Spolufinancováno Evropskou unií

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

Evidenční číslo smlouvy:

Smlouva o zabezpečení podpory provozu

Město Příbram
Sídlo: Tyršova 108, 261 19 Příbram
IČO: 00243132
jednající: Mgr. Janem Konvalinkou, starostou
Bankovní spojení: Česká spořitelna, a.s.
Číslo účtu: 27-521689309/0800
kontaktní osoba: Jan Drozen
na straně jedné jako „**Objednatel**“

a

Aricoma Systems a.s.
Sídlo: Hornopolní 3322/34, Moravská Ostrava, 702 00 Ostrava
Korespondenční adresa: Teslova 1202/3, 301 00 Plzeň
IČO: 04308697
DIČ: CZ04308697
jednající: Ladislav Kocour
Bankovní spojení: Česká spořitelna a.s.
Číslo účtu: 6563752/0800
kontaktní osoba: Tomáš Makula
tel./fax kontaktní osoby: +420 602 717 377
e-mail: Tomas.Makula@autocont.cz
zápis ve veřejném rejstříku: OR vedený Krajským soudem v Ostravě, sp. zn. B/11012
na straně druhé jako „**Zhotovitel**“
(Objednatel a Zhotovitel jsou dále společně též označováni jako „**Strany**“ nebo „**Smluvní strany“** nebo kdokoli z nich jednotlivě též „**Strana**“ nebo „**Smluvní strana**“)

uzavírají v souladu s § 1746 odst. 2. a § 2358 a § 2371 a násl. z. č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen „občanský zákoník“), a zákonem č.121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „autorský zákon“) tuto Smlouvu o zabezpečení podpory provozu (dále jen „**Smlouva**“).

Preambule

Předmět veřejné zakázky je spolufinancován Evropskou unií z Integrovaného regionálního operačního programu, 4. výzva IROP - KYBERNETICKÁ BEZPEČNOST – SC 1.1 (PR), název projektu je „Kybernetická bezpečnost města Příbram“, registrační číslo CZ.06.01.01/00/22_004/0000060.

Výběr Zhotovitele plnění dle této Smlouvy byl proveden Objednatelem v nadlimitním zadávacím řízení realizovaného dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**“).

Objednatel vybral v zadávacím řízení veřejné zakázky s názvem " Kybernetická bezpečnost města Příbram" a uveřejněné na Věstníku veřejných zakázek dne 30. 11. 2023 pod ev. číslem Z2023-054369 (dále jen „Veřejná zakázka“) nabídku Zhotovitele na realizaci zakázky vyhodnocenou jako nejvýhodnější.

0. Definice a Úvodní ustanovení

Definice.

Není-li dále výslovně uvedeno jinak, následující termíny jsou definovány v této Smlouvě takto:

„**Nabídka**“ znamená nabídku Zhotovitele doručenou Objednateli v rámci Zadávacího řízení;

„**Dodávky**“ znamenají dodávky a služby poskytované Zhotovitelem Objednateli dle této Smlouvy, specifikované níže v čl. II této Smlouvy;

„**Software**“ znamená veškeré systémové a aplikační programové vybavení, potřebné k řádnému, plně funkčnímu, nepřetržitému a bezporuchovému fungování předmětu plnění, které bude předmětem Dodávek;

„Právní předpisy“ znamená všechny platné a účinné obecně závazné právní předpisy České republiky a EU, a to zejména předpisy související s poskytováním Dodávek dle této Smlouvy;

„Spor“ znamená jakýkoliv spor vzniklý ze Smlouvy nebo v souvislosti s ní;

„Vyšší moc“ znamená mimořádnou událost nebo okolnost, kterou nemohla žádná ze Stran před uzavřením Smlouvy předvídat, která je mimo kontrolu kterékoliv Strany a nebyla způsobena úmyslně nebo z nedbalosti jednáním nebo opomenutím kterékoliv Strany a která podstatným způsobem ztěžuje nebo znemožňuje plnění povinností dle Smlouvy kteroukoliv ze Stran. Takovými událostmi nebo okolnostmi jsou zejména, nikoliv však výlučně, válka, teroristický útok, občanské nepokoje, vzpoura, přítomnost ionizujícího nebo radioaktivního záření, požár, výbuch, záplava či jiné živelné nebo přírodní katastrofy. Výslovně se stanoví, že Vyšší mocí není stávka personálu Zhotovitele ani hospodářské poměry Stran.

„**Důvěrné informace**“ – jedná se zejména o informace, jejichž ochranu upravuje zákona o zpracování osobních údajů a GDPR (osobní údaje zaměstnanců a obchodních partnerů úřadu…), jakož i data o veřejně podporovaných subjektech a elektronické identity zadavatele dle nařízení eIDAS.

„**Smlouva o dílo**“ – smlouva o dílo uzavřená mezi Zhotovitelem a Objednatelem, v souvislosti, s níž Smluvní strany uzavřely tuto Smlouvu a v jejímž rámci vzniklo dílo, jež je předmětem činnosti Zhotovitele dle této Smlouvy.

(B) Výklad

Slova v jednotném čísle rovněž zahrnují množné číslo a slova v množném čísle zahrnují i číslo jednotné.

Ustanovení obsahující slovo „souhlasit“, „souhlas“ nebo „dohoda“ nebo slova podobného významu vyžadují, aby souhlas nebo dohoda byly učiněny písemně.

„Písemný“ nebo „písemně“ znamená psaný rukou, strojem, tištěný, případně zhotovený elektronicky a existující ve formě trvalého záznamu.

Pokud se v textu této Smlouvy vyskytuje spojení „poskytování Dodávek“ a z příslušného ustanovení nevyplývá jinak, rozumí se Dodávkou i zajištění služeb nezbytných pro zajištění funkčnosti předmětu díla dle požadavků Zadávací dokumentace.

Výklad veškerých pojmů a ujednání bude prováděn s ohledem na účel a cíle Veřejné zakázky, na jejímž základě byla uzavřena tato Smlouva, které přímo či nepřímo vyplývají ze Zadávací dokumentace nebo této Smlouvy.

(C) Komunikace mezi Stranami

Kdykoliv se v této Smlouvě vyžaduje vyhotovení nebo vystavení souhlasů, osvědčení, svolení, rozhodnutí, oznámení a žádosti jakoukoliv osobou, tato sdělení musejí být doručena na kontaktní adresy uvedené v čl. XII. a způsobem uvedeným v čl. XIII. této Smlouvy.

Veškerá komunikace podle Smlouvy bude probíhat výlučně v českém nebo slovenském jazyce.

I. Předmět Smlouvy

1.1. Zhotovitel se touto Smlouvou zavazuje poskytovat na svůj náklad a nebezpečí podporu provozu díla specifikovaného v čl. II. této Smlouvy (dále jen „**dílo**“) a Objednatel se zavazuje za poskytované zabezpečení podpory provozu díla zaplatit Zhotoviteli cenu ve výši a za podmínek sjednaných v této Smlouvě.

1.2. Zhotovitel poskytuje Objednateli práva duševního vlastnictví dle čl. XV. této Smlouvy.

1.3. Objednatel je povinen dodaný Software užívat v souladu s touto Smlouvou, v souladu s licenčními podmínkami vlastníka autorských práv k Software, a dle platných zákonných norem. Dodaný Software musí umožňovat zpřístupnění programových produktů za účelem integrace s jinými informačními systémy a to obvyklou formou komunikačního rozhraní například API, webové služby, atp. včetně potřebné dokumentace komunikačního rozhraní. Zhotovitel jako součást plnění zajistí, aby licenční ani technické podmínky možností integrace s dalšími systémy nevytvořily jakékoliv další požadavky na Objednatele.

1.4. Zhotovitel se zavazuje splnit všechna ustanovení Zadávací dokumentace i závazky obsažené v Nabídce.

II. Specifikace plnění

2.1. Předmětem plnění jsou služby spočívající v podpoře provozu provozního informačního portálu.

2.2. Smluvní strany se dohodly, že předmětem této Smlouvy je provedení všech plnění dle přílohy č. 1 - Technické specifikace směřujících k zabezpečení podpory provozu (dále také jen „služby“). Předmětem Smlouvy jsou rovněž činnosti, práce a dodávky, které nejsou v dokladech uvedených v tomto odstavci Smlouvy obsaženy, ale o kterých Zhotovitel věděl nebo podle svých odborných znalostí vědět měl anebo mohl, že jsou k řádnému a kvalitnímu plnění dané povahy třeba, a dále, které jsou s řádným plněním nutně spojeny a vyplývají ze standardní praxe plnění analogického charakteru.

Specifikace předmětu Smlouvy je obsažena zejména v Příloze č. 1 - Technická specifikace.

2.3. Předmět díla bude proveden v rozsahu, způsobem a v jakosti stanovené:

(a) touto Smlouvou;

(b) technickými podmínkami, které jsou jako Příloha č. 1 součástí této Smlouvy;

(c) Návrhem Zhotovitele, které je přílohou č. 2 této Smlouvy;

(d) písemnými pokyny Objednatele řádně podepsanými oprávněným zástupcem Objednatele;

(e) obecně závaznými právními předpisy, normami, zvyklostmi v příslušné oblasti a veškerými podklady předanými Objednatelem Zhotoviteli podle této Smlouvy a případnými pozdějšími změnami shora uvedené dokumentace, které byly vyvolány potřebami zjištěnými v průběhu provádění předmětu díla nebo okolnostmi Smluvními stranami nepředvídanými, rozhodnutími, resp. vyjádřeními veřejnoprávních orgánů s tím, že Objednatel je oprávněn upravit způsob provádění předmětu díla; veškeré požadované změny se však musí týkat následné funkčnosti předmětu díla v kontextu původních požadavků na funkčnost díla ze strany Objednatele a závazných právních předpisů.

2.4. Nepředvídaným plněním se rozumí:

a) plnění svým rozsahem nebo povahou nad rámec plnění dle této Smlouvy, tj. takové plnění Zhotovitele, které nebylo součástí řešení provedení předmětu díla vyplývajícího z této Smlouvy, obecně závazných právních předpisů na provedení předmětu díla touto Smlouvou dohodnutého rozsahu a kvality či ověřené technické praxe; nebo

b) plnění vyvolané zásadní změnou dodávky předmětu díla provedené na základě zvláštního požadavku Objednatele, a to pouze a výlučně po uzavření písemného dodatku k této Smlouvě uzavřeného v souladu se ZZVZ.

Za nepředvídané plnění se nepovažují zejména:

a) plnění jinak splňující podmínky této Smlouvy na nepředvídané práce, o kterých prokazatelně Zhotovitel při podpisu této Smlouvy věděl nebo nemohl nevědět; nebo

b) plnění, jejichž provedení bylo vyvoláno prodlením Zhotovitele s prováděním předmětu díla nebo prodlením s poskytováním s ním spojených plnění, za které Zhotovitel odpovídá; nebo

c) plnění, která jsou důsledkem vadného plnění Zhotovitele, dále i plnění, která jsou v souladu s řešením provedení předmětu díla, a tato pouze zpřesňují.

2.5. Změny předmětu díla, včetně ceny a doby plnění, budou-li změnou ovlivněny, které splňují požadavky článku II. odst. 2.4. této Smlouvy, musí být specifikovány v písemném dodatku k této Smlouvě (uzavřeného v souladu se ZZVZ) a pro Zhotovitele se stanou závaznými vždy ode dne účinnosti příslušného písemného dodatku Smlouvy.

2.6. Zhotovitel je povinen při svém plnění dodržovat a splňovat požadavky všech platných a účinných právních předpisů a technických norem, které se vztahují k předmětu této Smlouvy, a to zejména:

- zákon 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů,
- zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů,
- zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů,
- zákon č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů,
- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

III. Doba a místo plnění

3.1. Smlouva se uzavírá na dobu neurčitou.

3.2. Zahájení poskytování podpory provozu díla nastane po převzetí díla zadavatelem, tj. po uvedení díla do ostrého provozu.

3.3. Místem plnění jsou budovy uvedeny v Příloze č. 1 Smlouvy o dílo.

3.4. Místem předání a převzetí díla je sídlo Objednatele.

IV. Cena a způsob plnění, platební podmínky

4.1. Smluvní strany se dohodly na ceně za provedení předmětu Smlouvy, viz odst. 4.3. Uvedená cena bez DPH je cenou pevnou a nejvýše přípustnou po celou dobu trvání Smlouvy. V případě změny legislativy bude účtována DPH podle platných předpisů.

4.2. V ceně předmětu Smlouvy jsou zahrnuty veškeré náklady Zhotovitele, které při plnění svého závazku dle této Smlouvy vynaloží. Cena předmětu Smlouvy nebude po dobu do ukončení této Smlouvy předmětem zvýšení, není-li dále stanoveno jinak. Zhotovitel prohlašuje, že všechny technické, finanční, věcné a ostatní podmínky díla zahrnul do kalkulace ceny předmětu Smlouvy. Zhotovitel výslovně prohlašuje, že součástí ceny předmětu Smlouvy jsou i veškeré náklady spojené se splněním podmínek pro realizaci předmětu Smlouvy dle obecně závazných právních předpisů.

4.3. Objednatel uhradí cenu předmětu Smlouvy následovně:

a) Cena za poskytování služeb základní podpory provozu bude uhrazena **vždy po ukončení kalendářního měsíce, ve kterém byly zajištěny služby podpory provozu**. V případě, že v daném

kalendářním měsíci nebylo poskytování služeb podpory provozu zajištěno po celé období, bude cena vypočtena jako podíl z nabídkové (měsíční) ceny za podporu provozu a období, po které bylo poskytování služeb podpory provozu skutečně zajištěno.

Nabídková cena za základní servisní podporu				
Základní servisní podpora - služby	Cena v Kč bez DPH za 1. - 12. měsíc	Cena v Kč bez DPH za 13. - 24. měsíc	Cena v Kč bez DPH za 25. – 36. měsíc	Cena v Kč bez DPH za 37. – 48. měsíc a další následující měsíce účinnosti smlouvy
Cena celkem za 1 měsíc základní servisní podpory	*15 000 (jedná se o cenu v Kč bez DPH za 1 měsíc)*	*15 000 (jedná se o cenu v Kč bez DPH za 1 měsíc)*	*15 000 (jedná se o cenu v Kč bez DPH za 1 měsíc)*	*15 000 (jedná se o cenu v Kč bez DPH za 1 měsíc)*

b) Cena za poskytnutí služeb rozšířené podpory provozu, bude uhrazena na základě objemu skutečně poskytnutých služeb, vždy po ukončení kalendářního měsíce, ve kterém byli tyto služby poskytnuty. Výpočet ceny bude proveden jako součin objemu skutečně poskytnutých v hodinách (s přesností na desetiny) a hodinové sazba ve výši *2 000* Kč bez DPH.

4.4. Cena dle předchozího odstavce bude uhrazena na základě Zhotovitelem vystaveného daňového dokladu - faktury.

Faktura bude vystavena se splatností 30 kalendářních dní ode dne doručení Objednateli. Smluvní strany se vzájemně dohodly, že daň z přidané hodnoty bude Zhotovitelem účtována v sazbách dle právních předpisů platných v době uskutečnitelného zdanitelného plnění pro to které účtované dílčí plnění dle předchozího odstavce.

Faktura bude vystavena vždy za každý kalendářní měsíc realizovaného plnění, a to nejpozději do 5 pracovních dní od konce kalendářního měsíce, za který je faktura vystavena.

Každá faktura vystavená Zhotovitelem dle této Smlouvy musí obsahovat pojmové náležitosti daňového dokladu stanovené zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů a zákonem č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, a dále následující údaje:

- název a registrační číslo projektu dle Preambule této Smlouvy
- číslo Smlouvy
- identifikaci Objednatele podle Smlouvy
- identifikaci Zhotovitele podle Smlouvy
- označení banky a číslo účtu, na který má být platba zaplacena, včetně konstantního a variabilního symbolu
- den splatnosti a den uskutečnění zdanitelného plnění
- název a popis poskytnutých služeb s odkazem na Smlouvu
- účtovanou částku bez DPH
- vyčíslenou částku DPH
- celkovou částku včetně DPH
- jakékoliv další údaje vyžadované pro účetní a daňový doklad příslušnými Právními předpisy

V případě, že daňový doklad nebude obsahovat uvedené údaje či bude neúplný či nebude mít všechny přílohy, není Objednatel povinen na jeho základě plnit a nedostává se do prodlení. Zhotovitel je

povinen takový daňový doklad opravit, aby splňoval podmínky stanovené touto Smlouvou. Lhůta splatnosti běží znovu od doručení nové nebo opravené faktury.

Objednatelem podepsaný předávací protokol nezbavuje Zhotovitele odpovědnosti za řádné provedení předmětu díla jako celku bez vad a nedodělků.

4.5. Strany se dohodly, že Objednatel je oprávněn požadovat po Zhotoviteli bližší vysvětlení, objasnění nebo zdůvodnění částek obsažených ve fakturách, a to na základě písemné výzvy adresované Zhotoviteli. Od okamžiku odeslání písemné výzvy k objasnění do prokázání oprávněnosti požadovaných plateb se lhůta splatnosti faktury prodlužuje.

4.6. Objednatel je oprávněn ponížit Zhotovitelem fakturovanou úhradu ceny o jakékoliv případné smluvní pokuty, náhrady škod a další platby splatné ve prospěch Objednatele vůči Zhotoviteli. Pouze Objednatel je oprávněn započíst jakékoliv své splatné pohledávky dle Smlouvy vůči pohledávkám Zhotovitele.

4.7. Pokud Zhotovitel poruší povinnosti ze Smlouvy podstatným způsobem, je Objednatel oprávněn pozastavit jakoukoliv platbu na základě faktury až do odstranění prodlení nebo porušení povinnosti Zhotovitele.

4.8. Veškeré změny, doplňky nebo rozšíření, které nejsou součástí předmětu díla dle Smlouvy nebo Smlouvy o dílo, musí být vždy před jejich realizací písemně odsouhlaseny Objednatelem, formou odsouhlasení požadavku Objednatelem v systému HelpDesk. Objednatel zadá požadavek na doplňky nebo rozšíření, které nejsou součástí předmětu díla dle Smlouvy nebo Smlouvy o dílo prostřednictvím systému HelpDesk nebo kontaktních osob a Zhotovitel Objednateli zpracuje nacenění v podobě časové náročnosti splnění daného požadavku dle jednotkové sazby za poskytnutí služeb rozšířené podpory provozu, jak je uvedena v odst. 4.3 Smlouvy. Provedené úpravy de odsouhlaseného nacenění pak budou fakturovány v souladu s tímto článkem dle skutečně odvedené práce. Pokud Zhotovitel provede některé z těchto prací bez předchozího písemného odsouhlasení Objednatelem, má Objednatel právo odmítnout jejich úhradu a cena za jejich provedení je součástí ceny za provedení předmětu díla.

4.9. Úhrada ceny za provedení předmětu díla, ať již jako celku či dílčích plnění, nemá vliv na možnost uplatnění práva Objednatele z vad předmětu díla.

4.10. Zhotovitel je oprávněn jednou během kalendářního roku, nejdříve však za jeden rok od účinnosti této Smlouvy, vyvolat jednání o navýšení cen uvedených v odst. 4.3 Smlouvy, s odkazem na nárůst inflace vztahující se k předmětu plnění Smlouvy, pokud bude meziroční růst přesahovat 3 %. Inflací se rozumí meziroční inflace měřená vzrůstem úhrnného indexu spotřebitelských cen zboží a služeb, kterou udává každým kalendářním rokem Český statistický úřad za rok předcházející vyjádřená v procentech, kdy dojednaná nová cena (měsíční paušál a hodinová sazba) je limitována právě růstem inflace. Zhotovitel je povinen v rámci tohoto jednání předložit podrobnou kalkulaci prokazující jeho růst nákladů a ospravedlňující jeho žádost o navýšení cen, a Objednatel je povinen se tímto návrhem zabývat.

V. Součinnost smluvních stran

5.1. Smluvní strany se zavazují vyvinout veškeré úsilí k vytvoření potřebných podmínek pro realizaci díla dle podmínek stanovených touto Smlouvou, které vyplývají z jejich smluvního postavení. To platí i v případech, kde to není výslovně stanoveno ustanovením této Smlouvy.

5.2. Pokud jsou kterékoli ze Smluvních stran známy skutečnosti, které jí budou bránit, aby dostála svým smluvním povinnostem, sdělí tuto skutečnost neprodleně písemně druhé Smluvní straně. Smluvní strany se dále zavazují neprodleně odstranit v rámci svých možností všechny okolnosti, bránící z její strany splnění jejich smluvních povinností.

5.3. Zhotovitel se zavazuje, že na základě skutečností zjištěných v průběhu plnění povinností dle této Smlouvy navrhne a provede opatření směřující k dodržení podmínek stanovených touto Smlouvou pro naplnění Smlouvy, k ochraně Objednatele před škodami, ztrátami a zbytečnými výdaji a že poskytne Objednateli, zástupci Objednatele jednajícímu ve věcech technických a jiným osobám zúčastněným na provádění díla veškeré potřebné doklady, konzultace, pomoc a jinou součinnost.

5.4 Zhotovitel je podle ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů, osobou povinou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou zboží nebo služeb z veřejných výdajů.

VI. Prohlášení, práva a závazky smluvních stran

6.1. Zhotovitel prohlašuje, že ke dni podpisu Smlouvy:

(a) není jako právnická osoba v likvidaci;

(b) není proti němu vedeno konkursní řízení ani vyrovnací řízení ve smyslu zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení, ve znění pozdějších předpisů (dále jen „insolvenční zákon“) a takové řízení nebylo zastaveno či zrušeno z důvodu nedostatku majetku Zhotovitele a dále není předlužen či neschopen plnit své splatné závazky vůči svým věřitelům;

(c) uzavření/m této Smlouvy:

- neporuší správní rozhodnutí orgánu státní správy České republiky;
- neporuší ustanovení žádné dohody, Smlouvy či jiného ujednání, které uzavřel se třetí osobou;
- nebude mít za následek újmu nebo požadavek na splacení jakéhokoli správního poplatku, dotací nebo jiného závazku Zhotovitele;

(d) neučinil nic, ať již sám anebo za spolupráce či prostřednictvím třetí osoby, co by omezilo či znemožnilo dosažení účelu této Smlouvy;

(e) není osobou, na kterou by se vztahovaly sankce související s nařízením Rady (EU) 2022/576 ze dne 8. dubna 2022 kterým se mění nařízení (EU) č. 833/2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině a že splňuje požadavky uvedené v článku 5k odst. 1 písm. a) – c) výše uvedeného Nařízení.

6.2. Zhotovitel se zavazuje, že Objednateli bezodkladně po vzniku takové skutečnosti písemně oznámí:

(a) podání návrhu na prohlášení konkursu na majetek Zhotovitele dle insolvenčního zákona; nebo

(b) podání návrhu na vyrovnání na majetek Zhotovitele dle insolvenčního zákona; nebo

(c) vstup Zhotovitele do likvidace; nebo

(d) splnění podmínek prohlášení konkursu na majetek Zhotovitele, tj. zejména že Zhotovitel je předlužen anebo insolventní; nebo

(e) rozhodnutí o provedení přeměny Zhotovitele, zejména fúzí, převodem jmění na společníka či rozdělením, provedení změny právní formy Zhotovitele či provedení jiných organizačních změn; nebo

(f) omezení či ukončení činnosti Zhotovitele, která bezprostředně souvisí s předmětem této Smlouvy; nebo

(g) všechny skutečnosti, které by mohly mít vliv na přechod či vypořádání závazků Zhotovitele vůči Objednateli vyplývajících z této Smlouvy či s touto Smlouvou souvisejících; nebo

(h) rozhodnutí o zrušení Zhotovitele.

6.3. Zhotovitel prohlašuje, že

(a) je odborně způsobilý ke splnění všech svých závazků podle této Smlouvy, a to s ohledem na předmět plnění, se kterým se náležitě seznámil, a že

(b) před podpisem této Smlouvy se řádně seznámil a překontroloval předané materiální podklady a dokumentaci a řádně prověřil místní podmínky a všechny nejasné podmínky pro realizaci díla či jeho části si vyjasnil s Objednatelem nebo místním šetřením,

(c) Smlouva byla Zhotovitelem řádně schválena a podepsána a zakládá platný závazek Zhotovitele, vynutitelný vůči němu v souladu s podmínkami v ní uvedenými,

(d) podpisem ani plněním Smlouvy Zhotovitel neporušuje žádné ustanovení svých zakladatelských dokumentů ani žádnou jinou smlouvu nebo ujednání, jehož je Zhotovitel stranou, nebo kterým je Zhotovitel nebo jeho majetek vázán, ani žádný zákon či jiný právní předpis nebo rozhodnutí státního orgánu,

(e) podle nejlepšího vědomí Zhotovitele proti němu neprobíhá žádné soudní, rozhodčí ani správní řízení, které by mohlo negativně ovlivnit platnost, účinnosti nebo vymahatelnost Smlouvy nebo plnění jakýchkoliv povinností Zhotovitele podle této Smlouvy, ani nehrozí zahájení žádného takového řízení.

