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

Čl. 1 Smluvní strany

Kupující:	**Město Jindřichův Hradec**
Sídlo:	Klášterská 135/II, 377 01 Jindřichův Hradec
IČ:	00246875
DIČ:	CZ00246875
Zastoupený:	Mgr. Ing. Michal Kozár, MBA, starosta města
Kontaktní osoba:	Ivo Šicner, vedoucí oddělení informatiky a VT, email: [redacted], tel: +420 [redacted]
Bankovní spojení:	[redacted]
Číslo účtu:	[redacted]

jako kupující, na straně jedné

(dále jen kupující)

a

Prodávající:	**Aricoma Systems a. s.**
Sídlo:	Hornopolní 3322/34, 702 00, Ostrava
IČ:	04308697
DIČ:	CZ04308697
Zastoupený/Jednající:	Jaroslav Dvořák, člen představenstva
Kontaktní osoba:	Ladislav Kocour, ředitel regionálního centra
Bankovní spojení:	[redacted]
Číslo účtu:	[redacted]
Zápis v OR:	vedeném u rejstříkového soudu v Ostravě, spisová značka B 11012

jako prodávající na straně druhé

(dále jen prodávající)

Čl. 2 Úvodní ustanovení

2.1. Tato smlouva je uzavírána v návaznosti na veřejnou zakázku s názvem „Dodávka IT infrastruktury a licencí pro zvýšení kybernetické bezpečnosti“, zadávanou kupujícím jakožto zadavatelem, a bude realizována jako součást projektu „Zvýšení kybernetické bezpečnosti města Jindřichův Hradec“, reg. č.: CZ.31.2.0/0.0/0.0/23_093/0008708.

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

Čl. 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, 2 a 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.

Čl. 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 2 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.

Čl. 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,
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.

Čl. 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 Čl. 4 této smlouvy kupní cenu ve výši

12 362 280,00 Kč bez DPH,

tj. 14 958 358,80 Kč včetně DPH,

když DPH ve výši 21% činí 2 596 078,80 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 registrační číslo a název projektu „CZ.31.2.0/0.0/0.0/23_093/0008708 – Zvýšení kybernetické bezpečnosti města Jindřichův Hradec“, a doklad musí zároveň obsahovat informaci, že se jedná o projekt financovaný z NPO.

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.

Čl. 7 Předání a převzetí věci a vlastnické právo

7.1. Prodávající předá kupujícímu předmět plnění této smlouvy do 3 měsíců dnů od nabytí účinnosti této smlouvy, a to včetně realizace všech souvisejících služeb.

7.2. Místem dodání a předání předmětu plnění této smlouvy jsou technologické místnosti kupujícího na adresách:

- Lokalita A – MěÚ Klášterská 135 (hlavní budova),
- Lokalita B – MěÚ Masarykovo nám. 168,
- Lokalita C – MěÚ Janderova 147,
- Lokalita D – KDS Masarykovo nám. 107,
- Lokalita E – Infocentrum Panská 136,
- Lokalita F – Stará radnice nám. Míru 88 (výstavní dům).

Před dodávkou zařízení je prodávající povinen vyzvat kontaktní osobu kupujícího k potvrzení rozdělení jednotlivých dodávek mezi výše uvedené technologické místnosti.

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.

7.7. Pokud prodávající předmět plnění nedoručí vlastními prostředky, ale využije k tomu dopravce, považuje se za odevzdání věci kupujícímu až okamžik doručení takovým dopravcem. Ustanovení § 2090 a § 2091 zákona č. 89/2012 Sb., občanského zákoníku, se nepoužijí.

Čl. 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.

Čl. 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:

- Vedoucí realizačního týmu (projektový manažer) – [redacted]
- Bezpečnostní analytik – [redacted]
- Síťový specialista – [redacted]

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.).

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

10.4. 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.

10.5. Prodávající se zavazuje poskytnout součinnosti při změnách projektu, a to v době jeho udržitelnosti, která je 5 let od ukončení doby realizace projektu. Prodávající bere na vědomí, že jakékoli změny v předmětu smlouvy, termínech dodávky či jiných klíčových parametrech musí být předem schváleny poskytovatelem dotace. Bez tohoto souhlasu není kupující oprávněn provádět žádné změny, které by mohly ovlivnit financování projektu.

10.6. Kupující při své činnosti postupuje v souladu s cíli a zásadami udržitelného rozvoje a zásadou „významně nepoškozovat“ (DNSH), tedy nepodporovat nebo nevykonávat hospodářské činnosti, které významně poškozují kterýkoli environmentální cíl. Prodávající se touto Smlouvou zavazuje předcházet vzniku odpadů, a to zejména v oblastech zpětného odběru elektroodpadu, rozebírání výrobků na části dle druhu materiálu, a vytvářet minimální produkce obalů.

Čl. 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.

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 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 vady provedené implementační práce se prodávající zavazuje odstranit závadu do 14 kalendářních dnů ode dne nahlášení vady kupujícím.

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 a ve lhůtách dle přílohy č. 1.

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.

Čl. 12 Smluvní pokuty

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

12.2. Pro případ prodlení prodávajícího s dodávkou předmětu plnění této smlouvy v rozsahu a termínech uvedených v této smlouvě se stanovuje smluvní pokuta ve výši 0,1 % z kupní ceny bez DPH za každý den prodlení.

12.3. 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.

12.4. V případě prodlení prodávajícího s odstraněním nahlášené závady na příslušenství se stanovuje smluvní pokuta ve výši 200,- Kč za každý celý kalendářní týden prodlení.

12.5. V případě prodlení prodávajícího s odstraněním nahlášené závady v podobě provedených implementačních a konfiguračních prací dle čl. 11.4 se stanovuje smluvní pokuta ve výši 500,- Kč za každý celý pracovní den prodlení.

12.6. 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.

12.7. 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.

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

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

Čl. 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.

Čl. 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.

Čl. 15 Závěrečná ustanovení

15.1. Tato smlouva je vyhotovena v elektronickém originále, jež po podpisu druhou ze smluvních stran obdrží obě smluvní strany.

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. Přílohami této smlouvy jsou:

- Příloha č. 1 – Technická specifikace zadavatele (kupujícího)
- Příloha č. 2 – Technická specifikace účastníka zadávacího řízení (prodávajícího) z jeho vítězné nabídky
- Příloha č. 3 – Cenová tabulka z nabídky prodávajícího

15.5. 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).

15.6. 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.

15.7. 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.

15.8. Znění této smlouvy je v souladu s návrhem zadání veřejné zakázky schváleným usnesením Rady města Jindřichův Hradec č. 124/5R/2025 ze dne 12. 2. 2025. Zadání zakázky a uzavření kupní smlouvy bylo schváleno usnesením Rady města Jindřichův Hradec č. 492/18R/2025 ze dne 11. 6. 2025.

Za kupujícího	**Za prodávajícího**
V Jindřichově Hradci dne ……	V Českých Budějovicích dne……..
……	……
Mgr. Ing. Michal Kozár, MBA	**Jaroslav Dvořák**
starosta města	člen představenstva

Příloha č. 1 smlouvy – Technická specifikace zadavatele (kupujícího)

Technická dokumentace

Dodávka IT infrastruktury a licencí pro zvýšení kybernetické bezpečnosti

Verze 07 ze dne 04.04.2025

Obsah dokumentu – Příloha č.1 – Technická specifikace zadavatele

1. Technická specifikace zadavatele (kupujícího)

Zadavatel požaduje dodávku jednotlivých komponent dle této technické dokumentace včetně příslušenství v níže uvedené minimální specifikaci.

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

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 agendových informačních systémů nad touto platformou vybudovaných a provozovaných, které předmětnou infrastrukturu užívají a slouží k výkonu veřejné správy zadavatele.

Propojení zařízení – SFP moduly a kabely

Všechny dodané technologie musejí být v rámci dodávky propojeny odpovídajícím způsobem a technologií, tedy zejména pro všechny síťové karty jednotlivých zařízení musejí být dodány i SFP a obdobné moduly a kabely do serverovny kupujícího, které takové propojení v kvalitě požadované u každého ze zařízení umožní. V případě 10Gbit karet musí být dodány SFP prvky a kabely umožňující využití této maximální rychlosti karty, v případě jiných rychlostí toto pravidlo musí být dodrženo stejně.

Plnění jednotlivých komponent dle specifikace níže je požadováno v následujícím rozsahu, a to včetně příslušenství:

Položka plnění	Počet kusů
Virtualizační server s příslušenstvím	2
Licence OS serverů pro pokrytí pořizovaných virtualizačních serverů	2
Licence SW pro virtualizaci	1
Záložní zdroj s příslušenstvím	1
NG firewall s příslušenstvím	2
Core přepínače s příslušenstvím pro propojení primární a záložní lokality	4
Přístupové přepínače typ 48 p s příslušenstvím	7
Přístupové přepínače typ 24 p s příslušenstvím	12
Licence Anti-X řešení včetně EDR	260
SW pro provozní dohled nad IT prostředím	1
SW pro dvoufaktorovou autentizaci a správu karet	1
Hybridní čipová karta	200
Čtečka čipových karet	200
Licence SW Single SignOn	1

1.1. Virtualizační server s příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Základní a výkonové požadavky	Typ zařízení: - server v provedení k instalaci do 19" racku, maximálně 2U. - server s rackmount příslušenstvím včetně pohyblivého ramene pro zachycení kabeláže.
	CPU architektura x86 max. 16 plnohodnotných jader. V testu na cpubenchmark.net minimálně 36 000 bodů. Max. počet CPU je omezen na 1 a počet jader je omezen na 16 core z důvodu licencování OS a aplikací.
	Paměť: - 256GB, typu DDR5 s taktem 5600MT/s, Dual Rank - počet paměťových modulů a rozmístění musí být zvoleno pro optimální výkon s CPU - možnost zvýšení kapacity na dvojnásobek, 512GB při použití identických modulů, bez nutnosti výměny dodaných
	OS Boot: - musí být zajištěn dvojicí disků v RAID1 a kapacitou min. 480GB, nesmí se jednat o rotační disky
	LAN konektivita - min. 1 ks Ethernet adapter Dual Port 10/25GbE Adapter včetně 2 ks MM zářičů 10GE SFP+ včetně 2m kabelů LC/LC-LC/LC. - min. 1ks Ethernet adapter 2× 1GbE 1000BASE-T
	Dodávka zahrnuje 1× 2portové FC karty pro připojení do SAN sítě.
	Napájení a chlazení - server musí být vybaven redundantním napájením a chlazením, hot-plug vyměnitelné za provozu - 2ks hot-swap zdroje napájení dimenzované pro plné osazení serveru disky, CPU, RAM a PCIe zařízení, musí splňovat požadavky na certifikaci energetické účinnosti Platinum dle 80 PLUS (https://cs.wikipedia.org/wiki/80_Plus) nebo lepší; případně na stejné nebo vyšší úrovni účinnosti podle jiné certifikace
Funkční požadavky	Server musí být osazen TPM 2.0
	Vyčítání přes SNMP celkového zdraví serveru bez nutnosti instalovat OS – jeden parametr v MIB
	IPMI 2.0 popř. obdoba, možnost vzdáleného převzetí grafické konsole bez závislosti na OS, webový klient HTML5, vzdálený mount DVD media, USB, dedikovaný port (není součástí požadovaného počtu ethernet portů)
	Kompatibilita s VMWARE LifeCycle manager – z důvodu potřeby zajištění kompatibility se stávající virtualizační platformou zadavatele
	Kompatibilita všech komponent s OS VMWARE ESXi 8.x (stávající virtualizační platformou zadavatele)
Záruka, záruční servis a technická podpora	Je požadována záruka a záruční servis na dobu 5 let s reakční dobou na založený incident do konce následujícího pracovního dne (NBD).

Parametr	Popis minimální úrovně parametru
	Servisní zásahy provádí technik s příslušnou znalostí (technik výrobce nebo jeho autorizovaného zastoupení).
	Aktualizace systému budou dostupné min. po dobu záruky a záručního servisu zdarma, nabízené přehledně v servisním portálu po zadání sériového čísla.

1.2. Licence OS serverů pro pokrytí pořizovaných virtualizačních serverů

Je požadována dodávka následujících licencí:

Počet	Typ licence
V počtu k pokrytí všech jader procesorů virtualizačních serverů v rámci plnění této specifikace (zadavatel předpokládá 32 jader nebo méně)	Microsoft Windows Server Datacenter 2022 v rozsahu k pokrytí dodaných procesorových core v každém produkčním serveru dle této specifikace.
- V případě dodávky licencí produktů společnosti Microsoft jsou požadovány licence, jejichž pravost je garantovaná a ověřitelná u vlastníka autorských práv Microsoft. - V případě dodávky licencí produktů společnosti Microsoft účastník 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 kupujícího. - V případě dodávky licencí produktů společnosti Microsoft se vyžaduje dodání licencí formou licenčního portálu vázaného na koncového zákazníka (kupujícího), jehož součástí budou: o seznam nabízených licencí a jejich počet, o instalační médium, o instalační klíče, o 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.	

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.

1.3. Licence SW pro virtualizaci

Počet	Typ licence
V počtu k pokrytí všech jader procesorů virtualizačních serverů v rámci plnění této specifikace (zadavatel předpokládá 32 jader nebo méně)	VMware vSphere Standard, per Core
- Pro dodávané virtualizační servery je požadována dodávka virtualizačního software (hypervisoru) VMware vSphere kompatibilního se stávajícím serverovým virtualizačním prostředím VMware kupujícího k licenčnímu pokrytí všech serverů, které jsou součástí tohoto plnění.	

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.

1.4. Záložní zdroj s příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Základní specifikace	Záložní zdroj napájení (UPS)
	Pro montáž do 19" rozvaděče, výška maximálně 2U
	Maximální hloubka 70 cm
	Typ použitých baterií – bezúdržbové, hermeticky uzavřené, ventilem řízené olověné baterie
Výkonová a funkční specifikace	Parametry vstupního napětí – 230 V, 50/60 Hz +/- 3 Hz (autodetekce)
	Parametry výstupního napětí – 220/230/240 V (volitelné), 50 Hz/60 Hz (volitelné)
	Max. nastavitelný výkon 2 700 W
	Doba provozu při plné zátěži min. 3 minuty
	Jmenovitý výkon 3 000 VA
	Topologie – Line Interactive
	Výstupní přípojky: min. 1× IEC 320 C19, min. 8× IEC 320 C13
	Vstupní přípojky: min. 1× IEC 320 C20
	Přední ovládací panel s LCD, s akustickým a vizuálním varováním
	Licence management software pro bezpečné vypnutí virtuálních serverů pro 2 pořizované ESX servery a dále pro stávající ESX4 a ESX5 *(již provozované v prostředí zadavatele).*
	Vzdálená správa a dohled pomocí síťové komunikace (požadavek na min. 10/100 Mbit síťový RJ45 konektor)
	Podpora protokolů HTTPS, SSH, SNMPv2c a SNMPv3
Záruka a záruční servis	Záruka na UPS s výjimkou baterie min. 60 měsíců, včetně podpory pro firmware síťové karty a požadovaného SW.
	Záruka na baterie min. 24 měsíců.

