikací a síťových portů,
	  o Neobvyklé injektování do procesů,
	  o Modifikace částí aplikací,
	  o Změny v registru.
	• Indikátory útoku pracující s behaviorální detekcí.
	• Indikátory útoku pracující s reputací.
	• Možnost tvorby vlastních IoC.
	• Řešení umožnuje analýzu vektorů útoku.
	• Vizibilita do WMI.
	• Vizibilita do spouštěných skriptů (PowerShellem, CScriptem, WScriptem…).
	• Přehled o veškerém použitém softwaru a jeho verzích.

	• Schopnost detekce škodlivých spustitelných souborů a skriptů.
	• Pokročilé možnosti analýzy:
	  o exploitů,
	  o rootkitů,
	  o síťových útoků,
	  o bezsouborového malwaru.
	• Schopnost analýzy RAM paměti.
	• Detekce rootkitů v UEFI a MFT.
	• Schopno detekovat laterální pohyb útočníka.
	• Tagování objektů.
	• Terminal (interaktivní Shell).
	• Možnost ruční analýzy procesů a veškerých spustitelných souborů včetně DLL knihoven a skriptů.
	• Prioritizace vzniklých incidentů za pomocí algoritmů strojového učení.
	• Detekce více než 300 typů obecného podezřelého chování: dumpování přihlašovacích údajů, změna konfigurace firewallu, mazání logů, změna hosts souboru, smazání Shadow Copy, nainstalování nového certifikát, vypnutí aktualizací…
	• Detekce s využitím modelů strojového učení a neuronových sítí.
	• Schopnost zobrazení detekcí provedených antimalware produktem.
	• Možnost spouštět předkonfigurované nápravné akce, které se sami spustí za při splnění definovaných podmínek.
	• Okamžitá síťová izolace, ukončení procesu, vymazání/stažení souboru.
	• Snížení počtu falešně pozitivních výsledků za pomocí algoritmů strojového a hlubokého učení.
	• Řešení je schopno generovat tzv. forest / full execution tree model.
	• Možnost vyhledávání pomocí nově vytvořených IoC nad historickými daty.
	• Provázání s technikami popsanými v knowledge base MITRE ATT&CK.
	• Možnost analyzovat
	  o veškeré události až 3 měsíce zpětně,
	  o bezpečnostní incidenty až 3 roky zpětně.
	• Možnost provozu v offline prostředí.
	• Možnost logování činností uživatele.
	• Přihlašování do konzole za využití 2FA.
	• Podpora exportu do SIEMu.
	• REST API.
	• Možnost provozu EDR serveru na systému Windows.
	• Možnost provozu centrálního serveru on-premise.
	• Možnost provozu s databázemi:

	○ MS SQL, ○ MySQL. • platnost licence min. 60 měsíců, včetně nároku na opravné a nové verze software, vč. technické podpory výrobce.

Kryptografické prostředky

V rámci zachování kompatibility se stávajícím poštovním serverem požadujeme dodání serverové licence Microsoft Exchange Server Standard v nejnovější verzi.

Parametr	Minimální požadavek
Výrobce, název, verze a licenční program serverového OS	MICROSOFT CSP Exchange Server Standard 2019 CSP Exchange Server Standard 2019 User CAL
Typ licence	serverová
Kompatibilita	Plná kompatibilita se stávajících poštovním serverem Microsoft Exchange.
Technické a licenční požadavky na uživatelské licence	• kompatibilita s nabízeným serverovým OS • kompatibilita s používanou správou uživatelů (Active directory) • kompatibilita s OS na koncových stanicích uživatelů
Počet uživatelských licencí	• dodání licencí minimálně pro přístup 250 uživatelů k nabízenému poštovnímu serveru, jsou-li dle licenčních podmínek výrobce nutné

Nástroj pro zajišťování úrovně dostupnosti informací

Servery pro zvýšení dostupnosti infrastruktury úřadu – celkem 2 ks

Pro provoz aplikační architektury je v rámci návrhu řešení požadována dodávka dvou serverů, které zajistí dostupnost aplikací a dat úřadu.