6.4. Zhotovitel se zavazuje:

(a) při provádění předmětu díla postupovat s odbornou péčí a dodržovat Právní předpisy a rozhodnutí orgánů veřejné správy,

(b) udržovat a obnovovat po celou dobu účinnosti této Smlouvy veškeré nezbytné souhlasy, povolení, oprávnění či licence potřebné k řádnému poskytování Dodávek v souladu s Právními předpisy, přičemž Zhotovitel odškodní Objednatele v případě, že tak Zhotovitel opomněl nebo opomene kdykoliv v průběhu trvání Smlouvy učinit.

6.5. Objednatel je oprávněn postoupit jakákoliv práva a povinnosti z této Smlouvy na kteroukoliv třetí osobu, s čímž Zhotovitel podpisem Smlouvy vyslovuje svůj souhlas.

6.6. Zhotovitel se zavazuje uhradit Objednateli do deseti dnů poté, kdy k tomu bude Objednatelem písemně vyzván, veškeré pokuty či další sankce, které byly Objednateli vyměřeny (pravomocným rozhodnutím) státními orgány v souvislosti s porušením povinností Zhotovitele stanovených touto Smlouvou či obecně závaznými právními předpisy při provádění předmětu díla nebo uspokojit veškeré nároky třetích osob, o kterých bude pravomocně rozhodnuto příslušným orgánem veřejné moci, jež vznikly v souvislosti s porušením povinností Zhotovitele stanovených touto Smlouvou či obecně závaznými právními předpisy při provádění předmětu díla. Úhrada bude provedena na účet Objednatele uvedený v záhlaví této Smlouvy.

6.7. Objednatel neudělil Zhotoviteli žádné oprávnění uzavírat pracovně právní či jiné vztahy jménem Objednatele nebo jednat jménem Objednatele.

6.8 Zhotovitel se zavazuje, že pokud pro plnění díla použije třetí osoby v jiném než pracovněprávním vztahu, tak s takovými osobami ošetří veškeré vztahy a zejména autorská práva tak, aby tyto třetí osoby nemohly vznášet jakékoli nároky vůči Objednateli. Zhotovitel je povinen na základě výzvy Objednatele předložit seznam osob, které se na plnění díla podíleli spolu se specifikací právního vztahu, na základě kterého tak činily, a současně prokázat splnění povinnosti podle předchozí věty. V případě, že Zhotovitel tuto skutečnost na základě písemné výzvy Objednatele do 30 dní od doručení výzvy Zhotoviteli nedoloží, zavazuje se zaplatit Objednateli smluvní pokutu ve výši 1 000 Kč za každý i započatý den prodlení.

6.9. Objednatel prohlašuje, že podpisem ani plněním Smlouvy Objednatel neporušuje žádné ustanovení svých zakladatelských dokumentů ani žádnou jinou smlouvu nebo ujednání, jehož je Objednatel stranou, nebo kterým je Objednatel nebo jeho majetek vázán, ani žádný zákon či jiný právní předpis nebo rozhodnutí státního orgánu.

VII. Nebezpečí škody

7.1. Objednatel zodpovídá za škodu, způsobenou na zapůjčeném zařízení, které je v majetku Zhotovitele a toto zařízení bylo zapůjčeno Objednateli.

7.2. Objednatel je povinen provádět bezpečnostní zálohy dat v souladu s pravidly běžnými pro nakládání s daty v informačních systémech. Zhotovitel nenese odpovědnost za ztrátu nebo poškození dat nebo datových struktur Objednatele, s výjimkou případu, že k nim prokazatelně došlo při užívání plnění dodaného Zhotovitelem, na které se vztahuje záruka. Zhotovitel nepřebírá žádné záruky ani odpovědnost za data uložená v paměťových médiích.

VIII. Podmínky provádění plnění

8.1. Zhotovitel se zavazuje:

a) zajistit provádění předmětu díla tak, aby provádění předmětu Smlouvy v co nejmenší míře omezovalo činnost Objednatele;

b) zajistit provádění předmětu díla tak, aby provádění předmětu díla bylo prováděno pod odborným dozorem Zhotovitele, který bude garantovat dodržování postupů nabídnutých Zhotovitelem v Nabídce nebo postupů dohodnutých s Objednatelem v průběhu plnění; totéž platí pro práce poddodavatelů;

c) neprodleně, nejpozději však do tří dnů, písemně oznámit Objednateli veškeré skutečnosti a okolnosti, které při poskytování Dodávek zjistil nebo se o nich dozvěděl a které mohou mít vliv na poskytování plnění;

d) vyvstane-li v průběhu provádění předmětu Smlouvy nutnost upřesnění způsobu jeho provedení, neprodleně si vyžádat předchozí písemný souhlas či pokyn Objednatele;

e) písemně upozornit Objednatele na nevhodnost, případně nepřípustnost podkladových materiálů, pokynů a věcí, které mu byly předány Objednatelem nebo Objednatelem požadovaných změn, ať již z hlediska důsledků pro jakost a provedení předmět Smlouvy či rozporu s podklady pro uzavření této Smlouvy, ustanoveními nebo rozhodnutími orgánů veřejné správy či obecně závaznými právními předpisy či jinými normami, a to bezodkladně poté, co tuto skutečnost zjistí či mohl zjistit. V případě, že Objednatel bude, i přes upozornění Zhotovitele, písemně trvat na užití podkladových materiálů, pokynů a věcí, které byly Zhotoviteli předány Objednatelem, je Zhotovitel oprávněn odmítnout jejich plnění pouze tehdy, pokud by se jejich splněním mohl vystavit správnímu či trestnímu postihu;

f) vždy předkládat návrhy veškerých písemných podkladů a dokumentů souvisejících s poskytováním plnění, nestanovuje-li Zadávací dokumentace či dohoda stran jinak

g) seznámit se s riziky na pracovištích, resp. v místě plnění v sídle Objednatele, vnitřními firemními předpisy a informacemi, které mají vliv na BOZP a PO na daném pracovišti, kde provádí smluvenou činnost. Dále si je Zhotovitel vědom své povinnosti dostatečně a bez zbytečného odkladu informovat všechny zúčastněné pracovníky vlastní organizace (případně odborovou organizaci či zástupce zaměstnanců pro oblast BOZP, a nepůsobí-li u nich, přímo své zaměstnance) o rizicích a přijatých opatřeních, které získal.

8.2. Zhotovitel bude svým jménem projednávat a hradit náklady vyplývající z projednaných záležitostí přímo souvisejících s jeho činností při realizaci předmětu díla a dokončení předmětu díla, které jsou v jeho kompetenci a za které plně odpovídá.

Zhotovitel na sebe přejímá zodpovědnost za škody způsobené všemi osobami zúčastněnými na provádění předmětu díla na straně Zhotovitele, stejně tak za škody způsobené svou činností Objednateli nebo třetím osobám.

Zhotovitel není oprávněn postoupit jakákoliv práva anebo povinnosti z této Smlouvy na třetí osoby bez předchozího písemného souhlasu Objednatele.

Zhotovitel je povinen:

a) zajistit a financovat veškeré poddodavatelské práce a nese za ně záruku vůči Objednateli v plném rozsahu dle této Smlouvy,

b) zajistit, aby všichni poddodavatelé měli platná příslušná oprávnění, koncese, certifikace, licence a rovněž odbornou kvalifikaci a dostatek odborných zkušeností, jež jsou nezbytné pro poskytování příslušných částí Dodávek dle jejich smluv se Zhotovitelem,

c) jednat s poddodavateli v souladu se zásadami poctivého obchodního styku tzn. zejména uhradit poddodavatelům sjednanou cenu za řádné a včasné poskytnutí příslušných částí Dodávek,

d) dodržet požadavek týkající se identifikace poddodavatelů, kteří se mají zapojit do realizace předmětu plnění, a to před zahájením plněním služeb ze strany těchto poddodavatelů.

8.3. Zhotovitel se zavazuje reagovat na nahlášené chyby funkčnosti či požadavky na servisní zásah v časech dle definovaných skupin incidentů a též zahajovat a ukončovat odstraňování uvedených chyb funkčnosti a uvedené servisní zásahy.

8.4. Objednatel je oprávněn:

a) sám či prostřednictvím třetí osoby vykonávat v místě provádění předmětu díla dozor Objednatele a v jeho průběhu zejména sledovat, zda jsou práce prováděny podle Smlouvy a právních předpisů;

b) pokud Zhotovitel nesplní jakoukoliv povinnost podle této Smlouvy a nesplní ji ani v dodatečné lhůtě stanovené touto Smlouvou, je Objednatel, aniž by tím byla dotčena jakákoliv jiná práva a nároky Objednatele dle této Smlouvy, oprávněn, nikoliv však povinen, podle svého uvážení splnit povinnost Zhotovitele nebo pověřit splněním této povinnosti jiné osoby na náklady Zhotovitele,

c) po Zhotoviteli požadovat, aby pro splnění Smlouvy nevyužíval člena týmu Zhotovitele, který prokazatelně:

- plní své povinnosti nekompetentně nebo nedbale, nebo

- neplní nebo porušuje některá ustanovení této Smlouvy nebo právních předpisů,

přičemž takový člen týmu Zhotovitele musí být po výzvě Objednatele bez zbytečného odkladu nahrazen jiným členem s odpovídající kvalifikací.

8.6. Pokud dojde v průběhu plnění předmětu Smlouvy k výměně zařízení, např. z důvodu skončení jeho životnosti, bude plnění předmětu Smlouvy pokračovat příslušnou aktualizací provozní dokumentace, případně katalogových listů či jiné pořizované dokumentace.

IX. Záruka za jakost

9.1. Na poskytované služby poskytuje Zhotovitel záruku v délce 3 měsíců.

X. Smluvní pokuty a úrok z prodlení, odpovědnost za škodu

10.1. Smluvní strany se dohodly na tom, že v případě porušení ustanovení čl. VIII. odst. 8.3. této Smlouvy Zhotovitelem je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 10 % (deseti procent) z měsíční platby za podporu provozu v Kč bez DPH za každé jedno porušení povinnosti v měsíci..

10.2. V případě, kdy nastane některá ze situací uvedených v čl. XI. odst. 11.4. písm. a) až c) této Smlouvy je Zhotovitel povinen zaplatit smluvní pokutu ve výši 10 000 Kč (slovy: deset tisíc korun českých), a to za každý jednotlivý případ. Oprávnění požadovat smluvní pokutu není podmíněno přistoupením Objednatele k výpovědi či odstoupení od Smlouvy. Tím není dotčen nárok Objednatele na náhradu škody.

10.3. V případě, kdy nastane některá ze situací uvedených v čl. XVI. odst. 16.6. je Zhotovitel povinen zaplatit smluvní pokutu ve výši 100 000 Kč (slovy: stotisíc korun českých), a to za každý jednotlivý případ. Úhradou smluvní pokuty není dotčen nárok Objednatele na náhradu škody.

10.4. Smluvní strany se dohodly na tom, že v případě prodlení s úhradou odměny dle ustanovení čl. IV. této Smlouvy je Objednatel povinen uhradit Zhotoviteli úrok z prodlení ve 0,1 % (slovy: jedna desetina procenta) z nezaplacené částky v Kč bez DPH za každý den prodlení.

10.5. Smluvní pokuta je splatná do 21 dní ode dne, kdy byla povinné straně doručena písemná výzva k jejímu zaplacení ze strany oprávněné strany, a to na účet oprávněné strany uvedený v písemné výzvě, případně může být smluvní pokuta uhrazena i formou poskytnutí slevy z částky měsíční splátky za poskytování podpory provozu. Ustanovením o smluvní pokutě není dotčeno právo oprávněné strany na náhradu škody v plné výši s tím, že zaplacená smluvní pokuta se na úhradu škody nezapočítává. Případným odstoupení od Smlouvy nárok na úhradu smluvní pokuty nezaniká. Zhotovitel dává Objednateli výslovný souhlas k případnému zápočtu vzájemných pohledávek.

10.6. V případě, že porušením povinnosti Zhotovitele podle této Smlouvy vznikne Objednateli škoda, jejímž důsledkem bude odejmutí dotace nebo její části poskytovatelem dotačního titulu, odpovídá Zhotovitel Objednateli za škodu až do výše finančního postihu ze strany poskytovatele dotačního titulu uplatněného vůči Objednateli a Zhotovitel se zavazuje tuto škodu Objednateli nahradit, a to na písemnou výzvu Objednatele se splatností 21 dní ode dne doručení výzvy Zhotoviteli. Případným odstoupení od Smlouvy nárok na odškodnění dle tohoto odstavce nezaniká. Zhotovitel dává Objednateli výslovný souhlas k případnému zápočtu vzájemných pohledávek.

XI. Ukončení Smlouvy

11.1. Smluvní strany se dohodly, že tuto Smlouvu mohou ukončit pouze za podmínek dále upravených v této Smlouvě a nebo v případech, které stanoví zákon.

11.2. Výpovědí nejsou dotčena práva a povinnosti stran vzniklé před účinností ukončení Smlouvy.

11.3. Výpověď ze strany Objednatele – Objednatel je oprávněn tuto Smlouvu vypovědět s účinky výpovědi k okamžiku doručení oznámení Zhotoviteli v těchto případech:

a) Zhotovitel poruší povinnost z této Smlouvy zvlášť závažným způsobem, a to zejména neplnění parametrů servisních služeb podle přílohy č. 1 Smlouvy o dílo (Technická specifikace),

b) Zhotovitel porušil některou ze svých povinností uvedených v čl. VIII. Smlouvy;

c) Zhotovitel porušil některý ze svých závazků dle čl. VI. odst. 6.2. Smlouvy nebo se ukáže nepravdivým, neúplným či zkresleným některé z prohlášení Zhotovitele dle čl. VI. odst. 6.1. této Smlouvy,

d) Zhotovitel poruší povinnost mlčenlivosti dle čl. XVI. odst. 16.6. této Smlouvy,

e) Zhotovitel přestane být subjektem oprávněným poskytovat Dodávky dle této Smlouvy,

f) Zhotovitel nebo jeho poddodavatel bude identifikován jako osoba definovaná v článku 5k odst. 1 písm. a) – c) nařízení (EU) č. 833/2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině.

11.4. V případě ukončení této Smlouvy výpovědí dle odstavce11.3. ze strany Objednatele vzniká Objednateli vůči Zhotoviteli nárok na úhradu prokázaných vícenákladů (tj. nákladů vynaložených Objednatelem nad cenu za provedení předmět díla) vynaložených na dokončení předmětu Smlouvy třetí osobou a na úhradu škod vzniklých prodlením se splněním předmětu Smlouvy. Nárok Objednatele účtovat Zhotoviteli smluvní pokutu tím nezaniká.

11.5. Výpověď Smlouvy ze strany Objednatele – jestliže Zhotovitel poruší některou povinnost podle Smlouvy, může Objednatel oznámením vyzvat Zhotovitele, aby toto porušení napravil v přiměřené lhůtě stanovené jednoznačně Objednatelem s tím, že taková lhůta nesmí být kratší než patnáct (15) dnů. Objednatel je oprávněn Smlouvu vypovědět s výpovědní lhůtou alespoň tři (3) měsíce, jež počíná běžet prvního dne měsíce následujícího po měsíci, ve kterém byla výpověď doručena Zhotoviteli, pokud:

a) Zhotovitel poruší povinnost z této Smlouvy jiným než zvlášť závažným způsobem a neprovede nápravu takového porušení povinností ani v dodatečné lhůtě stanovené Objednatelem,

b) opakovaně dojde k tomu, že Zhotovitel neodstraní výpadek poskytování služeb bez zbytečného prodlení.

11.6. Rozhodnutí Objednatele vypovědět tuto Smlouvu není na újmu jakýmkoli dalším právům Objednatele vyplývajícím ze Smlouvy, právních předpisů nebo vzniklým z jiného titulu.

11.7. Výpověď Smlouvy ze strany Zhotovitele – Zhotovitel je oprávněn tuto Smlouvu vypovědět s výpovědní lhůtou 3 měsíců, jež počíná běžet prvního dne měsíce následujícího po měsíci, ve kterém byla výpověď doručena Objednateli, pokud je Objednatel v prodlení s platbou Zhotoviteli podle čl. IV této Smlouvy po dobu delší než 60 dnů od data splatnosti.

11.8. Kterákoliv Smluvní strana je oprávněna vypovědět tuto Smlouvu i bez udání důvodu s výpovědní lhůtou 6 měsíců, jež počíná běžet prvního dne měsíce následujícího po měsíci, ve kterém byla výpověď doručena druhé Smluvní straně.

11.9. Rozhodnutí Zhotovitele vypovědět tuto Smlouvu není na újmu jakýmkoli dalším právům Zhotovitele vyplývajícím ze Smlouvy.

XII. Adresy pro doručování

12.1. Smluvní strany této Smlouvy se dohodly následujícím způsobem na adrese pro doručování písemné korespondence:

(a) adresa pro doručování Objednateli je: Tyršova 108, 261 01 Příbram, mail: e-podatelna@pribram.eu, datová schránka: 2ebbrqu.

(b) adresa pro doručování Zhotoviteli je: Teslova 1202/3, 301 00 Plzeň,

datová schránka: ctb7phe.

12.2. Smluvní strany se dohodly, že v případě změny sídla, a tím i adresy pro doručování, budou písemné informovat o této skutečnosti bez zbytečného odkladu druhou Smluvní stranu. Do doby nové adresy doručování se doručuje na stávající adresy.

XIII. Doručování

13.1. Smluvní strany se dohodly, že doručovat si budou zejména prostřednictvím datových schránek. Jiným způsobem (osobně nebo prostřednictvím držitele poštovní licence) je doručování možné pouze v případě, že je to vzhledem ke všem okolnostem vhodnější a doručování prostřednictvím datové schránky není možné (z důvodu času nebo věcně). Smluvní strany jsou povinné udržovat nastavení své datové schránky tak, aby doručování běžných písemností v souvislosti s touto Smlouvou umožňovaly (viz § 18a odst. 1 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů). Smluvní strany jsou dále povinny zajistit, aby se do datové schránky přihlásila oprávněna osoba od podpisu této Smlouvy minimálně každý třetí pracovní den. Porušení této povinnosti má pro účely této Smlouvy za následek, že zásilka platí za odmítnutou, resp. že bylo doručení zmařeno.

13.2. Aniž by tím byly dotčeny další prostředky, kterými lze prokázat doručení, má se za to, že oznámení bylo řádně doručené:

a) při doručování osobně:

- dnem faktického přijetí oznámení příjemcem; nebo
- dnem, v němž bylo doručeno osobě na příjemcově adrese určené k přebírání listovních zásilek; nebo
- dnem, kdy bylo doručováno osobě na příjemcově adrese určené k přebírání listovních zásilek, a tato osoba odmítla listovní zásilku převzít; nebo
- dnem, kdy příjemce při prvním pokusu o doručení zásilku z jakýchkoli důvodů nepřevzal či odmítl zásilku převzít, a to i přesto, že se v místě doručení nezdržuje, pokud byla na zásilce uvedena adresa pro doručování dle čl. XII. odst. 12.1., resp. 12.2. této Smlouvy.

b) při doručování prostřednictvím držitele poštovní licence:

- se má za to, že došlá zásilka odeslaná s využitím provozovatele poštovních služeb došla třetí pracovní den po odeslání, byla-li však odeslána na adresu v jiném státu, pak patnáctý pracovní den po odeslání, a to doručování na adresy pro doručování dle čl. XII. odst. 12.1., resp. 12.2. této Smlouvy.

c) při doručování do datové schránky:

- okamžikem přihlášení oprávněné osoby do datové schránky,
- pro případ, že se do datové schránky oprávněná osoba nepřihlásí ani čtvrtý pracovní den od dodání zprávy do datové schránky platí, že zásilka je doručena pátým pracovním dnem od odeslání analogicky podle § 570 věta za středníkem občanského zákoníku pro zmaření doručení.

13.3. Pro vyloučení pochybností smluvní strany uvádějí, že oznamování závad a jiných incidentů a další komunikaci související s poskytováním podpory při jejich řešení bude probíhat prostřednictvím systému typu Helpdesk v souladu s přílohou č. 1 Smlouvy o dílo – Technická specifikace. Pro tuto komunikaci se ostatní ustanovení tohoto čl. XIII. neuplatní.

XIV. Společná ustanovení

Pokud není v předchozích částech této Smlouvy uvedeno něco jiného, vztahují se na ně příslušné články společných ustanovení.

14.1. Smluvní strany se dohodly na tom, že jakákoliv peněžitá plnění dle Smlouvy jsou řádně a včas splněna, pokud byla příslušná částka odepsána z účtu povinné strany ve prospěch účtu oprávněné smluvní strany (věřitele) nejpozději v poslední den splatnosti.

14.2. V případě Sporů souvisejících se Smlouvou se Smluvní strany vždy pokusí o smírné řešení. Nedojde-li k takovému řešení a není-li dále uvedeno jinak, rozhodne o sporu místně a věcně příslušný soud Objednatele.

14.3. Smluvní strany se zavazují:

(a) vzájemně včas a řádně informovat o všech podstatných skutečnostech, které mohou mít vliv na plnění dle této Smlouvy,

(b) vyvinout potřebnou součinnost k plnění této Smlouvy.

14.4. Pokud kterékoliv ustanovení této Smlouvy nebo jeho část bude neplatné či nevynutitelné, anebo se stane neplatným či nevynutitelným nebo bude shledáno neplatným či nevynutitelným soudem či jiným příslušným orgánem, pak tato neplatnost či nevynutitelnost nebude mít vliv na platnost či vynutitelnost ostatních ustanovení Smlouvy nebo jejich částí.

14.5. Tato Smlouva může být měněna nebo doplňována pouze písemnými oboustranně odsouhlasenými, a průběžně číslovanými dodatky, podepsanými oprávněnými zástupci obou Smluvních stran, které musí být obsaženy na jedné listině.

14.6. Přílohy uvedené v textu této Smlouvy a sumarizované v závěrečných ustanoveních Smlouvy tvoří součást Smlouvy.

14.7. Žádná Strana neuděluje druhé Straně právo užívat její ochranné známky či jiná označení (včetně ochranných známek či označení v rámci podniku) pro účely propagace nebo publikování bez předchozího písemného souhlasu druhé Strany.

14.8. Smlouva nezakládá žádné zastoupení, společný podnik nebo partnerství mezi Objednatelem a Zhotovitelem. Obě Strany mohou svobodně uzavírat obdobné Smlouvy s jinými stranami za účelem vývoje, nákupu či poskytování konkurenčních produktů a služeb.

14.9. Žádný z vedoucích projektu či zaměstnanců nebo konzultantů kterékoliv z obou Stran není oprávněn poskytovat záruky třetím stranám, které nejsou součástí Smlouvy a obě strany prohlašují, že se nespoléhaly na žádná taková ústní či písemná prohlášení při poskytování záruk, s výjimkou oprávněných statutárních zástupců obou Stran.

14.10. Obě Strany svým podpisem potvrzují, že tuto Smlouvu četly, rozumí jí a souhlasí s tím, že budou jejími podmínkami vázány. Dále souhlasí, že tato Smlouva nahrazuje jakékoliv předchozí dohody mezi Stranami a je nadřazena všem předchozím návrhům ústním či písemným a veškeré další komunikaci mezi oběma Stranami vztahující se k předmětu Smlouvy.

14.11. Žádná ze Stran neuveřejní bez předchozího písemného souhlasu druhé Strany žádné prohlášení týkající se této Smlouvy.

14.12. Pokud není uvedeno jinak, není ani jedna ze Stran oprávněna jednat jménem druhé Strany či zastupovat druhou Stranu jakýmkoliv způsobem při smluvních jednáních.

XV. Autorské právo a ochrana duševního vlastnictví

15.1. Veškerá data zpracovávaná při poskytování služeb dle této Smlouvy jsou ve vlastnictví Objednatele; tedy Objednatel je dle dohody stran pořizovatelem příslušných databází ve smyslu § 89 autorského zákona.

15.2. Pro předměty práv duševního vlastnictví, jež Zhotovitel předá Objednateli nebo jinak použije při plnění této Smlouvy, se použijí ustanovení čl. XVI Smlouvy o dílo obdobně, vč. souvisejících práv a povinností, zejm. povinnosti předat související dokumentaci a zdrojový kód, udělení souhlasu se zásahy do předmětů práv duševního vlastnictví, ošetření případných práv třetích osob, předání komponentů „Individualizovaného software“ v rozsahu nezbytném pro další rozvoj díla a informací o použitém „Individualizovaném software“ a souvisejících licenčních podmínkách.

15.3. Cena za plný rozsah licencí dle tohoto článku (vč. případného poskytnutí uživatelské a technické dokumentace) je obsažena v odměně za příslušné plnění dle této Smlouvy. Zhotovitel prohlašuje, že před podáním nabídky do Zadávacího řízení pečlivě zvážil veškeré přínosy, které může poskytnutí těchto licencí Objednateli přinést, a že úplata za licence, která je zahrnuta v odměně za příslušné plnění dle této Smlouvy, představuje adekvátní protiplnění Zhotoviteli za poskytnutí licencí. Zhotovitel dále prohlašuje a zavazuje se zajistit, že nositelům práv duševního vlastnictví k předmětu práv duševního vlastnictví, které je plněním dle této Smlouvy, nepřísluší a nebude příslušet vůči Objednateli žádné právo na odměnu, či jakékoliv jiné plnění v souvislosti s užitím příslušného plnění.

15.4. Udělení veškerých práv Objednateli na základě licencí nebo jiných oprávnění k užití předmětu práv duševního vlastnictví dle tohoto článku nelze ze strany Zhotovitele vypovědět nebo jinak jednostranně zrušit a ukončení závazku z této Smlouvy nemá vliv na udělení těchto práv.