1.5. NG Firewall s příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Základní specifikace	HW appliance (VM appliance ani software řešení není akceptovatelné)
	Podpora režimu vysoké dostupnosti minimálně jako Active/Active a Active/Passive, cluster o dvou fyzických zařízeních
	Velikost 1RU
	Podpora duálního napájení (redundantní zdroj)
	Minimálně 4× 10 GbE SFP+ sítová rozhraní
	Minimálně 8× GE SFP síťová rozhraní
	Minimálně 18× 1 GbE RJ45 síťová rozhraní
	Management rozhraní 1× 1 GbE RJ45 a sériový konzolový port
Výkonové požadavky	Minimální propustnost firewallu pro IPv4 i IPv6 provoz 25Gbps (měřeno na UDP komunikaci o paketech s velikostí 512 B)
	Počet současně navázaných spojení firewallu min. 3 000 000, počet nových spojení za sekundu min. 250 000
	Celková propustnost IPSEC VPN min. 12Gbps
	Propustnost SSL VPN min. 2Gbps
	Propustnost funkce SSL inspekce min. 4Gbps
	Počet CPS u spojení kontrolovaných pomocí SSL inspekce min. 1500 (spojení za sekundu)
	Propustnost funkce IPS min. 5 Gbps (reálná hodnota, měřeno na běžném provozu – real world traffic, včetně logování)
	Propustnost funkcí next generation firewallingu (stavový firewall, IPS, analýza aplikací) min. 3,5Gbps (reálná hodnota, měřeno na běžném provozu – real world traffic)
	Propustnost funkcí ochrany před hrozbami (stavový firewall, IPS, analýza aplikací, ochrana před škodlivým kódem) min. 3Gbps (reálná hodnota, měřeno na běžném provozu – real world traffic)
	Udávaná latence firewallu (udp provoz) max. 5 µs
	Min. počet současně připojených uživatelů SSL VPN 500
	Min. počet site-to-site IPSEC tunelů 16000
Funkční požadavky	Grafické konfigurační rozhraní (např. webový prohlížeč) a příkazový řádek bez omezení na počet administrátorů
	Bezpečnostní funkce obecně označovaných jako Next Generation Firewall
	Podpora virtualizace na daném HW, vytváření a provozování tzv. virtuálních kontextů – min. 10 virtuálních kontextů v ceně zařízení; každý virtuální kontext musí pracovat izolovaně, možnost propojovat jednotlivé virtuální kontext pomocí interní virtuálních propojů bez nutnosti použití fyzických interface
	Podpora stavového firewallingu pro IPv4 i IPv6, podpora NAT 64/46

Příloha č. 1 – Technická specifikace zadavatele (kupujícího)

Parametr	Popis minimální úrovně parametru
	Možnost nasazení ve všech z následujících režimů (kombinace možné pomocí použití různých režimů pro různé virtuální kontexty): L2 bridge režim (inline), L3 router/NAT režim (inline), explicitní proxy (inline/out of path), transparentní proxy (inline)
	Plnohodnotná správa z lokálního management rozhraní (a to i v případě využití nástroje centrální správy, neboť i v takovém případě musí být možné firewall, resp. firewall cluster, plnohodnotně konfigurovat ve chvíli, kdy z jakéhokoliv důvodu centrální správy bude nedostupná)
	Ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, RADIUS, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign-On
	Podpora lokální databáze a vzdálené databáze (RADIUS, LDAP, TACACS+, SAML, Kerberos) pro ověřování uživatelů
	Ověřování uživatelů pomocí SSO funkcionality pomocí RADIUS Single Sign-On a AD pollingu
	Funkce QoS, traffic shaping a SD-WAN minimálně v režimu vytvoření overlay a underlay virtuálních sítových rozhraní zahrnující fyzické propoje, IPSEC tunely či jiná rozhraní s možností definice pravidel pro řízení směrování, strategie využívání jednotlivých linek současně a monitorování stavu jednotlivých linek
	Podpora funkcí VPN brány – IPSec VPN (dle platných standardů pro možnost propojení se zařízeními třetích stran); - SSL VPN pro klientský přístup s tunelovacím režimem včetně klienta pro osobní počítače i mobilní platformy, portálový režim pro bezklientský přístup
	VPN klient pro neomezený počet přistupujících zařízení součástí nabídky
	Podpora funkce SSL inspekce (MITM) včetně podpory TLS 1.3
	Antivirový engine musí být vybaven lokální databází vzorků škodlivého kódu a AI/ML enginem pro identifikaci podezřelých či neznámých vzorků
	Funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, podpora rozpoznávání škodlivého kódu určeného pro mobilní zařízení (tzv. mobile malware), detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak), podpora sanitarizace aktivního obsahu běžných kancelářských dokumentů (odstranění např. skriptů či maker z dokumentu, extrakce obsahu dokumentu do neškodné podoby); podpora napojení na sandboxovací funkce včetně funkce akceptace lokálních signaturových databází generovaných sandboxem, vše bez nutnosti instalace pluginů do prohlížeče.
	Funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora min. 4000 aplikací, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace
	Možnost definice zakázaných slov pro vyhledávání na internetu
	Podpora funkce safe search pro populární vyhledavače
	Funkce kategorizace webových stránek (web filtering) s podporou minimálně 60 kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), podpora definice časové kvóty, kterou nesmí daný uživatel na dané kategorii za den překročit, výrobcem aktualizovaná a udržovaná databáze, vynikající pokrytí českého internetu; požadované akce – povolení stránky, logování stránky, brouzdání s proklikem, nutnost autentizace uživatele pro určitou kategorii, možnost definice časových kvót pro uživatele a kategorie webu

Příloha č. 1 – Technická specifikace zadavatele (kupujícího)

Parametr	Popis minimální úrovně parametru
	Podpora kategorizace streamovaných videí a kanálů min. pro platformu Youtube a Vimeo
	Funkce ochrany před sítovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možností definovat různé profily na různý druh komunikace, možnost vytvářet vlastní signatury, integrovaný anomální filtr a mechanismus kontroly validity vybraných protokolů
	Možnost blokovat sítový provoz na základě URL, kategorie webové stránky, IP adresy (rozsahu), GeoIP databáze, data a času
	Funkce ochrany před unikem citlivých dat (Data Leak Prevention), která umí zachytit pokus o odeslaní/upload označeného dokumentu přes internet na základě vodoznaků, popisu regulárním výrazem atp.
	Podpora dvoufaktorové autentizace pomocí HW nebo mobilních OTP tokenů, součástí dodávky musí být jako príslušenství 2 ks HW/mobilní tokeny a plně funkční řešení dvoufaktorového OTP ověřování uživatelů pro administrátory a uživatele VPN
	Obousměrná integrace (min. ve smyslu sdílení informací o odhalených hrozbách a provozně/telemetrický informací) nabízeného firewallu s dalšími instalovanými bezpečnostní prvky (mailová brána, sandbox, nástroj pro sběr a vyhodnocování logů, nástroj pro centrální správu)
	Podpora režimu nasazení v režimu WCCP (WCCP v2)
	Podpora konfiguračních PAC souborů pro režim nasazení explicitní proxy
	Podpora ICAP rozhraní pro obousměrnou integraci s externími servery
	Podpora tunelování provozu pomocí technologie GRE
	Podpora automaticky aktivovaného bypass režimu v případě přetížení systému a jeho inspekčních funkcí
	Analýza a zabezpečení DNS dotazů (ochrana před DNS poisoningem), filtrování DNS dotazů na základě kategorizace
	Možnost filtrovat Java applety, ActiveX prvky, Cookie soubory ve webovém provozu
	Integrovaná funkce load balancingu (reverzní proxy) s podporou základní algoritmů pro rozklad zátěže (round robin, váhování, nejkratší odezva, nejmenší počet aktivních spojení) s detekcí stavu reálných serverů na pozadí, podpora funkce ssl offloading a ssl inspekce pro rozkládaný provoz
Príslušenství – kabely a transceivery	Požadujeme dodání 2 ks SFP+ MM (300 m), včetně 2m kabelů LC/LC-LC/LC.
Záruka, záruční servis a technická podpora	Záruka 60 měsíců, servisní zásah následující pracovní den od nahlášení závady, v místě instalace. Servis je poskytován výrobcem firewallu.
	Technická podpora výrobce v délce 60 měsíců spočívající zejména v nároku na aktualizační balíčky zranitelností, opravné balíčky a patche, podpora bude uhrazena současně s dodávkou.

1.6. Core přepínače s příslušenstvím pro propojení primární a záložní lokality

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Základní požadavky	Třída zařízení: L3 switch, podpora provozu jako ToR
	Formát zařízení do racku
	Velikost zařízení: max. 1U
	min. 24× SFP/SFP+ 100M/1/10G portů s volitelným fyzickým rozhraním
	min. 4× SFP/SFP+/SFP28/SFP56 1/10/25/50G portů s volitelným fyzickým rozhraním
	Chlazení typu Front-to-Back
	Všechny ethernet porty jsou dostupné zepředu
Výkonové požadavky	Celková propustnost přepínače min. 880 Gb/s
	Celkový paketový výkon přepínače min. 650 Mpps
	Propustnost stohovacího propojení min. 200 Gbps
	Minimálně 8 MB paketový buffer
	2× Hot-Swap zdroje min. 250 W
Funkční požadavky	Podpora "jumbo rámců" včetně velikosti min. 9198 Byte
	Podpora linkové agregace IEEE 802.3AX
	Konfigurovatelné rozkládání LACP zátěže podle L2, L3
	Počet LACP skupin/linek ve skupině - min. 256/8
	Počet záznamů v tabulce MAC adres - min. 29 000
	Počet záznamů v tabulce ARP – min. 28 000
	Protokol pro definici šířených VLAN – MVRP
	Podpora VLAN podle IEEE 802.1Q, minimálně 4 000 aktivních VLAN
	VLAN translace – swap 802.1Q tagů na trunk portu
	Podpora zařazování do VLAN podle standardu 802.1v
	IEEE 802.1s – Multiple Spanning Tree
	STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)
	Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED
	Detekce jednosměrnosti optické linky (např. UDLD)
	DHCP server
	DHCP relay pro IPv4 a IPv6
	Podpora NTPv4 pro IPv4 a IPv6 včetně VRF a MD5 autentizace
	Statické směrování IPv4 a IPv6
	Počet záznamů ve směrovací tabulce min. 64 000
	Dynamické směrování OSPFv2, OSPFv3 a BGP včetně podpory BFD

Parametr	Popis minimální úrovně parametru
	Podpora BGP a MP-BGP včetně podpory BFD
	Podpora Layer-3 routed port
	IGMP v2 a v3
	MLD v1 a v2
	Hardware podpora IPv4 a IPv6 ACL
	ACL definice na základě skupiny fyzických portů
	ACL aplikovatelný na interface, LAG, VLAN
	BPDU a Root guard
	DHCP snooping pro IPv4 a IPv6
	HW ochrana proti zahlcení portu (broadcast/multicast/icmp) nastavitelná na kbps a pps
	802.1x ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port
	Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)
	Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675
	Podpora Critical VLAN
	Podpora uživatelských rolí definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely.
	Uživatelské role mohou být lokálně definované v přepínači nebo mohou být dynamicky stáhnuty z RADIUS serveru na základě výsledku autorizace.
	Podpora IPv6 RA Guard
	IP source guard / dynamic IP lockdown
	Podpora Dynamic ARP protection
	Port security
	Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU
	Podpora IPv4 a IPv6 QoS
	IEEE 802.1p – minimální počet front - 8
Management	CLI formou RJ45 serial konsole port
	Konfigurace zařízení v člověku čitelné textové formě
	OoB management formou portu RJ45 s podporou ethernetu
	USB port pro přenos konfigurace a firmware
	Podpora SSHv2, SFTP a HTTPS pro IPv4 a IPv6
	Podpora RSA s délkou klíče minimálně 4096 bitů
	Podpora grafického uživatelského webového rozhraní. Možnost vytváření vlastních diagnostických a korelačních skriptů a jejich grafických interpretací v jazyce Python (korelace libovolných událostí a hodnot v podobě grafů)

Parametr	Popis minimální úrovně parametru
	Podpora SNMPv2c a SNMPv3
	Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
	TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)
	SPAN a ERSPAN port mirroring, alespoň 4 různé obousměrné session
	TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více SYSLOG serverů
	Podpora automatických i manuálních snapshotů systému a možnost automatického obnovení předchozí konfigurace v případě konfigurační chyby
	Podpora standardního Linux Shellu (BASH) pro debugging a skriptování
	Podpora skriptování v jazyce Python – lokální interpret jazyka v přepínači
	Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní)
	Interpretace uživatelských skriptů monitorujících definované parametry síťového provozu s možností automatické reakce na události
	Interní SSD úložiště pro sběr provozních dat a pokročilou diagnostiku zařízení
	Podpora OVSDB
	Analýza síťového provozu sFlow podle RFC 3176
	Ochrana proti nahrání modifikovaného SW prostřednictvím image signing a secure boot, ověřující autentičnost a integritu OS prostřednictvím TPM chipu
	Podpora integrace s automatizačními nástroji (Ansible, NAPALM)
	Podpora REST API v režimech read-only a read-write pro automatizaci nastavení
Příslušenství – kabely a transceivery	Požadujeme dodání 1 ks SFP56 DAC kabel 0,65m, 15 ks SFP+ SM, 8 ks SFP+ MM.
Záruka a záruční servis	Záruka a záruční servis v délce 60 měsíců, odstranění závady nejpozději do 2 pracovních dní (servis je poskytován výrobcem nebo autorizovaným zastoupením), oprava v místě instalace.

1.7. Přístupové přepínače typ 48p s příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Základní a výkonnostní specifikace	Třída zařízení: L2+ switch
	Formát zařízení do racku
	Velikost zařízení: 1U
	min. 48× 10/100/1000Mbit metalických portů
	min. 4× 10Gbit/s SFP+ nezávislých optických portů s volitelným fyzickým rozhraním
	10GE interface zpětně kompatibilní s 1Gbit/s transceivery
	Všechny ethernet porty jsou dostupné zepředu
	Interní napájecí zdroj

	Podpora PoE+ dle standardu 802.3at
	Dostupný výkon pro PoE+ napájení 370 W
	Podpora Energy Efficient Ethernet (802.3az)
	Celková propustnost přepínače 176 Gb/s
	Celkový paketový výkon přepínače 98 Mpps
	Minimálně 12 MB paketový buffer
	Maximální přípustná hloubka přepínače 33 cm
Základní funkce a protokoly	Podpora "jumbo rámců" včetně velikosti 9220 Byte
	Podpora linkové agregace IEEE 802.3ad
	Konfigurovatelné rozkládání LACP zátěže podle L3 a L4
	Minimální počet LACP skupin/linek ve skupině: 8/8
	Protokol pro definici šířených VLAN: MVRP
	Podpora VLAN podle IEEE 802.1Q, minimálně 512 aktivních VLAN
	IEEE 802.1s – Multiple Spanning Tree
	STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)
	Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED
	Detekce jednosměrnosti optické linky (např. UDLD)
	NTP pro IPv4 a IPv6 včetně MD5 autentizace
	Statické směrování IPv4 a IPv6
	IGMP v2 a v3
	MLD v1 a v2
	Hardware podpora IPv4 a IPv6 ACL
	ACL definice na základě skupiny fyzických portů
	ACL aplikovatelný na rozhraní IN včetně virtuálních VLAN
	BPDU guard a Root guard
	HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na množství paketů za vteřinu
	ICMPv4 a ICMPv6 rate-limiting per port
	Ověřování 802.1X včetně více uživatelů na port, minimálně 32 uživatelů/port
	Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)
	802.1X s podporou odlišných Preauth VLAN, Fail VLAN a Critical VLAN
	Dynamické zařazování do VLAN
	802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení)
	Port security – omezení počtu MAC adres na port, statické MAC

	Ochrana proti opakovaným výpadkům linek (flapování) s možností konfigurace citlivosti a akce při překročení
	Ochrana control plane (CPU) před útoky typu DoS
	Podpora IPv4 a IPv6 QoS
	Minimálně 8 front pro IEEE 802.1p
Management	CLI formou 1× USB-C Console Port
	Konfigurace zařízení v člověku čitelné textové formě
	Podpora automatických i manuálních snapshotů konfigurace systému
	USB port pro diagnostiku, přenos konfigurace a firmware
	Podpora managementu přes IPv4 i IPv6
	SSHv2 a a SFTP
	Podpora SNMPv2c a SNMPv3
	RMON
	Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
	Lokálně vynucené RBAC na úrovni přepínače
	Dualní flash image
	TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů
	Podpora Syslog over TLS
	Podpora RADIUS včetně RADIUS CoA (RFC3576)
	Podpora RADIUS IPSEC
	Aktivní monitoring dostupnosti RADIUS přednastaveným jménem a heslem
	Podpora TACACS+
	Analýza síťového provozu sFlow podle RFC 3176
	Port mirroring (SPAN), alespoň 4 různé obousměrné session
	Podpora Zero Touch Provisioning (ZTP)
	REST API pro automatizaci nastavení
	Automatická konfigurace portu podle připojeného zařízení
	Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů
Záruka a záruční servis	Záruka a záruční servis v délce 60 měsíců, odstranění závady nejpozději do 2 pracovních dní (servis je poskytován výrobcem nebo autorizovaným zastoupením), oprava v místě instalace.