Parametr	Minimální požadavek
Výrobce a model	HPE DL360 Gen10+ 8SFF NC CTO Svr
Provedení, příslušenství	1U, varianta rack, kolejnice do RACKu a rameno pro uchycení kabeláže
CPU	server osazen 2x CPU s parametry každého z nich 8 fyzických jader, 16 vláken, minimální taktovací frekvence 3.6GHz, min. 18MB Cache. Výkon každého CPU min. 22 150 bodů v syntetickém benchmarku CPU Benchmark společnosti Passmark (High End CPUs)
RAM – sloty	• min. 32 DIMM slotů pro paměti typu DDR4 3200MT/s, rozšiřitelnost až na 2TB RAM v případě RDIMM a až 8TB v případě LRDIMM • podpora 256GB modulů LRDIMM 3200MT/s

	• podpora technologie Persistent Memory s možností osadit až 16 modulů o velikosti 512GB.
RAM – požadovaná kapacita	384GB RAM DDR4/3200MT/s (použity 32GB moduly), další paměťové sloty volné pro pozdější upgrade pamětí bez výměny modulů a bez snížení frekvence
PCIe sloty	• min. 3x PCIe sloty • alespoň dva sloty v provedení PCIe 4.0 x16 plné délky a výšky • dedikovaný slot pro diskový řadič (nezabírající PCIe sloty)
HDD – pozice	• min. 10 pozic na pevné disky v rámci šasi serveru • min. 2x M2 SSD nezabírající výše uvedené sloty na HDD • podpora NVMe disků
HDD	min. 2x 240GB SSD v RAID1 nebo min. 2x 480GB M2 NVMe SSD na specializované bootovací kartě
RAID radič	řadič disků s podporou RAID nejméně 0, 1, 5, 10+0 a možností připojení až 14x HDD
Flash paměť	• podpora alespoň 32GB microSD karet zapojených v RAID1 s možností bootování nasazeného hypervizoru • interní USB a SD konektor pro aplikační klíče
Optická mechanika	možnost osazení interní DVD-RW mechaniky
USB porty	• min. 5 USB portů, z toho min. 3x USB 3.0 • nepřipouští se PCIe karta
Napájení – zdroje	• redundantní, hot-plug napájecí zdroje, min. 800W; účinnost min. 94%, napájení jednofázové 220-240V s možností nastavení limitů výkonu a spotřeby v BIOSu serveru
Ventilátory	• redundantní, za provozu vyměnitelné ventilátory
Ethernet porty	• min. 4x 1Gbit/s RJ-45 Ethernet porty • min. 2x 10Gbit/s SFP+ Ethernet porty typu OCP3
SAN porty	• 2x 16Gb FC SAN porty osazené SR FC16 SFP+ moduly pro připojení k diskovému poli
Interface	• TPM 2.0 čip • VGA port • LED panel indikující stavy serveru (min. procesory, RAM, LAN karty, napájecí zdroje, ventilátory) • sériový port integrovaný přímo na základní desku serveru (nepřipouští se PCIe karta) • možnost doplnění serveru o Display port pro připojení monitoru

	(KVM) na čelním panelu serveru
Management serveru - vlastnosti	Integrovaný nezávislý procesor pro vzdálenou správu umožňující: • dedikovaný LAN RJ-45 port umožňující zabezpečený přístup přes síť – webovým prohlížečem i SSH • připojení virtuálních médií (FDD, DVD, ISO i jejich image, USB klíče, adresáře pro čtení) • plně integrovanou grafickou konzoli s možností sdílení více uživateli současně • integrovaný nástroj pro upgrade firmware s možností automatické aktualizace od výrobce HW • sledování hardwarových senzorů (teplota, napětí, stav, chybové senzory) • možnost skupinového update firmware všech serverů v jednom poolu • nezávislý procesor musí pracovat i při nenabootovaném operačním systému serveru • podpora rollback firmware serveru • musí umožnit průběžné sledování parametrů serveru, hardwarový stav serveru, včetně uložení event. logu • zabezpečený přístup pomocí vzdálené konzole pro přímou správu OS serveru • detekci a zasílání SNMP zpráv o chybových stavech hardware • podporu standartu SNMP/ SSL/ SSH/ IPMI • řízení přístupových práv k centrální části SW a k management nástrojům na serverech pomocí účtů Active Directory domény • server musí být schopen zajistit bezpečný provoz firmware komponent v serveru (minimálně HDD, SSD, síťové adaptéry, BIOS a vzdálenou správu) po celou dobu životnosti serveru. Server musí být schopen autonomně monitorovat autenticitu firmware na těchto komponentách. V případě zjištění neschváleného firmware musí být schopen automaticky uvést stav poškozené komponenty do bezpečného stavu. Pokud tato funkcionalita vyžaduje licenci, musí být součástí nabídky
Podporované OS	• Microsoft Windows Server 2016 a vyšší • Red Hat Enterprise Linux 7.9 a vyšší • SUSE Linux Enterprise Server 12 a vyšší • Ubuntu • Oracle Linux 7.9 a vyšší
Podpora virtualizace	• Citrix Hypervisor 8.2 • VMware vSphere 6.7 a vyšší • MS Hyper-V 2016 a vyšší • Red Hat KVM