XVI. Ochrana informací

16.1. Smluvní strany jsou si vědomy toho, že v rámci plnění této Smlouvy:

(a) si mohou vzájemně úmyslně nebo i opominutím poskytnout informace, které budou považovány za důvěrné (dále „důvěrné informace“),

(b) mohou jejich zaměstnanci získat vědomou činností druhé strany nebo i jejím opominutím přístup k důvěrným informacím druhé strany.

16.2. Strany se zavazují, že žádná z nich nezpřístupní třetí osobě důvěrné informace, které při plnění této Smlouvy nebo v souvislosti s plněním Smlouvy získala od druhé Strany.

16.3. Za třetí osoby se nepovažují:

(a) zaměstnanci Stran a osoby v obdobném postavení,

(b) orgány Stran a jejich členové a

(c) Poddodavatelé Zhotovitele,

za předpokladu, že se podílejí na plnění Smlouvy. Důvěrné informace jsou jim zpřístupněny výhradně za tímto účelem a zpřístupnění důvěrných informací je v rozsahu nezbytně nutném pro naplnění jeho účelu a za stejných podmínek, jaké jsou stanoveny Stranám ve Smlouvě.

16.4. Veškeré důvěrné informace zůstávají výhradním vlastnictvím předávající strany a přijímající strana vyvine pro zachování jejich důvěrnosti a pro jejich ochranu stejné úsilí, jako by se jednalo o její vlastní důvěrné informace. S výjimkou plnění této Smlouvy se obě strany zavazují neduplikovat žádným způsobem důvěrné informace druhé strany, nepředat je třetí straně ani svým vlastním zaměstnancům a zástupcům s výjimkou těch, kteří s nimi potřebují být seznámeni, aby mohli splnit tuto Smlouvu. Obě strany se zároveň zavazují nepoužít důvěrné informace druhé strany jinak než za účelem plnění této Smlouvy.

16.5 Smluvní strany se výslovně dohodly, že za důvěrné informace nejsou považovány informace poskytnuté v rámci Veřejné zakázky, tzn. Zadávací dokumentace, Nabídka Zhotovitele, smluvní dokumentace jakož i informace a dokumentace předané Zhotovitelem v rámci realizace předmětu plnění. Smluvní strany prohlašují, že skutečnosti uvedené v této Smlouvě nepovažují za obchodní tajemství ve smyslu § 504 občanského zákoníku, tímto výslovně souhlasí se zveřejněním veškerých náležitostí a podmínek této Smlouvy nebo souvisejících dokumentů a informací, včetně zveřejnění této Smlouvy jako celku, v rámci informací zpřístupňovaných veřejnosti bez stanovení jakýchkoli dalších podmínek, a to i prostřednictvím dálkového přístupu, zejména na webových stránkách města. V případě utajovaných příloh (například podléhající obchodnímu tajemství) poskytovatel při podpisu Smlouvy předal nabyvateli verzi strany nebo přílohy, která zůstane neveřejná – z této listiny musí být patrný alespoň obsah tohoto dokumentu.

16.6. Strany se zavazují v plném rozsahu zachovávat povinnost mlčenlivosti a povinnost chránit důvěrné informace vyplývající ze Smlouvy a též z příslušných právních předpisů, zejména povinnosti vyplývající ze zákona č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů. Strany se v této souvislosti zavazují poučit veškeré osoby, které se budou podílet na plnění Smlouvy, o výše uvedených povinnostech mlčenlivosti a ochrany důvěrných informací a dále se zavazují vhodným způsobem zajistit dodržování těchto povinností všemi osobami podílejícími se na plnění Smlouvy.

16.7 Budou-li informace poskytnuté Objednatelem či třetími stranami, které jsou nezbytné pro plnění Smlouvy, obsahovat data podléhající režimu zvláštní ochrany podle zákona č. 110/2019 Sb., ., o zpracování osobních údajů, ve znění pozdějších předpisů , zavazuje se Zhotovitel zabezpečit splnění všech ohlašovacích povinností, které citovaný zákon vyžaduje po zpracovateli osobních údajů, a v případě, že v rámci plnění povinností dle této Smlouvy je Zhotovitel povinen údaje od subjektů údajů též získat, pak je povinen obstarat předepsané souhlasy subjektů osobních údajů předaných ke zpracování.

16.8. Pokud jsou důvěrné informace poskytovány v písemné podobě nebo ve formě textových souborů na počítačových médiích, je předávající strana povinna upozornit přijímající stranu na důvěrnost takového materiálu jejím vyznačením alespoň na titulní stránce.

16.9. Bez ohledu na výše uvedená ustanovení se za důvěrné nepovažují informace, které:

(a) se staly veřejně známými, aniž by to zavinila záměrně či opominutím přijímající strana,

(b) měla přijímající strana legálně k dispozici před uzavřením této Smlouvy, pokud takové informace nebyly předmětem jiné, dříve mezi Smluvními stranami uzavřené smlouvy o ochraně informací,

(c) jsou výsledkem postupu, při kterém k nim přijímající strana dospěje nezávisle a je to schopna doložit svými záznamy nebo důvěrnými informacemi třetí strany,

(d) po podpisu této Smlouvy poskytne přijímající straně třetí osoba, jež takové informace přitom nezíská přímo ani nepřímo od strany, jež je jejich vlastníkem.

16.10. Zhotovitel je dále povinen:

a) Zajistit, aby osobní údaje nebyly uchovávány mimo území České republiky, resp. mimo EU;

b) bez zbytečného odkladu informovat Objednatele o porušení zabezpečení osobních údajů a být nápomocen při plnění povinností Objednatele, zejména povinnosti reagovat na žádosti o výkon práv subjektů údajů, povinnosti ohlašovat případy porušení zabezpečení osobních údajů dozorovému úřadu dle čl. 33 obecného nařízení o ochraně osobních údajů, povinnosti oznamovat případy porušení zabezpečení osobních údajů subjektu údajů dle čl. 34 obecného nařízení o ochraně osobních údajů, povinnosti posoudit vliv na ochranu osobních údajů dle čl. 35 obecného nařízení o ochraně osobních údajů a povinnosti provádět předchozí konzultace dle čl. 36 obecného nařízení o ochraně osobních údajů, a že za tímto účelem zajistí nebo přijme vhodná technická a organizační opatření, o kterých ihned informuje Objednatele;

c) po ukončení Smlouvy řádně naložit se zpracovávanými osobními údaji, např. že všechny osobní údaje vymaže, nebo je vrátí Objednateli a vymaže existující kopie, dle požadavku Objednatele;

d) při porušení povinností stanovených touto Smlouvou v případech, kdy byla v důsledku nedodržení zásad a pravidel ochrany osobních údajů uložena Objednateli pokuta ze strany příslušných dozorujících a kontrolních orgánů, je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši odpovídající vyměřené pokutě. Úhradou této smluvní pokuty není dotčeno právo na náhradu škody vzniklé Objednateli nad rámec takto vyměřené pokuty

16.11. Ustanovení tohoto článku není dotčeno ukončením účinnosti této Smlouvy z jakéhokoliv důvodu po dobu dalších 5 let od ukončení účinnosti Smlouvy. Ochrana osobních údajů třetích osob není lhůtou omezena.

XVII. Závěrečná ustanovení

17.1. Tato Smlouva nabývá platnosti dnem jejího podpisu oběma Smluvními stranami a účinnosti dnem jejího uveřejnění v Registru smluv dle zákona č. 340/2015 Sb., o registru smluv o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv). Smlouvu se zavazuje bez zbytečného odkladu v Registru smluv uveřejnit Objednatel.

17.2. Smluvní strany se dohodly, že v případě zániku právního vztahu založeného touto Smlouvou zůstávají v platnosti a účinnosti i nadále ustanovení, z jejichž povahy vyplývá, že mají zůstat nedotčena zánikem právního vztahu založeného touto Smlouvou.

17.3. Znění této smlouvy bylo schváleno Radou města Příbrami dne 18.3.2024, číslo usnesení 321/2024.

17.4. Součást této Smlouvy tvoří:

Příloha č. 1: Technická specifikace

Příloha č. 2: Návrh Zhotovitele – Popis nabízeného technického řešení

V případě rozporu mezi různými částmi této Smlouvy, není-li určeno jinak, mají přednost dokumenty této Smlouvy v následujícím pořadí:

- Technická specifikace
- Návrh Zhotovitele
- očíslované články této Smlouvy
- ostatní přílohy.

V Příbrami, dne

Mgr. Jan Konvalinka
Digitálně podepsal Mgr. Jan Konvalinka
Datum: 2024.04.09 11:17:05 +02'00'

za Objednatele

Ladislav Kocour
Digitálně podepsal Ladislav Kocour
Datum: 2024.04.09 14:09:50 +02'00'

za Zhotovitele

1. Předmět plnění

(1) Předmětem plnění veřejné zakázky je dodávka a implementace technologií pro zvýšení kybernetické bezpečnosti informačních systémů (IS) a komunikačních systémů (KS) zadavatele v souladu se standardy kybernetické bezpečnosti (dále také jen „dodávka“, „systém“, „řešení“ nebo „technologie“) včetně nezbytných služeb, podrobná specifikace dodávek a služeb je uvedena v dalších kapitolách tohoto dokumentu. Součástí plnění je dále podpora provozu na dobu minimálně 60 měsíců po předání řešení do ostrého provozu. Řešení musí být navrženo tak, aby náklady na provoz systému byly co nejmenší.

(2) I u technických parametrů, u kterých není výslovně uvedeno, že jde o požadovanou minimální či maximální hodnotu, lze nabídnout i řešení „lepší“, tedy řešení přesahující (ve smyslu výhodnějším z pohledu užitné hodnoty) hodnotu stanoveného požadavku, ledaže ze zadávacích podmínek výslovně vyplývá, že musí být splněna přesně daná hodnota.

(3) Předmětem plnění veřejné zakázky jsou zařízení a systémy uvedené v následující tabulce, včetně služeb (komodity):

Komodita	Zajišťovaná oblast	Stručný popis položky	ID opatření	Jednotka	Počet jednotek
K.1	Zabezpečení datových rozvaděčů	Zabezpečení centrálních datových rozvaděčů	ID001	komplet	2
		Zabezpečení podružných datových rozvaděčů	ID001	komplet	10
K.2	Zvýšení zabezpečení sítě LAN	Páteřní přepínače	ID002	ks	3
		Přístupové přepínače 24p	ID002	ks	6
		Přístupové přepínače 48p	ID002	ks	6
		Místní přepínače	ID002	ks	27
		Rozšíření optických tras	ID002	komplet	1
K.3	Zvýšení zabezpečení sítě WiFI	Bezdrátové přístupové body	ID002	ks	44
K.4	Zavedení nástrojů ověřování zařízení přistupujících do počítačové sítě – 802.1x	Systém bezpečného přístupu do sítě 802.1x	ID002	komplet	1
K.5	Systém pro centrální správu sítě	Systém centrální správy sítě	ID002	komplet	1
K.6	Interní segmentační firewall	Interní segmentační firewall	ID002	ks	2
K.7	Správa privilegovaných účtů	SW pro správu privilegovaných účtů a přístupů	ID003	komplet	1
K.8	Ochrana koncových zařízení	Pokročilá anti-X ochrana	ID004	komplet	1
		Pokročilá ochrana koncových zařízení s rozšířenou detekční schopností	ID004	komplet	1

K.9	Monitorování práce s digitálními daty	SW pro monitorování práce s digitálními daty	ID005	ks	1
K.10	Ochrana datové základny úřadu	Záložní server	ID006	ks	1
		Diskové úložiště	ID006	ks	1
		Zabezpečené úložiště záloh s řízenou retencí	ID006	ks	1
		SW licence operačních systémů záložního serveru	ID006	ks	1
		SW licence zabezpečeného úložiště	ID006	ks	1
		Datové rozvaděče 19" vč. non IT technologií	ID006	ks	2
		Tenký klient	ID006	ks	50
K.11	Centrální komunikační systém úřadu	Hlasová brána	-	ks	1
		Centrální komunikační systém úřadu	-	ks	1

2. Popis současného stavu

2.1. Popis organizace a její členění

(1) Organizace Město Příbram (dále jen Město) sídlí v Městském úřadě Příbram (dále MÚ nebo MěÚ), kde pracuje většina zaměstnanců a je zde umístěná významná část IT technologií. Město je zřizovatelem organizací v oblasti kultury, dopravy, školství a sociální.

(2) Město Příbram je veřejnoprávní korporací (právnická osoba veřejného práva), která podle zákona číslo 128/2000 Sb., o obcích (obecní zřízení), vykonává působnost v oblasti veřejné správy.

(3) Městský úřad Příbram (dále také jen „MěÚ“) jako orgán města vykonává samostatnou působnost a přenesenou působnost státní správy na svém základním správním obvodu a dále zajišťuje výkon státní správy i pro další obce (74 obcí) v rámci svého obvodu s rozšířenou působností.

2.2. Popis lokalit

(1) Z pohledu IT jsou pro Město nejvýznamnějšími lokalitami MÚ budovy Generála Tesaříka 19 a Tyršova 108. V těchto lokalitách jsou umístěny technologie TC ORP. Provoz datových center je zajišťován vlastními zaměstnanci Města ve spolupráci s externími specializovanými firmami.

(2) Projekt bude realizován v těchto lokalitách:

(a) Budova radnice: Městský úřad Příbram, Tyršova 108, 261 01 Příbram

(b) Budova OSVZ: Městský úřad Příbram, nám. T. G. Masaryka 107, 261 01 Příbram

(c) Zámeček: Městský úřad Příbram, Tyršova 106, 261 01 Příbram

(d) Stavební úřad a OKRM: Městský úřad Příbram, Na Příkopech 105, 261 01 Příbram

(e) Budova Čp. 19: Městský úřad Příbram, Generála Tesaříka 19, 261 01 Příbram

(f) MP: nám. T. G. Masaryka 121, Příbram I, 261 01 Příbram

(g) OŽP: Městský úřad Příbram, U nemocnice 19B, 261 01 Příbram I

(h) Centrální spisovna: Městský úřad Příbram, Kpt. Olesinského 41, 42, 261 01 Příbram

(i) Městská realitní kancelář, Čs. armády 5, 261 01 Příbram IV

(j) Městské kulturní centrum, Špitálská 18, Příbram I

(k) Informační centrum města Příbram, Pražská 129, 261 01 Příbram I

2.3. Popis stávajícího HW prostředí

(1) TC je technicky i provozně navrženo, vybudováno a provozováno pro poskytování vysoce dostupných infrastrukturních ICT služeb Městu a jeho organizacím.

(2) Současná ICT infrastruktura Města je tvořena především TC, které představuje plně virtualizovanou a vysoce dostupnou serverovou infrastrukturu pro provoz systémů a aplikací Města. TC je koncepčně a technologicky připravené pro další rozšiřování. Rozšiřitelnost byla prakticky ověřena při rozšiřování TC o 2 virtualizační uzly a VDI infrastrukturu v uplynulých čtyřech letech a bude využita i v tomto projektu.

(3) Serverová infrastruktura MěÚ zahrnuje dvojici virtualizačních serverů umístěných v hlavní lokalitě. Jedná se o servery HP DL385 Gen10 (768 GB RAM, 1x AMD Epyc 7502 32 core). Na serverech běží virtualizační systém MS Hyper-V 2019. Virtuální servery jsou rozloženy mezi oba fyzické servery. Vysoká dostupnost je řešena na úrovní serverů, geografická redundance není dostupná. Na serverech jsou provozovány terminálové servery pro běh aplikací v terminálovém módu.

(4) Diskové pole pro produkční data je tvořeno SW komponentou v rámci HCI (hyperkonvergované infrastruktury). Data jsou umístěna na lokálních SSD discích virtualizačních serverů a jsou mezi oběma servery replikována. Kapacita úložiště je 25TB.

(5) Pro zálohování virtuálních serverů a dat z diskového pole je nasazen zálohovací server HP DL380 Gen9. Zálohuje se na diskové pole Lenovo v3800 připojené pomocí technologie fiberchannel k tomuto serveru. Pro uložení off-line záloh je využit síťový NAS Synology. Celá zálohovací infrastruktura je umístěna v lokalitě v záložní lokalitě Tyršova 108. Pro správu zálohování je využit Veeam Backup Essentials Enterprise, kdy pořízená licence umožňuje pokrýt zálohování neomezeného počtu fyzických a virtuálních serverů.

(6) Síťová infrastruktura zahrnuje kombinaci více druhů přepínačů. V klíčových lokalitách se jedná o přepínače výrobce Cisco. Aktuální modelové řady (Catalyst 9200 a Catalyst 9300) jsou v tabulce níže označeny zeleně (8ks). Zbylé přepínače nesplňují požadavky na zabezpečení přístupové infrastruktury úřadu (12ks). Jedná se o řady produktů uváděné na trh před více než 10ti lety a tudíž nepodporují aktuální protokoly standardu 802.1x (mikrosegmentace, mac-based autentizaci apod.). Přepínače rovněž nepodporují technologii PoE a ve většině případů jde o přepínače s rychlostí 100Mb/s.

(7) Díky nedostatečně dimenzované kabeláži jsou v mnoha kancelářích umístěny stolní přepínače bez možnosti správy. Tyto tudíž představují vysoké riziko zneužití pro neoprávněný přístup do lokální sítě úřadu. Celkem je takových přepínačů 27ks.

(8) Bezdrátová síť je řešena na zařízeních určených pro domácí a kancelářské nasazení. Jedná so o prvky Ubiquity různého stáří.

(9) Rozložení přepínačů do lokalit:

Hlavní lokalita – Gen. Tesaříka 19		
Catalyst 9200L 48 4x10G	4	ks
Catalyst 9300 48 -network module NM-46	2	ks
WS-C3750G-24T	1	ks
Budova Gen. Tesaříka 19a		
WS-C3750G-24TS	1	ks
Na příkopech 105 – Stavební úřad		
WS-C3750-48TS	1	ks

Zámeček – Tyršova 106		
WS-C3750-48TS	1	ks
Tyršova 107 – Odbor sociálních věcí		
WS-C3750G-24T	1	ks
WS-C3750-48TS	1	ks
Budova Tyršova 108		
WS-C3750G-24T	1	ks
WS-C3750-48TS	3	ks
Náměstí T.G.Masaryka 121 - městská policie		
Catalyst 9300 24 -network module NM-46	1	ks
Pražská 129 - infocentrum		
WS-C3750-48TS	1	ks
ČS. Armády 5 - Městská realitní kancelář		
Catalyst 9300 24 -network module NM-46	1	ks
Náměstí T.G.Masaryka 101 - Zasedačka RD		
WS-C2950G-48 EI	1	ks

(10) Záložní napájení je řešeno prostřednictvím několika diskrétních UPS. Výkon ani rozložení UPS nevyhovuje požadavkům infrastruktury.

(11) Provozní monitoring celého prostředí je prováděn nástrojem Zabbix a Wazuh.

(12) Zabezpečení přístupu k internetu využívá dvojice NGFW (Next generation firewall) ForiGate-200D, zapojených do vysoce dostupného clusteru.

(13) Město má implementovánu adresářovou službu Active Directory. Jmenné a adresní síťové služby (DNS a DHCP) jsou využívány nativní ve Windows Server.

(14) Pro autentizaci uživatelů do KIVS jsou využívány tokeny TokenME a čtečky čipových karet Omnikey.

(15) Koncové stanice (počítače) jsou různého stáří (cca. 7-1 let), provozovaným operačním systémem jsou Windows 10.

(16) Tiskové prostředí je tvořeno lokálními tiskárnami (různé modely, převážně HP) - desítky kusů a síťovými (i multifunkčními) tiskárna mi (různé modely, převážně Minolta a Develop) – cca. 20 kusů.

(17) Správci systémů jsou vyškoleni na správu provozního prostředí na bázi produktů Microsoft a používaných síťových technologií.

2.4. Popis stávajícího SW prostředí

(1) Systémové služby TC jsou provozovány na platformě Microsoft, jde zejména o následující systémy:

(a) Microsoft Windows 2012 R2

(b) Microsoft MS SQL 2008 R2 Standard

(c) Microsoft MS Exchange 2010 Standard

(d) Microsoft MS SharePoint Foundation 2010

(2) Primární adresářovou službou je Active Directory provozovaná na redundantních replikovaných řadičích, které zajišťují také služby DNS a DHCP.

(3) Standardním kancelářským balíkem využívaným pro potřeby Města je Microsoft Office, s ohledem na sjednocení uživatelského rozhraní a kompatibilitu dokumentů ve verzi 2019 a vyšší. Standardně jsou využívány aplikace Word, Excel, Outlook a OneNote.

(4) K ukládání sdílených souborů je kromě prostředků Windows serveru. Dále je využíván DMS (Document Management System) na bázi technologie MS Sharepoint, vybudovaný jako součást TC, na této platformě je také provozován portál úředníka.

(5) Virtualizační platformou TC je Microsoft Hyper-V ve verzi 2012 R2. Jsou implementovány a využívány pokročilé funkce Hyper-V – High availability, Live Migration, virtuální switche apod. Pro některé aplikace je používána virtualizační platforma VMware.

(6) Město využívá jednotný agendový systém na platformě PROXIO Marbes včetně napojení na systém základních registrů a má implementován systém EOS (Evidence organizační struktury). Agendový systém pokrývá pouze část agend.

2.5. Popis dokumentace

(1) K provozování a řízení rozvoje TC je využívána a udržována Provozní dokumentace.

(2) Provozní dokumentace popisuje aktuální nastavení technologií, hardwarových a softwarových systémů TC. Softwarové systémy jsou popsány v rozsahu infrastrukturních služeb (AD, DNS, DHCP apod.), Hyper-V, Exchange.

(3) Citlivé údaje (přístupové účty apod.) jsou součástí Bezpečnostní dokumentace a jsou uloženy odděleně od Provozních dokumentací

(4) Relevantní části dokumentace budou Dodavateli zpřístupněny až po podpisu Smlouvy o dílo k této zakázce ve formátech MS Office (xls, doc).

(5) Dodavatel je povinen zajistit nezbytné doplnění dokumentace TC reflektující provedené změny.

2.6. Popis způsobu řešení incidentů

(1) Zadavatel pro řešení incidentů a podporu uživatelů využívá vlastní systém „Úkolovník“.

(2) Zadavatel také zajišťuje podporu 1. úrovně a většinu běžných problémů jsou schopni vyřešit interní pracovníci Zadavatele.

(3) Incidenty a požadavky, které nevyřeší interní specialisté, jsou předávány do helpdeskových systémů dodavatele systému, který vykazuje incident nebo na který směřuje požadavek uživatele. Hlášení incidentů a požadavků je prováděno telefonicky, emailem nebo přímo zadáním ticketu/požadavku do helpdeskového systému dodavatele.

2.7. Popis servisních oken

(1) TC nemá pevně definovaná pravidelná servisní okna. Aplikace aktualizací a oprav virtuálních serverů provádějí specialisté Města dle potřeby a s přihlédnutím k minimalizaci omezení uživatelů.

(2)

3. Požadované parametry technického řešení

3.1. Obecné požadavky

(1) Zadavatel při výstavbě, správě a provozu technologií striktně dodržuje hledisko technologické neutrálnosti, tj. využití technologií takovým způsobem, který neomezuje implementaci technologií různých výrobců – tuto strategii musí splňovat i řešení dodané v rámci této veřejné zakázky.

(2) Pokud uchazeč vyžaduje využití konkrétních softwarových produktů a jím zvolený přístup k řešení zadání je na takových konkrétních řešeních závislý, musí jejich pořízení zahrnout ve své nabídce v potřebném rozsahu a v rámci nabídnuté ceny.

(3) Za předpokladu, že uchazečem navržené řešení vyžaduje fyzickou infrastrukturu (např. servery, úložiště, komunikační prvky atd.) neobsaženou v popisu předmětu plnění, zahrne uchazeč do své ceny všechny náklady na její pořízení, instalaci, konfiguraci a další služby potřebné pro uvedení do provozu.

(4) Uchazeč ve své nabídce detailně popíše vazby na stávající systémy Zadavatele, které jsou nezbytné pro správné fungování řešení nabízeného uchazečem.

(5) Zadavatel z důvodů co nejjednodušší a jednotné správy a minimalizace provozních nákladů vyžaduje využití stávajících prostředků a používaných technologií. V případě, že uchazeč vyžaduje ve svém řešení stejné nebo podobné funkce, jaké poskytují stávající prostředky a technologie, je povinen využít nebo vhodným způsobem rozšířit stávající prostředky.

(6) Žádné z nabízených řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány.

(7) Uchazeč prokáže, že všechny dodávky, které dodá Zadavateli:

(a) jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,

(b) mají plnou záruku od výrobce,

(c) mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,

(d) obsahuji licenci na používání příslušného softwaru,

(e) jsou určeny pro provoz v České republice,

(f) z databází výrobce, distributora či prodejce bude možné výše uvedené skutečnosti doložit.

Tyto skutečnosti uchazeč doloží čestným prohlášením distributora, popř. uchazečem samotným, nelze-li prohlášení distributora získat. Zadavatel si vyhrazuje právo na zjištění původu výrobku při jejich převzetí, a to dle příslušných sériových čísel a právo podpisu akceptačního protokolu, osvědčujícího převzetí dodávky, až po ověření původu výrobku.