1.8. Přístupové přepínače typ 24p s příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Základní a výkonnostní specifikace	Třída zařízení: L2+ switch
	Formát zařízení do racku
	Velikost zařízení: 1U
	min. 24× 10/100/1000Mbit metalických portů
	min. 4× 10Gbit/s SFP+ nezávislých optických portů s volitelným fyzickým rozhraním
	10GE interface zpětně kompatibilní s 1Gbit/s transceivery
	Všechny ethernet porty jsou dostupné zepředu
	Interní napájecí zdroj
	Podpora PoE+ dle standardu 802.3at
	Dostupný výkon pro PoE+ napájení 370 W
	Podpora Energy Efficient Ethernet (802.3az)
	Celková propustnost přepínače 128 Gb/s
	Celkový paketový výkon přepínače 95 Mpps
	Minimálně 12 MB paketový buffer
	Maximální přípustná hloubka přepínače 33 cm
Základní funkce a protokoly	Podpora "jumbo rámců" včetně velikosti 9220 Byte
	Podpora linkové agregace IEEE 802.3ad
	Konfigurovatelné rozkládání LACP zátěže podle L3 a L4
	Minimální počet LACP skupin/linek ve skupině: 8/8
	Protokol pro definici šířených VLAN: MVRP
	Podpora VLAN podle IEEE 802.1Q, minimálně 512 aktivních VLAN
	IEEE 802.1s – Multiple Spanning Tree
	STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)
	Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED
	Detekce jednosměrnosti optické linky (např. UDLD)
	NTP pro IPv4 a IPv6 včetně MD5 autentizace
	Statické směrování IPv4 a IPv6
	IGMP v2 a v3
	MLD v1 a v2
	Hardware podpora IPv4 a IPv6 ACL
	ACL definice na základě skupiny fyzických portů
	ACL aplikovatelný na rozhraní IN včetně virtuálních VLAN

	BPDU guard a Root guard
	HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na množství paketů za vteřinu
	ICMPv4 a ICMPv6 rate-limiting per port
	Ověřování 802.1X včetně více uživatelů na port, minimálně 32 uživatelů/port
	Konfiguovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)
	802.1X s podporou odlišných Preauth VLAN, Fail VLAN a Critical VLAN
	Dynamické zařazování do VLAN
	802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení)
	Port security – omezení počtu MAC adres na port, statické MAC
	Ochrana proti opakovaným výpadkům linek (flapování) s možností konfigurace citlivosti a akce při překročení
	Ochrana control plane (CPU) před útoky typu DoS
	Podpora IPv4 a IPv6 QoS
	Minimálně 8 front pro IEEE 802.1p
Management	CLI formou 1× USB-C Console Port
	Konfigurace zařízení v člověku čitelné textové formě
	Podpora automatických i manuálních snapshotů konfigurace systému
	USB port pro diagnostiku, přenos konfigurace a firmware
	Podpora managementu přes IPv4 i IPv6
	SSHv2 a a SFTP
	Podpora SNMPv2c a SNMPv3
	RMON
	Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
	Lokálně vynucené RBAC na úrovni přepínače
	Dualní flash image
	TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů
	Podpora Syslog over TLS
	Podpora RADIUS včetně RADIUS CoA (RFC3576)
	Podpora RADIUS IPSEC
	Aktivní monitoring dostupnosti RADIUS přednastaveným jménem a heslem
	Podpora TACACS+
	Analýza síťového provozu sFlow podle RFC 3176
	Port mirroring (SPAN), alespoň 4 různé obousměrné session
	Podpora Zero Touch Provisioning (ZTP)

	REST API pro automatizaci nastavení
	Automatická konfigurace portu podle připojeného zařízení
	Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů
Záruka a záručnísí servis	Záruka a záruční servis v délce 60 měsíců, odstranění závady nejpozději do 2 pracovních dní (servis je poskytován výrobcem nebo autorizovaným zastoupením), oprava v místě instalace

Příslušenství přístupových přepínačů

Pro všechny dodávané přístupové přepínače požadujeme následující celkový počet příslušenství v podobě SFP modulů a kabelů:

- 26 ks SFP+ MM, včetně 2 m propojovacích kabelů LC/LC-LC/LC
- 26 ks SFP+ SM, včetně 2 m propojovacích kabelů LC/LC-LC/LC
- Záruka na příslušenství: 36 měsíců

Cena příslušenství musí být zohledněna v ceně samotných přepínačů.

1.9. Licence Anti-X řešení včetně EDR

Dodávané řešení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Verze	Licence komplexního SW pro ochranu před škodlivým softwarem pro 260 zařízení, včetně příslušenství uvedeného níže v podobě EDR a sandboxu pro tyto licence.
Základní technické požadavky	Oblast Prevence
	Pokročilá ochrana před hrozbami.
	Hlášení událostí do jedné management konsole.
	Ochrana před útoky, které šifrují MBR.
	Multiplatformní ochrana proti malwaru pro systémy Windows, Linux i macOS z jedné management konsole.
	Ochrana i pro starší verze systému Windows.
	Filtrování webových kategorií (zejména drogy, hazard, zbraně, extrémismus, násilí, sex, zločin, rasismus).
	Blokování malware i na renomovaných stránkách.
	Blokování phishingovým webů.
	Ochrana proti exploitům.
	Ochrana před útoky využívajícími dosud neznámé zranitelnosti tzv. nultého dne.
	Ochrana proti bez souborovým útokům.
	Ochrana proti síťovým útokům a hrozbám.
	DLP integrované do koncových bodů bez nutnosti instalace pluginů, s předdefinovanou sadou detekčních pravidel pro běžné typy dat a v případě potřeby možnost vytvořit vlastní pravidla pomocí regulárních výrazů.
	Pokročilá ochrana pro virtualizovaná prostředí VMware i Hyper-V. Možnost volby mezi tenkým a plným klientem.

	Dynamická obrana s automatizovanou ochranou proti aktivním útočníkům a útokům na klávesnici.
	Sandbox.
	Strojové učení.
	Umělá inteligence.
	Ochrana AV klienta proti odinstalaci nebo změně unikátním heslem, které je odlišné pro každou stanici.
	Oblast Detekce
	Pokročilá detekce hrozeb – detekce neznámého malware a potenciálně nežádoucí aplikace.
	Detekce ransomware na základě jeho chování.
	Zastavení nových variant a dosud neviděných ransomware útoků.
	Kontrola aplikací – možnost kontrolovat instalaci, sledovat používání nebo blokovat spouštění aplikací na koncových bodech podle předdefinovaných kategorií.
	Detekce a analýza hrozeb a anomálií.
	Detekce hackerských nástrojů.
	Vyšetřování detekcí řízené umělou inteligencí.
	Kontrola stavu účtů pro identifikaci odchylek v zabezpečení a upozornění na rizikové chybné konfigurace.
	Kontrola připojovaných zařízení – možnost vytváření zásad pro blokování jednotek USB, možnost zablokovat jednotlivé značky nebo modely.
	Oblast reakce
	Plná funkcionalita pro EDR/XDR.
	Možnost integrace produktů třetích stran, například s firewallem, jako zdrojů informací pro XDR.
	Režim uzamknutí serverového OS neumožňující spuštění jakékoliv neschválené aplikace.
	Automatizované izolování napadeného koncového bodu.
	Aktivní zmírnění útoků.
	Automatizované čištění malwaru nebo zablokování hrozby.
	Zastavení ransomwaru a šifrování souborů a poté automatické vrácení zašifrovaných souborů zpět do bezpečného stavu bez ohledu na velikost nebo typ souboru.
	Vizualizace incidentu. Upozornění na útok, poskytnutí podrobností o útoku, automatizace reakce pomocí nástroje XDR, možnost požádat o pomoc tým výrobce.
	Živý terminál pro vyšetřování incidentu. Průvodce vyšetřováním poskytuje návrhy dalších kroků, jako je prozkoumání zvýrazněných procesů a izolace počítače.
	Možnost vzdáleně přistupovat k zařízením se systémy Windows, Mac a Linux prostřednictvím příkazového řádku a provádět další šetření, instalovat a odinstalovávat software nebo odstraňovat problémy, které nejsou vyřešeny automaticky.

	Možnost použití příkazového řádku pro provozní činnosti IT, jako je restartování nebo instalace a odinstalace softwaru.
	Podpora API.
Délka platnosti licence a technická podpora (společně pro Anti-X, EDR i sandbox)	Je požadována dodávka licence s délkou trvání 3 let, včetně nároků na subskripce (přístup k databázi virových definic) a aktualizace software (nové verze programového vybavení, opravné balíčky, patche a bezpečnostní aktualizace). Dále zadavatel požaduje nárok na subskripce (přístup k databázi virových definic), opravné balíčky, patche a bezpečnostní aktualizace na další 2 roky *(tj. do celkové doby 5 let, kdy tyto dva roky dodavatel nacení v cenové tabulce do sloupce E – Technická podpora)* – ta bude uhrazeno současně s dodávkou.

1.10. SW pro provozní dohled nad IT prostředím

Dodávané řešení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Správa a dohled sítě	Požadujeme unifikovaný nástroj pro řešení dohledu a správy sítě pro veškeré nabízené síťové prvky, drátové tak i bezdrátové.
	Ucelený dohledový a management nástroj správy musí být stejného výrobce jako jsou dodávané síťové prvky.
	Musí obsahovat konfiguračním workflow, umožňující jednoduché nasazení a nastavení síťového prostředí, zejména složitějších scénářů, jako např. zavedení IEEE 802.1x.
	Musí umožnit hromadnou konfiguraci i výstupy skrze CLI spravovaných přepínačů
	Nástroj musí podporovat „Zero Touch Provisioning“ dodávaných prvků
	Nástroj musí disponovat přehledy, reporty i celkovou kontrolou zdraví jednotlivých prvků sítě či celé lokace.
	Nástroj bude zabezpečovat automatizované sledování, plánování a nasazování aktuálních verzí firmware tak, aby byl zabezpečen dlouhodobý, bezpečný a hladký provoz, včetně odstraňování případných chyb či rozšiřování palety funkcí firmware. Musí umožnit správu životního cyklu zařízení.
Technická podpora	Je požadován nárok na aktualizace software (nové verze programového vybavení, opravné balíčky, patche a bezpečnostní aktualizace) v minimální délce 60 měsíců, podpora bude uhrazena současně s dodávkou.

1.11. SW pro dvoufaktorovou autentizaci a správu karet

Dodávané řešení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Základní popis	Nástroj pro autentizaci uživatelů identifikačním prostředkem vůči adresářové službě AD, včetně nástrojů pro správu identifikačních prostředků (karet) a certifikátů.
Oblast: autentizace uživatelů identifikačním prostředkem vůči adresářové službě AD	
Rozhraní	Grafické rozhraní v českém jazyce s podporou SSO uživatele přihlášeného do domény Active Directory.

Parametr	Popis minimální úrovně parametru
Obnova certifikátů	Automatické hlídání expirace uživatelských doménových i kvalifikovaných certifikátů a vyvolání průvodce pro jeho jednoduchou automatizovanou uživatelskou obnovu podle nastavených politik.
Autentizace	Autentizace uživatele ve operačních systémech MS Windows včetně RDS (Remote Desktop Services) všech verzích aktuálně podporovaných výrobcem Microsoft.
Správa	Uživatelská správa uložených certifikátů a bezpečnostních údajů (PIN, QPIN, PUK).
Správa certifikátů	Export / import certifikátů/klíčů, z/na identifikační prostředek, smazání certifikátů nebo privátního klíče, od/registrace certifikátu ve Windows, testování integrity a použitelnosti.
Oblast: nástroj pro správu identifikačních prostředků (karet) a certifikátů	
Předávání veřejných doménových klíčů	Automatizované předávání veřejných klíčů doménových certifikátů do stávajícího systému Microsoft Active Directory.
Prostředky	Podpora kontaktních, bezkontaktních i hybridních identifikačních prostředků.
Evidence	Systém umožní evidovat minimálně: - typ prostředku – kontaktní, bezkontaktní, hybridní - druh prostředku – uživatelský, administrační atd. - stav prostředku – používaný, k recyklaci, skartovaný - historii prostředku – datum zavedení do evidence, vydání uživateli, recyklace - držitele prostředku – aktuálního držitele i všechny předchozí držitele - data uložená v prostředku – zejména certifikáty, včetně historie
Integrace	Napojení na Active Directory (zdroj dat o uživatelích, autentizace uživatelů, řízení rolí podle členství ve skupinách) a interní certifikační autoritu (certifikáty).
Správa certifikátů	Správa certifikátů (doménových i kvalifikovaných) ve webovém prostředí systému: - vydávání (ukládání) certifikátů na identifikační prostředek, vytvoření + tisk protokolu o vystavení - odvolání certifikátu - vydávání "v zastoupení" – např. personalista vydá novému zaměstnanci identifikační prostředek včetně certifikátu zaměstnance - včasné (konfigurovatelné) e-mailové upozornění na vypršení platnosti certifikátu
Certifikační autority	Systém musí umožnit použití jakékoliv certifikačních autority od kvalifikovaných poskytovatelů certifikačních služeb.
Operace	Recyklace identifikačních prostředků s pevným i náhodným PIN/PUK, změna uživatele, odblokování PIN (i vzdálené), tisk protokolů.
Otevřenost nástroje	Integrované API pro autorizované poskytování veřejných informací o uložených prostředcích, certifikátech a kvalifikovaných elektronických pečetí pro systémy třetích stran včetně dokumentace.
Ostatní	Možnost evidovat min. 500 identifikačních prostředků (karet).
Technická podpora	Je požadován nárok na aktualizace software (nové verze programového vybavení, opravné balíčky, patche a bezpečnostní aktualizace) v minimální délce 60 měsíců, podpora bude uhrazena současně s dodávkou.