Záruka, servis	• min. 5 let na kompletní HW, max. odezva NBD on-site po nahlášení problému • servis je poskytován certifikovaným servisním partnerem, případně přímo výrobcem • podpora musí zahrnovat jak HW, tak SW výrobce i výrobců SW třetích stran, minimálně Microsoft, VMware, RHEL, SLES. Tato SW podpora musí být v ceně řešení a musí být poskytována v českém jazyce • jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému • servisní zásahy budou prováděny vždy v místě instalace zařízení. Nabízené zařízení musí být pokryto oficiální podporou výrobce tak, aby v případě závady, kterou není Dodavatel schopen odstranit, mohl Zadavatel tuto závadu eskalovat přímo k technické podpoře výrobce zařízení • zadavatel musí mít možnost si sám legálně stahovat bezpečnostní záplaty i nové verze Software/Firmware pro nabízené zařízení přímo ze stránek výrobce zařízení
Certifikace dodavatele, původ zboží	• Jsou splněny „Požadavky na certifikaci dodavatele HW a původ zboží“
Kompatibilita	• Servery, disková pole a pásková knihovna budou od jednoho výrobce z důvodu zajištění maximální kompatibility a jednotného servisního místa a managementu

Zajištění podkladových licencí serverových operačních systémů produkčních serverů – 2 ks

Parametr	Minimální požadavek
Výrobce, název, verze a licenční program serverového OS	Microsoft MS WS22 16C DC ROK en/cs/pl/ru/sv SW
Verze	Serverový operační systém v nejnovější verzi s podporou virtualizace
Počet serverových licencí	• neomezený počet serverů v serverovém virtuálním prostředí VMware vSphere • licence pro min. 2x osazené CPU v každém serveru • licence dle počtu procesorových jader
Vlastnosti OS	• adresářové služby kompatibilní s X. 509 • adresářová služba umožňuje obsahovat objekty typu uživatel, skupina, počítač a další • autentizace protokoly Kerberos V5, NTLMv2, NTLM

	• centrálně řízené politiky uživatelů a počítačů • možnost funkcí DNS, DHCP, WINS • možnost sdílení souborů a nastavování práv na objekty adresářové služby • sdílení souborů pomocí protokolu CIFS • distribuovaný souborový systém a delta replikace • možnost sdílení tiskáren a nastavování práv na objekty adresářové služby • možnost grafického uživatelského rozhraní v češtině • možnost downgrade na nižší verzi • Plná kompatibilita se stávajícími operačními systémy Microsoft Windows Server
Technické a licenční požadavky na uživatelské licence	• kompatibilita s nabízeným serverovým OS • kompatibilita s používanou správou uživatelů (Active directory) • kompatibilita s OS na koncových stanicích uživatelů
Počet uživatelských licencí	• kodání licencí minimálně pro přístup 200 uživatelů k nabízenému serverovému OS, jsou-li dle licenčních podmínek výrobce nabízeného serverového OS nutné
Správa systému	• pro správu operačního systému požadujeme grafické nástroje s jednoduchou obsluhou
Dokumentace	• požadujeme podrobnou technickou dokumentaci v elektronické podobě

Zálohovací server – 1 ks

Z důvodu zajištění spolehlivého a bezpečného zálohování je požadována dodávka nového zálohovacího serveru.