3.2. Specifické požadavky

3.2.1. K.1 – Zabezpečení datových rozvaděčů

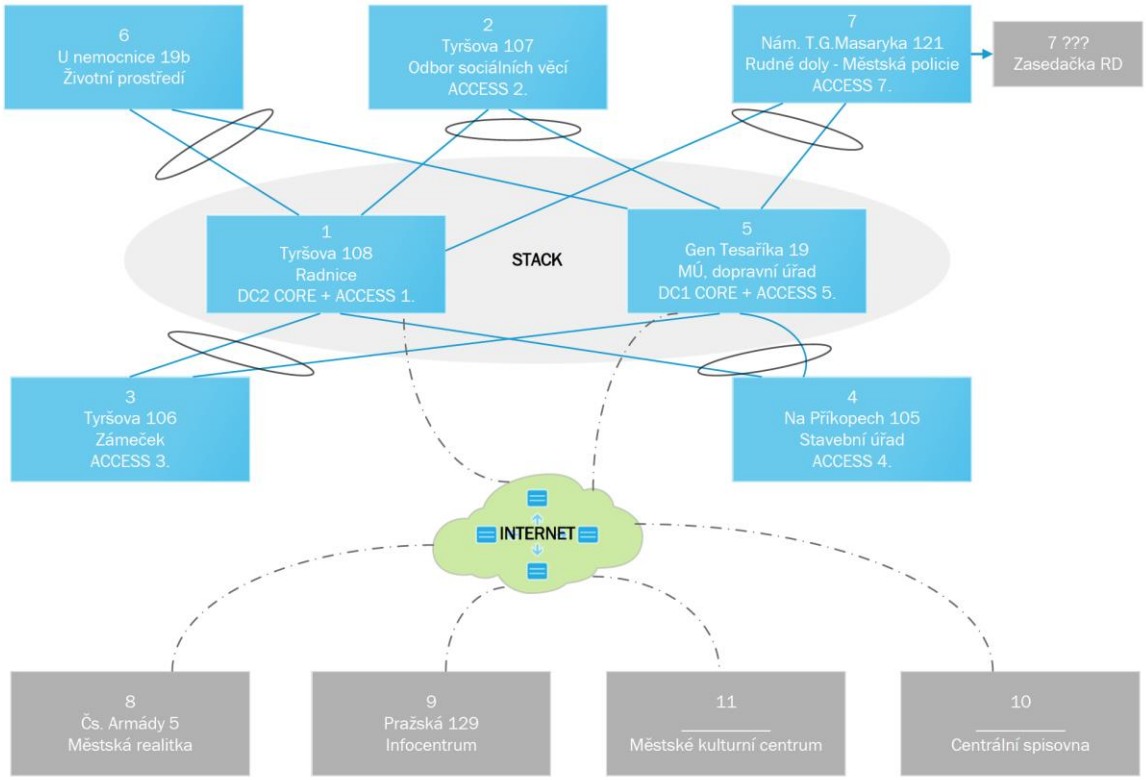
(1) Pro bezchybný provoz potřebných aplikací a agend úřadu je nutné mít stabilní datovou síť, která nebude chybovat a nebude mít výpadky. Pro zabezpečení provozu datové sítě, IP telefonní ústředny a IP telefonů je nutné zabezpečit nepřetržitou dodávku el. energie. Z tohoto důvodu je nutná instalace patřičných záložních zdrojů, které budou fitrovat jak špičky napětí, tak pomohou i překrýt krátkodobé výpadky dodávky el. energie z distribuční sítě.

(2) V místech, kde jsou umístěny centrální technologie, proto budou instalovány záložní zdroje UPS s možností připojení externích baterií pro prodloužení doby zálohy. Kde dané zdroje musí umožňovat bezchybný provoz všech připojených technologií a vzdálený monitoring stavu. Ve 10 dalších podružných rozvaděčích budou instalovány v rackových skříních další záložní zdroje UPS včetně vzdáleného monitoringu jejich stavu.

(3) Kromě záložních napájecích zdrojů budou všechny racky také osazeny systémem pro monitoring provozních veličin, minimálně kontrolou vstupu, kontrolu teploty a vlhkosti, detekce požáru. Tento systém bude umožňovat přímé zasílání notifikací minimálně pomocí emailových zpráv. Zároveň musí být všechny dohledové jednotky integrované do stávajícího centrálního dohledového systému Zabbix.

3.2.2. K.2 – Zvýšení zabezpečení sítě LAN

(1) Zvýšení zabezpečení sítě LAN spočívá ve modernizaci přepínačů LAN a nasazení jednotné úrovně zabezpečení sítě LAN. To zahrnuje jednak zvýšení dostupnosti LAN díky redundantnímu zapojení mezi obě centrální lokality. Cílový předpokládaný návrh je schematicky naznačen na následujícím obrázku.



(2) Design předpokládá osazení v primárním datovém centru 2ks páteřních přepínačů a v záložním datovém centru 1ks páteřního přepínače. Všechny podružné rozvaděče a maximum přístupových přepínačů pak bude propojeno redundantně do obou datových center.

(3) Aby bylo takové zapojení možné, je nutné doplnit stávající optické linky o technologii CWDM, která umožní vytvořit další logické spoje na jednom fyzickém páru optických vláken. Konkrétní návrh vlnových délek a rozložení mezi jednotlivé spoje, bude součástí návrhu dodavatele před samotným zprovozněním.

(4) Po zprovoznění přepínačů a jejich propojení, dojde ke konfiguraci bezpečnostních mechanismů, jako např. k segmentaci lokální sítě, zabezpečení klíčových linek, zabezpečení servisních síťových protokolů (spanning-tree apod.). Všechna zařízení budou integrována do systému řízení přístupu do sítě a do systému centrální správy sítě.

3.2.3. K.3 – Zvýšení zabezpečení sítě WiFi

(1) Cílem Zadavatele je, aby síť WiFi v maximální možné míře kopírovala bezpečnostní mechanismy nasazené v sítí LAN. Síť bude řídit dvojice bezdrátových kontrolérů ve vysoce dostupné konfiguraci tak, aby výpadek jednoho kontroleru neovlivnil fungování bezdrátové sítě.

(2) Bezdrátové přístupové body budou rozmístěny v rámci prostor Zadavatele dle návrhu připraveného v rámci předimplementační analýzy.

(3) Bezdrátové sítě budou reflektovat segmentaci do bezpečnostních zón navržených v rámci implementace systému 802.1x. Jinak se bude zacházet s veřejnou sítí (musí být implementován captive portál a izolace klientů), jinak se sítí určenou pro zařízení Zadavatele (802.1x, WPA3, certifikáty atd.).

3.2.4. K.4 – Zavedení nástrojů ověřování zařízení přistupujících do počítačové sítě – 802.1x

Zadavatel plánuje zavést ověřování zařízení přistupujících do drátové i bezdrátové sítě. Předpokládá, že systém bude splňovat následující parametry:

(1) Systém musí umožňovat nasazení a správu Network Admission Control (NAC) založený na standardu IEEE 802.1X. Tento řeší bezpečné připojení koncových stanic a konkrétních uživatelů na základě procesu autentizace (rozpoznání identity zařízení a uživatele) a autorizace (zpřístupnění konkrétních datových zdrojů podle uživatelské role, stavu koncového zařízení) a dalších atributů v rámci kontextu uživatele.

(2) Integrované funkce zajišťují komunikaci s AAA serverem (RADIUS) a nastavují komplexní, přitom unifikované, bezpečnostní politiky pro autentizaci a autorizaci koncových bodů.

(3) Architektura musí zaručit, že všichni uživatelé (mobilní zaměstnanci, ale i dodavatelé nebo hosté) budou vždy jednoznačně identifikováni a prostřednictví přidělených rolí jim bude zajištěn bezpečný přístup ke všem informacím v síti, na které mají nárok.

(4) Po ověření identity uživatele je mu přiřazena jedna z předem definovaných rolí, prostřednictvím které se může následně pohybovat v síti se všemi odpovídajícími právy i omezeními. Využitím informace získané při ověření identity spolu s rolemi skupin uživatelů nebo serverů připojených k síti, minimalizujeme rizika neoprávněných přístupů a zjednodušujeme celý proces nasazení bezpečnostních pravidel v síti i jejich následnou správu.

(5) Bezpečnostní management musí poskytnout zjednodušenou správu bezpečnostních politik a umožnit tak jejich konzistentní nastavení v rámci celé sítě. Předpokladem je řízení pravidel přístupu na LAN, WLAN (včetně tzv. „Guest Access“). Přitom v procesu definice pravidel bude bráno v úvahu více parametrů, které má systém k dispozici (identita uživatele, pracovní skupina, místo, čas, typ zařízení atd.). Budou definovány různé třídy přístupu podle různých vstupních parametrů, které budou aplikovány v definicích pravidel (policy).

(6) Komunikaci koncové stanice musí být možné dynamicky přesunout do jiného pracovního segmentu (ale i např. karantény) nebo uplatnit přístupové filtry tzv. „za běhu“ pomocí řízení CoA (Change of Authorization = proces aplikace pravidel pomocí rozšíření protokolu RADIUS) na základě aktuálního vyhodnocení vstupních parametrů (typ koncového zařízení, jeho stav, apod.).

(7) Systém by měl být rozšiřitelný i o řízení bezpečného transportu datovou sítí (implementace šifrování na rozhraních přepínačů) a možnosti škálovatelné filtrace přístupů k datovým zdrojům na základě uživatelských bezpečnostních rolí.

(8) Důraz je kladen na vysokou dostupnost celého řešení (redundanci), centrální správu, dohled a možnosti vyhodnocení událostí, generace reportů apod. na jednom místě.

3.2.5. K.5 – Systém pro centrální správu sítě

(1) Do systému pro centrální správu sítě budou začleněny všechny zařízení dodané v rámci části LAN i WiFi, dále pak stávající zařízení Cisco Catalyst 9200 a Cisco Catalyst 9300. Systém centrální správy musí umožnit konfiguraci síťových politik pro celou síť. Zároveň systém musí umožnit mikrosegmentaci na všech zapojených zařízeních.

(2) Politiky pro síťová zařízení musí být sdílená pro aktivní prvky LAN i WiFi, stejně tak pro uživatele, kteří se přes tyto sítě připojují.

3.2.6. K.6 – Interní segmentační firewall

(1) V návaznosti na části K.2, K.3 a K.4 bude nasazen interní segmentační firewall, který bude oddělovat jednotlivé bezpečnostní segmenty a bude řídit prostupy mezi nimi a také přístup směrem k IS úřadu.

(2) Firewall bude nasazen jako cluster složený z dvou plně redundantních uzlů s tím, že každý uzel musí být schopen plnohodnotně pokrýt všechny nároky, zároveň je požadováno, aby firewall bych

schopen fungovat v režimu active/active. Firewall musí disponovat detekčními a prevenčními schopnostmi obvyklými u Next Generation firewallů (NGFW). Politiky musí být navázány na identitu zařízení/uživatelů, na aplikační protokoly a kontext (čas, místo apod.).

3.2.7. K.7 – Správa privilegovaných účtů

(1) Cílem zadavatele je pořízení systému pro řízení a správu privilegovaných účtů (dále jen PIM/PAM), který zajistí jednotnou správu přístupu k privilegovaným účtům a monitorování operací prováděných pod těmito účty s vazbou na konkrétního administrátora, který v danou chvíli účet používá, včetně dvou faktorové autentizace a poskytnutí podrobného seznámení se správou dodaného systému pro IT pracovníky zadavatele.

(2) Jednotlivé informační systémy jsou spravovány privilegovanými účty, které jsou využívány pro správu aplikací nebo systémových služeb a jako takové představují významné bezpečnostní riziko.

(3) Z hlediska bezpečnosti umožňují téměř neomezený přístup a manipulaci s informačními aktivy úřadu, v případě kompromitace privilegovaného účtu je úřad vystaven velkému riziku zneužití nebo vyzrazení informací nebo jejich zneužití.

(4) Požadavek řídit privilegované účty je hlavním požadavkem zákona (ZKB) a standardů kybernetické bezpečnost, týká se zajištění bezpečnosti informačních systémů, nejen, které jsou určeny jako významné informační systémy (VIS) nebo informační systémy kritické informační infrastruktury (IS KII). Nenaplnění těchto požadavků může vést k uvalení sankcí ze strany Národního bezpečnostního úřadu, který provádí cílené audity zaměřené na posouzení souladu se ZKB a VKB.

(5) Cílem nasazení tohoto systému je řešit:

a) Vyhledání a inventarizace privilegovaných účtů
b) Bezpečná správa hesel a SSH klíčů pro privilegované účty
c) Komplexní správa privilegovaných účtů – uživatelů
d) Bezpečný přístup na cílový systém pomocí jump serveru prostřednictvím zvoleného komunikačního protokolu, aplikace a příslušného privilegovaného účtu
e) Centrální kontrolní bod pro izolaci, řízení a sledování všech aktivit správců
f) Monitoring a nahrávání vzdálených relací a aktivit privilegovaných účtů ve video formátu s možností kontextového vyhledávání
g) Kontrola čtyř očí (Dual Control) a oddělení rolí (Segregation of Duties)
h) Auditní stopa a personalizace využití sdílených účtů
i) Bezpečný mechanismus pro vyzvedávání hesel a SSH klíčů pro aplikace

(6) Systém, který bude zajišťovat jednotnou správu a monitoring privilegovaných účtů Zadavatele.

(7) Řešení musí být instalováno ve formě virtuálního serveru, který bude provozován na stávající virtualizační infrastruktuře Zadavatele (Microsoft Hyper-V).

(8) Zadavatel požaduje, aby vlastní přihlašovací údaje a klíče k cílovým systémům (operačním systémům, databázím, zařízením apod.) byly v chráněné a šifrované databázi systému.

(10) Pojem privilegovaný účet označuje účet v operačním nebo informačním systému, který má vysoké oprávnění. Jedná se o účty typu root v Linux/UNIX systémech, účty typu Administrátor ve Windows systémech, systémové účty používané aplikacemi nebo sdílené účty, které nejsou vázané na fyzickou osobu.S těmito účty pracují privilegovaní uživatelé. Pojem privilegovaný uživatel označuje fyzickou osobu, která používá privilegované účty. Jedná se o pracovníky provozu, dodavatele, nebo vývojáře. Cílový systém označuje systém, na který se privilegovaný uživatel připojuje prostřednictvím privilegovaných účtů.

3.2.8. K.8 – Ochrana koncových zařízení

3.2.8.1 – pokročilá ochrana koncových zařízení – EPM

(1) Endpoint Privilege Management (EPM) je bezpečnostní technologie, která se zaměřuje na správu oprávnění a privilegií a řízení přístupu k aplikacím na koncových zařízeních.

(2) Cílem projektu je implementace bezpečnostního software EPM pro ochranu koncových zařízení, jako jsou počítače a servery, před zneužitím oprávnění a privilegií a snížení rizika zneužití aplikací.

(3) Tento nástroj bude umožňovat správu přístupů k citlivým informacím a systémům pomocí správy oprávnění a privilegií a definovat, které aplikace jsou povoleny a které jsou zakázány pro použití na koncových zařízeních. Nástroj by měl detekovat a zamezit rizikům v reálném čase, jako jsou pokusy o zneužití přístupových práv, krádeže údajů nebo infekci počítače malwarem. Díky centralizovanému řízení a sledování přístupových práv na koncových zařízeních, je možné snadno spravovat bezpečnostní rizika a chránit se tak před útoky, které by mohly způsobit ztrátu citlivých dat nebo zpomalit podnikové procesy.

(4) Systém EPM musí zajistit funkce, které jsou důležité pro ochranu koncových zařízení a citlivých informací.

a) Snížení rizika zneužití oprávnění a privilegií - Implementace EPM umožňuje organizacím definovat, kdo a jaké oprávnění a privilegia má na koncových zařízeních. To pomáhá minimalizovat riziko zneužití oprávnění a privilegií a snižuje tak pravděpodobnost, že budou útočníci moci získat přístup k citlivým informacím nebo systémům.
b) Snížení rizika zneužití aplikací - Implementace application controlu umožní úřadu definovat, které aplikace jsou povoleny a které jsou zakázány pro použití na koncových zařízeních. To sníží riziko zneužití aplikací, které mohou obsahovat malware nebo jiný škodlivý software, a minimalizuje tak pravděpodobnost, že budou útočníci moci získat přístup k citlivým informacím nebo systémům.
c) Ochrana proti novým a neznámým hrozbám - Implementace application controlu umožní chránit se před novými a neznámými hrozbami tím, že blokuje aplikace, které nebyly schváleny jako bezpečné. To umožňuje úřadu chránit se proti hrozbám, které dosud nebyly identifikovány nebo na které neexistuje aktualizovaný antivirový software.
d) Centralizovaná správa oprávnění a privilegií - Implementace EPM umožní centralizovaně spravovat oprávnění a privilegia pro všechna koncová zařízení. To usnadňuje správu a sledování přístupových práv a minimalizuje rizika spojená s ruční správou oprávnění.
e) Centralizovaná správa aplikací - Implementace application controlu umožňuje centralizovaně spravovat aplikace pro všechna koncová zařízení. To umožní správu a sledování aplikací a minimalizuje rizika spojená s ruční správou aplikací.
f) Sledování a auditování aplikací - Implementace application controlu umožní sledovat a auditovat aplikace, které jsou instalovány na koncových zařízeních. To umožňuje rychle zjistit, kdy a kdo nainstaloval nebezpečnou aplikaci a minimalizuje riziko, že organizace se dozví o útoku až později, kdy mohou být následky mnohem horší.

(5) Podpora musí být zajištěna pro následující typy OS, které zadavatel provozuje:

a) Windows 10 x32 & x64, Windows 11 x64
b) Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022
c) macOS Monterey 12, macOS Ventura 13
d) Red Hat Enterprise Linux 7, 8, 9, SUSE Linux Enterprise 12 and 15, CentOS 7, Ubuntu 18.04, 20.04, 22.04

(6) EPM musí zajistit správu přístupu k citlivým informacím a systémům pomocí správy oprávnění a privilegií a definovat, které aplikace jsou povoleny a které jsou zakázány pro použití na koncových zařízeních. Nástroj musí detekovat a zamezit rizikům v reálném čase, jako jsou pokusy o zneužití přístupových práv, krádeže údajů nebo infekci počítače malwarem.

3.2.8.2 – pokročilá ochrana Anti-X

(1) Systém dodaný a implementovaný v rámci této komodity bude představovat účinnou ochranu všech koncových zařízení úřadu proti známým hrozbám založeným na detekci signatur (antivir, antimalware, síťová IDS/IPS) a také na detekci na základě chování (funkcionalita EDR/XDR, detekce anomálií, analýza rizik koncové stanice a další.) včetně integrace s MITRE modelem.

(2) Zadavatel v současnosti využívá externích služeb bezpečnostního dohledu (SOC), je proto požadováno, aby byl systém Anti-X schopen integrace s nástroji SIEM a to minimálně na úrovni zasílání zpráv ve formátu CEF, popřípadě Syslog.

3.2.9. K.9 – Monitorování práce s digitálními daty

(1) DLP (Data Loss Prevention) je technologie, která slouží k ochraně citlivých informací a zabránění jejich úniku z organizace. Cílem je implementovat DLP nástroj, který umožní zadavateli monitorovat a chránit data, která jsou považována za citlivá ze zákona (např. GDPR), nebo z pohledu interních předpisů zadavatele. Zároveň také musí napomáhat identifikovat zaměstnance s potenciálně rizikovým chováním.

(2) Technologie DLP musí splňovat následující požadavky:

a) identifikovat citlivá data
b) vyhledat citlivá data na úložištích a v počítačích uživatelů
c) zabránit jejich neautorizovaným výskytům či přesunům a provádět v tomto smyslu bezpečnostní audit.
d) sledovat rizikové chování zaměstnanců.

(3) DLP systém bude zajišťovat jednotnou správu a monitoring práce uživatelů s citlivými daty zadavatele a jejich následnou ochranu před zneužitím nebo odcizením.

(4) Zadavatel požaduje, aby systém zajišťoval ochranu dat na koncových zařízení uživatelů a serverech a byl centrálně řízen management konzolí.

(5) DLP Systém musí být do budoucna rozšiřitelný o tzv. Network DLP, který bude schopen detekovat únik citlivých informací přes komunikační kanály internetové pošty na SMTP protokolu a webového provozu na protokolech HTTP/HTTPS a o systém UEBA, který zajišťuje sledování chování uživatelů a automatické nastavení rizikovosti uživatelů.

(6) Analýza citlivých dat představuje nejdůležitější část projektu. Na základě spolupráce s dodavatelem bude provedena analýza dat, která budou následně monitorována nebo chráněna pomocí DLP systému. Tato akce je klíčová pro to, aby bylo možné pokrýt co nejvíce citlivých informací, které musí být sledovány a zároveň aby systém DLP nezatěžoval systémy zadavatele, ať už se jedná o koncové stanice, servery nebo sítovou infrastrukturu.

(7) Analýza citlivých informací musí pokrýt tyto oblasti:

a) Data na úložištích – úložiště, kde mohou být uložena citlivá data
b) Data generovaná aplikacemi – aplikace, které generují citlivá data
c) Data generovaná ve webových aplikacích – webové aplikace, ze kterých uživatelé exportují data a ukládají je na svých koncových zařízení nebo sdílených úložištích
d) Práce uživatele s daty:
    I. Vytvoření citlivých dat
    II. Ukládání citlivých dat
    III. Modifikace citlivých dat
    IV. Odesílání, kopírování citlivých dat
    V. Sledování pohybu dat
    VI. Zálohování a archivace dat

(8) DLP (Data Loss Prevention) umožní monitorovat, detekovat a kontrolovat tok dat v rámci firemní sítě. Aby byl DLP systém efektivní, musí splňovat určité technické požadavky. Tyto požadavky se týkají především integrace s dalšími systémy, podpory klasifikace různých typů dat, schopnosti detekovat a reagovat na různé hrozby, výkonu a škálovatelnosti systému, a také možnosti zpracovávat data v reálném čase.

3.2.10. K.10 – Ochrana datové základny úřadu

(1) Serverové prostředí zadavatele je v současnosti umístěno v primárním datovém centru. Cílem této části projektu je vybudování záložního (disaster recovery) datového centra. Do tohoto datového centra se bude průběžně online replikovat serverové prostředí z primárního datového centra. V případě výpadku tohoto DC, musí být v řádu minut zajištěn náběh kompletních služeb ze záložního datového centra. K náběhu musí dojít automatizovaně a řízeně. Pro zajištění výše popsané funkcionality musí dojít k pořízení dále popsaných komponent.

(2) Záložní server – tento server musí disponovat dostatečným výkonem, aby byl schopen pokrýt nároky celého serverového prostředí úřadu (konkrétní požadavky na záložní server jsou definovány v kapitole 3.3).

(3) Diskové úložiště – diskové úložiště musí poskytovat záložnímu serveru dostatek úložné kapacity pro uložení replik všech chráněných virtuálních serverů, zároveň musí mít i odpovídající výkon pro spuštění a provoz serverového prostředí v případě výpadku. (konkrétní požadavky na diskové úložiště jsou definovány v kapitole 3.3).

(4) OS záložního serveru – v rámci projektu dojde k pořízení licencí operačního systému, který bude schopen integrace se stávajícím clusterem MS Hyper-V serveru. Operační systém nesmí být licencován na základě počtu virtuálních serverů a licence musí pokrýt počet jader CPU záložního serveru.

(5) Licence databázového serveru – dodávka zahrnuje rovněž licence databázového serveru Microsoft SQL v aktuální verzi (použití tohoto typu databázového serveru je přímo určeno aplikacemi provozovanými v IT prostředí úřadu). Licence musí být určena pro provoz ve virtualizovaném prostředí a musí být schopna migrace mezi nody Hyper-V clusteru dle provozních okolností zadavatele bez dalšího omezení.

(6) SW licence zabezpečeného úložiště – SW vlastnosti, které mohou být realizovány buď funkcionalitou samotného diskového úložiště, případně mohou být realizovány pomocí nadstavbového software produktu. Funkcionality musí zahrnovat konzistentní replikaci minimálně na úrovni virtuálních serverů běžících v primární lokalitě. Replikaci celých skupin serverů (dle funkčních bloků infrastruktury), možnost replikace oběma směry (např. po obnovení po výpadku primární lokality). Zároveň je vyžadováno, aby bylo možné spustit replikované servery v odděleném prostředí bez dopadu na funkčnost primárního prostředí.

(7) Úložiště záloh s řízenou retencí – pásková knihovna standardu LTO9 (https://www.lto.org/lto-9/) pro uložení offline záloh. Dojde k pořízení páskové knihovny, která bude osazena min. 1 mechanikou LTO Ultrium 9 a musí mít kapacitu minimálně 24 pásek. Mechanika musí být plně integrovaná do stávajícího systému pro zálohování infrastruktury úřadu.

(8) Vzhledem k tomu, že zadavatel nedisponuje dostatečným prostorem ve stávajících rackových skříních a zároveň musí dojít k přidání dalších zařízení, budou dodány datové rozvaděče vč. non IT technologií, do stávajících technologických prostor. Dodávka bude zahrnovat rovněž instalaci na místo a připojení k datovým a silovým rozvodům.

(9) Pro bezpečné připojení koncových uživatelů k centrálním aplikacím úřadu slouží stávající infrastruktura terminálové přístupu Cirtix XenApp. V rámci předmětu plnění bude pořízeno 50ks tenkých klientů, které budou začleněny do stávajícího systému centrální správy tenkých klientů.