1.12. Hybridní čipová karta

Dodávané řešení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Základní popis	Hybridní karta s kontaktní (čipovou) částí smart card a bezkontaktní částí s čipem EM4102
Provedení	Čipové karty ve formátu ID-1 (velikost bankovní karty).
	Čipové karty musí být stejného typu a provedení – není možné v rámci plnění dodat více typů technologií nebo produktů čipových karet nebo čteček čipových karet.
Určení	Karty budou primárně určeny pro dvoufaktorovou autentizaci do operačního systému MS Windows 10 nebo vyšší.
Požadované funkce	- silná dvoufaktorová autentizace - elektronický podpis - bezpečné uložení kryptografických klíčů na čipu - uložení certifikátů třetích stran - automatická obnova certifikátů - karta je certifikovaným kvalifikovaným prostředkem (QSCD) - kvalifikovaný elektronický podpis (dle eIDAS)
Bezpečnost	- privátní klíč uložený na kartě není možné z karty vyexportovat - klíče pro kvalifikovaný elektronický podpis jsou generovány v čipu - klíče, které nejsou určeny pro kvalifikovaný elektronický podpis, mohou být generovány v čipu anebo mohou být na kartu importovány - ke klíčovým párům lze na kartu uložit i příslušné certifikáty
Certifikáty	Na kartu lze uložit certifikáty od různých certifikačních autorit (vlastní doménové certifikáty, certifikáty veřejných certifikačních autorit), včetně kvalifikovaných certifikátů, vydaných akreditovanými poskytovateli (např. PostSignum České pošty).
Potisk	Jednostranný barevný potisk – zahrnuje logo města Jindřichův Hradec a označení karty (MEU-001 až MEU-200).
Záruka	24 měsíců.

1.13. Čtečka čipových karet

Dodávané řešení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Základní popis	Stolní čtečka dodávaných hybridních čipových karet s kontaktním čipem (čtečka pro kontaktní čipovou část dodávaných karet).
Provedení	USB čtečky čipových karet musí být stejného typu a provedení – není možné v rámci plnění dodat více typů technologií nebo produktů čipových karet nebo čteček čipových karet.
	Komunikační rozhraní USB 2.0+.
	Čtečka připojitelná prostřednictvím konektoru USB-A.

Kompatibilita	Kompatibilita čtečky s dodávanými čipovými kartami a SW pro autentizaci uživatelů pomocí identifikačních karet.
Podporované OS	MS Windows 10 nebo vyšší, Linux v aktuálních verzích jádra, MacOS 10.15.7 nebo vyšší.
Mechanická odolnost	Výrobcem deklarovaná odolnost min. 50.000 zasunutí/vysunutí karty.
Záruka	24 měsíců.

1.14. Licence SW Single Sign-On

Dodávané řešení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Základní popis	Nástroj Single Sign-On (SSO) umožňující se uživatelům přihlašovat k SW systémům pomocí jediné identity.
Provázanost s Active Directory	Nasazení řešení musí zajistit centralizovanou správu autentizace a autorizace uživatelů s využitím stávající infrastruktury Active Directory.
	Možnost přihlášení k aplikacím pomocí stejných přihlašovacích údajů, které jsou používány v doménovém prostředí.
Provázanost s multi faktorovou autentizací	Řešení musí být provázané a funkční s dodávaným řešením multifaktorové autentizace (tj. ověření uživatele s využitím více faktorů).
	Podpora autentizačních předmětů – kontaktní čipové karty, kombinace jméno/heslo/PIN a jejich vzájemných kombinací.
Požadované funkcionality	Dodané řešení musí obsahovat grafické uživatelské rozhraní pro vyváření, editaci a správu Single Sign-On napojení (konektorů/profilů). Toto prostředí musí být intuitivní, uživatelsky přívětivé. Uživatel nesmí být nucen psát kód, programovat, používat příkazy příkazové řádky a podobně. Rozhraní musí umožnit zadavateli vytvářet vlastní napojení (konektory/profily) na další aplikace (webové i nativní) uživatelsky, vlastními silami. Tedy bez nutnosti objednávání nových napojení u dodavatele a bez nutnosti úprav kódu napojovaných aplikací.
	Samostatná správa hesel – SSO musí podporovat resetování hesel uživatelů tak, aby uživatelé mohli samostatně obnovit přihlašovací údaje, tedy bez nutnosti pomoci administrátorů.
	Podpora politik pro zámek účtu po definovaném počtu neúspěšných pokusů o přihlášení.
	Nástroj umožní automatické přihlašování dříve ověřeného uživatele do navazujících systémů typu: - webové aplikace, - cloudové služby – MS 365, MS Azure, Google Workspace, - umožní napojení agendových IS zadavatele prostřednictvím dodaných služeb a dokumentace k těmto službám.
	SSO musí umožnit přístup do navázaných aplikací prostřednictvím autentizace z Active Directory z právě aktivní session.
	Uložené přihlašovací údaje musí být dostupné pouze uživateli, kterému náleží.

Systémové požadavky	Kompatibilita s desktopovými operačními systémy MS Windows 10 nebo vyšší a serverovými systémy MS Windows Server 2019 nebo vyšší.
	Podporované prohlížeče: - Microsoft Edge Chromium verze 130 a novější - Google Chrome verze 119 a novější
	Z důvodu nasazení do prostředí zadavatele musí SSO musí podporovat autentizační protokoly: SAML, LDAP, RADIUS, OpenID Connect.
Integrace s cloudovými aplikacemi	Schopnost SSO autentizovat uživatele do aplikací a systémů, které jsou poskytovány jako SaaS (Software-as-a-Service), zejména Office 365, AZURE, Google Workspace.
Šifrování dat	Komunikace mezi SSO serverem, klientskými zařízeními a řadiči domény musí být šifrována, pomocí SSL nebo jinou adekvátní formou.
	Uložené přihlašovací údaje musí být šifrovány pomocí kryptografických prostředků, které jsou aktuálně považovány za bezpečné.
Správa a údržba	SSO řešení musí umožňovat správu uživatelských účtů, přístupů a autentizačních metod prostřednictvím centralizované konzole. Správci IT musí mít přístup k administrátorské konzoli pro: - přidávání a odebírání uživatelských účtů, - konfiguraci politik autentizace, správu přístupových práv k jednotlivým aplikacím.
	Nástroj musí obsahovat správce hesel pro všechny uživatele. Funkce zobrazení hesla v čitelné podobě musí být zabezpečena zadáním hesla a PIN.
Audit a logování	SSO musí zaznamenávat autentizační události, zejména: - přihlášení a odhlášení uživatelů, - změny v uživatelských přístupových právech, - pokusů o neúspěšné přihlášení. Tyto záznamy musí nástroj evidovat min. za posledních 12 měsíců a musí být exportovatelné do systémů pro správu událostí a bezpečnostních informací (SIEM).
Technická podpora	Je požadován nárok na aktualizace software (nové verze programového vybavení, opravné balíčky, patche a bezpečnostní aktualizace) v minimální délce 60 měsíců, podpora bude uhrazena současně s dodávkou.

2. Požadavky na instalační a implementační práce

Dodané řešení bude sloužit pro jako vysoce dostupná hyperkonvergovaná infrastruktura pro chod agendových IS úřadu a jeho zálohování. Dodávka musí obsahovat kompletní instalaci a implementaci řešení, nad kterým pak bude v režii kupujícího se třetí stranou provedena implementace agendových systémů (virtuální databázové, aplikační a komunikační servery) a konfigurace úloh pro zálohování nově vytvořených virtuálních serverů s agendovými IS.

Implementace dodávaného řešení bude provedena po odsouhlasení zadavatelem a v souladu s „best practice“ a dle doporučení výrobců jednotlivých komponent dodávaného řešení k datu realizace plnění.

Náklady na provedení implementačních služeb musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují a nelze je vyčíslit zvlášť.

Dodavatel je povinen zahrnout do nabídky i veškeré další činnosti a prostředky, které jsou nezbytné pro řádnou dodávku plnění v rozsahu doporučeném výrobci a dle tzv. nejlepších praktik, i v případě, pokud nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné.

Základní popis IT prostředí kupujícího:

- existují dvě oddělená datová centra DC1 a DC2,
- v DC1 jsou umístěny 3 virtualizační servery (celkem s 22 VM), management a backup server, produkční diskové pole, UPS, a záložní diskové úložiště,
- v DC2 je umístěno záložní diskové úložiště,
- fyzické servery jsou virtualizovány technologií VMware,
- propoj mezi budovami MěÚ (DC1 a DC2) je zajištěn optickým spojem 10 Gb, ten je zakončen v optických vanách LC konektory,
- konektivita do internetu je zakončena v datovém centru DC1,
- není instalován fyzický firewall, resp. je nasazen fyzický linuxový server a firewallová ochrana je řešena prostřednictvím aplikace na tomto serveru.
- zálohování virtuálních serverů a dat z produkčního diskového pole je nasazen zálohovací server – zálohuje se na síťový NAS Synology (42 TB), uložení off-line záloh probíhá na druhý NAS Synology (21 TB).
- pro zálohování je využit Veeam Backup Essentials Enterprise.

2.1. Specifikace konkrétních instalačních a implementačních požadavků

V rámci předmětu plnění kupující požaduje provedení min. následujících služeb pro následující oblasti plnění:

Obecné požadavky
• dodávka požadovaného hardware a software, • doprava hardware do místa instalace, • montáž dodaných zařízení do stávajících datových rozvaděčů, • redundantní zapojení napájení jednotlivých zařízení mimo a přes pro ně vyhrazené UPS, • konfigurace portů pro správu a karet pro vzdálenou správu jednotlivých zařízení a jejich připojení do vyhrazené sítě pro správu, • aktualizace firmware v jednotlivých zařízeních a jejich komponentách na nejnovější doporučené verze, • zabezpečení přístupu ke správě jednotlivých zařízení, konfigurace synchronizace jejich času, konfigurace SNMP parametrů pro možnost vzdáleného dohledu, konfigurace SMTP pro zasílání e-mailové notifikace o stavu zařízení, • kompletní ověření funkčnosti celého řešení   ○ vytvoření testovacích virtuálních serverů ve virtualizační infrastruktuře,

- simulovaný výpadek jednoho z páteřních přepínačů,
- odpojení jednoho z propojů mezi páteřními přepínači,
- simulovaný výpadek celé jedné lokality (datového centra),
- otestování redundantního napájení jednotlivých zařízení střídavým odpojením jednoho z napájecích zdrojů,
- otestování funkčnosti korektního vypnutí jednotlivých serverů při výpadku napájení,
- otestování funkčnosti vypnutí celé infrastruktury při výpadku napájení a jejího korektního nastartování po obnovení napájení,

- propojení celého řešení do stávající síťové infrastruktury.

Implementační služby

Virtualizační server s příslušenstvím

• návrh přesunu dat a systémů (VM) ze stávajících produkčních serverů,
• instalace a konfigurace hypervizoru na příslušných serverech,
• instalace operačního systému a jeho aktualizací, instalace ovladačů a nástrojů pro správu od výrobce serveru.
• provedení migrace kupujícím odsouhlasených virtuálních serverů (nutno realizovat mimo běžnou pracovní dobu úřadu) – migrace těchto serverů proběhne ze stávajícího virtuálního prostředí do nově nasazovaného (případnou součinnost dodavatelů agendových systémů provozovaných v těchto VM zajistí kupující).
• začlenění nové serverové infrastruktury do stávajícího prostředí, konfigurace prvků vysoké dostupnosti,
• nasazení a konfigurace virtuálních switchů,
• konfigurace UPS a instalace software na servery a jejich konfigurace pro řízené vypínání serverů v případě výpadku napájení,
• ověření funkčnosti dodaného řešení v min. rozsahu:
  ○ vytvoření testovacích virtuálních serverů ve virtualizační infrastruktuře,
  ○ otestování odstávky dodávaného serveru (plánovaná i neplánovaná),
  ○ otestování funkcionality high-availability clusteru a restartu testovacího virtuálního serveru v druhé lokalitě,
  ○ otestování redundantního napájení jednotlivých zařízení střídavým odpojením jednoho z napájecích zdrojů,
  ○ otestování funkčnosti korektního vypnutí jednotlivých serverů při výpadku napájení,
  ○ otestování funkčnosti vypnutí celé infrastruktury při výpadku napájení a jejího korektního nastartování po obnovení napájení.

Licence OS serverů
• migrace a nová konfigurace služeb ze stávajících serverů na nově dodané servery (minimálně MS AD, DNS, DHCP, doménová MS Certifikační autorita), • zajištění optimálního rozložení zátěže, zajištění vysoké dostupnosti serverů, • revize, redefinice a redesign struktury MS Active Directory dle nových bezpečnostních požadavků, • revize nastavení group-policy, • dodavatel provede nastavení zálohování nově nasazeného prostředí ve stávající platformě Veeam Backup Essentials Enterprise.

Záložní zdroj s příslušenstvím
• fyzická instalace zařízení, • zapojení zařízení, • konfigurace UPS a instalace software na servery a jejich konfigurace pro řízené vypínání serverů v případě výpadku napájení,

• nastavení pravidelných self-testů UPS, • nastavení komunikace (emailové notifikace).

NG firewall s příslušenstvím
• návrh migrace na nové firewally (export pravidel ze stávajících firewallů pro potřebu analýzy zajistí zadavatel), předložení převodní tabulky FW pravidel a dalších nastavení, • návrh segmentace sítě pro nově nasazované technologie (minimálně oddělení jednotlivých typů komunikace do samostatných VLAN), • návrh adresního plánu pro potřeby nově nasazovaných technologií s ohledem na segmentaci stávající sítě v budoucnu • návrh konvence DNS názvů pro jednotlivá zařízení, • návrh a nasazení oddělené sítě pro správu, • návrh a implementace firewallu včetně vhodné konfigurace UTM (antivir, IPS, aplikační kontrola, URL filtrace dle kategorií), a začlenění firewallu do LAN prostředí.

Core a přístupové přepínače
• sestohování páteřních přepínačů a přístupových přepínačů a jejich propojení, • zprovoznění managementu síťového prostředí, včetně zavedení 802.1x, • konfigurace agregačních skupin (LACP) na přepínačích pro propojení přepínačů, připojení serverů, • konfigurace VLAN, trunk portů a přístupových portů na jednotlivých přepínačích.

Licence Anti-X řešení včetně EDR
• vytvoření politik pro jednotlivé typy koncových zařízení, • otestování politik, • vytvoření plánu nasazení na koncová zařízení, • provedení kompletního nasazení.

SW pro provozní dohled nad IT prostředím
• instalace a konfigurace nástroje pro provozní dohled nad přepínači, připojení monitorovaných zařízení. • vytvoření přehledového dashboardu a výstupů pro obsluhu.

Software pro dvoufaktorovou autentizaci a správu karet
• analýza prostředí se zaměřením na zavedení vícefaktorové autentizace, • vybudování interní PKI (Public Key Infrastructure) včetně certifikační autority integrované s Active Directory, návrh a implementace šablon certifikátů, • vybudování systému vícefaktorové autentizace s využitím kontaktních identifikačních prostředků (čipových/Smart karet). **Instalace externích čteček na koncová zařízení ani distribuce identifikačních medií uživatelům není součástí plnění,** • návrh a vybudování systému pro správu kompletního životního cyklu identifikačních prostředků (karet a doménových i veřejných certifikátů) včetně uživatelské běžné správy a obnovy platnosti, • návrh procesů souvisejících se řízením životního cyklu karet a certifikátů včetně jejich vystavování a přidělování zaměstnancům personálním oddělením, • návrh a realizace zálohování,

• provedení potřebných konfigurací souvisejících systémů, • návrh a provedení akceptačních testů včetně výkonových testů.
Single Sign-On
• zpracování plánu nasazení SSO do prostředí zadavatele, • instalace nástroje SSO, • provedení integrace s Active Directory a konfigurace skupinových politik (GPO) pro řízení přístupu a autentizace, • nastavení uživatelských profilů a propojení s přihlašovacími službami Windows serveru, • testování funkčnosti systému v rámci pilotního provozu.