Parametr	**Minimální požadavek**
Výrobce a model	HPE DL380 Gen10+ 8SFF NC CTO Svr
Provedení, příslušenství	2U, varianta rack, kolejnice do RACKu a rameno pro uchycení kabeláže
CPU	server osazen 2x CPU s parametry 8 fyzických jader, 16 vláken, minimální taktovací frekvence 2.8GHz, min. 12MB Cache. Výkon každého CPU min. 19 200 bodů v syntetickém benchmarku CPU Benchmark společnosti Passmark (High End CPUs)
RAM - sloty	• min. 32 DIMM slotů pro paměti typu DDR4 3200MT/s, rozšiřitelnost až na 2TB RAM v případě RDIMM a až 8TB v případě LRDIMM • podpora 256GB modulů LRDIMM 3200MT/s

	• podpora technologie Persistent Memory s možností osadit až 16 modulů o velikosti 512GB
RAM – požadovaná kapacita	• 64GB RAM DDR4/3200MT/s (použity 32GB moduly), další paměťové sloty volné pro pozdější upgrade pamětí bez výměny modulů a bez snížení frekvence
PCIe sloty	• min. 6x PCIe sloty (s možností rozšíření až na 8x PCIe) • alespoň dva sloty v provedení PCIe 4.0 x16 plné délky a výšky • dedikovaný slot pro diskový řadič (nezabírající PCIe sloty)
HDD – pozice	• min. 8 pozic s možností rozšíření až na 26 pozic v rámci šasi serveru • min. 2x M2 SSD nezabírající výše uvedené sloty na HDD • podpora NVMe disků
HDD	• min. 2x 960GB SSD MU v RAID1
RAID radič	• řadič disků s podporou RAID nejméně 0, 1, 5, 10+0 a možností připojení až 14x HDD
Flash paměť	• podpora alespoň 32GB microSD karet zapojených v RAID1 s možností bootování nasazeného hypervizoru • interní USB a SD konektor pro aplikační klíče
Optická mechanika	• možnost osazení interní DVD-RW mechaniky
USB porty	• min. 5 USB portů, z toho min. 3x USB 3.0 • nepřipouští se PCIe karta
Napájení – zdroje	• redundantní, hot-plug napájecí zdroje, min. 800W; účinnost min. 94%, napájení jednofázové 220-240V s možností nastavení limitů výkonu a spotřeby v BIOSu serveru
Ventilátory	• redundantní, za provozu vyměnitelné ventilátory
Ethernet porty	• 4x 1Gbit/s RJ-45 Ethernet porty • 2x 10Gbit/s SFP+ Ethernet porty typu OCP3 • 2x 10/25Gbit/s SFP28 Ethernet porty
SAN porty	• 2-port 16Gb FC SAN HBA osazené SR FC16 SFP+ moduly pro připojení k diskovému poli • 1-port 16Gb FC SAN HBA osazené SR FC16 SFP+ modulem pro připojení páskové knihovny
Interface	• TPM 2.0 čip

	• VGA port • LED panel indikující stavy serveru (min. procesory, RAM, LAN karty, napájecí zdroje, ventilátory) • sériový port integrovaný přímo na základní desku serveru (nepřipouští se PCIe karta) • možnost doplnění serveru o Display port pro připojení monitoru (KVM) na čelním panelu serveru
Management serveru - vlastnosti	Integrovaný nezávislý procesor pro vzdálenou správu umožňující: • dedikovaný LAN RJ-45 port umožňující zabezpečený přístup přes síť – webovým prohlížečem i SSH • připojení virtuálních médií (FDD, DVD, ISO i jejich image, USB klíče, adresáře pro čtení) • plně integrovanou grafickou konzoli s možností sdílení více uživateli současně • integrovaný nástroj pro upgrade firmware s možností automatické aktualizace od výrobce HW • sledování hardwarových senzorů (teplota, napětí, stav, chybové senzory) • možnost skupinového update firmware všech serverů v jednom poolu • nezávislý procesor musí pracovat i při nenabootovaném operačním systému serveru • podpora rollback firmware serveru • musí umožnit průběžné sledování parametrů serveru, hardwarový stav serveru, včetně uložení event. logu • zabezpečený přístup pomocí vzdálené konzole pro přímou správu OS serveru • detekci a zasílání SNMP zpráv o chybových stavech hardware • podporu standartu SNMP/ SSL/ SSH/ IPMI • řízení přístupových práv k centrální části SW a k management nástrojům na serverech pomocí účtů Active Directory domény • server musí být schopen zajistit bezpečný provoz firmware komponent v serveru (minimálně HDD, SSD, síťové adaptéry, BIOS a vzdálenou správu) po celou dobu životnosti serveru. Server musí být schopen autonomně monitorovat autenticitu firmware na těchto komponentách. V případě zjištění neschváleného firmware musí být schopen automaticky uvést stav poškozené komponenty do bezpečného stavu. Pokud tato funkcionalita vyžaduje licenci, musí být součástí nabídky.
Podporované OS	• Microsoft Windows Server 2016 a vyšší • Red Hat Enterprise Linux 7.9 a vyšší • SUSE Linux Enterprise Server 12 a vyšší • Ubuntu