3.2.13. K.11 – Centrální komunikační systém úřadu

(1) Pro zajištění bezpečné hlasové komunikace úřadu, dojde k pořízení IP telefonní ústředny s přidanými funkcionalitami.

(2) Nad rámec běžné hlasové komunikace, bude telefonní ústředna integrována se stávajícími adresářovými službami úřadu (Microsoft AD) na úrovni globálního telefonního seznamu a identifikace volajícího. Zároveň musí být součástí dodávky integrace s MS Outlook pro všechny uživatele úřadu. Integrace umožní vytáčení hovorů z přímo z prostředí aplikace, hovor je následně uskutečněn přímo z fyzického telefonního přístroje.

(3) Vzhledem k tomu, že zadavatel disponuje stávajícími 250ks telefonních přístrojů, je požadováno, aby pořizovaná telefonní ústředna byla plně kompatibilní se stávajícími přístroji, a to minimálně na úrovní následujících funkcionalit:

(a) Předávání hovoru

(b) Volání jiného účastníka, střídání hovorů

(c) Přidržení hovorů

(d) Skupinové hovory

(e) Konferenční hovory

(f) Parkování hovoru

(g) Zpětné voláni

(4) Součástí dodávky musí být také hlasová brána, která umožní připojení telefonní ústředny do JTS.

(5) Vzhledem k delšímu životnímu cyklu IP telefonní ústředny, musí být součástí dodávky technická podpora výrobce ústředny v délce 7 let.

3.3. Specifické požadavky – povinné parametry řešení

(1) V zadávací dokumentaci, část 3b Povinné parametry, jsou v tabulkách jsou uvedeny minimální požadované (povinné) parametry dodávaného řešení.

(2) **Účastník ve své nabídce detailně popíše způsob naplnění každého povinného parametru včetně značkové specifikace nabízených dodávek. Účastník tedy uvede konkrétní technické parametry nabízeného zboží, vč. uvedení výrobce a obchodního / typového označení jednotlivých komponentů. Údaje o výrobci a obchodním (či typovém) označení budou uvedeny a doloženy v tabulkách povinných parametrů; konkrétní parametry mohou být buď rovněž doplněny do tabulky, nebo mohou být doloženy jinde v nabídce např. formou katalogových listů apod., v takovém případě ale musí být v tabulce odkázáno na část nabídky, ve které je možné naplnění parametru ověřit.**

(3) **Popis způsobu naplnění každého povinného parametru bude konkrétní, úplný a musí prokazovat (nepostačuje pouze potvrzení či zkopírování požadavku Zadavatele), že nabízené řešení jednoznačně splňuje všechny požadavky.**

(4) **Uchazeč musí všechny povinné parametry splnit, v případě nesplnění je jeho nabídka vyloučena.**

(5) **Uchazeč musí uvádět úplné produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení).**

(6) **Požadavek na maximální využitelný prostor pro poptávané zařízení tzn. výšky zařízení (v jednotkách U) je založený na objektivní skutečnosti tzn. omezeném prostoru v rackových skříních a zároveň omezeném prostoru pro umístění racku v prostorách zadavatele. Uchazeč může v odůvodněných případech překročit požadavek na maximální velikost výšky konkrétního zařízení, tak jak je stanoven v kap. 3.3., ale celkový souček výšek dodávaných zařízení v racku však nesmí překročit celkový součet požadovaných výšek zařízení v daném racku.**

3.4. Požadavky na kompatibilitu s ostatními systémy

(1) Veškeré softwarové komponenty nabízeného řešení budou provozovány ve virtuálním prostředí Microsoft Hyper-V a musí být pro běh v tomto prostředí výrobcem podporovány.

3.5. Požadavky na typy klientů

(1) Webová rozhraní nabízených systémů a zařízení být funkční v obvyklých internetových prohlížečích – min. Edge, Chrome, Safari v aktuálních verzích bez potřeby instalace speciálních doplňků či plug-in modulů.

3.6. Požadavky na bezpečnost informací

(1) Veškeré nástroje pro správu musí umožňovat správu interních účtů (min. jméno a heslo) a/nebo napojení na LDAP/Active Directory.

(2) Veškeré nástroje pro správu musí umožňovat definici s minimálně 2 úrovněmi oprávnění – monitoring (pouze čtení), administrátor (plná správa)

(3) Veškeré nástroje pro správu musí komunikovat se zařízeními šifrovanými protokoly (SSH apod.). Také v případě vestavěných nástrojů (např. www rozhraní hardware) musí být použita šifrovaná komunikace (např. HTTPS).

(4) Bezpečnost vnější komunikace publikovaných webových rozhraní aplikací a systémů bude zajištěna použitím tzv. „hvězdičkového“ (wildcard) certifikátu veřejné certifikační autority, tj. takové autority, jejíž kořenový certifikát je součástí běžných operačních systémů a je automaticky obnovován v rámci běžných updatů operačních systémů. Účastník může využít stávající certifikát zadavatele nebo dodat jím preferovaný jako součást nabízeného řešení.

3.7. Požadavky na záruky a licence

(1) Zadavatel požaduje zajištění potřebných licencí pro implementaci a následný provoz zařízení dodávaných v předmětu plnění.

(2) Pro každý softwarový produkt, který uchazeč nabídne v rámci svého řešení, budou v nabídce výslovně uvedeny všechny licenční nebo výkonové požadavky spojené s instalací a provozem řešení, včetně uvedení konkrétní infrastruktury, na které bude řešení provozováno.

(3) Licence musí umožnit plnou funkcionalitu zařízení v rozsahu uvedeném v části 3a a 3b zadávací dokumentace a musí umožnit plnohodnotný přístup uživatelů.

(4) Zadavatel požaduje záruku na veškeré dodané technologie v délce trvání minimálně 24 měsíců od okamžiku předání do zkušebního provozu. Uchazeč ve své nabídce výslovně uvede všechny podmínky záruk.

(5) Uchazeč ve své nabídce uvede ceny záruky do příslušné části kalkulace (část 1 Zadávací dokumentace) takto:

(a) Standardní záruka a standardní podpora běžně poskytovaná výrobcem technologie na území České republiky bude součástí pořizovací ceny zařízení.

(b) Cenu nadstandardních záruk a nadstandardních podpor (včetně aktualizací software/firmware apod.) požadovaných Zadavatelem (tj. rozdíl mezi Standardními zárukami a podporami a požadavky Zadavatele) Uchazeče uvede v položce "Nadstandardní záruky a podpory výrobců" a to dle charakteru zařízení do části hardware nebo software.

(6) Veškeré opravy po dobu záruky budou provedeny bez dalších nákladů pro zadavatele. Veškeré komponenty, náhradní díly a práce, poskytnuté v rámci záruky budou poskytnuty bezplatně.

(7) Hlášení záručních závad, řízení a evidence průběhu jejich řešení bude probíhat stejným způsobem a s využitím stejného helpdeskového systému jako u podpory provozu dle kap. 5. Servisní podpora výrobce bude v českém jazyce.

(8) Minimální rozsah licencí a minimální požadavky na nadstandardní záruku a podporu výrobců jsou uvedeny v následující tabulce:

Kom.	Zajišťovaná oblast	Stručný popis položky	ID opatření	Požadavky na licence	Požadavky na nadstandardní záruku a podporu výrobců
K.1	Zabezpečení datových rozvaděčů	Zabezpečení centrálních datových rozvaděčů	ID001	Licence pro přístup do monitorovacího systému pro 5 uživatelů	-
		Zabezpečení podružných datových rozvaděčů	ID001		-
K.2	Zvýšení zabezpečení sítě LAN	Páteřní přepínače	ID002	-	Technická podpora a aktualizační balíčky zranitelností v délce 60 měsíců, 8x5 support na celé řešení od výrobce
		Přístupové přepínače 24p	ID002		
		Přístupové přepínače 48p	ID002		
		Místní přepínače	ID002		
		Rozšíření optických tras	ID002	-	-
K.3	Zvýšení zabezpečení sítě WiFI	Bezdrátové přístupové body	ID002	Licence pro centrální kontroler bezdrátové sítě	Technická podpora a aktualizační balíčky zranitelností v délce 60 měsíců, 8x5 support na celé řešení od výrobce
K.4	Zavedení nástrojů ověřování zařízení přistupujících do počítačové sítě – 802.1x	Systém bezpečného přístupu do sítě 802.1x	ID002	Licence pro současné ověření minimálně 300 zařízení	Technická podpora a aktualizační balíčky zranitelností v délce 60 měsíců, 8x5 support na celé řešení od výrobce
K.5	Systém pro centrální správu sítě	Systém centrální správy sítě	ID002	Licence pro všechny přepínače dodané v rámci projektu i pro stávající přepínače zadavatele	Technická podpora a aktualizační balíčky zranitelností v délce 60 měsíců, 8x5 support na celé řešení od výrobce
K.6	Interní segmentační firewall	Interní segmentační firewall	ID002	Licence pro UTM funkcionality	Technická podpora a aktualizační balíčky zranitelností v délce 60 měsíců, 24x7support na celé řešení od výrobce

K.7	Správa privilegovaných účtů	SW pro správu privilegovaných účtů a přístupů	ID003	Licence pro min. 50 přistupujících uživatelů nebo řízených privilegovaných účtů. Licence pro minimálně 100 cílových zařízení nebo aplikací.	Technická podpora a aktualizační balíčky zranitelností v délce 60 měsíců, 8x5 support na celé řešení od výrobce
K.8	Ochrana koncových zařízení	Pokročilá anti-X ochrana	ID004	Licence pro 200 koncových zařízení	Technická podpora a aktualizační balíčky zranitelností v délce 60 měsíců, 8x5 support na celé řešení od výrobce
		Pokročilá ochrana koncových zařízení s rozšířenou detekční schopností	ID004	Licence pro 170 koncových zařízení a 10 serverů	Technická podpora a aktualizační balíčky zranitelností v délce 60 měsíců, 8x5 support na celé řešení od výrobce
K.9	Monitorování práce s digitálními daty	SW pro monitorování práce s digitálními daty	ID005	Licence na zařízení – počítač nebo notebook uživatele a servery, kde bude DLP systém implementován. Licence musí obsahovat i jednotnou centrální management konzoli pro správu celého DLP systému. Licence pro 250 uživatelů	Technická podpora a aktualizační balíčky zranitelností v délce 60 měsíců, 8x5 support na celé řešení od výrobce
K.10	Ochrana datové základny úřadu	Záložní server	ID006	-	Záruka a technická podpora výrobce po dobu 60 měsíců v režimu 24x7 na místě instalace s reakční dobou na zahájení servisu 4 hodiny od nahlášení vady.
		Diskové úložiště	ID006	-	Záruka a technická podpora výrobce po dobu 60 měsíců v režimu 9x5 s odezvou následujícího pracovního dne (NBD) a včetně SW podpory, která umožňuje přístup k novým verzím FW, opravným patchům atd.
		Zabezpečené úložiště záloh s řízenou retencí	ID006	-	Záruka a technická podpora výrobce po dobu 60 měsíců v režimu 9x5 na místě s reakční dobou NBD od nahlášení závady

		SW licence operačních systémů záložního serveru	ID006	OS licence umožňující spuštění neomezeného množství virtuálních serverů, licence musí pokrývat všechna CPU jádra, dodaná v rámci Záložního serveru. DB licence pro provoz ve virtualizovaném prostředí, možnost migrace mezi nody Hyper-V bez dalšího omezení, minimálně pro 8 CPU jader.	-
		SW licence zabezpečeného úložiště	ID006	V dodávce musí být zahrnuty softwarové licence na ochranu min. 56 (stávajících) virtuálních serverů. V případě, že navržené řešení je licencováno na kapacitu, zadavatel požaduje zalicencovat provozovanou kapacitu datového úložiště.	Technická podpora a aktualizační balíčky zranitelností v délce 60 měsíců, 8x5 support na celé řešení od výrobce
		Datové rozvaděče 19" vč. non IT technologií	ID006	-	-
		Tenký klient	ID006	-	-
K.11	Centrální komunikační systém úřadu	Hlasová brána	-	-	Technická podpora a aktualizační balíčky zranitelností v délce 60 měsíců, 8x5 support na celé řešení od výrobce
		Centrální komunikační systém úřadu	-	-	Technická podpora a aktualizační balíčky zranitelností v délce 84 měsíců, 8x5 support na celé řešení od výrobce

4. Implementační služby

4.1. Obecné požadavky

(1) Zadavatel požaduje provést minimálně následující implementační práce na dodaných komponentech a případně dalších zařízeních. Uchazeč je dále povinen zahrnout do nabídky veškeré další činnosti a prostředky, které jsou nezbytné pro provedení díla v rozsahu doporučeném výrobci a dle tzv. nejlepších praktik, i v případě, pokud nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné. Implementační služby budou minimálně v následujícím rozsahu:

(a) Zajištění projektového vedení realizace předmětu plnění.

(b) Zpracování prováděcí dokumentace, která představuje projektovou dokumentaci, podle které se projekt bude realizovat. Součástí zpracování prováděcí dokumentace je mj. provedení předimplementační analýzy a zpracování finálního návrhu cílového stavu. Prováděcí dokumentace musí respektovat a využívat osvědčené praktiky (tzv. Best Practice) a doporučení výrobců nabízených technologií.

(c) Dodávku nabízených prvků a kompletní implementaci řešení provedenou podle prováděcí dokumentace a splňující povinné parametry technického řešení,

(d) Provedení školení,

(e) Zajištění zkušebního provozu,

(f) Provedení akceptačních testů,

(g) Zpracování provozní dokumentace v rozsahu detailního popisu skutečného provedení a popisu činností běžné údržby a administrace systémů a činností pro spolehlivé zajištění provozu.

(h) Předání do ostrého provozu,

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

(3) Uchazeč je dále povinen zahrnout do nabídky i další související služby minimálně v dále uvedeném rozsahu. Pro každou uvedenou službu uvede uchazeč podrobný popis způsobu provedení služby při realizaci předmětu plnění zohledňující požadavky zadavatele na technické řešení, včetně zajištění požadavků dle kapitoly 3, zajištění požadavků na podporu provozu dle kapitoly 5; a to vše při zohlednění stávajícího stavu:

Komodita	Oblast	Popis požadovaných činností
K.1	Zabezpečení datových rozvaděčů	1. Zavedení dohledu stavu prostředí v datových rozvaděčích zadavatele (kontrola vstupu, teploty a vlhkosti), zajištění notifikací při překročení prahových hodnot 2. Zajištění bezpečného napájení datových rozvaděčů Zadavatele, dodávka 12ks záložních napájecích zdrojů UPS včetně LAN konektivity a integrace se stávajícím dohledovým systémem Zadavatele Zabbix
K.2	Zvýšení zabezpečení sítě LAN	1. Dodání a nasazení páteřních přepínačů v georedundantním designu 2. Dodání a nasazení přístupových přepínačů 3. Dodání a nasazení místních přepínačů 4. Rozšíření stávajících optických tras a nasazení technologie CWDM
K.3	Zvýšení zabezpečení sítě WiFI	1. Implementace centrálního kontroleru bezdrátové sítě ve virtuální infrastruktuře 2. Dodání a instalace přístupových bodů bezdrátové sítě

Komodita	Oblast	Popis požadovaných činností
K.4	Zavedení nástrojů ověřování zařízení přistupujících do počítačové sítě – 802.1x	1. Analýza stávajícího síťového prostředí, návrh segmentované síťové infrastruktury 2.Dodávka a instalace systému pro centrální ověřování zařízení přistupujících do sítě 3. Zavedení segmentace a IEE802.1X vč. vytvoření bezpečnostních politik
K.5	Systém pro centrální správu sítě	1. Zavedení nástroje pro centrální správu síťových zařízení LAN i WiFi
K.6	Interní segmentační firewall	1.dodání a implementace redundantního clusteru interních segmentačních firewallů 2.ve vazbě na K.4 implementovat řízení komunikace mezi jednolitými segmenty sítě
K.7	Správa privilegovaných účtů	1.dodání a implementace systému pro jednotnou správu a monitoring privilegovaných účtů Zadavatele. 2.vytvoření bezpečnostních politik pro schvalování přístupů a práv
K.8	Ochrana koncových zařízení	1.Dodávka a implementace systému pokročilé Anti-X ochrany na koncových zařízeních Zadavatele, včetně funkcionality EDR/XDR. 2.Dodání systému pokročilé ochrany koncových zařízení EPM
K.9	Monitorování práce s digitálními daty	1.dodání systému typu Data Lost Prevention (DLP) 2.vytvoření politik pro klasifikaci dat 3.konfigurace systému dle vytvořených politik
K.10	Ochrana datové základny úřadu	1. Analýza současného způsobu ukládání a zálohování dat, návrh způsobu rozšíření virtualizace a zálohování bez významného omezení provozu. Dodání třetího uzlu serveru do záložní lokality úřadu pro zajištění DR funkcionality 2. Návrh rozšíření diskové virtualizace a dodání diskového úložiště pro záložní server (v záložní lokalitě) a konfigurace replikace dat z primární lokality na toto úložiště 3.dodání zabezpečeného úložiště záloh s řízenou retencí 4.dodání SW licence operačních systémů záložního serveru, včetně aktuální verze databázového serveru 5.sw licence pro zabezpečené úložiště zajišťující konzistentní replikaci virtuálních serverů a aplikací
K.11	Datové rozvaděče vč. Non IT technologií	1.dodání a kompletní instalace racků
K.12	Tenký klient	Dodávka tenkých klientů
K.13	Centrální komunikační systém úřadu	1.Dodávka a implementace HW IP telefonní ústředny 2.Dodávka a implementace SW IP telefonní ústředny 3.Dodávka a implementace hlasové brány

(4) Uchazeč dle svého uvážení může doplnit v nabídce další služby, které jsou dle jeho názoru potřebné pro úspěšnou realizaci zakázky.

(5) Veškerá dokumentace musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standartních formátech (MS Office) používaných zadavatelem.

4.2. Požadavky na zpracování prováděcí dokumentace

(1) Uchazeč 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.

(2) Jako podklad pro zpracování prováděcí dokumentace tedy uchazeč provede předimplementační analýzu, která bude zohledňovat stávající prostředí zadavatele ve vztahu ke konkrétnímu nabízenému plnění uchazeče, zejména pak s ohledem na uchazečem použité technické řešení, minimálně pro následující oblasti:

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

(b) Způsob začlenění nabízených komodit do prostředí zadavatele.

(c) Síťová infrastruktura ve vztahu k plánovanému využití.

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

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

(f) Integrace nabízených softwarových systémů.

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

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

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

(j) Integrace s virtualizační platformou Microsoft Hyper-V ve vysoce dostupném režimu a integrace s dohledovým systémem Zadavatele (provoz a správu systému zajišťuje externí partner) min. v rozsahu doporučení parametrů pro sledování.

(k) Požadované součinnosti Zadavatele.

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

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

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

(b) Nutné a doporučené optimalizační a konfigurační změny dodávaných systému i všech navázaných systémů,

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

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

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

(f) Detailní popis zajištění bezpečnosti informací,

(g) Detailní harmonogram projektu včetně uvedení kritických milníků,

(h) Vazby na stávající systémy a jejich konfigurace,

(i) Návrh akceptačních kritérií a akceptačních testů,

(j) Detailní popis navrhovaných školení.

(k) Obsah a rozsah provozní dokumentace.

(4) Před zahájením projektu budou provedeny vstupní externí penetrační testy, výsledky budou uchazeči poskytnuty a relevantní opatření bude uchazeč povinen zapracovat do svého řešení tzn. i do prováděcí dokumentace. Realizace vstupních externích penetračních testů není součástí předmětu plnění.

(5) Prováděcí dokumentace bude ve lhůtě do 10 pracovních dní od předání zhotovitelem připomínkována objednatelem a připomínky budou ze strany zhotovitele vypořádány (tj.

zapracovány, případně s jasným a konkrétním písemným zdůvodněním odmítnuty jako nevalidní). Ze strany objednatele nebude v rámci připomínkování v případě nepravdivých, nepřesných nebo věcně nejasných informací v této dokumentaci požadováno její opravování na správné znění, bude se pouze jednat o vyznačení výše uvedených nedokonalostí a bude na zhotoviteli jejich řádné zpracování.

(6) **Prováděcí dokumentace musí být před zahájením realizace dalších etap plnění výslovně schválena zadavatelem**.

(7) Na základě provedené implementace bude prováděcí dokumentace aktualizována na skutečně provedenou včetně detailní konfigurace, a to jak funkční, tak provedené nastavení včetně podložení provedenými analytickými podklady a dokumenty. Aktualizovaná prováděcí dokumentace bude součástí dokumentace předávané v rámci předávacího protokolu.

4.3. Harmonogram realizace

(1) Uchazeč zajistí projektové vedení po celou dobu realizace zakázky osobou odpovědnou za realizaci předmětu plnění, která bude hlavní kontaktní osobou a která bude přítomna při všech jednáních týkajících se projektu.

(2) Zadavatel vyžaduje dodržení následujícího harmonogramu plnění – zde jsou uvedeny maximální možné lhůty pro jednotlivé kritické milníky. Údaj D značí datum účinnosti smlouvy o dílo, čísla značí počet kalendářních dnů. Údaj A značí datum předání díla, čísla značí počet kalendářních měsíců.

Poř. č.	Aktivita projektu	Nejpozdější termín pro dokončení aktivity
Etapa 1 - dodávky a implementace		
E1.1	Předimplementační analýza a zhotovení Prováděcí dokumentace	D+60
E1.2	Předání Prováděcí dokumentace Zadavateli, připomínkové řízení	D+60
E1.3	Zapracování připomínek a předání finální verze Prováděcí dokumentace – akceptace Zadavatelem	D+60
E1.4	Dodávky a implementace	D+360
E1.5	Školení uživatelů a administrátorů	D+360
E1.6	Zkušební provoz	D+360
E1.7	Akceptační testy	D+360
Etapa 2 - podpora provozu		
E2.1	Produkční provoz	A+min. 48 (měs)

(3) Uchazeč může dle svého uvážení výše uvedené maximální lhůty trvání v rámci Etapy 1 zkrátit při dodržení všech částí předmětu plnění a bez snížení kvality dodávaných služeb.

(4) Maximální lhůty trvání nesmí uchazeč při tvorbě detailního harmonogramu prodloužit.

(5) Uchazeč uvede závazný harmonogram plnění ve své nabídce a zároveň v návrhu smlouvy o dílo.

(6) Uchazeč uvede potřebnou součinnost zadavatele pro splnění harmonogramu plnění ve své nabídce.

4.4. Požadavky na školení

(1) Uchazeč zajistí školení pracovníků Zadavatele – administrátorů a uživatelů – na zařízení a systémy, dodávané v rámci této veřejné zakázky, a to minimálně v rozsahu předávané provozní dokumentace.

(2) Školení zajistí seznámení pracovníků Zadavatele se všemi podstatnými částmi díla v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin a pracovníkům bude vystaveno osvědčení o školení s uvedením rozsahu školení. Budou provedena tato školení:

(a) Školení administrátorů – minimální rozsah školení je 8 hodin, předpokládá se účast max. 6 účastníků, školení bude probíhat v sídle Zadavatele.

(b) Školení uživatelů – minimální rozsah školení je 2 hodiny, předpokládá se účast max. 200 účastníků, školení bude probíhat v sídle Zadavatele.

(3) Náklady na školení musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují a nelze je vyčíslit zvlášť.

4.5. Požadavky na provedení akceptačních testů a přechod do zkušebního (testovacího) provozu

(1) Uchazeč navrhne způsob a provedení akceptačních testů. Akceptační testy musí pro všechny komodity vždy zahrnovat minimálně:

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

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

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

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

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

(f) Výkonové testy prokazující shodu s požadovanými výkonnostními parametry a dále výrobcem deklarovanými či s ohledem na technologii objektivně očekávatelnými parametry:

(i) Propustnost a zpoždění (latence) u firewallu

(ii) Disaster recovery scénář přechodu vybraných virtuálních serverů z primární lokality do záložní a plnohodnotné zprovoznění služeb do definovaného času.

(iii) Propustnost a zpoždění (latence) u páteřního přepínače

(2) O provedení akceptace a jejím výsledku musí být vyhotoven písemný akceptační protokol. Šablony akceptačních protokolů budou předány zadavatelem při zahájení projektu, pro zapracování uchazečem do prováděcí dokumentace.

(3) Uchazeč zajistí pro každou komoditu zkušební (testovací) provoz v délce minimálně 30 dnů včetně technické podpory minimálně 1 specialisty na dodané řešení s dojezdem maximálně do 4 hodin od nahlášení požadavku v pracovní den v době od 8h do 17h. V případě předávání díla po částech (viz bod (4)) je uchazeč povinen zajistit zkušební (testovací) provoz pro předávané části díla až do doby zahájení plného provozu díla jako celku, při dodržení minimální požadované lhůty pro zkušební provoz.

(4) Dílo lze předávat i po jednotlivých částech (komoditách, v členění dle tabulky uvedené v kapitole 1, bod (2)), při dodržení následujících podmínek – dílo je možné předávat po

jednotlivých komoditách, přičemž podmínkou předání pro každou komoditu je provedení akceptačních testů alespoň v rozsahu bodu (1).