2.2. Požadavky na předimplementační analýzu

Dodavatel před implementací řešení zpracuje předimplementační analýzu, minimálně pro následující oblasti:

- způsob začlenění nabízeného řešení do stávajícího ICT prostředí,
- analýza požadavků na síťovou infrastrukturu,
- analýza požadavků na ukládání a zálohování dat, obnovu dat, toky a objemy dat,
- požadavky na rekonfigurace stávajících systémů ve vztahu k plánovanému využití,
- dopady implementace na dostupnost a funkčnost stávajících služeb,
- další podklady relevantní pro návrh řešení,
- požadovaná součinnost kupujícího,
- návrh opatření k odstranění neshod zjištěných v průběhu analýzy.

Výstupem předimplementační analýzy bude písemná zpráva podléhající schválení kupujícím.

2.3. Požadavky na zpracování prováděcí dokumentace

Dodavatel 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.

Prováděcí dokumentace musí být před zahájením prací písemně schválena kupujícím.

Prováděcí dokumentace musí zohlednit podmínky stávajícího stavu, požadavky cílového stavu a musí obsahovat minimálně tyto části:

- detailní popis cílového stavu včetně popisu funkcionalit jednotlivých HW a SW částí systému,
- způsob zajištění koordinace realizace předmětu plnění s běžným provozem,
- detailní návrh a popis postupu implementace předmětu plnění,
- detailní popis zajištění bezpečnosti informací,
- detailní harmonogram projektu včetně uvedení kritických milníků,
- návrh designu úložišť a virtuálních serverů a jeho konfigurace,
- návrh designu zálohování a jeho konfigurace,
- návrh designu síťového řešení a jeho konfigurace,
- návrh monitorování řešení monitorovacími nástroji,
- vazby na stávající systémy a jejich konfigurace,
- návrh akceptačních kritérií a akceptačních testů,
- detailní popis navrhovaných zaškolení administrátorů.

2.4. Požadavky na provozní dokumentaci

Provozní dokumentace bude zpracována a předána v rozsahu detailního popisu skutečného provedení popisu činností běžné údržby a činností pro spolehlivé zajištění provozu. Popis činností běžné údržby bude pokrývat všechny dodané systémy.

2.5. Požadavky na zaškolení

Dodavatel zajistí zaškolení zaměstnanců Zadavatele – administrátorů – na zařízení a systémy, v rámci tohoto plnění, a to minimálně v rozsahu předávané provozní dokumentace.

- zaškolení zajistí seznámení specialistů IT kupujícího se všemi podstatnými částmi plnění v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin,
- minimální rozsah zaškolení je 8 hodin,
- zaškolení bude probíhat v sídle kupujícího,
- předpokládá se účast 2 administrátorů,
- náklady na zaškolení musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují.

2.6. Požadavky na provedení zkušebního provozu a akceptačních testů

- Dodavatel zajistí pro realizovanou část zkušební provoz v délce minimálně 5 dnů se zajištěním technické podpory specialistů na dodané řešení s možností nahlášení požadavku v pracovní den v době od 8 hod. do 16 hod. a dobou reakce od nahlášení požadavku do 4 hod.
- Dodavatel navrhne způsob a provedení akceptačních testů, který bude podléhat schválení ze strany kupujícího.
- Součástí akceptačních testů musí být minimálně kompletní ověření funkčnosti celého řešení dle této specifikace, a to minimálně v následujícím rozsahu
    - Ověření (otestování) požadovaných funkcí a parametrů.
    - Provedení zátěžových testů a změření výkonových parametrů (rychlost, odezvy aplikací) na testovacím prostředí.
    - Otestování vysoké dostupnost řešení na testovacím prostředí.
    - Provedení zálohy a ukázkové obnovy dat na testovacím prostření.
    - Testovací prostředí pro ověření funkčnosti a schopností nově implementovaných technologií bude navrženo prodávajícím v rámci prováděcí dokumentace a musí respektovat omezení plynoucí z nutnosti zachovat plný provoz stávajících technologií do okamžiku převzetí činností nově nasazenou technologií. Jeho rozsah a forma provedené bude podléhat schválení kupujícím jako součást odsouhlasení prováděcí dokumentace.
- O provedení akceptace a jejím výsledku musí být vyhotoven písemný protokol.
- Přechodem do ostrého provozu se rozumí okamžik úspěšné akceptace plnění včetně vypořádání všech vad a nedodělků.

2.7. Další požadavky na záruky, záruční servis a další podmínky v rámci záruky

Nabídne-li Dodavatel v rámci svého řešení HW, na něž výrobce standardně (tj. v rámci standardní dodávky a ceny) poskytuje horší záruku, popř. podporu, požaduje kupující zahrnout do nabídky cenu povýšení záruky, popř. podpory na jím požadovanou úroveň.

Kupující požaduje přístup k aktualizacím software a firmware dodaného HW v kupní ceně minimálně po dobu záruky.

Veškeré opravy po dobu záruky budou provedeny bez dalších nákladů pro kupujícího.

Není-li uvedeno u dané položky požadovaného HW jinak, požaduje zadavatel provedení záruční opravy do deseti pracovních dnů.

3. Harmonogram plnění

Kupující požaduje dodržení následujícího harmonogramu plnění – zde jsou uvedeny maximální možné lhůty pro realizaci dodávky. Údaj D značí datum nabytí účinnosti kupní smlouvy. Čísla značí počet kalendářních dnů.

Aktivita	Termín splnění
Nabytí účinnosti smlouvy (uveřejnění v registru smluv)	D
Předimplementační analýza – zpracování	D+10
Předimplementační analýza – připomínkové řízení, schválení	D+15
Prováděcí dokumentace – zpracování	D+25
Prováděcí dokumentace – připomínkové řízení, schválení	D+30
Realizace předmětu plnění	D+80
Školení administrátorů	D+80
Zkušební provoz	D+85
Akceptace předmětu plnění	D+3 měsíce

Dodavatel může dle svého uvážení výše uvedené maximální lhůty trvání zkrátit při dodržení všech částí předmětu plnění a bez snížení kvality dodávaných služeb.

Maximální lhůty trvání nesmí Dodavatel při tvorbě detailního harmonogramu prodloužit.

Detailní harmonogram plnění uvede Dodavatel ve své nabídce.

Dodavatel uvede potřebnou součinnost kupujícího pro splnění harmonogramu plnění ve své nabídce.

Příloha č. 2 smlouvy – Technická specifikace účastníka zadávacího řízení (prodávajícího) z jeho vítězné nabídky

- *Technická specifikace prodávajícího z jeho nabídky (strana 26 až 47)*
- *Objasnění nabídky prodávajícího na základě Žádosti o objasnění předložených dokladů ze dne 21. 5. 2025 (2 strany)*

6 Technická specifikace (prodávajícího)

Nabízíme dodávku jednotlivých komponent dle specifikace dále a to včetně příslušenství:

Položka plnění	Počet kusů
Virtualizační server s příslušenstvím	2
Licence OS serverů pro pokrytí pořizovaných virtualizačních serverů	2
Licence SW pro virtualizaci	1
Záložní zdroj s příslušenstvím	1
NG firewall s příslušenstvím	2
Core přepínače s příslušenstvím pro propojení primární a záložní lokality	4
Přístupové přepínače typ 48 p s příslušenstvím	7
Přístupové přepínače typ 24 p s příslušenstvím	12
Licence Anti-X řešení včetně EDR	260
SW pro provozní dohled nad IT prostředím	1
SW pro dvoufaktorovou autentizaci a správu karet	1
Hybridní čipová karta	200
Čtečka čipových karet	200
Licence SW Single SignOn	1

Položka kod	Název položky	Nabídka specifikace	Počet ks
[redacted]	Virtualizační server s příslušenstvím	HPE ProLiant DL320 Gen11 8SFF Configure-to-order Server	2
	Licence OS serverů pro pokrytí pořizovaných virtualizačních serverů	Microsoft Windows Server 2025 16-core Datacenter	2
	Licence SW pro virtualizaci	VMware vSphere Standard 8 - 32Core	1
	Záložní zdroj s příslušenstvím	APC Smart-UPS 3000VA LCD RM 2U 230V a příslušenství	1
	NG firewall s příslušenstvím	FortiGate 200F, Licence, Unified Threat Protection + FortiCare F	2
	Core přepínače s příslušenstvím pro propojení primární a záložní lokality	HPE Aruba Networking CX 6300M 24-port SFP+ and 4-port SFF	4
	Přístupové přepínače typ 48 p s příslušenstvím	HPE Aruba Networking CX 6100 48G Class4 PoE 4SFP+ 370W	7
	Přístupové přepínače typ 24 p s příslušenstvím	HPE Aruba Networking CX 6100 24G Class4 PoE 4SFP+ 370W	12
	Licence Anti-X řešení včetně EDR	ESET PROTECT Elite+ESET MDR+ESET Premium Support	260
	SW pro provozní dohled nad IT prostředím	HPE Aruba Networking Central Switch Foundation	1
	SW pro dvoufaktorovou autentizaci a správu karet	Licence SW Monet CMS, Kartové centrum, ACEx, NTFMail	1
	Hybridní čipová karta	Čipová karta ProID+Q	200
	Čtečka čipových karet	Čtečka čipových karet	200
	Licence SW Single SignOn	MFA a SSO licence Imprivata OneSign	1

Součásti dodávky jsou veškeré SFP moduly, kabely a další materiálové příslušenství nutné pro zprovoznění nabízených technologií dle požadavků zadavatele. Součástí je také dokumentace a zařízení splňuji veškeré požadavky zadavatele uvedené v technické specifikaci jakou součásti zadávací dokumentace.

Virtualizační server s příslušenstvím

[redacted] **HPE ProLiant DL320 Gen11 8SFF Configure-to-order Server**

Každý jeden kus zařízení splňuje následující technické požadavky:

Parametr	Popis minimální úrovně parametru
Základní a výkonové požadavky	Typ zařízení: - server v provedení k instalaci do 19" racku, maximálně 2U. - server s rackmount příslušenstvím včetně pohyblivého ramene pro zachycení kabeláže.
	CPU architektura x86 max. 16 plnohodnotných jader. V testu na cpubenchmark.net minimálně 36 000 bodů. Max. počet CPU je omezen na 1 a počet jader je omezen na 16 core z důvodu licencování OS a aplikací.
	Paměť: - 256GB, typu DDR5 s taktem 5600MT/s, Dual Rank - počet paměťových modulů a rozmístění musí být zvoleno pro optimální výkon s CPU - možnost zvýšení kapacity na dvojnásobek, 512GB při použití identických modulů, bez nutnosti výměny dodaných
	OS Boot: - musí být zajištěn dvojicí disků v RAID1 a kapacitou min. 480GB, nesmí se jednat o rotační disky
	LAN konektivita - min. 1 ks Ethernet adapter Dual Port 10/25GbE Adapter včetně 2 ks MM zářičů 10GE SFP+ včetně 2m kabelů LC/LC-LC/LC. - min. 1ks Ethernet adapter 2× 1GbE 1000BASE-T
	Dodávka zahrnuje 1× 2portové FC karty pro připojení do SAN sítě.
	Napájení a chlazení - server musí být vybaven redundantním napájením a chlazením, hot-plug vyměnitelné za provozu - 2ks hot-swap zdroje napájení dimenzované pro plné osazení serveru disky, CPU, RAM a PCIe zařízení, musí splňovat požadavky na certifikaci energetické účinnosti Platinum dle 80 PLUS (https://cs.wikipedia.org/wiki/80_Plus) nebo lepší; případně na stejné nebo vyšší úrovni účinnosti podle jiné certifikace
Funkční požadavky	Server musí být osazen TPM 2.0
	Vyčítání přes SNMP celkového zdraví serveru bez nutnosti instalovat OS – jeden parametr v MIB
	IPMI 2.0 popř. obdoba, možnost vzdáleného převzetí grafické konsole bez závislosti na OS, webový klient HTML5, vzdálený mount DVD media, USB, dedikovaný port (není součástí požadovaného počtu ethernet portů)
	Kompatibilita s VMWARE LifeCycle manager – z důvodu potřeby zajištění kompatibility se stávající virtualizační platformou zadavatele
	Kompatibilita všech komponent s OS VMWARE ESXi 8.x (stávající virtualizační platformou zadavatele)
Záruka, záruční servis a technická podpora	Je požadována záruka a záruční servis na dobu 5 let s reakční dobou na založený incident do konce následujícího pracovního dne (NBD).

Parametr	Popis minimální úrovně parametru
	Servisní zásahy provádí technik s příslušnou znalostí (technik výrobce nebo jeho autorizovaného zastoupení).
	Aktualizace systému budou dostupné min. po dobu záruky a záručního servisu zdarma, nabízené přehledně v servisním portálu po zadání sériového čísla.

Licence OS serverů pro pokrytí pořizovaných virtualizačních serverů

[redacted] **Microsoft Windows Server 2025 16-core Datacenter**

Je nabízena dodávka následujících licencí:

Počet	Typ licence
V počtu k pokrytí všech jader procesorů virtualizačních serverů v rámci plnění této specifikace (zadavatel předpokládá 32 jader nebo méně)	Microsoft Windows Server Datacenter 2022 v rozsahu k pokrytí dodaných procesorových core v každém produkčním serveru dle této specifikace.
- V případě dodávky licencí produktů společnosti Microsoft jsou požadovány licence, jejichž pravost je garantovaná a ověřitelná u vlastníka autorských práv Microsoft. - V případě dodávky licencí produktů společnosti Microsoft účastník 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 kupujícího. - V případě dodávky licencí produktů společnosti Microsoft se vyžaduje dodání licencí formou licenčního portálu vázaného na koncového zákazníka (kupujícího), jehož součástí budou: o seznam nabízených licencí a jejich počet, o instalační médium, o instalační klíče, o 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.	

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.

Licence SW pro virtualizaci

[redacted] **VMware vSphere Standard 8 - 32Core**

Počet	Typ licence
V počtu k pokrytí všech jader procesorů virtualizačních serverů v rámci plnění této specifikace (zadavatel předpokládá 32 jader nebo méně)	VMware vSphere Standard, per Core

- Pro dodávané virtualizační servery je požadována dodávka virtualizačního software (hypervisoru) VMware vSphere kompatibilního se stávajícím serverovým virtualizačním prostředím VMware kupujícího k licenčnímu pokrytí všech serverů, které jsou součástí tohoto plnění.

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.

Záložní zdroj s příslušenstvím

[redacted] **APC Smart-UPS 3000VA LCD RM 2U 230V a příslušenství**

Každý jeden kus zařízení splňuje následující technické požadavky:

Parametr	Popis minimální úrovně parametru
Základní specifikace	Záložní zdroj napájení (UPS)
	Pro montáž do 19" rozvaděče, výška maximálně 2U
	Maximální hloubka 70 cm
	Typ použitých baterií – bezúdržbové, hermeticky uzavřené, ventilem řízené olověné baterie
Výkonová a funkční specifikace	Parametry vstupního napětí – 230 V, 50/60 Hz +/- 3 Hz (autodetekce)
	Parametry výstupního napětí – 220/230/240 V (volitelné), 50 Hz/60 Hz (volitelné)
	Max. nastavitelný výkon 2 700 W
	Doba provozu při plné zátěži min. 3 minuty
	Jmenovitý výkon 3 000 VA
	Topologie – Line Interactive
	Výstupní přípojky: min. 1× IEC 320 C19, min. 8× IEC 320 C13
	Vstupní přípojky: min. 1× IEC 320 C20
	Přední ovládací panel s LCD, s akustickým a vizuálním varováním
	Licence management software pro bezpečné vypnutí virtuálních serverů pro 2 pořizované ESX servery a dále pro stávající ESX4 a ESX5 *(již provozované v prostředí zadavatele).*
	Vzdálená správa a dohled pomocí síťové komunikace (požadavek na min. 10/100 Mbit síťový RJ45 konektor)
	Podpora protokolů HTTPS, SSH, SNMPv2c a SNMPv3
Záruka a záruční servis	Záruka na UPS s výjimkou baterie min. 60 měsíců, včetně podpory pro firmware síťové karty a požadovaného SW.
	Záruka na baterie min. 24 měsíců.