	• Oracle Linux 7.9 a vyšší
Podpora virtualizace	• Citrix Hypervisor 8.2 • VMware vSphere 6.7 a vyšší • MS Hyper-V 2016 a vyšší • Red Hat KVM
Záruka, servis	• min. 5 let na kompletní HW, max. odezva NBD on-site po nahlášení problému • servis je poskytován certifikovaným servisním partnerem, případně přímo výrobcem • podpora musí zahrnovat jak HW, tak SW výrobce i výrobců SW třetích stran, minimálně Microsoft, VMware, RHEL, SLES. Tato SW podpora musí být v ceně řešení a musí být poskytována v českém jazyce • jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému • servisní zásahy budou prováděny vždy v místě instalace zařízení. Nabízené zařízení musí být pokryto oficiální podporou výrobce tak, aby v případě závady, kterou není Dodavatel schopen odstranit, mohl Zadavatel tuto závadu eskalovat přímo k technické podpoře výrobce zařízení • zadavatel musí mít možnost si sám legálně stahovat bezpečnostní záplaty i nové verze Software/Firmware pro nabízené zařízení přímo ze stránek výrobce zařízení
Certifikace dodavatele, původ zboží	• Jsou splněny „Požadavky na certifikaci dodavatele HW a původ zboží“
Kompatibilita	• Servery, disková pole a pásková knihovna budou od jednoho výrobce z důvodu zajištění maximální kompatibility a jednotného servisního místa a managementu

Zajištění podkladové licence serverového operačního systému zálohovacího serveru – 1 ks

Pro nasazení nového zálohovacího serveru je nutné zajistit podkladovou licenci pro operační systém 100% kompatibilní se současně provozovanou serverovou platformou v nejnovější dostupné verzi.

Parametr	**Minimální požadavek**
Výrobce, název, verze a licenční program serverového OS	Microsoft MS WS22 16C DC ROK en/cs/pl/ru/sv SW
Verze	Serverový operační systém v nejnovější verzi s podporou virtualizace

Počet serverových licencí	• pro provoz 2 serverů v serverovém virtuálním prostředí VMware vSphere nebo přímo na fyzickém HW • licence pro min. 2 CPU sockety
Vlastnosti OS	• adresářové služby kompatibilní s X. 509 • adresářová služba umožňuje obsahovat objekty typu uživatel, skupina, počítač a další • autentizace protokoly Kerberos V5, NTLMv2, NTLM • centrálně řízené politiky uživatelů a počítačů • možnost funkcí DNS, DHCP, WINS • možnost sdílení souborů a nastavování práv na objekty adresářové služby • sdílení souborů pomocí protokolu CIFS • distribuovaný souborový systém a delta replikace • možnost sdílení tiskáren a nastavování práv na objekty adresářové služby • možnost grafického uživatelského rozhraní v češtině • možnost downgrade na nižší verzi • plná kompatibilita se stávajícími operačními systémy Microsoft Windows Server • Vlastnosti a funkce obdobné s Microsoft Windows Server 2022 Standard
Správa systému	• pro správu operačního systému požadujeme grafické nástroje s jednoduchou obsluhou.
Dokumentace	• požadujeme podrobnou technickou dokumentaci v elektronické podobě.

Produkční diskové úložiště – 1 ks

Z důvodu zvýšení výkonu, kapacity a bezpečnosti diskového subsystému požaduje dodání nového diskového úložiště.