Etapa č. E1.4 – Dodávka a implementace	**Etapa č. E.1.6 – Zkušební provoz**	**Etapa č. E.1.7 – Zahájení plného provozu a poskytování technické podpory**
V případě hardware dodání kompletního zařízení, v případě software dodání licencí. Provedení akceptačních testů alespoň v rozsahu bodu (1)(a), (c)	Provedení akceptačních testů alespoň v rozsahu bodu (1)(b), (e)	Provedení akceptačních testů v rozsahu bodu (1)(d), (f)

(5) Po provedení akceptačních testů všech komodit, budou provedeny výstupní externí penetrační testy a uchazeč bude v rámci zkušebního provozu povinen vyřešit případné relevantní nedostatky dodaného řešení. Realizace výstupních externích penetračních testů není součástí předmětu plnění.

(6) Při předávání díla po částech bude po předání jednotlivých částí a dokončení díla jako celku následovat, akceptační řízení v plném rozsahu a předání celého díla. Jako podklad pro akceptaci celého díla budou sloužit akceptační protokoly s informacemi ohledně pokrytí požadavků akceptačních testů a zkušebního provozu z jednotlivých částí tzn. že již není nutné opakování akceptačních testů.

(7) Přechodem do plného provozu se rozumí okamžik akceptace díla v plném rozsahu včetně vypořádání všech vad a nedodělků.

4.6. Požadavky na dokumentaci

(1) Uchazeč zpracuje provozní dokumentaci, která bude detailně popisovat konfiguraci zhotoveného díla a jeho vazby na stávající systémy.

(2) Provozní dokumentace bude vycházet z prováděcí dokumentace, která bude před předáním do provozu aktualizovaná dle skutečného stavu.

(3) Součástí provozní dokumentace bude popis úkonů doporučené údržby a specifikace intervalů jejích provádění a další dokumentaci v rozsahu stanoveném v prováděcí dokumentaci.

(4) Součástí předané dokumentace budou podrobné uživatelské postupy pro Wifi připojení mobilních zařízení (tablety, chytré telefony, notebooky) s operačními systémy Windows 7 a 10, Android, iOS a macOS zohledňující nasazení systému řízení přístupů na bázi IEEE 802.1X.

(5) Uchazeč uvede do nabídky kompletní podmínky pro zajištění provozu dodaných prvků, včetně požadavků na aktualizace software (maintenance).

(6) Zhotovitel dále dodá uživatelskou dokumentaci, která bude obsahovat minimálně základní popis práce s dodaným řešením, dále bude popisovat funkcionality řešení, a to pro potřebu řádné orientace a práce uživatele. Dokumentace musí být zhotovena v českém jazyce. Dokumentace bude dodána v elektronické podobě umožňující její zobrazení a čtení prostřednictvím běžných nástrojů typu kancelářského balíku nebo ve formátu PDF.

(7) Zhotovitel dále dodá administrátorskou dokumentaci pro objednatele, která bude obsahovat popis správy a údržby dodaného řešení. Dokumentace musí být zhotovena v českém jazyce.

(8) Dokumentace bude dodána v elektronické podobě umožňující její zobrazení a čtení prostřednictvím běžných nástrojů typu kancelářského balíku nebo ve formátu PDF.

5. Požadavky na podporu provozu

5.1. Obecná pravidla provozu

(1) Zadavatel požaduje detailní návrh podmínek podpory provozu, zajišťující plnohodnotný provoz předmětu plnění od doby předání do provozu. Uchazeč podle svého uvážení může provést úpravu parametrů, pokud takové úpravy nepovedou ke zhoršení podmínek zajištění podpory provozu.

(2) Pro hlášení servisních požadavků zajistí Uchazeč Zadavateli přístup ke svému helpdeskovému systému s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení. Detailní popis helpdeskového systému a jeho obsluhy musí být součástí nabídky. Provozní doba helpdeskového systému musí být minimálně 8-17 hod. v pracovních dnech.

(3) Běžná pracovní doba zadavatele je období mezi 8:00 a 17:00 v pracovní dny.

(4) Pravidla vzdáleného přístupu budou vítěznému uchazeči předána při podpisu smlouvy.

(5) Neplánované zásahy do systému, které mohou ovlivnit uživatelské prostředí, jsou uživatelům oznámeny minimálně 1 hodinu před zahájením poskytování služby nebo činnosti.

(6) Plánované zásahy do systému, které mohou ovlivnit uživatelské prostředí, jsou uživatelům oznámeny minimálně 24 hodin před zahájením poskytování služby nebo činnosti

5.2. Požadavky na podporu provozu

(1) Rozsah základní servisní podpory:

(a) Provádění aktualizací firmware a software dodaných produktů (nezahrnuje upgrade na nové hlavní verze software) v rozsahu 3 hod měsíčně. Četnost aktualizací řídí Uchazeč s ohledem na zajištění spolehlivého provozu systémů a jejich bezpečnost a kritičnost aktualizací.

(b) Helpdeskový systém s on-line přístupem (web, e-mail) pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení.

(2) Rozsah rozšířené servisní podpory:

(a) Řešení Incidentů - pokud se během řešení Incidentu ukáže, že se jedná o vadu, která spadá pod záruku systému, nebude se čas potřebný pro řešení incidentu Zadavateli účtovat.

(b) Řešení Incidentů může být zahájeno na základně požadavku Zadavatele, na základě Zadavatelem schváleného požadavku třetí strany nebo na základě schváleného podnětu uchazeče.

(c) Odborná podpora – vzdálené konzultace pro podporované služby/produkty

(3) Pro případ, že bude zadavatel požadovat služby rozšířené servisní podpory podle odst. (2), budou tyto služby vyúčtovány na konci měsíce v hodinové sazbě uvedené v Kalkulaci ceny, dle skutečně realizovaných hodin rozšířené servisní podpory. Předpokládaný rozsah služeb rozšířené servisní podpory pro účely přípravy nabídky je 1 hodina měsíčně.

5.3. Způsob poskytování servisní podpory

(1) Servisní podpora je poskytována zejména následujícím způsobem:

(a) Prostřednictvím pracovníka uchazeče Vzdálenou správou

(b) Prostřednictvím pracovníka uchazeče přímo na pracovišti Zadavatele

(c) Prostřednictvím pracovníka uchazeče formou vzdálené konzultace

(2) Uchazeč provede záznam o provedení servisní podpory, v záznamu uveden relevantní informace včetně doby poskytování servisní podpory a záznam zašle elektronicky zadavateli. Servisní služby, které jsou poskytovány vzdálenou formou, mohou být evidovány v elektronickém seznamu provedených úkonů.

(3) Zadavatel je povinen zabezpečit uchazeči podmínky pro řádné plnění, zejména

(a) zajistit a udržovat podmínky pro Vzdálený přístup uchazeče,

(b) zajistit dostupnost nebo odpovídající zástup Odpovědné osoby Zadavatele, vyhrazení odpovídajících časových kapacit Odpovědné osoby Zadavatele a zajištění efektivní součinnosti odborných pracovníků Zadavatele,

(c) zabezpečit přítomnost kvalifikované osoby, která poskytne pracovníku uchazeče veškeré informace či přístupy potřebné k podpoře předmětného systému, resp. informace o zařízeních a programovém vybavení souvisejícím s předmětným systémem,

(d) umožnit uchazeči v případě nutnosti a po předchozím oznámení odstavení technických prostředků z běžného provozu,

(e) zajistit součinnost třetí strany, jestliže je to pro provedení služby potřebné.

(4) uchazeč je v případě potřeby též z vlastní iniciativy oprávněn požádat Zadavatele o dodatečné údaje o Incidentu a o nezbytnou součinnost Zadavatele na řešení Incidentu, bez které nelze zahájit či pokračovat v řešení Incidentu.

(5) Zadavatel je povinen

(a) elektronicky potvrdit uchazeči provedení služby,

(b) zajistit zálohování dat i programů a výměnu zálohovacích médií dle zálohovacího plánu, jejich dostupnost v případě potřeba a jejich uložení na bezpečných místech tak, aby bylo nešlo k jejich ztrátě nebo poškození,

(c) poskytovat potřebné nebo vyžádané informace a podklady včetně dokumentace k předmětnému systému nebo zařízení a programovému vybavení, které s ním souvisí.

5.4. Postup při řešení incidentů

(1) Zadavatel bude incident oznamovat uchazeči bez zbytečného odkladu jedním ze způsobů a na kontaktních místech uvedených ve Smlouvě o zabezpečení provozu, kam budou mít zajištěny přístup pověřené osoby Zadavatele.

(2) Součástí nahlášení požadavku Zadavatelem musí být:

(a) popis Incidentu nebo Požadavku,

(b) jiné relevantní upřesňující informace, včetně případných textových či obrazových příloh nezbytných pro replikaci incidentu,

(c) kontaktní osoba.

(3) Uchazečem používaný systém pro HelpDesk musí pokrýt uvedené informace pro nahlášení požadavku.

(4) Uchazeč zahájí řešení incidentu do 5 pracovních hodin od nahlášení, za pracovní hodiny se považuje období mezi 8:00 a 17:00 v pracovní dny.

(5) Uchazeč neprodleně potvrdí obdržení požadavku v systému HelpDesk a poskytne Zadavateli informace o předpokládaném způsobu řešení požadavku, požadavcích na součinnost Zadavatele a předpokládaný termín vyřešení požadavku.

(6) Uchazeč v průběhu řešení požadavku, pokud mu to charakter požadavku a způsob řešení umožňuje, průběžně informuje Zadavatele o aktuálním stavu a případných změnách v

předpokládaném způsobu, požadované součinnosti a termínů vyřešení. V případě že uchazeč v průběhu řešení požadavku zjistí, že se jedná o Incident, jehož zdroj je prvek třetích stran, informuje Zadavatele o této skutečnosti, předpokládaném způsobu, požadované součinnosti a termínů vyřešení a pokračuje v řešení v režimu BE (Best Effort) tzn. uchazeč vyvine maximální možné úsilí na provedení požadavku a zejména na zajištění požadovaných parametrů předmětu plnění v nejkratší možné době.

(7) Zjistí-li uchazeč v průběhu řešení Incidentu, že Incident je neodstranitelný, je v rámci Běžné pracovní doby povinen nepřetržitě pracovat na náhradním řešení a informovat o tomto stavu Zadavatele.

(8) Zjistí-li uchazeč v průběhu řešení Incidentu, že Incident má přímou souvislost s neodborným či neoprávněným jednáním osob Zadavatele případně byl Incident vyvolán produkty či službami třetí osoby, je uchazeč povinen bezodkladně informovat o tomto stavu Zadavatele. Zadavatel se zavazuje bezodkladně uhradit v plné výši náklady nad rámec této smlouvy uchazečem prokazatelně vynaložené k řešení Incidentu, přičemž samotná identifikace Incidentu je součástí plnění této smlouvy.

(9) Zadavatel je oprávněn dořešení Incidentu kdykoliv zastavit či pozastavit, přičemž nárok uchazeče na úhradu již vynaložených prostředků zůstává nedotčen. Incident je v tomto případě považován za vyřešený.

(10) V případě úspěšného vyřešení požadavku, je řešitel před ukončením požadavku povinen provést ověření funkčnosti služby (pokud je to možné). Iniciátora Incidentu informuje o:

(a) v případě Incidentu specifikuje příčinu (pokud je známa),

(b) vyzve iniciátora k ověření funkčnosti služby.

(11) Po ověření funkčnosti ze strany Zadavatele se Požadavek považuje za vyřešený.

(12) Po vyřešení požadavku uchazeč požadavek uzavře v systému HelpDesk a informuje Zadavatele.

(13) Zadavatel má právo ve lhůtě 10 dnů od uzavření požadavku vznést výhrady nebo připomínky ke způsobu řešení nebo k výslednému stavu; v takovém případě se požadavek nepovažuje za uzavřený a Strany se zavazují zahájit společné jednání za účelem odstranění veškerých vzájemných rozporů a nalezení shody nad způsobem řešení nebo výsledném stavu, a to nejpozději do pěti (5) pracovních dnů od výzvy kterékoliv Strany.

5.5. Záruky na servisní služby

(1) Zadavatel požaduje záruku na veškeré servisní služby provedené v rámci podpory provozu v délce trvání minimálně 3 měsíců (není-li u konkrétní služby uvedeno jinak) od okamžiku realizace. Veškeré opravy po dobu záruky budou bez dalších nákladů pro provozovatele.

4 Popis nabízeného technického řešení

4.1 Čestné prohlášení o původu nabízené dodávky

Čestně prohlašujeme, že:

1. Žádné z nabízených řešení není v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce jsou v době podání nabídky součástí stabilní verze operačního systému/firmware.

2. Všechny dodávky, které v rámci plnění dodáme Zadavateli:

    a. jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,

    b. mají plnou záruku od výrobce,

    c. mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,

    d. obsahuji licenci na používání příslušného softwaru,

    e. jsou určeny pro provoz v České republice,

    f. z databází výrobce, distributora či prodejce bude možné výše uvedené skutečnosti doložit.

V Plzni dne 08.01.2024

.....

[redacted]

4.2 Naplnění specifických parametrů

4.2.1 Obecné požadavky

4.2.1.1 Kompatibilita s ostatními systémy

Veškeré čistě softwarové komponenty nabízeného řešení budou provozovány ve virtuálním prostředí Microsoft Hyper-V a budou pro běh v tomto prostředí výrobcem podporovány.

4.2.1.2 Výkonnostní požadavky pro SW produkty

(a) Systém bezpečného přístupu do sítě 802.1x

CPU: min. 16 CPU jader
RAM: min. 32 GB RAM
HDD: min. 1000 GB

(b) Systém centrální správy sítě

CPU: min. 16 CPU jader
RAM: min. 128 GB
HDD: min. 1000 GB

(c) SW pro správu privilegovaných účtů a přístupů (centrální komponenty

CPU: min. 16 CPU jader
RAM: min. 16 GB RAM
HDD: min. 1500 GB

(d) Pokročilá anti-X ochrana (centrální komponenty)

CPU: min. 8 CPU jader
RAM: min. 16 GB RAM
HDD: min. 500 GB

(e) Pokročilá ochrana koncových zařízení s rozšířenou detekční schopností

CPU: min. 16 CPU jader
RAM: min. 32 GB RAM
HDD: min. 500 GB

(f) SW pro monitorování práce s digitálními daty

CPU: min. 16 CPU jader
RAM: min. 32 GB RAM
HDD: min. 500 GB

(g) SW licence operačních systémů záložního serveru

Jedná se operační systém záložního serveru, u kterého nelze specifikovat výkonové požadavky. Ty budou stanoveny v rámci tvorby prováděcí dokumentace.

Pro databázový server nelze rovněž přesně stanovit výkonové požadavky. Ty budou detailně rozpracovány po analýze požadavků stávajících aplikací Zadavatele v úvodní etapě realizace – tvorbě prováděcí dokumentace.

(h) SW licence zabezpečeného úložiště

Pro management komponenty jsou požadavky následující:

CPU: min. 16 CPU jader
RAM: min. 32 GB RAM
HDD: min. 500 GB

4.2.2 K.1 – Zabezpečení datových rozvaděčů

(1)

Součástí dodávky je instalace záložních zdrojů, které budou filtrovat jak špičky napětí, tak pomohou i překrýt krátkodobé výpadky dodávky el. energie z distribuční sítě.

(2)

V místech, kde jsou umístěny centrální technologie, budou instalovány záložní zdroje UPS s možností připojení externích baterií pro prodloužení doby zálohy. Ty budou umožňovat bezchybný provoz všech připojených technologií a vzdálený monitoring stavu. Ve dalších podružných rozvaděčích budou instalovány v rackových skříních další záložní zdroje UPS včetně vzdáleného monitoringu jejich stavu.

(3)

Kromě záložních napájecích zdrojů budou všechny racky také osazeny systémem pro monitoring provozních veličin, minimálně kontrolou vstupu, kontrolu teploty a vlhkosti, detekce požáru. Tento systém bude umožňovat přímé zasílání notifikací minimálně pomocí emailových zpráv. Zároveň budou všechny dohledové jednotky integrované do stávajícího centrálního dohledového systému Zabbix.

4.2.3 K.2 Zvýšení zabezpečení sítě LAN

(1)

Zvýšení zabezpečení sítě LAN spočívá ve modernizaci přepínačů LAN a nasazení jednotné úrovně zabezpečení sítě LAN. To zahrnuje jednak zvýšení dostupnosti LAN díky redundantnímu zapojení mezi obě centrální lokality.

(2)

Dodávka zahrnuje osazení v primárním datovém centru 2ks páteřních přepínačů a v záložním datovém centru 1ks páteřního přepínače. Všechny podružné rozvaděče a maximum přístupových přepínačů pak bude propojeno redundantně do obou datových center.

(3)

Aby bylo takové zapojení možné, je nutné doplnit stávající optické linky o technologii CWDM, která umožní vytvořit další logické spoje na jednom fyzickém páru optických vláken. Konkrétní návrh vlnových délek a rozložení mezi jednotlivé spoje, bude součástí návrhu dodavatele před samotným zprovozněním.

(4)

Po zprovoznění přepínačů a jejich propojení, dojde ke konfiguraci bezpečnostních mechanismů, jako např. k segmentaci lokální sítě, zabezpečení klíčových linek, zabezpečení servisních síťových protokolů (spanning-tree apod.). Všechna zařízení budou integrována do systému řízení přístupu do sítě a do systému centrální správy sítě.

4.2.4 Zvýšení zabezpečení sítě WiFi

(1)

Síť bude řídit dvojice bezdrátových kontrolérů ve vysoce dostupné konfiguraci tak, aby výpadek jednoho kontroleru neovlivnil fungování bezdrátové sítě.

(2)

Bezdrátové přístupové body budou rozmístěny v rámci prostor Zadavatele dle návrhu připraveného v rámci předimplementační analýzy.

(3)

Bezdrátové sítě budou reflektovat segmentaci do bezpečnostních zón navržených v rámci implementace systému 802.1x. Jinak se bude zacházet s veřejnou sítí (musí být implementován captive portál a izolace klientů), jinak se sítí určenou pro zařízení Zadavatele (802.1x, WPA3, certifikáty atd.).

4.2.5 K.4 – Zavedení nástrojů ověřování zařízení přistupujících do počítačové sítě – 802.1x

Součástí dodávky je zavedení ověřování zařízení přistupujících do drátové i bezdrátové sítě. Systém bude splňovat následující parametry:

(1)

Systém bude umožňovat nasazení a správu Network Admission Control (NAC) založený na standardu IEEE 802.1X. Tento řeší bezpečné připojení koncových stanic a konkrétních uživatelů na základě procesu autentizace (rozpoznání identity zařízení a uživatele) a autorizace (zpřístupnění konkrétních datových zdrojů podle uživatelské role, stavu koncového zařízení) a dalších atributů v rámci kontextu uživatele.

(2)

Integrované funkce zajišťují komunikaci s AAA serverem (RADIUS) a nastavují komplexní, přitom unifikované, bezpečnostní politiky pro autentizaci a autorizaci koncových bodů.

(3)

Architektura bude zaručovat, že všichni uživatelé (mobilní zaměstnanci, ale i dodavatelé nebo hosté) budou vždy jednoznačně identifikováni a prostřednictví přidělených rolí jim bude zajištěn bezpečný přístup ke všem informacím v síti, na které mají nárok.

(4)

Po ověření identity uživatele je mu přiřazena jedna z předem definovaných rolí, prostřednictvím které se může následně pohybovat v síti se všemi odpovídajícími právy i omezeními. Využitím informace získané při ověření identity spolu s rolemi skupin uživatelů nebo serverů připojených k síti, minimalizujeme rizika neoprávněných přístupů a zjednodušujeme celý proces nasazení bezpečnostních pravidel v síti i jejich následnou správu.

(5)

Bezpečnostní management bude poskytovat zjednodušenou správu bezpečnostních politik a umožní tak jejich konzistentní nastavení v rámci celé sítě. Předpokladem je řízení pravidel přístupu na LAN, WLAN (včetně tzv. „Guest Access“). Přitom v procesu definice pravidel bude bráno v úvahu více parametrů, které má systém k dispozici (identita uživatele, pracovní skupina, místo, čas, typ zařízení atd.). Budou definovány různé třídy přístupu podle různých vstupních parametrů, které budou aplikovány v definicích pravidel (policy).

(6)

Komunikaci koncové stanice bude možné dynamicky přesunout do jiného pracovního segmentu (ale i např. karantény) nebo uplatnit přístupové filtry tzv. „za běhu“ pomocí řízení CoA (Change of Authorization = proces aplikace pravidel pomocí rozšíření protokolu RADIUS) na základě aktuálního vyhodnocení vstupních parametrů (typ koncového zařízení, jeho stav, apod.).

(7)

Systém by měl být rozšířitelný i o řízení bezpečného transportu datovou sítí (implementace šifrování na rozhraních přepínačů) a možnosti škálovatelné filtrace přístupů k datovým zdrojům na základě uživatelských bezpečnostních rolí.

(8)

Důraz je kladen na vysokou dostupnost celého řešení (redundanci), centrální správu, dohled a možnosti vyhodnocení událostí, generace reportů apod. na jednom místě.

4.2.6 K.5 – Systém pro centrální správu sítě

(1)

Do systému pro centrální správu sítě budou začleněny všechny zařízení dodané v rámci části LAN i WiFi, dále pak stávající zařízení Cisco Catalyst 9200 a Cisco Catalyst 9300. Systém centrální bude umožňovat konfiguraci síťových politik pro celou síť. Zároveň systém umožní mikrosegmentaci na všech zapojených zařízeních.

(2)

Politiky pro síťová zařízení budou sdílené pro aktivní prvky LAN i WiFi, stejně tak pro uživatele, kteří se přes tyto sítě připojují.

4.2.7 K.6 – Interní segmentační firewall

(1)

V návaznosti na části K.2, K.3 a K.4 bude nasazen interní segmentační firewall, který bude oddělovat jednotlivé bezpečnostní segmenty a bude řídit prostupy mezi nimi a také přístup směrem k IS úřadu.

(2)

Firewall bude nasazen jako cluster složený z dvou plně redundantních uzlů s tím, že každý bude schopen plnohodnotně pokrýt všechny nároky, firewall bude schopen fungovat v režimu active/active. Firewall bude disponovat detekčními a prevenčními schopnostmi obvyklými u Next Generation firewallů (NGFW). Politiky budou navázány na identitu zařízení/uživatelů, na aplikační protokoly a kontext (čas, místo apod.).

4.2.8 K.7 – Správa privilegovaných účtů

(1)Součástí naší dodávky je systém pro řízení a správu privilegovaných účtů (dále jen PIM/PAM), který zajistí jednotnou správu přístupu k privilegovaným účtům a monitorování operací prováděných pod těmito účty s vazbou na konkrétního administrátora, který v danou chvíli účet používá, včetně dvou faktorové autentizace a poskytnutí podrobného seznámení se správou dodaného systému pro IT pracovníky zadavatele.

(2) Systém bude zajišťovat jednotnou správu a monitoring privilegovaných účtů Zadavatele.

(3) Řešení bude instalováno ve formě virtuálního serveru, který bude provozován na stávající virtualizační infrastruktuře Zadavatele (Microsoft Hyper-V).

(4) Vlastní přihlašovací údaje a klíče k cílovým systémům (operačním systémům, databázím, zařízením apod.) budou v chráněné a šifrované databázi systému.

4.2.9 K8 - pokročilá Anti-X ochrana

(1)

Systém dodaný a implementovaný v rámci této komodity bude představovat účinnou ochranu všech koncových zařízení úřadu proti známým hrozbám založeným na detekci signatur (antivir, antimalware, síťová IDS/IPS) a také na detekci na základě chování (funkcionalita EDR/XDR, detekce anomálií, analýza rizik koncové stanice a další.) včetně integrace s MITRE modelem.

(2)

Námi dodaný systém Anti-X bude schopen integrace s nástroji SIEM a to na úrovni zasílání zpráv ve formátu Syslog.

4.2.10 K.9 – Monitorování práce s digitálními daty

(1) Součástí naší dodávky je DLP nástroj, který umožní zadavateli monitorovat a chránit data, která jsou považována za citlivá ze zákona (např. GDPR), nebo z pohledu interních předpisů zadavatele. Zároveň také bude napomáhat identifikovat zaměstnance s potenciálně rizikovým chováním.

(2) Systém mimo jiné splňuje následující požadavky:

a)

umí identifikovat citlivá data

b)

umí vyhledat citlivá data na úložištích a v počítačích uživatelů

c)

umí zabránit jejich neautorizovaným výskytům či přesunům a provádět v tomto smyslu bezpečnostní audit.

d)

umí sledovat rizikové chování zaměstnanců.

(3) DLP systém bude zajišťovat jednotnou správu a monitoring práce uživatelů s citlivými daty zadavatele a jejich následnou ochranu před zneužitím nebo odcizením.

(4) Systém bude zajišťovat ochranu dat na koncových zařízení uživatelů a serverech a bude centrálně řízen management konzolí.

(5) DLP Systém je do budoucna rozšiřitelný o tzv. Network DLP, který bude schopen detekovat únik citlivých informací přes komunikační kanály internetové pošty na SMTP protokolu a webového provozu na protokolech HTTP/HTTPS a o systém UEBA, který zajišťuje sledování chování uživatelů a automatické nastavení rizikovosti uživatelů.