NG Firewall s příslušenstvím

[redacted] **FortiGate 200F, Licence, Unified Threat Protection + FortiCare Premium 5YR**

Každý jeden kus zařízení splňuje následující technické požadavky:

Parametr	Popis minimální úrovně parametru
Základní specifikace	HW appliance (VM appliance ani software řešení není akceptovatelné)
	Podpora režimu vysoké dostupnosti minimálně jako Active/Active a Active/Passive, cluster o dvou fyzických zařízeních
	Velikost 1RU
	Podpora duálního napájení (redundantní zdroj)
	Minimálně 4× 10 GbE SFP+ sítová rozhraní
	Minimálně 8× GE SFP síťová rozhraní
	Minimálně 18× 1 GbE RJ45 síťová rozhraní
	Management rozhraní 1× 1 GbE RJ45 a sériový konzolový port
Výkonové požadavky	Minimální propustnost firewallu pro IPv4 i IPv6 provoz 25Gbps (měřeno na UDP komunikaci o paketech s velikostí 512 B)
	Počet současně navázaných spojení firewallu min. 3 000 000, počet nových spojení za sekundu min. 250 000
	Celková propustnost IPSEC VPN min. 12Gbps
	Propustnost SSL VPN min. 2Gbps
	Propustnost funkce SSL inspekce min. 4Gbps
	Počet CPS u spojení kontrolovaných pomocí SSL inspekce min. 1500 (spojení za sekundu)
	Propustnost funkce IPS min. 5 Gbps (reálná hodnota, měřeno na běžném provozu – real world traffic, včetně logování)
	Propustnost funkcí next generation firewallingu (stavový firewall, IPS, analýza aplikací) min. 3,5Gbps (reálná hodnota, měřeno na běžném provozu – real world traffic)
	Propustnost funkcí ochrany před hrozbami (stavový firewall, IPS, analýza aplikací, ochrana před škodlivým kódem) min. 3Gbps (reálná hodnota, měřeno na běžném provozu – real world traffic)
	Udávaná latence firewallu (udp provoz) max. 5 µs
	Min. počet současně připojených uživatelů SSL VPN 500
	Min. počet site-to-site IPSEC tunelů 16000
Funkční požadavky	Grafické konfigurační rozhraní (např. webový prohlížeč) a příkazový řádek bez omezení na počet administrátorů
	Bezpečnostní funkce obecně označovaných jako Next Generation Firewall
	Podpora virtualizace na daném HW, vytváření a provozování tzv. virtuálních kontextů – min. 10 virtuálních kontextů v ceně zařízení; každý virtuální kontext musí pracovat izolovaně, možnost propojovat jednotlivé virtuální kontext pomocí interní virtuálních propojů bez nutnosti použití fyzických interface
	Podpora stavového firewallingu pro IPv4 i IPv6, podpora NAT 64/46
	Možnost nasazení ve všech z následujících režimů (kombinace možné pomocí použití různých režimů pro různé virtuální kontexty): L2 bridge režim (inline), L3 router/NAT režim (inline), explicitní proxy (inline/out of path), transparentní proxy (inline)

Parametr	Popis minimální úrovně parametru
	Plnohodnotná správa z lokálního management rozhraní (a to i v případě využití nástroje centrální správy, neboť i v takovém případě musí být možné firewall, resp. firewall cluster, plnohodnotně konfigurovat ve chvíli, kdy z jakéhokoliv důvodu centrální správy bude nedostupná)
	Ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, RADIUS, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign-On
	Podpora lokální databáze a vzdálené databáze (RADIUS, LDAP, TACACS+, SAML, Kerberos) pro ověřování uživatelů
	Ověřování uživatelů pomocí SSO funkcionality pomocí RADIUS Single Sign-On a AD pollingu
	Funkce QoS, traffic shaping a SD-WAN minimálně v režimu vytvoření overlay a underlay virtuálních sítových rozhraní zahrnující fyzické propoje, IPSEC tunely či jiná rozhraní s možností definice pravidel pro řízení směrování, strategie využívání jednotlivých linek současně a monitorování stavu jednotlivých linek
	Podpora funkcí VPN brány – IPSec VPN (dle platných standardů pro možnost propojení se zařízeními třetích stran); - SSL VPN pro klientský přistup s tunelovacím režimem včetně klienta pro osobní počítače i mobilní platformy, portálový režim pro bezklientský přístup
	VPN klient pro neomezený počet přistupujících zařízení součástí nabídky
	Podpora funkce SSL inspekce (MITM) včetně podpory TLS 1.3
	Antivirový engine musí být vybaven lokální databází vzorků škodlivého kódu a AI/ML enginem pro identifikaci podezřelých či neznámých vzorků
	Funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, podpora rozpoznávání škodlivého kódu určeného pro mobilní zařízení (tzv. mobile malware), detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak), podpora sanitarizace aktivního obsahu běžných kancelářských dokumentů (odstranění např. skriptů či maker z dokumentu, extrakce obsahu dokumentu do neškodné podoby); podpora napojení na sandboxovací funkce včetně funkce akceptace lokálních signaturových databází generovaných sandboxem, vše bez nutnosti instalace pluginů do prohlížeče.
	Funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora min. 4000 aplikací, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace
	Možnost definice zakázaných slov pro vyhledávání na internetu
	Podpora funkce safe search pro populární vyhledavače
	Funkce kategorizace webových stránek (web filtering) s podporou minimálně 60 kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), podpora definice časové kvóty, kterou nesmí daný uživatel na dané kategorii za den překročit, výrobcem aktualizovaná a udržovaná databáze, vynikající pokrytí českého internetu; požadované akce – povolení stránky, logování stránky, brouzdání s proklikem, nutnost autentizace uživatele pro určitou kategorii, možnost definice časových kvót pro uživatele a kategorie webu
	Podpora kategorizace streamovaných videí a kanálů min. pro platformu Youtube a Vimeo
	Funkce ochrany před sítovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možností definovat různé profily na různý druh komunikace, možnost vytvářet vlastní signatury, integrovaný anomální filtr a mechanismus kontroly validity vybraných protokolů
	Možnost blokovat sítový provoz na základě URL, kategorie webové stránky, IP adresy (rozsahu), GeoIP databáze, data a času

Parametr	Popis minimální úrovně parametru
	Funkce ochrany před unikem citlivých dat (Data Leak Prevention), která umí zachytit pokus o odeslaní/upload označeného dokumentu přes internet na základě vodoznaků, popisu regulárním výrazem atp.
	Podpora dvoufaktorové autentizace pomocí HW nebo mobilních OTP tokenů, součástí dodávky musí být jako příslušenství 2 ks HW/mobilní tokeny a plně funkční řešení dvoufaktorového OTP ověřování uživatelů pro administrátory a uživatele VPN
	Obousměrná integrace (min. ve smyslu sdílení informací o odhalených hrozbách a provozně/telemetrický informací) nabízeného firewallu s dalšími instalovanými bezpečnostní prvky (mailová brána, sandbox, nástroj pro sběr a vyhodnocování logů, nástroj pro centrální správu)
	Podpora režimu nasazení v režimu WCCP (WCCP v2)
	Podpora konfiguračních PAC souborů pro režim nasazení explicitní proxy
	Podpora ICAP rozhraní pro obousměrnou integraci s externími servery
	Podpora tunelování provozu pomocí technologie GRE
	Podpora automaticky aktivovaného bypass režimu v případě přetížení systému a jeho inspekčních funkcí
	Analýza a zabezpečení DNS dotazů (ochrana před DNS poisoningem), filtrování DNS dotazů na základě kategorizace
	Možnost filtrovat Java applety, ActiveX prvky, Cookie soubory ve webovém provozu
	Integrovaná funkce load balancingu (reverzní proxy) s podporou základní algoritmů pro rozklad zátěže (round robin, váhování, nejkratší odezva, nejmenší počet aktivních spojení) s detekcí stavu reálných serverů na pozadí, podpora funkce ssl offloading a ssl inspekce pro rozkládaný provoz
Příslušenství – kabely a transceivery	Požadujeme dodání 2 ks SFP+ MM (300 m), včetně 2m kabelů LC/LC-LC/LC.
Záruka, záruční servis a technická podpora	Záruka 60 měsíců, servisní zásah následující pracovní den od nahlášení závady, v místě instalace. Servis je poskytován výrobcem firewallu.
	Technická podpora výrobce v délce 60 měsíců spočívající zejména v nároku na aktualizační balíčky zranitelností, opravné balíčky a patche, podpora bude uhrazena současně s dodávkou.

Core přepínače s příslušenstvím pro propojení primární a záložní lokality

[redacted] Aruba Networking CX 6300M 24-port SFP+ and 4-port SFP56 Switch

Každý jeden kus zařízení splňuje následující technické požadavky:

Parametr	Popis minimální úrovně parametru
Základní požadavky	Třída zařízení: L3 switch, podpora provozu jako ToR
	Formát zařízení do racku
	Velikost zařízení: max. 1U
	min. 24× SFP/SFP+ 100M/1/10G portů s volitelným fyzickým rozhraním
	min. 4× SFP/SFP+/SFP28/SFP56 1/10/25/50G portů s volitelným fyzickým rozhraním
	Chlazení typu Front-to-Back

Parametr	Popis minimální úrovně parametru
	Všechny ethernet porty jsou dostupné zepředu
Výkonové požadavky	Celková propustnost přepínače min. 880 Gb/s
	Celkový paketový výkon přepínače min. 650 Mpps
	Propustnost stohovacího propojení min. 200 Gbps
	Minimálně 8 MB paketový buffer
	2× Hot-Swap zdroje min. 250 W
Funkční požadavky	Podpora "jumbo rámců" včetně velikosti min. 9198 Byte
	Podpora linkové agregace IEEE 802.3AX
	Konfigurovatelné rozkládání LACP zátěže podle L2, L3
	Počet LACP skupin/linek ve skupině - min. 256/8
	Počet záznamů v tabulce MAC adres - min. 29 000
	Počet záznamů v tabulce ARP – min. 28 000
	Protokol pro definici šířených VLAN – MVRP
	Podpora VLAN podle IEEE 802.1Q, minimálně 4 000 aktivních VLAN
	VLAN translace – swap 802.1Q tagů na trunk portu
	Podpora zařazování do VLAN podle standardu 802.1v
	IEEE 802.1s – Multiple Spanning Tree
	STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)
	Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED
	Detekce jednosměrnosti optické linky (např. UDLD)
	DHCP server
	DHCP relay pro IPv4 a IPv6
	Podpora NTPv4 pro IPv4 a IPv6 včetně VRF a MD5 autentizace
	Statické směrování IPv4 a IPv6
	Počet záznamů ve směrovací tabulce min. 64 000
	Dynamické směrování OSPFv2, OSPFv3 a BGP včetně podpory BFD
	Podpora BGP a MP-BGP včetně podpory BFD
	Podpora Layer-3 routed port
	IGMP v2 a v3
	MLD v1 a v2
	Hardware podpora IPv4 a IPv6 ACL
	ACL definice na základě skupiny fyzických portů
	ACL aplikovatelný na interface, LAG, VLAN
	BPDU a Root guard

Parametr	Popis minimální úrovně parametru
	DHCP snooping pro IPv4 a IPv6
	HW ochrana proti zahlcení portu (broadcast/multicast/icmp) nastavitelná na kbps a pps
	802.1x ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port
	Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)
	Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675
	Podpora Critical VLAN
	Podpora uživatelských rolí definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely.
	Uživatelské role mohou být lokálně definované v přepínači nebo mohou být dynamicky stáhnuty z RADIUS serveru na základě výsledku autorizace.
	Podpora IPv6 RA Guard
	IP source guard / dynamic IP lockdown
	Podpora Dynamic ARP protection
	Port security
	Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU
	Podpora IPv4 a IPv6 QoS
	IEEE 802.1p – minimální počet front - 8
Management	CLI formou RJ45 serial konsole port
	Konfigurace zařízení v člověku čitelné textové formě
	OoB management formou portu RJ45 s podporou ethernetu
	USB port pro přenos konfigurace a firmware
	Podpora SSHv2, SFTP a HTTPS pro IPv4 a IPv6
	Podpora RSA s délkou klíče minimálně 4096 bitů
	Podpora grafického uživatelského webového rozhraní. Možnost vytváření vlastních diagnostických a korelačních skriptů a jejich grafických interpretací v jazyce Python (korelace libovolných událostí a hodnot v podobě grafů)
	Podpora SNMPv2c a SNMPv3
	Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
	TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)
	SPAN a ERSPAN port mirroring, alespoň 4 různé obousměrné session
	TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více SYSLOG serverů
	Podpora automatických i manuálních snapshotů systému a možnost automatického obnovení předchozí konfigurace v případě konfigurační chyby
	Podpora standardního Linux Shellu (BASH) pro debugging a skriptování
	Podpora skriptování v jazyce Python – lokální interpret jazyka v přepínači

Parametr	Popis minimální úrovně parametru
	Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní)
	Interpretace uživatelských skriptů monitorujících definované parametry síťového provozu s možností automatické reakce na události
	Interní SSD úložiště pro sběr provozních dat a pokročilou diagnostiku zařízení
	Podpora OVSDB
	Analýza síťového provozu sFlow podle RFC 3176
	Ochrana proti nahrání modifikovaného SW prostřednictvím image signing a secure boot, ověřující autentičnost a integritu OS prostřednictvím TPM chipu
	Podpora integrace s automatizačními nástroji (Ansible, NAPALM)
	Podpora REST API v režimech read-only a read-write pro automatizaci nastavení
Příslušenství – kabely a transceivery	Požadujeme dodání 1 ks SFP56 DAC kabel 0,65m, 15 ks SFP+ SM, 8 ks SFP+ MM.
Záruka a záruční servis	Záruka a záruční servis v délce 60 měsíců, odstranění závady nejpozději do 2 pracovních dní (servis je poskytován výrobcem nebo autorizovaným zastoupením), oprava v místě instalace.