Parametr	**Minimální požadavek**
Výrobce a model	HPE MSA 2062 16Gb FC SFF Strg
Provedení, příslušenství	• základní jednotka max. 2U - v rámci 2U musí být k dispozici základní jednotka pole (2x řadiče a napájení) a základní osazení disky • redundantní napájení dimenzované pro plný počet disků a řadiče (základní jednotka)
RAID řadiče	• 2x hot-swap diskový řadič, dual-active architektura s možností rozkládat zátěž mezi řadiči

	• podpora RAID 0, 1, 5, 6, 10 s možností libovolné kombinace
RAM – požadovaná kapacita	• každý řadič osazen min. 12GB paměti typu RAM (nikoliv SSD cache apod.)
HDD – pozice	• min. 24x 2,5" hot-plug diskových pozic v rámci základní jednotky • možnost osazení min. 120 LFF nebo 240 SFF HDD/SSD; podpora až 2PB hrubé kapacity • pole musí být rozšiřitelné pomocí expanzních polic • možnost kombinovat SSD, rotační SAS i rotační NL SAS disky, bez omezení
HDD	• 2x 1,9TB SAS 12G SSD Hot Plug jako čtecí cache • 10x 3.84TB SAS Hot Plug SFF SSD
SAN porty	• min. 8x FC16 SFP+ pro přímé (direct attach) připojení k serverům (4x na řadič), vč. osazených SFP+ modulů
Další vlastnosti	• 12Gbit/s SAS připojení disků (Backend konektivita) • battery-free zálohovaná cache se super kapacitory nebo compact flash • min. 6x LC-LC MM OM3 5m originální optický kabel (není povolen OEM kabel) • 2x dedikovaný 1000baseT management port • SSD disky musí být konfigurovatelné jako datové nebo také v režimu minimálně read akcelerátoru (cache) • disková skupina musí umožňovat rozložení přes více expanzních polic • podpora ThinProvisioning, Space Reclamation, Thin Rebuild • podpora distribuovaného RAID a hot-spare disku • automatický 3-vrstvý tiering (SSD, SAS a NL SAS tier) • podpora VAAI, LDAP • všechny softwarové funkcionality a licence bez omezení na počet serverů nebo kapacitu pole • bezel lock kit • možnost integrace diskového pole přímo do rozhraní VMware vCenter • pole musí podporovat připojení až 8 serverů v zapojení DAS • pole je v základu licencováno na plný počet připojitelných fyzických serverů • podpora asynchronní replikace přes IP a FC • min. 512 snapshotů na pole • min. 1024 volumů na pole • počet připojených hostů až 1024 • podpora diskových poolů až do velikosti 1PB

Podporované OS	• RedHat Linux, SuSe Linux, Oracle Linux, MS Windows Server 2016-2022, VMware vSphere 6, 7, 8, HP-UX
Záruka, servis	• záruka min. 5 let v režimu 24x7, on-site zahájení opravy do 4 hodin od nahlášení (nikoliv diagnostiky) • možnost automatického hlášení stavů systému do servisního střediska výrobce • jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému • servis je poskytován přímo výrobcem zařízení nebo certifikovaným servisním partnerem • servisní zásahy budou prováděny vždy v místě instalace zařízení. Nabízené zařízení musí být pokryto oficiální podporou výrobce tak, aby v případě závady, kterou není Dodavatel schopen odstranit, mohl Zadavatel tuto závadu eskalovat přímo k technické podpoře výrobce zařízení • zadavatel musí mít možnost si sám legálně stahovat bezpečnostní záplaty i nové verze Software/Firmware pro nabízené zařízení přímo ze stránek výrobce zařízení
Certifikace dodavatele, původ zboží	• Jsou splněny „Požadavky na certifikaci dodavatele HW a původ zboží“
Kompatibilita	• Servery, disková pole a pásková knihovna budou od jednoho výrobce z důvodu zajištění maximální kompatibility a jednotného servisního místa a managementu

Zálohovací diskové úložiště – 1 ks

Z důvodu zvýšení výkonu, kapacity a bezpečnosti zálohování požaduje dodání nového diskového specializovaného diskového úložiště pro ukládání záloh.

Parametr	**Minimální požadavek**
Výrobce a model	HPE StoreOnce 3660 80TB Base System
Provedení, příslušenství	• rackmount, včetně montážního kitu do standardního 19" racku • základní jednotka max. 2U v jejímž rámci musí být k dispozici základní jednotka pole a základní osazení disky redundantní napájení dimenzované pro plný počet disků a řadiče (základní jednotka)
HDD – pozice	• min. 12x 3,5" SAS 12G hot-plug diskových pozic v rámci základní jednotky
HDD	• 10x 8TB SAS 12G Hot Plug HDD