(6) Jako součást plnění bude provedena analýza dat, která budou následně monitorována nebo chráněna pomocí DLP systému. Tato akce je klíčová pro to, aby bylo možné pokrýt co nejvíce citlivých informací, které musí být sledovány a zároveň aby systém DLP nezatěžoval systémy zadavatele, ať už se jedná o koncové stanice, servery nebo sítovou infrastrukturu.

(7) Analýza citlivých informací bude pokrývat minimálně tyto oblasti:

a)

Data na úložištích – úložiště, kde mohou být uložena citlivá data

b)

Data generovaná aplikacemi – aplikace, které generují citlivá data

c)

Data generovaná ve webových aplikacích – webové aplikace, ze kterých uživatelé exportují data a ukládají je na svých koncových zařízení nebo sdílených úložištích

d)

Práce uživatele s daty:

I.

Vytvoření citlivých dat

II.

Ukládání citlivých dat

III.

Modifikace citlivých dat

IV.

Odesílání, kopírování citlivých dat

V.

Sledování pohybu dat

VI.

Zálohování a archivace dat

(8) DLP (Data Loss Prevention) bude monitorovat, detekovat a kontrolovat tok dat v rámci firemní sítě.

4.2.11 K.10 – Ochrana datové základny úřadu

(1)

Součástí naší dodávky je vybudování záložního (disaster recovery) datového centra. Do tohoto datového centra se bude průběžně online replikovat serverové prostředí z primárního datového centra. V případě výpadku tohoto DC, bude v řádu minut zajištěn náběh kompletních služeb ze záložního datového centra. K náběhu může dojít automatizovaně a řízeně.

(2)

Záložní server – disponuje dostatečným výkonem, aby byl schopen pokrýt nároky celého serverového prostředí úřadu

(3)

Diskové úložiště – diskové úložiště bude poskytovat záložnímu serveru dostatek úložné kapacity pro uložení replik všech chráněných virtuálních serverů, zároveň bude mít i odpovídající výkon pro spuštění a provoz serverového prostředí v případě výpadku.

(4)

OS záložního serveru – součástí naší nabídky jsou i licence operačního systému, který bude schopen integrace se stávajícím clusterem MS Hyper-V serveru. Operační systém není licencován na základě počtu virtuálních serverů a licence musí pokrývají počet jader CPU záložního serveru.

(5)

Licence databázového serveru – dodávka zahrnuje rovněž licence databázového serveru Microsoft SQL v aktuální verzi. Licence je určena pro provoz ve virtualizovaném prostředí a je schopna migrace mezi nody Hyper-V clusteru dle provozních okolností zadavatele bez dalšího omezení.

(6)

SW licence zabezpečeného úložiště – požadované SW vlastnosti jsou v rámci naší nabídky realizovány pomocí nadstavbového software produktu Zerto. Funkcionality zahrnují konzistentní replikaci na úrovni virtuálních serverů běžících v primární lokalitě. Replikaci celých skupin serverů (dle funkčních bloků infrastruktury), možnost replikace oběma směry (např. po obnovení po výpadku primární lokality). Zároveň je možné spustit replikované servery v odděleném prostředí bez dopadu na funkčnost primárního prostředí.

(7)

Úložiště záloh s řízenou retencí – pásková knihovna standardu LTO9 (https://www.lto.org/lto-9/) pro uložení offline záloh. V rámci naší nabídky je uvažováno pořízení páskové knihovny, která bude osazena 1 mechanikou LTO Ultrium 9 a má kapacitu 24 pásek. Mechanika musí bude plně integrovaná do stávajícího systému pro zálohování infrastruktury úřadu.

(8)

V rámci naší nabídky budou dodány datové rozvaděče vč. non IT technologií, do stávajících technologických prostor. Dodávka bude zahrnovat rovněž instalaci na místo a připojení k datovým a silovým rozvodům.

(9)

Pro bezpečné připojení koncových uživatelů k centrálním aplikacím úřadu slouží stávající infrastruktura terminálové přístupu Cirtix XenApp. V rámci plnění bude pořízeno 50ks tenkých klientů, které budou začleněny do stávajícího systému centrální správy tenkých klientů.

4.2.12 K.11 – Centrální komunikační systém úřadu

(1)

Pro zajištění bezpečné hlasové komunikace úřadu, nabízíme pořízení IP telefonní ústředny s přidanými funkcionalitami.

(2)

Nad rámec běžné hlasové komunikace, bude telefonní ústředna integrována se stávajícími adresářovými službami úřadu (Microsoft AD) na úrovni globálního telefonního seznamu a identifikace volajícího. Zároveň musí být součástí dodávky integrace s MS Outlook pro všechny uživatele úřadu. Integrace umožní vytáčení hovorů z přímo z prostředí aplikace, hovor je následně uskutečněn přímo z fyzického telefonního přístroje.

(3)

Vzhledem k tomu, že zadavatel disponuje stávajícími 250ks telefonních přístrojů, je součástí naší dodávky ústředna, která je plně kompatibilní se stávajícími přístroji, a to na úrovní následujících funkcionalit:

(a)

Předávání hovoru

(b)

Volání jiného účastníka, střídání hovorů

(c)

Přidržení hovorů

(d)

Skupinové hovory

(e)

Konferenční hovory

(f)

Parkování hovoru

(g)

Zpětné voláni

(4)

Součástí dodávky je také hlasová brána, která umožní připojení telefonní ústředny do JTS.

(5)

Vzhledem k delšímu životnímu cyklu IP telefonní ústředny, je součástí dodávky technická podpora výrobce ústředny v délce 7 let.

4.3 K.1a - Zabezpečení centrálních datových rozvaděčů

4.3.1 Nabízené řešení

4.3.1.1 Záložní zdroj – datové centrum

[redacted]

4.3.1.2 Monitoring prostředí

[redacted]

4.3.2 Způsob naplnění minimálních požadavků

4.3.2.1 Záložní zdroj – datové centrum

Položka	Popis parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně uvedení výrobce, obchodního označení, konkrétní konfigurace, produktového čísla, případně uvede konkrétní parametry	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
Záložní zdroj - Datové centrum	Typ: On-line	Online s dvojitou konverzí	Kapitola 4.3.1.1
	Instalace Rack 19"	ANO, sada součástí	Kapitola 4.3.1.1
	Možnost instalace mimo rack	ANO	Kapitola 4.3.1.1
	Dohledová ETH karta	ANO	Kapitola 4.3.1.1
	Včetně monitoringu a ovládání přes IP (RJ45 ethernet)	ANO	Kapitola 4.3.1.1
	Možnost připojení enviromentálních senzorů	ANO,[redacted]	Kapitola 4.3.1.1
	Minimální kapacita UPS 2500VA	3000 VA	Kapitola 4.3.1.1
	STATUS LED	ANO	Kapitola 4.3.1.1
	Možnost instalace přídavného bateriového modulu	ANO	Kapitola 4.3.1.1
	Vstupní napětí 140 - 280V	ANO,[redacted]	Kapitola 4.3.1.1
	Vstupní frekvence 50/60Hz +/- 3Hz	ANO,[redacted]	Kapitola 4.3.1.1
	Maximální přechodový čas 10ms	ANO	Kapitola 4.3.1.1
	Pracovní teplota 0-40C	ANO	Kapitola 4.3.1.1
	Výstupní konektory IEC 320 C13 - min. 7	ANO, 8	Kapitola 4.3.1.1

	Výstupní konektory IEC 320 C19 - min. 2	ANO, 2	Kapitola 4.3.1.1
	Battery power Vah - min. 700Vah	ANO, 700VAh	Kapitola 4.3.1.1

4.3.2.2 Monitoring prostředí

Položka	Popis parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně uvedení výrobce, obchodního označení, konkrétní konfigurace, produktového čísla, případně uvede konkrétní parametry	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
Monitoring prostředí	Ethernet port	ANO	Kapitola 4.3.1.2.
	WiFi+	ANO	Kapitola 4.3.1.2.
	1-Wire senzory	ANO - 8	Kapitola 4.3.1.2.
	RJ11 min. 1 port	ANO, 1xRJ11	Kapitola 4.3.1.2.
	Podpora napájení PoE	ANO	Kapitola 4.3.1.2.
	Počet připojitelných senzorů min. 5	ANO-8	Kapitola 4.3.1.2.
	Monitoring teploty	ANO	Kapitola 4.3.1.2.
	HTTPS	ANO	Kapitola 4.3.1.2.
	SNMP - SNMPv1 a SNMPv3	ANO	Kapitola 4.3.1.2.
	SNMP Trap	ANO	Kapitola 4.3.1.2.
	Podpora NET-GSM	ANO	Kapitola 4.3.1.2.
	SYSLOG	ANO	Kapitola 4.3.1.2.
	Možnost začlenění do dohledových systémů třetích stran	ANO	Kapitola 4.3.1.2.
	SMTP a SMTP TLS	ANO	Kapitola 4.3.1.2.
	IPv6	ANO	Kapitola 4.3.1.2.
	Podpora PIR senzorů	ANO	Kapitola 4.3.1.2.
	Podpora sensorů detekce požáru	ANO	Kapitola 4.3.1.2.
	Podpora senzorů zaplavení	ANO	Kapitola 4.3.1.2.
	Podpora senzorů vlhkosti	ANO	Kapitola 4.3.1.2.
	Podpora detektorů dveřních kontaktů	ANO	Kapitola 4.3.1.2.
	Podpora detektoru napájení 230V	ANO	Kapitola 4.3.1.2.
	Email alerting	ANO	Kapitola 4.3.1.2.
	Podpora PUSH protokolu	ANO	Kapitola 4.3.1.2.

4.4 K.1b - Zabezpečení podružných datových rozvaděčů

4.4.1 Nabízené řešení

4.4.1.1 Záložní zdroj - Přístupová lokalita

[redacted]

4.4.1.2 Monitoring prostředí

[redacted]

4.4.2 Způsob naplnění minimálních požadavků

4.4.2.1 Záložní zdroj - Přístupová lokalita

Položka	Popis parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně uvedení výrobce, obchodního označení, konkrétní konfigurace, produktového čísla, případně uvede konkrétní parametry	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
Záložní zdroj - Přístupová lokalita	Typ: Line-intaractive	ANO	Kapitola 4.4.1.1
	Instalace	V racku	Kapitola 4.4.1.1
	Možnost instalace mimo rack	ANO	Kapitola 4.4.1.1
	Včetně monitoringu a ovládání přes IP (RJ45 ethernet)	ANO	Kapitola 4.4.1.1
	Možnost připojení enviromentálních senzorů pomocí MGMT karty	ANO, součástí	Kapitola 4.4.1.1
	Minimální kapacita UPS 700VA	750VA	Kapitola 4.4.1.1

	STATUS LED	ANO	Kapitola 4.4.1.1
	Vstupní napětí min. 165V - 280V	160-286V	Kapitola 4.4.1.1
	Vstupní frekvence 50/60Hz	ANO	Kapitola 4.4.1.1
	Maximální přechodový čas max. 10ms	ANO	Kapitola 4.4.1.1
	Pracovní teplota 0-40C	ANO	Kapitola 4.4.1.1
	Výstupní konektory IEC 320 C13	ANO	Kapitola 4.4.1.1
	Battery power 310Vah	312VAh	Kapitola 4.4.1.1

4.4.2.2 Monitoring prostředí

Položka	Popis parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně uvedení výrobce, obchodního označení, konkrétní konfigurace, produktového čísla, případně uvede konkrétní parametry	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
Monitoring prostředí	Ethernet port	ANO	Kapitola 4.4.1.2
	WiFi+	ANO	Kapitola 4.4.1.2
	1-Wire senzory	ANO - 8	Kapitola 4.4.1.2
	RJ11 min. 1 port	ANO, 1xRJ11	Kapitola 4.4.1.2
	Podpora napájení PoE	ANO	Kapitola 4.4.1.2
	Počet připojitelných senzorů min. 5	ANO-8	Kapitola 4.4.1.2
	Monitoring teploty	ANO	Kapitola 4.4.1.2
	HTTPS	ANO	Kapitola 4.4.1.2
	SNMP - SNMPv1 a SNMPv3	ANO	Kapitola 4.4.1.2
	SNMP Trap	ANO	Kapitola 4.4.1.2
	Podpora NET-GSM	ANO	Kapitola 4.4.1.2
	SYSLOG	ANO	Kapitola 4.4.1.2
	Možnost začlenění do dohledových systémů třetích stran	ANO	Kapitola 4.4.1.2
	SMTP a SMTP TLS	ANO	Kapitola 4.4.1.2
	IPv6	ANO	Kapitola 4.4.1.2
	Podpora PIR senzorů	ANO	Kapitola 4.4.1.2
	Podpora sensorů detekce požáru	ANO	Kapitola 4.4.1.2
	Podpora senzorů zaplavení	ANO	Kapitola 4.4.1.2
	Podpora senzorů vlhkosti	ANO	Kapitola 4.4.1.2
	Podpora detektorů dveřních kontaktů	ANO	Kapitola 4.4.1.2

	Podpora detektoru napájení 230V	ANO	Kapitola 4.4.1.2
	Email alerting	ANO	Kapitola 4.4.1.2
	Podpora PUSH protokolu	ANO	Kapitola 4.4.1.2

4.5 K.2a - Páteřní přepínače

4.5.1 Nabízené řešení

4.5.2 Způsob naplnění minimálních požadavků

Položka	Popis parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně uvedení výrobce, obchodního označení, konkrétní konfigurace, produktového čísla, případně uvede konkrétní parametry	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
Páteřní přepínač	Typ přepínače L2/L3	ANO	Kapitola 4.5.1
	Formát přepínače - stohovatelný	ANO	Kapitola 4.5.1
	Počet dedikovaných stohovacích portů - 2 (případně porty neomezující min. počet portů pro připojení zařízení)	ANO, 2ks	Kapitola 4.5.1
	Minimální počet zařízení ve stohu - 8	ANO – 8	Kapitola 4.5.1
	Stateful Switch Over v rámci stohu	ANO	Kapitola 4.5.1
	Min. přepínací kapacita - 1 Tbps	ANO	Kapitola 4.5.1
	Min. paketový výkon přepínače - 744 Mpps	ANO	Kapitola 4.5.1
	Vzdálený port mirroring (ERSPAN)	ANO	Kapitola 4.5.1
	Min. velikost sdíleného systémového bufferu 16MB	ANO	Kapitola 4.5.1
	Redundantní ventilátory vyměnitelné za chodu zařízení	ANO	Kapitola 4.5.1
	Non-stop Forwarding	ANO	Kapitola 4.5.1
	Sdílení výkonu napájecích zdrojů napříč celým stohem	ANO	Kapitola 4.5.1
	Interní redundantní napájecí zdroj součástí dodávky	ANO	Kapitola 4.5.1
	Stohovací zdrojový kabel součástí dodávky	ANO	Kapitola 4.5.1

	Počet portů 1/10/25G SFP28 - 12, součástí každého přípínače 10ks 10G-BASE SFP+ moduly a 2ks 25G-BASE modulů, konkrétní vlnové délky CWDM budou zvoleny na základě prováděcí dokumentace	ANO, [redacted]	Kapitola 4.5.1
	Možnost přepínač rožšířit o modul s volitelným fyzickým rozhraním	ANO[redacted]	Kapitola 4.5.1
	Velikost MAC address tabulky - 32000	ANO	Kapitola 4.5.1
	Min. počet IPv4 routes - 39000	ANO	Kapitola 4.5.1
	Min. počet IPv6 routes - 19500	ANO	Kapitola 4.5.1
	Min. počet konfigurovatelných security ACL - 5000	ANO	Kapitola 4.5.1
	IEEE 802.3ad (Link Aggregation)	ANO	Kapitola 4.5.1
	IEEE 802.3ad přes více přepínačů ve stohu	ANO	Kapitola 4.5.1
	Minimálně 8 linek jako součást Link Aggregation Group trunku	ANO	Kapitola 4.5.1
	Minimální počet konfigurovatelných Link Aggregation Group trunků - 128	ANO	Kapitola 4.5.1
	Podpora protokolů:IEEE 802.1Q, IEEE 802.1x, IEEE 802.1w - Rapid Spanning Tree Protocol, IEEE 802.1ae, IEEE 802.3az, IEEE 802.1ar	ANO	Kapitola 4.5.1
	Minimální počet aktivních VLAN - 1000	ANO	Kapitola 4.5.1
	Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ANO	Kapitola 4.5.1
	Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	ANO	Kapitola 4.5.1
	Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů	ANO	Kapitola 4.5.1
	RADIUS CoA	ANO	Kapitola 4.5.1
	Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO	Kapitola 4.5.1
	Podpora jumbo rámců (min. 9198 bytes)	ANO	Kapitola 4.5.1
	Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO	Kapitola 4.5.1
	Směrování protokolů IPv4 a IPv6 v hardware	ANO	Kapitola 4.5.1
	OSPFv2 i OSPFv3	ANO	Kapitola 4.5.1
	Graceful Insertion and Removal	ANO	Kapitola 4.5.1
	IP Multicast (PIM SSM, PIM SM)	ANO	Kapitola 4.5.1
	Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)	ANO	Kapitola 4.5.1
	First Hop Redundancy Protokol (např. VRRP, HSRP)	ANO	Kapitola 4.5.1
	Reverse path check (uRPF) pro IPv4 i IPv6	ANO	Kapitola 4.5.1

	IGMPv2, IGMPv3, IGMP snooping, MLD snooping	ANO	Kapitola 4.5.1
	DHCP relay	ANO	Kapitola 4.5.1
	Minimální počet HW QoS front - 8	ANO	Kapitola 4.5.1
	QoS classification – ACL, DSCP, CoS based, QoS marking - DSCP, CoS, QoS - Strict Priority Queue	ANO	Kapitola 4.5.1
	Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	Kapitola 4.5.1
	QoS Policing	ANO	Kapitola 4.5.1
	QoS-Per Flow policing - min. 2 úrovně	ANO	Kapitola 4.5.1
	QoS-Hierarchical QoS	ANO	Kapitola 4.5.1
	First Hop Redundancy Protokol pro IPv6 (HSRPnebo VRRP)	ANO	Kapitola 4.5.1
	IPv6 services (Telnet, SSH, Syslog, DHCP)	ANO	Kapitola 4.5.1
	IPv6 QoS	ANO	Kapitola 4.5.1
	IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)	ANO	Kapitola 4.5.1
	IPv6 Port ACL, VLAN ACL	ANO	Kapitola 4.5.1
	Možnost definovat povolené MAC adresy na portu	ANO	Kapitola 4.5.1
	PACL, VACL	ANO	Kapitola 4.5.1
	Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ANO	Kapitola 4.5.1
	Bezpečnostní funkce umožňující ochranu proti připojení -autorizovaného DHCP serveru	ANO	Kapitola 4.5.1
	Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO	Kapitola 4.5.1
	Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ANO	Kapitola 4.5.1
	Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO	Kapitola 4.5.1
	Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení	ANO	Kapitola 4.5.1
	HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů	ANO	Kapitola 4.5.1
	Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	Kapitola 4.5.1
	Multicast DNS (mDNS) gateway	ANO	Kapitola 4.5.1

	Application Visibility - Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)	ANO	Kapitola 4.5.1
	Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	Kapitola 4.5.1
	Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, hodnota TTL, ICMP kód, IGMP type	ANO	Kapitola 4.5.1
	Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	Kapitola 4.5.1
	Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG	ANO	Kapitola 4.5.1
	Python scripting	ANO	Kapitola 4.5.1
	Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení	ANO	Kapitola 4.5.1
	SNMPv2/v3	ANO	Kapitola 4.5.1
	Podpora network boot (iPXE) pres IPv4 i IPv6	ANO	Kapitola 4.5.1
	Inventarizovatelnost komponent integrovanou RFID identifikací	ANO	Kapitola 4.5.1
	TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	Kapitola 4.5.1
	NTPv3 server	ANO	Kapitola 4.5.1

4.6 K.2b - Přístupové přepínače 24p

4.6.1 Nabízené řešení

[redacted]

4.6.2 Způsob naplnění minimálních požadavků

Položka	Popis parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně uvedení výrobce, obchodního označení, konkrétní	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru

		konfigurace, produktového čísla, případně uvede konkrétní parametry	
Přístupový přepínač 24p	Typ přepínače L2/L3	ANO	Kapitola 4.6.1
	Formát přepínače stohovatelný	ANO	Kapitola 4.6.1
	Minimální kapacita sběrnice stohu 80 Gb/s	ANO	Kapitola 4.6.1
	Minimální kapacita přepínání 128 Gb/s	ANO	Kapitola 4.6.1
	Minimální paketová kapacita 95 Mp/s	ANO	Kapitola 4.6.1
	Stateful Switch Over v rámci stohu	ANO	Kapitola 4.6.1
	Velikost zařízení 1RU	ANO	Kapitola 4.6.1
	Min. velikost sdíleného systémového bufferu 6 MB	ANO	Kapitola 4.6.1
	Redundatní větráky	ANO	Kapitola 4.6.1
	Interní redundantní napájecí zdroj součástí dodávky	ANO	Kapitola 4.6.1
	Minimální počet zařízení ve stohu - 8	ANO [redacted]	Kapitola 4.6.1
	Počet dedikovaných stohovacích portů - 2 (případně porty neomezující min. počet portů pro připojení zařízení)	ANO, [redacted]	Kapitola 4.6.1
	Datový stohovací kabel požadován v délce min. 0.5m	ANO, [redacted]	Kapitola 4.6.1
	Počet portů 10/100/1000 Base-TX s PoE+ napájením - 24	ANO	Kapitola 4.6.1
	Minimální PoE budget - 370W (min 15,4 W/port)	ANO, [redacted]	Kapitola 4.6.1
	Podpora protokolů: IEEE 802.3af, IEEE 802.3at, IEEE 802.1Q, IEEE 802.1x, IEEE 802.1w - Rapid Spanning Tree Protocol, IEEE 802.1ae, IEEE 802.3az, IEEE 802.1ar	ANO	Kapitola 4.6.1
	Schopnost poskytovat PoE napájení připojeným zřízením i během restartu přepínače	ANO	Kapitola 4.6.1
	Inteligentní PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení	ANO	Kapitola 4.6.1
	Uplinkové porty s volitelným rozhraním SFP+ - 4x1/10GE SFP+, všechny porty osazeny 10G-BASE-SR SFP+ moduly	ANO	Kapitola 4.6.1
	Velikost MAC address tabulky - 16000	ANO	Kapitola 4.6.1
	Min. počet IPv4 routes - 3000	ANO	Kapitola 4.6.1
	Min. počet IPv6 routes - 1500	ANO	Kapitola 4.6.1
	Min. počet konfigurovatelných security ACL - 1500	ANO	Kapitola 4.6.1
	IEEE 802.3ad (Link Aggregation)	ANO	Kapitola 4.6.1

	IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis	ANO	Kapitola 4.6.1
	Minimálně 8 linek jako součást Link Aggregation Group trunku	ANO	Kapitola 4.6.1
	Minimální počet konfigurovatelných Link Aggregation Group trunků - 24	ANO	Kapitola 4.6.1
	Minimální počet aktivních VLAN - 512	ANO	Kapitola 4.6.1
	Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ANO	Kapitola 4.6.1
	Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	ANO	Kapitola 4.6.1
	Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů	ANO	Kapitola 4.6.1
	RADIUS CoA	ANO	Kapitola 4.6.1
	Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO	Kapitola 4.6.1
	Podpora jumbo rámců (min. 9198 bytes)	ANO	Kapitola 4.6.1
	Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO	Kapitola 4.6.1
	Směrování protokolů IPv4 a IPv6 v hardware	ANO	Kapitola 4.6.1
	VRRP	ANO	Kapitola 4.6.1
	Reverse path check (uRPF) pro IPv4 i IPv6	ANO	Kapitola 4.6.1
	IGMPv2, IGMPv3	ANO	Kapitola 4.6.1
	IGMP snooping	ANO	Kapitola 4.6.1
	MLD snooping	ANO	Kapitola 4.6.1
	Minimální počet HW QoS front - 8	ANO	Kapitola 4.6.1
	QoS classification – ACL, DSCP, CoS based	ANO	Kapitola 4.6.1
	QoS marking - DSCP, CoS	ANO	Kapitola 4.6.1
	Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	Kapitola 4.6.1
	QoS Policing	ANO	Kapitola 4.6.1
	QoS-Hierarchical QoS - minimálně 2 úrovně	ANO	Kapitola 4.6.1
	IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)	ANO	Kapitola 4.6.1
	Možnost definovat povolené MAC adresy na portu	ANO	Kapitola 4.6.1
	PACL, VACL	ANO	Kapitola 4.6.1
	Paketové filtry (ACL) jsou stále aplikovány a filtrují v případě, že jsou na nich prováděny změny	ANO	Kapitola 4.6.1
	Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ANO	Kapitola 4.6.1

	Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ANO	Kapitola 4.6.1
	Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO	Kapitola 4.6.1
	Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení	ANO	Kapitola 4.6.1
	HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů	ANO	Kapitola 4.6.1
	Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	Kapitola 4.6.1
	Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	Kapitola 4.6.1
	Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type	ANO	Kapitola 4.6.1
	Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	Kapitola 4.6.1
	SSHv2	ANO	Kapitola 4.6.1
	CLI rozhraní	ANO	Kapitola 4.6.1
	Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu	ANO	Kapitola 4.6.1
	Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG	ANO	Kapitola 4.6.1
	Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení	ANO	Kapitola 4.6.1
	Streaming telemetrie prostřednictvím NETCONF/XML	ANO	Kapitola 4.6.1
	SNMPv2/v3	ANO	Kapitola 4.6.1
	Podpora network boot (iPXE)	ANO	Kapitola 4.6.1
	TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	Kapitola 4.6.1
	NTPv3 server	ANO	Kapitola 4.6.1