Přístupové přepínače typ 48p s příslušenstvím

[redacted]HPE Aruba Networking CX 6100 48G Class4 PoE 4SFP+ 370W Switch

Každý jeden kus zařízení splňuje následující technické požadavky:

Parametr	Popis minimální úrovně parametru
Základní a výkonnostní specifikace	Třída zařízení: L2+ switch
	Formát zařízení do racku
	Velikost zařízení: 1U
	min. 48× 10/100/1000Mbit metalických portů
	min. 4× 10Gbit/s SFP+ nezávislých optických portů s volitelným fyzickým rozhraním
	10GE interface zpětně kompatibilní s 1Gbit/s transceivery
	Všechny ethernet porty jsou dostupné zepředu
	Interní napájecí zdroj
	Podpora PoE+ dle standardu 802.3at
	Dostupný výkon pro PoE+ napájení 370 W
	Podpora Energy Efficient Ethernet (802.3az)
	Celková propustnost přepínače 176 Gb/s
	Celkový paketový výkon přepínače 98 Mpps
	Minimálně 12 MB paketový buffer
	Maximální přípustná hloubka přepínače 33 cm

Základní funkce a protokoly	Podpora "jumbo rámců" včetně velikosti 9220 Byte
	Podpora linkové agregace IEEE 802.3ad
	Konfigurovatelné rozkládání LACP zátěže podle L3 a L4
	Minimální počet LACP skupin/linek ve skupině: 8/8
	Protokol pro definici šířených VLAN: MVRP
	Podpora VLAN podle IEEE 802.1Q, minimálně 512 aktivních VLAN
	IEEE 802.1s – Multiple Spanning Tree
	STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)
	Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED
	Detekce jednosměrnosti optické linky (např. UDLD)
	NTP pro IPv4 a IPv6 včetně MD5 autentizace
	Statické směrování IPv4 a IPv6
	IGMP v2 a v3
	MLD v1 a v2
	Hardware podpora IPv4 a IPv6 ACL
	ACL definice na základě skupiny fyzických portů
	ACL aplikovatelný na rozhraní IN včetně virtuálních VLAN
	BPDU guard a Root guard
	HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na množství paketů za vteřinu
	ICMPv4 a ICMPv6 rate-limiting per port
	Ověřování 802.1X včetně více uživatelů na port, minimálně 32 uživatelů/port
	Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)
	802.1X s podporou odlišných Preauth VLAN, Fail VLAN a Critical VLAN
	Dynamické zařazování do VLAN
	802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení)
	Port security – omezení počtu MAC adres na port, statické MAC
	Ochrana proti opakovaným výpadkům linek (flapování) s možností konfigurace citlivosti a akce při překročení
	Ochrana control plane (CPU) před útoky typu DoS
	Podpora IPv4 a IPv6 QoS
	Minimálně 8 front pro IEEE 802.1p
Management	CLI formou 1× USB-C Console Port
	Konfigurace zařízení v člověku čitelné textové formě
	Podpora automatických i manuálních snapshotů konfigurace systému

	USB port pro diagnostiku, přenos konfigurace a firmware
	Podpora managementu přes IPv4 i IPv6
	SSHv2 a a SFTP
	Podpora SNMPv2c a SNMPv3
	RMON
	Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
	Lokálně vynucené RBAC na úrovni přepínače
	Dualní flash image
	TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů
	Podpora Syslog over TLS
	Podpora RADIUS včetně RADIUS CoA (RFC3576)
	Podpora RADIUS IPSEC
	Aktivní monitoring dostupnosti RADIUS přednastaveným jménem a heslem
	Podpora TACACS+
	Analýza síťového provozu sFlow podle RFC 3176
	Port mirroring (SPAN), alespoň 4 různé obousměrné session
	Podpora Zero Touch Provisioning (ZTP)
	REST API pro automatizaci nastavení
	Automatická konfigurace portu podle připojeného zařízení
	Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů
Záruka a záruční servis	Záruka a záruční servis v délce 60 měsíců, odstranění závady nejpozději do 2 pracovních dní (servis je poskytován výrobcem nebo autorizovaným zastoupením), oprava v místě instalace.

Přístupové přepínače typ 24p s příslušenstvím

[redacted]HPE Aruba Networking CX 6100 24G Class4 PoE 4SFP+ 370W Switch

Každý jeden kus zařízení splňuje následující technické požadavky:

Parametr	Popis minimální úrovně parametru
Základní a výkonnostní specifikace	Třída zařízení: L2+ switch
	Formát zařízení do racku
	Velikost zařízení: 1U
	min. 24× 10/100/1000Mbit metalických portů
	min. 4× 10Gbit/s SFP+ nezávislých optických portů s volitelným fyzickým rozhraním
	10GE interface zpětně kompatibilní s 1Gbit/s transceivery
	Všechny ethernet porty jsou dostupné zepředu
	Interní napájecí zdroj

	Podpora PoE+ dle standardu 802.3at
	Dostupný výkon pro PoE+ napájení 370 W
	Podpora Energy Efficient Ethernet (802.3az)
	Celková propustnost přepínače 128 Gb/s
	Celkový paketový výkon přepínače 95 Mpps
	Minimálně 12 MB paketový buffer
	Maximální přípustná hloubka přepínače 33 cm
Základní funkce a protokoly	Podpora "jumbo rámců" včetně velikosti 9220 Byte
	Podpora linkové agregace IEEE 802.3ad
	Konfigurovatelné rozkládání LACP zátěže podle L3 a L4
	Minimální počet LACP skupin/linek ve skupině: 8/8
	Protokol pro definici šířených VLAN: MVRP
	Podpora VLAN podle IEEE 802.1Q, minimálně 512 aktivních VLAN
	IEEE 802.1s – Multiple Spanning Tree
	STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)
	Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED
	Detekce jednosměrnosti optické linky (např. UDLD)
	NTP pro IPv4 a IPv6 včetně MD5 autentizace
	Statické směrování IPv4 a IPv6
	IGMP v2 a v3
	MLD v1 a v2
	Hardware podpora IPv4 a IPv6 ACL
	ACL definice na základě skupiny fyzických portů
	ACL aplikovatelný na rozhraní IN včetně virtuálních VLAN
	BPDU guard a Root guard
	HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na množství paketů za vteřinu
	ICMPv4 a ICMPv6 rate-limiting per port
	Ověřování 802.1X včetně více uživatelů na port, minimálně 32 uživatelů/port
	Konfiguovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)
	802.1X s podporou odlišných Preauth VLAN, Fail VLAN a Critical VLAN
	Dynamické zařazování do VLAN
	802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení)
	Port security – omezení počtu MAC adres na port, statické MAC

	Ochrana proti opakovaným výpadkům linek (flapování) s možností konfigurace citlivosti a akce při překročení
	Ochrana control plane (CPU) před útoky typu DoS
	Podpora IPv4 a IPv6 QoS
	Minimálně 8 front pro IEEE 802.1p
Management	CLI formou 1× USB-C Console Port
	Konfigurace zařízení v člověku čitelné textové formě
	Podpora automatických i manuálních snapshotů konfigurace systému
	USB port pro diagnostiku, přenos konfigurace a firmware
	Podpora managementu přes IPv4 i IPv6
	SSHv2 a a SFTP
	Podpora SNMPv2c a SNMPv3
	RMON
	Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
	Lokálně vynucené RBAC na úrovni přepínače
	Dualní flash image
	TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů
	Podpora Syslog over TLS
	Podpora RADIUS včetně RADIUS CoA (RFC3576)
	Podpora RADIUS IPSEC
	Aktivní monitoring dostupnosti RADIUS přednastaveným jménem a heslem
	Podpora TACACS+
	Analýza síťového provozu sFlow podle RFC 3176
	Port mirroring (SPAN), alespoň 4 různé obousměrné session
	Podpora Zero Touch Provisioning (ZTP)
	REST API pro automatizaci nastavení
	Automatická konfigurace portu podle připojeného zařízení
	Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů
Záruka a zárušní servis	Záruka a záruční servis v délce 60 měsíců, odstranění závady nejpozději do 2 pracovních dní (servis je poskytován výrobcem nebo autorizovaným zastoupením), oprava v místě instalace

Příslušenství přístupových přepínačů

Pro všechny dodávané přístupové přepínače bude dodáno následující celkový počet příslušenství v podobě SFP modulů a kabelů:

- 26 ks SFP+ MM, včetně 2 m propojovacích kabelů LC/LC-LC/LC
- 26 ks SFP+ SM, včetně 2 m propojovacích kabelů LC/LC-LC/LC
- Záruka na příslušenství: 36 měsíců

Licence Anti-X řešení včetně EDR

[redacted]ESET PROTECT Elite+ESET MDR+ESET Premium Support

Dodávané řešení splňuje následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Verze	Licence komplexního SW pro ochranu před škodlivým softwarem pro 260 zařízení, včetně příslušenství uvedeného níže v podobě EDR a sandboxu pro tyto licence.
Základní technické požadavky	Oblast Prevence
	Pokročilá ochrana před hrozbami.
	Hlášení událostí do jedné management konsole.
	Ochrana před útoky, které šifrují MBR.
	Multiplatformní ochrana proti malwaru pro systémy Windows, Linux i macOS z jedné management konsole.
	Ochrana i pro starší verze systému Windows.
	Filtrování webových kategorií (zejména drogy, hazard, zbraně, extrémismus, násilí, sex, zločin, rasismus).
	Blokování malware i na renomovaných stránkách.
	Blokování phishingovým webů.
	Ochrana proti exploitům.
	Ochrana před útoky využívajícími dosud neznámé zranitelnosti tzv. nultého dne.
	Ochrana proti bez souborovým útokům.
	Ochrana proti síťovým útokům a hrozbám.
	DLP integrované do koncových bodů bez nutnosti instalace pluginů, s předdefinovanou sadou detekčních pravidel pro běžné typy dat a v případě potřeby možnost vytvořit vlastní pravidla pomocí regulárních výrazů.
	Pokročilá ochrana pro virtualizovaná prostředí VMware i Hyper-V. Možnost volby mezi tenkým a plným klientem.
	Dynamická obrana s automatizovanou ochranou proti aktivním útočníkům a útokům na klávesnici.
	Sandbox.
	Strojové učení.
	Umělá inteligence.
	Ochrana AV klienta proti odinstalaci nebo změně unikátním heslem, které je odlišné pro každou stanici.
	Oblast Detekce
	Pokročilá detekce hrozeb – detekce neznámého malware a potenciálně nežádoucí aplikace.
	Detekce ransomware na základě jeho chování.
	Zastavení nových variant a dosud neviděných ransomware útoků.

	Kontrola aplikací – možnost kontrolovat instalaci, sledovat používání nebo blokovat spouštění aplikací na koncových bodech podle předdefinovaných kategorií.
	Detekce a analýza hrozeb a anomálií.
	Detekce hackerských nástrojů.
	Vyšetřování detekcí řízené umělou inteligencí.
	Kontrola stavu účtů pro identifikaci odchylek v zabezpečení a upozornění na rizikové chybné konfigurace.
	Kontrola připojovaných zařízení – možnost vytváření zásad pro blokování jednotek USB, možnost zablokovat jednotlivé značky nebo modely.
	Oblast reakce
	Plná funkcionalita pro EDR/XDR.
	Možnost integrace produktů třetích stran, například s firewallem, jako zdrojů informací pro XDR.
	Režim uzamknutí serverového OS neumožňující spuštění jakékoliv neschválené aplikace.
	Automatizované izolování napadeného koncového bodu.
	Aktivní zmírnění útoků.
	Automatizované čištění malwaru nebo zablokování hrozby.
	Zastavení ransomwaru a šifrování souborů a poté automatické vrácení zašifrovaných souborů zpět do bezpečného stavu bez ohledu na velikost nebo typ souboru.
	Vizualizace incidentu. Upozornění na útok, poskytnutí podrobností o útoku, automatizace reakce pomocí nástroje XDR, možnost požádat o pomoc tým výrobce.
	Živý terminál pro vyšetřování incidentu. Průvodce vyšetřováním poskytuje návrhy dalších kroků, jako je prozkoumání zvýrazněných procesů a izolace počítače.
	Možnost vzdáleně přistupovat k zařízením se systémy Windows, Mac a Linux prostřednictvím příkazového řádku a provádět další šetření, instalovat a odinstalovávat software nebo odstraňovat problémy, které nejsou vyřešeny automaticky.
	Možnost použití příkazového řádku pro provozní činnosti IT, jako je restartování nebo instalace a odinstalace softwaru.
	Podpora API.
Délka platnosti licence a technická podpora (společně pro Anti-X, EDR i sandbox)	Je požadována dodávka licence s délkou trvání 3 let, včetně nároků na subskripce (přístup k databázi virových definic) a aktualizace software (nové verze programového vybavení, opravné balíčky, patche a bezpečnostní aktualizace). Dále zadavatel požaduje nárok na subskripce (přístup k databázi virových definic), opravné balíčky, patche a bezpečnostní aktualizace na další 2 roky *(tj. do celkové doby 5 let, kdy tyto dva roky dodavatel nacení v cenové tabulce do sloupce E – Technická podpora)* – ta bude uhrazeno současně s dodávkou.

SW pro provozní dohled nad IT prostředím

[redacted]HPE Aruba Networking Central Switch Foundation

Dodávané řešení splňuje následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Správa a dohled sítě	Požadujeme unifikovaný nástroj pro řešení dohledu a správy sítě pro veškeré nabízené síťové prvky, drátové tak i bezdrátové.
	Ucelený dohledový a management nástroj správy musí být stejného výrobce jako jsou dodávané síťové prvky.
	Musí obsahovat konfiguračním workflow, umožňující jednoduché nasazení a nastavení síťového prostředí, zejména složitějších scénářů, jako např. zavedení IEEE 802.1x.
	Musí umožnit hromadnou konfiguraci i výstupy skrze CLI spravovaných přepínačů
	Nástroj musí podporovat „Zero Touch Provisioning“ dodávaných prvků
	Nástroj musí disponovat přehledy, reporty i celkovou kontrolou zdraví jednotlivých prvků sítě či celé lokace.
	Nástroj bude zabezpečovat automatizované sledování, plánování a nasazování aktuálních verzí firmware tak, aby byl zabezpečen dlouhodobý, bezpečný a hladký provoz, včetně odstraňování případných chyb či rozšiřování palety funkcí firmware. Musí umožnit správu životního cyklu zařízení.
Technická podpora	Je požadován nárok na aktualizace software (nové verze programového vybavení, opravné balíčky, patche a bezpečnostní aktualizace) v minimální délce 60 měsíců, podpora bude uhrazena současně s dodávkou.

SW pro dvoufaktorovou autentizaci a správu karet

[redacted]Licence SW Monet CMS, Kartové centrum, ACEx, NTFMail

Dodávané řešení splňuje následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Základní popis	Nástroj pro autentizaci uživatelů identifikačním prostředkem vůči adresářové službě AD, včetně nástrojů pro správu identifikačních prostředků (karet) a certifikátů.
Oblast: autentizace uživatelů identifikačním prostředkem vůči adresářové službě AD	
Rozhraní	Grafické rozhraní v českém jazyce s podporou SSO uživatele přihlášeného do domény Active Directory.
Obnova certifikátů	Automatické hlídání expirace uživatelských doménových i kvalifikovaných certifikátů a vyvolání průvodce pro jeho jednoduchou automatizovanou uživatelskou obnovu podle nastavených politik.
Autentizace	Autentizace uživatele ve operačních systémech MS Windows včetně RDS (Remote Desktop Services) všech verzích aktuálně podporovaných výrobcem Microsoft.
Správa	Uživatelská správa uložených certifikátů a bezpečnostních údajů (PIN, QPIN, PUK).
Správa certifikátů	Export / import certifikátů/klíčů, z/na identifikační prostředek, smazání certifikátů nebo privátního klíče, od/registrace certifikátu ve Windows, testování integrity a použitelnosti.