SAN/LAN porty	• 2x 10/25 Gb SFP28 LAN port připojení k backup serveru, vč. 1ks SFP28/SFP28 3m DAC kabelu (není povolen OEM kabel) • možnost rozšíření o další porty (min. 2-p 32Gb FC HBA, 2-p 10Gb Base-T)
Další vlastnosti	• možnost rozšíření až na kapacitu 270TB přidáním disků (bez započtení redukčních technologií) • možnost rozšíření až na celkových 600TB efektivní kapacity (bez započtení redukčních technologií) • ochrana disků založená na hardware komponentech v režimu RAID 6 • emulace VTL a NAS target jako CIFS • možnost provádět úplnou kopii datových sad z disku do cloud úložiště • schopnost konfigurovat v jednom zařízení alespoň jednu kombinaci 60 páskových knihoven a NAS targetů společně s minimálně 120 000 VTL cartridge sloty • podpora konfigurace až 4000 VTL slotů na každou emulovanou LTO knihovnu • umožňuje selektivní obnovu přímo ze samotné diskové knihovny • podpora deduplikace s volitelnou podporou pro replikaci do vzdálené lokality v režimu “low bandwidth”, kdy do vzdálené lokality proudí pouze unikátní data bez duplicit • podpora inteligentní formy deduplikace založené na zdroji (na úrovni aplikace klienta, backup serveru a media serveru), tak aby do zařízení kopírovaly pouze jedinečná data bez duplicit • podpora příjmu dat ze vzdáleného místa nebo pobočky bez duplicit a přímo z aplikačních serverů (klientů) v režimu nízké šířky pásma (low bandwidth), aniž by používaly backup zařízení na vzdáleném místě / pobočce • schopnost flexibilně emulovat páskové mechaniky min. formátů LTO-5, LTO-6, LTO-7 • podpora funkce šifrování dat • možnost flexibilně zapínat a vypínat funkci deduplikace na prezentované VTL knihovně CIFS share • podpora pro VLAN tagging. IP porty zařízení musí také podporovat Port bonding v režimech “Adaptive Load balancing a Active-backup • zápis minimálně 25TB/h v režimu deduplikace na zdroji • nativní podpora replikace deduplikovaných dat na virtuální diskové pole (VSA – virtual storage appliance) • nativní integrace se zálohovacím SW Veeam Backup and Replication
Záruka, servis	• min. 5 let na kompletní HW, max. odezva NBD on-site po nahlášení problému

	• možnost automatického hlášení stavů systému do servisního střediska výrobce • jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému • servis je poskytován přímo výrobcem zařízení nebo certifikovaným servisním partnerem • servisní zásahy budou prováděny vždy v místě instalace zařízení. Nabízené zařízení musí být pokryto oficiální podporou výrobce tak, aby v případě závady, kterou není Dodavatel schopen odstranit, mohl Zadavatel tuto závadu eskalovat přímo k technické podpoře výrobce zařízení • zadavatel musí mít možnost si sám legálně stahovat bezpečnostní záplaty i nové verze Software/Firmware pro nabízené zařízení přímo ze stránek výrobce zařízení
Certifikace dodavatele, původ zboží	• Jsou splněny „Požadavky na certifikaci dodavatele HW a původ zboží“
Kompatibilita	• Servery, disková pole a pásková knihovna budou od jednoho výrobce z důvodu zajištění maximální kompatibility a jednotného servisního místa a managementu.

Pásková knihovna – 1 ks

Z důvodu zvýšení výkonu, kapacity a bezpečnosti zálohování požaduje dodání páskové knihovny pro bezpečné ukládání záloh.

Parametr	**Minimální požadavek**
Výrobce a model	HPE MSL3040 Scalable Base Module
Provedení, příslušenství	• rackmount, včetně montážního kitu do standardního 19" racku • základní jednotka max. 3U • redundantní napájecí zdroje
LTO mechaniky	• 1x LTO-9 FC drive • podpora až 48 LTO mechanik • podpora mechanik FC 8Gb/s a SAS 12Gb/s • možnost kombinace FC a SAS mechanik v expanzních modulech
LTO sloty	• min. 40 slotů v základní jednotce a rozšiřujících modulech • možnost rozšíření knihovna až na 600 slotů, max. 48U
LTO média	• 40x LTO-8 páskové médium • 1x LTO čisticí médium
Další vlastnosti	• SW pro datovou verifikaci a katalogizaci pásek součástí dodávky • kryptace dat, vč. potřebného SW a HW

	• možnost rozdělení knihovny na min. 20 logických particí
Záruka, servis	• min. 5 let na kompletní HW, max. odezva NBD on-site po nahlášení problému • jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému • servis je poskytován přímo výrobcem zařízení nebo certifikovaným servisním partnerem • servisní zásahy budou prováděny vždy v místě instalace zařízení. Nabízené zařízení musí být pokryto oficiální podporou výrobce tak, aby v případě závady, kterou není Dodavatel schopen odstranit, mohl Zadavatel tuto závadu eskalovat přímo k technické podpoře výrobce zařízení • zadavatel musí mít možnost si sám legálně stahovat bezpečnostní záplaty i nové verze Software/Firmware pro nabízené zařízení přímo ze stránek výrobce zařízení
Certifikace dodavatele, původ zboží	• Jsou splněny „Požadavky na certifikaci dodavatele HW a původ zboží“
Kompatibilita	• Servery, disková pole a pásková knihovna budou od jednoho výrobce z důvodu zajištění maximální kompatibility a jednotného servisního místa a managementu

Zálohování a obnova dat

Vzhledem k nutnosti zálohování nových i stávajících serverů, dat a aplikací požadujeme dodání moderního a bezpečného zálohovacího SW.

Parametr	**Minimální požadavek**
Výrobce, název, verze a licenční program	Veeam Veeam Pub Avail Univ Perp 1yr 24x7 E-LTU Veeam Avail Univ Perp Add 4yr 24x7 Sup
Požadované vlastnosti	• licence zálohovacího software pokrývající min. 2 fyzické servery, resp. 4 CPU sockety bez omezení počtu zálohovaných virtuálních serverů a objemu dat • integrované technologie komprimace a deduplikace pro efektivní ukládání dat • bezagentové řešení – bez nutnosti instalace agentů do zálohovaných virtuálních serverů či aplikací • možnost replikace virtuálních strojů na jiný virtualizační nod za chodu serveru • integrované řízení přechodu provozu na replikované servery (fail-over) a zpět (fail-back) včetně automatických zpětných dosynchronizací

	• provádění datově konzistentních záloh hlavních serverových aplikací – Microsoft SQL server, Active Directory, souborové systémy – bez nutnosti odstávky aplikace • automatické ověřování integrity zálohy spuštěním zálohovaného serveru přímo ze zálohy v izolovaném prostředí • podpora plnohodnotné replikace přes WAN pro replikaci virtuálních serverů do vzdálených lokalit • možnost využívání snapshotů, zálohování pouze dat změněných od poslední úspěšné zálohy • podpora operačních systémů Windows a Linux v zálohovaných virtuálních serverech • možnost ukládání záloh na diskový prostor, síťové úložiště a páskovou jednotku/knihovnu • podpora pro hypervizory vSphere, Hyper-V a AHV • zálohování na úrovni bitových kopií s plnou podporou aplikačně konzistentních snapshotů • podpora DR (disaster recovery). Možnost nouzového spuštění virtuálního serveru ze souboru zálohy bez nutnosti obnovy • vytváření a správa úloh (zálohování, obnova apod.) pomocí průvodců • zálohování NAS, podpora protokolů SMB a NFS • nativní zálohování a obnova AWS instancí vč. možnosti zálohování do služby Amazon S3 • nativní integrace objektových úložišť a on-line úložišť AWS, MS Azure, IBM Cloud, S3 • nativní podpora a integrace zálohování ze snapshotů primárních datových úložišť • možnost spuštění jednoho nebo více virtuálních počítačů přímo ze zálohy v izolovaném prostředí, tzv. sandboxing • automatický reporting úspěšných i neúspěšných úloh • běžné úlohy obnovy (obnovení souboru, databáze SQL, objekty Active Directory) provádět pomocí průvodců i na úrovni jednotlivých objektů (např. jeden účet Active Directory, jeden soubor apod.) přímo do původního umístění • integrované zálohování fyzických počítačů (klíčových pracovních stanic) a serverů s operačními systémy Windows a Linux. Bez omezení počtu zálohovaných systémů a objemu záloh. Pro tuto funkci je přípustné použití agentů
Podpora	• platnost licence min. 60 měsíců, včetně nároku na opravné a nové verze software, vč. technické podpory výrobce