Parametr	Popis minimální úrovně parametru
Oblast: nástroj pro správu identifikačních prostředků (karet) a certifikátů	
Předávání veřejných doménových klíčů	Automatizované předávání veřejných klíčů doménových certifikátů do stávajícího systému Microsoft Active Directory.
Prostředky	Podpora kontaktních, bezkontaktních i hybridních identifikačních prostředků.
Evidence	Systém umožní evidovat minimálně: - typ prostředku – kontaktní, bezkontaktní, hybridní - druh prostředku – uživatelský, administrační atd. - stav prostředku – používaný, k recyklaci, skartovaný - historii prostředku – datum zavedení do evidence, vydání uživateli, recyklace - držitele prostředku – aktuálního držitele i všechny předchozí držitele - data uložená v prostředku – zejména certifikáty, včetně historie
Integrace	Napojení na Active Directory (zdroj dat o uživatelích, autentizace uživatelů, řízení rolí podle členství ve skupinách) a interní certifikační autoritu (certifikáty).
Správa certifikátů	Správa certifikátů (doménových i kvalifikovaných) ve webovém prostředí systému: - vydávání (ukládání) certifikátů na identifikační prostředek, vytvoření + tisk protokolu o vystavení - odvolání certifikátu - vydávání "v zastoupení" – např. personalista vydá novému zaměstnanci identifikační prostředek včetně certifikátu zaměstnance - včasné (konfigurovatelné) e-mailové upozornění na vypršení platnosti certifikátu
Certifikační autority	Systém musí umožnit použití jakékoliv certifikačních autority od kvalifikovaných poskytovatelů certifikačních služeb.
Operace	Recyklace identifikačních prostředků s pevným i náhodným PIN/PUK, změna uživatele, odblokování PIN (i vzdálené), tisk protokolů.
Otevřenost nástroje	Integrované API pro autorizované poskytování veřejných informací o uložených prostředcích, certifikátech a kvalifikovaných elektronických pečetí pro systémy třetích stran včetně dokumentace.
Ostatní	Možnost evidovat min. 500 identifikačních prostředků (karet).
Technická podpora	Je požadován nárok na aktualizace software (nové verze programového vybavení, opravné balíčky, patche a bezpečnostní aktualizace) v minimální délce 60 měsíců, podpora bude uhrazena současně s dodávkou.

Hybridní čipová karta

[redacted]Čipová karta ProID+Q

Dodávané řešení splňuje následující minimální technické požadavky:

Parametr	**Popis minimální úrovně parametru**
Základní popis	Hybridní karta s kontaktní (čipovou) částí smart card a bezkontaktní částí s čipem EM4102
Provedení	Čipové karty ve formátu ID-1 (velikost bankovní karty).

	Čipové karty musí být stejného typu a provedení – není možné v rámci plnění dodat více typů technologií nebo produktů čipových karet nebo čteček čipových karet.
Určení	Karty budou primárně určeny pro dvoufaktorovou autentizaci do operačního systému MS Windows 10 nebo vyšší.
Požadované funkce	- silná dvoufaktorová autentizace - elektronický podpis - bezpečné uložení kryptografických klíčů na čipu - uložení certifikátů třetích stran - automatická obnova certifikátů - karta je certifikovaným kvalifikovaným prostředkem (QSCD) - kvalifikovaný elektronický podpis (dle eIDAS)
Bezpečnost	- privátní klíč uložený na kartě není možné z karty vyexportovat - klíče pro kvalifikovaný elektronický podpis jsou generovány v čipu - klíče, které nejsou určeny pro kvalifikovaný elektronický podpis, mohou být generovány v čipu anebo mohou být na kartu importovány - ke klíčovým párům lze na kartu uložit i příslušné certifikáty
Certifikáty	Na kartu lze uložit certifikáty od různých certifikačních autorit (vlastní doménové certifikáty, certifikáty veřejných certifikačních autorit), včetně kvalifikovaných certifikátů, vydaných akreditovanými poskytovateli (např. PostSignum České pošty).
Potisk	Jednostranný barevný potisk – zahrnuje logo města Jindřichův Hradec a označení karty (MEU-001 až MEU-200).
Záruka	24 měsíců.

Čtečka čipových karet

[redacted] Čtečka čipových karet

Dodávané řešení splňuje následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Základní popis	Stolní čtečka dodávaných hybridních čipových karet s kontaktním čipem (čtečka pro kontaktní čipovou část dodávaných karet).
Provedení	USB čtečky čipových karet musí být stejného typu a provedení – není možné v rámci plnění dodat více typů technologií nebo produktů čipových karet nebo čteček čipových karet.
	Komunikační rozhraní USB 2.0+.
	Čtečka připojitelná prostřednictvím konektoru USB-A.
Kompatibilita	Kompatibilita čtečky s dodávanými čipovými kartami a SW pro autentizaci uživatelů pomocí identifikačních karet.
Podporované OS	MS Windows 10 nebo vyšší, Linux v aktuálních verzích jádra, MacOS 10.15.7 nebo vyšší.
Mechanická odolnost	Výrobcem deklarovaná odolnost min. 50.000 zasunutí/vysunutí karty.
Záruka	24 měsíců.

Licence SW Single Sign-On

[redacted] MFA a SSO licence Imprivata OneSign

Dodávané řešení splňuje následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Základní popis	Nástroj Single Sign-On (SSO) umožňující se uživatelům přihlašovat k SW systémům pomocí jediné identity.
Provázanost s Active Directory	Nasazení řešení musí zajistit centralizovanou správu autentizace a autorizace uživatelů s využitím stávající infrastruktury Active Directory.
	Možnost přihlášení k aplikacím pomocí stejných přihlašovacích údajů, které jsou používány v doménovém prostředí.
Provázanost s multi faktorovou autentizací	Řešení musí být provázané a funkční s dodávaným řešením multifaktorové autentizace (tj. ověření uživatele s využitím více faktorů).
	Podpora autentizačních předmětů – kontaktní čipové karty, kombinace jméno/heslo/PIN a jejich vzájemných kombinací.
Požadované funkcionality	Dodané řešení musí obsahovat grafické uživatelské rozhraní pro vyváření, editaci a správu Single Sign-On napojení (konektorů/profilů). Toto prostředí musí být intuitivní, uživatelsky přívětivé. Uživatel nesmí být nucen psát kód, programovat, používat příkazy příkazové řádky a podobně. Rozhraní musí umožnit zadavateli vytvářet vlastní napojení (konektory/profily) na další aplikace (webové i nativní) uživatelsky, vlastními silami. Tedy bez nutnosti objednávání nových napojení u dodavatele a bez nutnosti úprav kódu napojovaných aplikací.
	Samostatná správa hesel – SSO musí podporovat resetování hesel uživatelů tak, aby uživatelé mohli samostatně obnovit přihlašovací údaje, tedy bez nutnosti pomoci administrátorů.
	Podpora politik pro zámek účtu po definovaném počtu neúspěšných pokusů o přihlášení.
	Nástroj umožní automatické přihlašování dříve ověřeného uživatele do navazujících systémů typu: - webové aplikace, - cloudové služby – MS 365, MS Azure, Google Workspace, - umožní napojení agendových IS zadavatele prostřednictvím dodaných služeb a dokumentace k těmto službám.
	SSO musí umožnit přístup do navázaných aplikací prostřednictvím autentizace z Active Directory z právě aktivní session.
	Uložené přihlašovací údaje musí být dostupné pouze uživateli, kterému náleží.
Systémové požadavky	Kompatibilita s desktopovými operačními systémy MS Windows 10 nebo vyšší a serverovými systémy MS Windows Server 2019 nebo vyšší.
	Podporované prohlížeče: - Microsoft Edge Chromium verze 130 a novější - Google Chrome verze 119 a novější
	Z důvodu nasazení do prostředí zadavatele musí SSO musí podporovat autentizační protokoly: SAML, LDAP, RADIUS, OpenID Connect.

Integrace s cloudovými aplikacemi	Schopnost SSO autentizovat uživatele do aplikací a systémů, které jsou poskytovány jako SaaS (Software-as-a-Service), zejména Office 365, AZURE, Google Workspace.
Šifrování dat	Komunikace mezi SSO serverem, klientskými zařízeními a řadiči domény musí být šifrována, pomocí SSL nebo jinou adekvátní formou.
	Uložené přihlašovací údaje musí být šifrovány pomocí kryptografických prostředků, které jsou aktuálně považovány za bezpečné.
Správa a údržba	SSO řešení musí umožňovat správu uživatelských účtů, přístupů a autentizačních metod prostřednictvím centralizované konzole. Správci IT musí mít přístup k administrátorské konzoli pro: - přidávání a odebírání uživatelských účtů, - konfiguraci politik autentizace, správu přístupových práv k jednotlivým aplikacím.
	Nástroj musí obsahovat správce hesel pro všechny uživatele. Funkce zobrazení hesla v čitelné podobě musí být zabezpečena zadáním hesla a PIN.
Audit a logování	SSO musí zaznamenávat autentizační události, zejména: - přihlášení a odhlášení uživatelů, - změny v uživatelských přístupových právech, - pokusů o neúspěšné přihlášení. Tyto záznamy musí nástroj evidovat min. za posledních 12 měsíců a musí být exportovatelné do systémů pro správu událostí a bezpečnostních informací (SIEM).
Technická podpora	Je požadován nárok na aktualizace software (nové verze programového vybavení, opravné balíčky, patche a bezpečnostní aktualizace) v minimální délce 60 měsíců, podpora bude uhrazena současně s dodávkou.

Instalační a implementační práce

Součástí dodávky jsou veškeré požadované instalační a implementační práce uvedené v Technické specifikaci jako součást Zadávací dokumentace.

21.05.2025

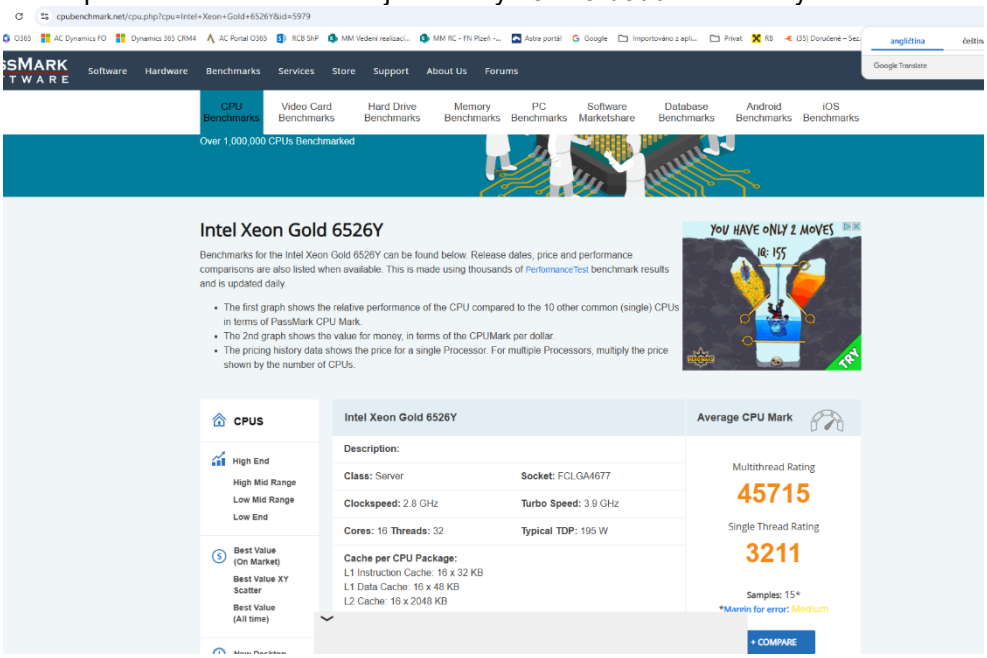
Město Jindřichův Hradec
Klášterská 135,,
377 01 Jindřichův Hradec
Ivan Nápravník
Odbor rozvoje – oddělení strategického rozvoje
Č.j.: ROZ/29869/25/Np

Vážení,

děkujeme vám za zaslání Žádosti o objasnění předložených dokladů a doplnění chybějících údajů a dokladů k zadávacímu řízení Dodávka IT infrastruktury a licencí pro zvýšení kybernetické bezpečnosti, Systémové číslo NEN: N006-25-V00008315 zadavatele Město Jindřichův Hradec.

Dále uvádíme doplnění a objasnění údajů k jednotlivým poptávaným bodům:

1) Uchazeč nabízí server HPE ProLiant DL320 Gen11 8SFF Configure-to-order Server s procesorem CPU **P67080-B21 INT Xeon-G 6526Y CPU for HPE**, který obsahuje 16 jader a v testu cpubenchmark.net dosahuje hodnoty **45 715 bodů** viz vložený otisk obrazovky.



2) Uchazeč nabízí čtečku čipových karet **Ctec.Q IDBridge CT30**, součástí příloh tohoto objasnění je produktový list čtečky s uvedením technických údajů pro ověření splnění zadávacích podmínek.
3) U položky "Licence Anti-X řešení včetně EDR" uchazeč nabízí skupinu produktů *ESET ESET PROTECT Elite+ESET MDR+ESET Premium Support* **včetně software řešení DLP (ochrana dat před únikem) Safetica ONE,** která administrativním nedopatřením není uvedeno ve výčtu produktů, ale je součástí tohoto nabízeného balíčku software, kompletní specifikace nabízeného balíku je tedy *ESET ESET PROTECT Elite+ESET MDR+ESET Premium Support+SafeticaONE*. ESET toto komplexní řešení nativně podporuje viz například https://digitalsecurityguide.eset.com/cz/unik-dat-predstavuje-bezpecnostni-katastrofu-jak-pomuze-dlp

S přátelským pozdravem

Ladislav Kocour
Digitálně podepsal Ladislav Kocour
Datum: 2025.05.21 11:34:35 +02'00'

Ladislav Kocour

Ředitel regionálního centra
Aricoma Systems a.s.
[redacted]

Příloha č. 1 – Datasheet Ctecka_IDBridge CT30

Příloha č. 3 smlouvy – Cenová tabulka z nabídky prodávajícího

Cenová tabulka veřejné zakázky s názvem Dodávka IT infrastruktury a licencí pro zvýšení kybernetické bezpečnosti

1. Účastník zadávacího řízení cenovou 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 celkem 5 let (maintenance, bezpečnostní update, patche, subskripce, nároky na aktualizační balíčky dat atd.) [Kč bez DPH]
Virtualizační server s příslušenstvím pro virtualizaci	2	[redacted] Kč	[redacted] Kč	---
Licence OS serverů pro pokrytí pořizovaných virtualiza	2	[redacted] Kč	---	---
Licence SW pro virtualizaci	1	[redacted] Kč	---	[redacted] Kč
Záložní zdroj s příslušenstvím	1	[redacted] Kč	[redacted] Kč	---
NG firewall s příslušenstvím	2	[redacted] Kč	[redacted] Kč	[redacted] Kč
Core přepínače s příslušenstvím pro propojení primárn	4	[redacted] Kč	[redacted] Kč	---
Přístupové přepínače typ 48p s příslušenstvím	7	[redacted] Kč	[redacted] Kč	---
Přístupové přepínače typ 24p s příslušenstvím	12	[redacted] Kč	[redacted] Kč	---
Licence Anti-X řešení včetně EDR	260	[redacted] Kč	---	[redacted] Kč
SW pro provozní dohled nad IT prostředím	1	[redacted] Kč	---	[redacted] Kč
SW pro dvoufaktorovou autentizaci a správu karet	1	[redacted] Kč	---	[redacted] Kč
Hybridní čipová karta	200	[redacted] Kč	---	---
Čtečka čipových karet	200	[redacted] Kč	---	---

Licence SW SingleSignOn	1	[redacted] Kč	---	[redacted] Kč
Souhrn		Kupní cena Kč bez DPH		12 362 280,00 Kč
		DPH ve výši 21 %		2 596 078,80 Kč
		Kupní cena Kč s DPH		14 958 358,80 Kč

V …Českých Budějovicích…… dne …7.5.2025……

Podpis osoby oprávněné za účastníka zadávacího řízení

Ing. Jaroslav Dvořák

Digitálně podepsal Ing. Jaroslav Dvořák
Datum: 2025.05.07 20:57:21 +02'00'