4.7 K.2c - Přístupové přepínače 48p

4.7.1 Nabízené řešení

[redacted]

4.7.2 Způsob naplnění minimálních požadavků

Položka	Popis parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně uvedení výrobce, obchodního označení, konkrétní konfigurace, produktového čísla, případně uvede konkrétní parametry	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
Přístupový přepínač 48p	Typ přepínače L2/L3	ANO	Kapitola 4.7.1
	Formát přepínače stohovatelný	ANO	Kapitola 4.7.1
	Minimální kapacita sběrnice stohu 80 Gb/s	ANO	Kapitola 4.7.1
	Minimální kapacita přepínání 176 Gb/s	ANO	Kapitola 4.7.1
	Minimální paketová kapacita 130 Mp/s	ANO	Kapitola 4.7.1
	Stateful Switch Over v rámci stohu	ANO	Kapitola 4.7.1
	Velikost zařízení 1RU	ANO	Kapitola 4.7.1
	Min. velikost sdíleného systémového bufferu 6 MB	ANO	Kapitola 4.7.1
	Redundatní větráky	ANO	Kapitola 4.7.1
	Interní redundantní napájecí zdroj součástí dodávky	ANO	Kapitola 4.7.1
	Minimální počet zařízení ve stohu - 8	ANO,[redacted]	Kapitola 4.7.1
	Počet dedikovaných stohovacích portů - 2 (případně porty neomezující min. počet portů pro připojení zařízení)	ANO,[redacted]	Kapitola 4.7.1
	Datový stohovací kabel požadován v délce min. 0.5m	ANO,[redacted]	Kapitola 4.7.1
	Počet portů 10/100/1000 Base-TX s PoE+ napájením - 48	ANO	Kapitola 4.7.1
	Minimální PoE budget - 740W (min 15,4 W/port)	ANO,[redacted]	Kapitola 4.7.1
	Podpora protokolů: IEEE 802.3af, IEEE 802.3at, IEEE 802.1Q, IEEE 802.1x, IEEE 802.1w - Rapid	ANO	Kapitola 4.7.1

	Spanning Tree Protocol, IEEE 802.1ae, IEEE 802.3az, IEEE 802.1ar		
	Schopnost poskytovat PoE napájení připojeným zřízením i během restartu přepínače	ANO	Kapitola 4.7.1
	Inteligentní PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení	ANO	Kapitola 4.7.1
	Uplinkové porty s volitelným rozhraním SFP+ - 4x1/10GE SFP+, všechny porty osazeny 10G-BASE-SR SFP+ moduly	ANO	Kapitola 4.7.1
	Velikost MAC address tabulky - 16000	ANO	Kapitola 4.7.1
	Min. počet IPv4 routes - 3000	ANO	Kapitola 4.7.1
	Min. počet IPv6 routes - 1500	ANO	Kapitola 4.7.1
	Min. počet konfigurovatelných security ACL - 1500	ANO	Kapitola 4.7.1
	IEEE 802.3ad (Link Aggregation)	ANO	Kapitola 4.7.1
	IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis	ANO	Kapitola 4.7.1
	Minimálně 8 linek jako součást Link Aggregation Group trunku	ANO	Kapitola 4.7.1
	Minimální počet konfigurovatelných Link Aggregation Group trunků - 24	ANO	Kapitola 4.7.1
	Minimální počet aktivních VLAN - 512	ANO	Kapitola 4.7.1
	Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ANO	Kapitola 4.7.1
	Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	ANO	Kapitola 4.7.1
	Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů	ANO	Kapitola 4.7.1
	RADIUS CoA	ANO	Kapitola 4.7.1
	Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO	Kapitola 4.7.1
	Podpora jumbo rámců (min. 9198 bytes)	ANO	Kapitola 4.7.1
	Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO	Kapitola 4.7.1
	Směrování protokolů IPv4 a IPv6 v hardware	ANO	Kapitola 4.7.1
	VRRP	ANO	Kapitola 4.7.1
	Reverse path check (uRPF) pro IPv4 i IPv6	ANO	Kapitola 4.7.1
	IGMPv2, IGMPv3	ANO	Kapitola 4.7.1
	IGMP snooping	ANO	Kapitola 4.7.1
	MLD snooping	ANO	Kapitola 4.7.1
	Minimální počet HW QoS front - 8	ANO	Kapitola 4.7.1
	QoS classification – ACL, DSCP, CoS based	ANO	Kapitola 4.7.1

	QoS marking - DSCP, CoS	ANO	Kapitola 4.7.1
	Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	Kapitola 4.7.1
	QoS Policing	ANO	Kapitola 4.7.1
	QoS-Hierarchical QoS - minimálně 2 úrovně	ANO	Kapitola 4.7.1
	IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)	ANO	Kapitola 4.7.1
	Možnost definovat povolené MAC adresy na portu	ANO	Kapitola 4.7.1
	PACL, VACL	ANO	Kapitola 4.7.1
	Paketové filtry (ACL) jsou stále aplikovány a filtrují v případě, že jsou na nich prováděny změny	ANO	Kapitola 4.7.1
	Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ANO	Kapitola 4.7.1
	Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ANO	Kapitola 4.7.1
	Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO	Kapitola 4.7.1
	Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení	ANO	Kapitola 4.7.1
	HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů	ANO	Kapitola 4.7.1
	Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	Kapitola 4.7.1
	Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	Kapitola 4.7.1
	Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type	ANO	Kapitola 4.7.1
	Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	Kapitola 4.7.1
	SSHv2	ANO	Kapitola 4.7.1
	CLI rozhraní	ANO	Kapitola 4.7.1
	Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu	ANO	Kapitola 4.7.1
	Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG	ANO	Kapitola 4.7.1

	Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení	ANO	Kapitola 4.7.1
	Streaming telemetrie prostřednictvím NETCONF/XML	ANO	Kapitola 4.7.1
	SNMPv2/v3	ANO	Kapitola 4.7.1
	Podpora network boot (iPXE)	ANO	Kapitola 4.7.1
	TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	Kapitola 4.7.1
	NTPv3 server	ANO	Kapitola 4.7.1

4.8 K.2d - Místní přepínače

4.8.1 Nabízené řešení

[redacted]

4.8.2 Způsob naplnění minimálních požadavků

Položka	Popis parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně uvedení výrobce, obchodního označení, konkrétní konfigurace, produktového čísla, případně uvede konkrétní parametry	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
Místní přepínač	Typ přepínače L2/L3	ANO	Kapitola 4.8.1
	Minimální kapacita přepínání 60 Gb/s	ANO	Kapitola 4.8.1
	Minimální paketová kapacita 44 Mp/s	ANO	Kapitola 4.8.1
	Min. velikost sdíleného systémového bufferu 6 Mb	ANO	Kapitola 4.8.1
	Z důvodu umístění v kancelářích je požadováno řešení bez ventilátorů - Fanless	ANO	Kapitola 4.8.1
	Počet portů 10/100/1000 Base-TX s PoE+ napájením - 8	ANO	Kapitola 4.8.1
	Minimální PoE budget 240W	ANO	Kapitola 4.8.1
	Podpora protokolů: IEEE 802.3af, IEEE 802.3at, IEEE 802.1Q, IEEE 802.1x, IEEE 802.1w - Rapid Spanning Tree Protocol, IEEE 802.1ae, IEEE 802.3az, IEEE 802.1ar, IEEE 802.3ad (Link Aggregation)	ANO	Kapitola 4.8.1
	Uplinkové porty s rychlostí 1Gbps a rozhraním RJ-45 - 2x 10/100/1000 Mbps	ANO	Kapitola 4.8.1

	Uplinkové porty s volitelným rozhraním SFP+ - 2x 1/10Gbps SFP+	ANO	Kapitola 4.8.1
	Velikost MAC address tabulky - 32000	ANO	Kapitola 4.8.1
	Min. počet IPv4 routes - 4000	ANO	Kapitola 4.8.1
	Min. počet IPv6 routes - 2000	ANO	Kapitola 4.8.1
	Min. počet konfigurovatelných security ACL - 1600	ANO	Kapitola 4.8.1
	IEEE 802.3ad (Link Aggregation)	ANO	Kapitola 4.8.1
	Minimální počet aktivních VLAN - 512	ANO	Kapitola 4.8.1
	Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ANO	Kapitola 4.8.1
	Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	ANO	Kapitola 4.8.1
	Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů	ANO	Kapitola 4.8.1
	RADIUS CoA	ANO	Kapitola 4.8.1
	Podpora instance spanning-tree protokolu per VLAN	ANO	Kapitola 4.8.1
	Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO	Kapitola 4.8.1
	Podpora jumbo rámců (min. 9198 bytes)	ANO	Kapitola 4.8.1
	Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO	Kapitola 4.8.1
	Směrování protokolů IPv4 a IPv6 v hardware	ANO	Kapitola 4.8.1
	VRRP	ANO	Kapitola 4.8.1
	Reverse path check (uRPF) pro IPv4 i IPv6	ANO	Kapitola 4.8.1
	IGMPv2, IGMPv3	ANO	Kapitola 4.8.1
	IGMP snooping	ANO	Kapitola 4.8.1
	MLD snooping	ANO	Kapitola 4.8.1
	Minimální počet HW QoS front - 8	ANO	Kapitola 4.8.1
	QoS classification – ACL, DSCP, CoS based	ANO	Kapitola 4.8.1
	QoS marking - DSCP, CoS	ANO	Kapitola 4.8.1
	Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	Kapitola 4.8.1
	QoS Policing	ANO	Kapitola 4.8.1
	QoS-Hierarchical QoS min. 2 úrovně	ANO	Kapitola 4.8.1
	IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)	ANO	Kapitola 4.8.1
	Možnost definovat povolené MAC adresy na portu	ANO	Kapitola 4.8.1
	PACL, VACL	ANO	Kapitola 4.8.1

	Paketové filtry (ACL) jsou stále aplikovány a filtrují v případě, že jsou na nich prováděny změny	ANO	Kapitola 4.8.1
	Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ANO	Kapitola 4.8.1
	Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ANO	Kapitola 4.8.1
	Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO	Kapitola 4.8.1
	Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení	ANO	Kapitola 4.8.1
	HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů	ANO	Kapitola 4.8.1
	Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	Kapitola 4.8.1
	Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	Kapitola 4.8.1
	Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type	ANO	Kapitola 4.8.1
	Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	Kapitola 4.8.1
	SSHv2	ANO	Kapitola 4.8.1
	CLI rozhraní	ANO	Kapitola 4.8.1
	Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení	ANO	Kapitola 4.8.1
	SNMPv2/v3	ANO	Kapitola 4.8.1
	Podpora network boot (iPXE)	ANO	Kapitola 4.8.1
	TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	Kapitola 4.8.1
	NTPv3 server	ANO	Kapitola 4.8.1

4.9 K.2e - Rozšíření optických tras

4.9.1 Nabízené řešení

4.9.1.1 CWDM spliter

[redacted]

4.9.1.2 Optický kabel

[redacted]

4.9.2 Způsob naplnění minimálních požadavků

4.9.2.1 CWDM spliter

Položka	Popis parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně uvedení výrobce, obchodního označení, konkrétní konfigurace, produktového čísla, případně uvede konkrétní parametry	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
CWDM spliter	Single mode	ANO	Kapitola 4.9.1.1
	Typ filtru CWDM	ANO	Kapitola 4.9.1.1
	Počet kanálů - min. 16	ANO, 16	Kapitola 4.9.1.1
	Použitelná vlnová délka 1270nm - 1610nm	ANO	Kapitola 4.9.1.1
	Maximální vložný útlum 3,5dB	ANO,	Kapitola 4.9.1.1
	Provedení BI-DI provoz po jednom vlákně	ANO	Kapitola 4.9.1.1
	Instalace do racku 19"	ANO	Kapitola 4.9.1.1
	V lokalitě s více filtry možnost instalace více modulů do jednoho šasi	ANO, [redacted]	Kapitola 4.9.1.1
	Zakončeno na konektory SC/APC nebo E2000/APC	ANO, [redacted]	Kapitola 4.9.1.1

4.9.2.2 Optický kabel

Položka	Popis parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně uvedení výrobce, obchodního označení, konkrétní konfigurace, produktového čísla, případně uvede konkrétní parametry	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
Optický kabel	Typ kabelu: single mode, závěsný Flat	ANO	Kapitola 4.9.1.2
	Možnost závěsné instalace	ANO	Kapitola 4.9.1.2
	Možnost instalace zatažením do chráničky	ANO	Kapitola 4.9.1.2
	Provozní rozsah teplot kabelu -30st - 50st C	ANO, [redacted]	Kapitola 4.9.1.2
	Použití doporučených kotvících materiálů výrobcem	ANO	Kapitola 4.9.1.2
	Minimální počet vláken 12	ANO [redacted]	Kapitola 4.9.1.2
	Maximální počet vláken 24	ANO –	Kapitola 4.9.1.2
	Typ vlákna: SMF ITU-T G.657.B (nebo s lepšími parametry)	ANO [redacted]	Kapitola 4.9.1.2
	Zakončení vláken na konektor SC/APC nebo E2000/APC	ANO, [redacted] bude takto instalováno	Kapitola 4.9.1.2
	Počet zakončených vláken min. 12	ANO, bude takto instalováno	Kapitola 4.9.1.2
	Ukončeno v rozvaděči/vaně	ANO, bude takto instalováno	Kapitola 4.9.1.2
	Minimální životnost kabelu 20 let	ANO	Kapitola 4.9.1.2
	Min. poloměr ohybu při zátěži - max. 160mm	ANO	Kapitola 4.9.1.2
	Min. poloměr ohybu bez zátěže - max. 100mm	ANO	Kapitola 4.9.1.2
	Maximální krátkodobá tahová zátěž - min. 1300N	ANO	Kapitola 4.9.1.2
	Maximální dlouhodobá tahová zátěž - min. 650N	ANO	Kapitola 4.9.1.2
	Maximální délka pole (těžké podmínky) - min. 40m	ANO	Kapitola 4.9.1.2
	Maximální délka pole (lehké podmínky) - min. 80m	ANO	Kapitola 4.9.1.2
	Maximální útlum trasy (pro všechna zakončená vlákna) - max. 2dB	ANO, bude takto instalováno	Kapitola 4.9.1.2
	Měření trasy s protokolem (pro všechna zakončená vlákna) - výkonové a OTDR	ANO, bude takto instalováno	Kapitola 4.9.1.2

4.10 K.3 - Zvýšení zabezpečení sítě WiFi - Bezdrátové přístupové body

4.10.1 Nabízené řešení

[redacted]

4.10.2 Způsob naplnění minimálních požadavků

Položka	Popis parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně uvedení výrobce, obchodního označení, konkrétní konfigurace, produktového čísla, případně uvede konkrétní parametry	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
Bezdrátový přístupový bod (AP)	Access Point (AP) vybavený radiem pro 2,4 a 5 GHz pásmo, podpora standardu 802.11a/b/g/n/ac a Wi-Fi6 (802.11ax)	ANO	Kapitola 4.10.1
	Podpora minimálně 4x4 MIMO, MU-MIMO, UL/DL OFDMA, TWT, BSS Coloring a až 160 MHz kanál pro 802.11ax	ANO	Kapitola 4.10.1
	Minimální počet inzerovaných SSID (BSSID) per radio - 8	ANO	Kapitola 4.10.1
	Podpora mechanismu pro optimalizaci fáze vysílaného bezdrátového signálu směrem k 802.11 n/ac/ax klientům (Tx Beam Forming)	ANO	Kapitola 4.10.1
	Podpora mechanismu pro přepojení klientů z 2,4GHz do 5GHz pásma	ANO	Kapitola 4.10.1
	Access Pointy obsahují X.509 certifikát s lokální platností pro nasazeni PKI	ANO	Kapitola 4.10.1
	Podpora autentizace Access Pointu do LAN sítě pomocí 802.1x, AP obsahují 802.1x supplikant	ANO	Kapitola 4.10.1
	Podpora detekce a monitorování problémů WLAN odchytáváním provozu na AP a jeho zasíláním do Ethernetového analyzátoru (např. Wireshark)	ANO	Kapitola 4.10.1
	Podpora přímého přístupu na příkazovou řádku AP přes serial konzoli a přes IPv4 pomocí Telnet a SSH	ANO	Kapitola 4.10.1

	Podpora spektrální analýzy (detekce zdroje rušivého signálu – interference)	ANO	Kapitola 4.10.1
	Podpora rozpoznání zdroje rušivého signálu podle signatur	ANO	Kapitola 4.10.1
	Access Point obsahuje Bluetooth low-energy (BLE) 5.0 rádio a USB 2.0 port	ANO	Kapitola 4.10.1
	1 x 100/1000/2500 Mbit/s RJ45 ethernet rozhraní kompatibilní s 802.3bz	ANO	Kapitola 4.10.1
	Možnost 802.3af/at PoE napájení AP z přepínače nebo injectoru, v případě použití 802.3af AP běží minimálně v režimu 2x2 MIMO pro obě rádiová pásma bez sníženého vysílacího výkonu	ANO	Kapitola 4.10.1
	AP uzavřené konstrukce bez větracích otvorů a ventilátoru	ANO	Kapitola 4.10.1
	Součástí AP je úchyt pro instalaci na strop nebo stěnu	ANO	Kapitola 4.10.1
	Důvěryhodný HW/SW – AP používá bezpečný zavaděč OS, ověřování podpisu OS, kontrolu autentičnosti HW a mechanizmy pro ochranu SW a HW proti útokům	ANO	Kapitola 4.10.1
	Součástí dodávky je redundantní kontroler bezdrátové sítě s plnou podporou dodávaných bezdrátových bodů (AP)	ANO	Kapitola 4.10.1
	Minimální podporovaná propustnost pro centrálně přepínaná data 1,5 Gb/s	ANO	Kapitola 4.10.1
	Licence dle počtu nově pořizovaných AP, možnost upgradu až na minimáně 500 registrovaných AP	ANO	Kapitola 4.10.1
	Redundance na úrovni kontrolerů a jejich portů, výpadek aktivního kontroleru v redundantním páru nemá žádný dopad na provoz již připojených klientů (tj. bez potřeby reautentizace)	ANO	Kapitola 4.10.1
	Lokální síť - možnost tunelování uživatelských dat z AP až na kontroler, možnost šifrování těchto uživatelských dat bez výrazného vlivu na propustnost	ANO	Kapitola 4.10.1
	Mesh síť - podpora mesh sítí, současné připojení normálních a mesh AP k jednomu kontroleru	ANO	Kapitola 4.10.1
	Vzdálené lokality - možnost lokálního bridgování uživatelských dat per SSID přímo na příslušném AP	ANO	Kapitola 4.10.1
	Šifrovaná řídící komunikace AP-kontroler	ANO	Kapitola 4.10.1
	Současná funkčnost AP pro přenos dat, analýzu spektra a detekci bezpečnostních incidentů	ANO	Kapitola 4.10.1
	Bezpečnost a Guest Access	ANO	Kapitola 4.10.1
	Podpora 802.11i, respektive jeho implementace WPA2 včetně enterprise variant autentizace/šifrování	ANO	Kapitola 4.10.1
	Podpora WPA3 – WPA3 Enterprise, WPA3 SAE, WPA3 OWE	ANO	Kapitola 4.10.1

	PSK autentizace vč. možnosti různých PSK klíčů pro různé klienty v rámci jednoho SSID	ANO	Kapitola 4.10.1
	Podpora standardu „802.11w“ pro ochranu řídících rámců na AP a klientovi	ANO	Kapitola 4.10.1
	Podpora standardu „802.11u“ pro výběr SSID a autentizaci klienta	ANO	Kapitola 4.10.1
	Integrované řešení návštěvnického přístupu s možností webové autentizace (včetně nativních IPv6 klientů), bezpečné oddělení od zaměstnaneckého provozu, funkční i v módu lokálního bridgování uživatelských dat přímo na AP	ANO	Kapitola 4.10.1
	Podpora řešení návštěvnického přístupu pro klienty bezdrátové i drátové sítě	ANO	Kapitola 4.10.1
	Možnost omezit počet klientů per SSID	ANO	Kapitola 4.10.1
	Lokální profilování zařízení – per uživatel a per zařízení	ANO	Kapitola 4.10.1
	Integrovaný IDS systém pro detekci cizích AP (Rogue AP) a klientů v AdHoc režimu, možnost vynuceného odpojení klientů od cizích AP	ANO	Kapitola 4.10.1
	Podpora Flexible NetFlow a exportu záznamů (dle RFC 3954) o datových tocích uživatelů (vč. zdrojové a cílové IP adresy, portů, WLAN ID, počtu paketů a objemu přenesených dat) směrem k externímu kolektoru	ANO	Kapitola 4.10.1
	Rychlý roaming	ANO	Kapitola 4.10.1
	Podpora standardu „802.11r“ pro rychlý roaming klientů mezi AP, možnost selektivního využití 802.11r na sdíleném SSID pouze pro zařízení, které tento standard podporují	ANO	Kapitola 4.10.1
	Podpora standardu „802.11k“ pro optimalizaci roamingu	ANO	Kapitola 4.10.1
	Podpora standardu „802.11v“ pro optimalizaci připojení klienta	ANO	Kapitola 4.10.1
	QoS a řízení provozu v bezdrátové síti	ANO	Kapitola 4.10.1
	Podpora 802.11e/WMM	ANO	Kapitola 4.10.1
	Diferenciace úrovní QoS pro různé služby a skupiny uživatelů (zaměstnance a návštěvníky), možnost obousměrného omezení propustnosti per klient.	ANO	Kapitola 4.10.1
	Mechanismy řízení přístupu (Call Admission Control) pro hasový i video provoz. Konfigurovatelné parametry max. zátěže a šířky pásma.	ANO	Kapitola 4.10.1
	Podpora Video-streamingu se spolehlivým multicastem	ANO	Kapitola 4.10.1
	Optimalizace multicast provozu v bezdrátové síti (IGMP snooping)	ANO	Kapitola 4.10.1
	Aplikační inspekce přenášeného provozu (DPI na 7. vrstvě ISO/OSI na základě aplikačních signatur) umožňující rozpoznání jednotlivých aplikací, grafické	ANO	Kapitola 4.10.1

	zobrazení statistik a možnost řízení QoS per rozpoznaná aplikace		
	Správa frekvenčního pásma, konfigurační profily	ANO	Kapitola 4.10.1
	Automatizovaná centrální správa frekvenčního pásma	ANO	Kapitola 4.10.1
	Monitoring rádiového spektra vč. 20/40/80/160 MHz kanálů, možnost okamžité automatické centralizovaně řízené reakce (změna kanálu nebo jeho šířky, změna vysílacího výkonu), grafické vyobrazení informací o kvalitě signálu	ANO	Kapitola 4.10.1
	Automatické zvýšení vysílacího výkonu okolních AP při výpadku AP („self healing“)	ANO	Kapitola 4.10.1
	Možnost detekce rušivých signálů (interference) a identifikace zdrojů interference na základě signatur	ANO	Kapitola 4.10.1
	Mesh síť – automatický výběr vhodného kanálu pro backhaul, automatické sestavení optimálního mesh stromu, monitorování všech kanálů na pozadí s rychlou konvergencí v případě výpadku primárního nadřazeného AP	ANO	Kapitola 4.10.1
	Troubleshooting radiového signálu a automatické řešení problému rušivého signálu, generování alarmů na základě překročení prahových hodnot kvality signálu	ANO	Kapitola 4.10.1
	Možnost definovat různé konfigurační profily a ty následně přiřadit vybraným AP (např. dle umístění AP, bezpečnostních pravidel atd.).	ANO	Kapitola 4.10.1
	Možnost vytvořit různé rádiové profily (nastavení kanálů, rychlostí) a ty následně přiřadit vybraným AP.	ANO	Kapitola 4.10.1
	Podpora IPv6	ANO	Kapitola 4.10.1
	Podpora IPv6 – management kontroleru (vč. Syslog, radius)	ANO	Kapitola 4.10.1
	Podpora IPv6 – komunikace AP-kontroler	ANO	Kapitola 4.10.1
	Podpora IPv6 – Guest Access i pro nativní klienty vč. webové autentizace pro IPv6 klienty	ANO	Kapitola 4.10.1
	Podpora IPv6 – IPv6 multicast, MLD snooping	ANO	Kapitola 4.10.1
	Podpora IPv6 – bezpečnost (RA Guard, IPv6 Source Guard, DHCPv6 Server Guard, ACL)	ANO	Kapitola 4.10.1
	Podpora IPv6 – ND cache na kontroleru, optimalizace přenosu ND zpráv, rate-limiting pro RA	ANO	Kapitola 4.10.1
	Dohled a správa kontroleru, zabezpečení SW	ANO	Kapitola 4.10.1
	Centrální administrace správců s granularitou přístupových práv	ANO	Kapitola 4.10.1
	Podpora správy přes CLI nebo přes IP pomocí SSH/telnet a https web GUI, SNMP	ANO	Kapitola 4.10.1
	Podpora API rozhraní pro plnou konfiguraci kontroleru pomocí NETCONF, RESTCONF za použití YANG	ANO	Kapitola 4.10.1

	data modelů. Podpora exportu provozních dat z kontroleru.		
	Důvěryhodný SW – kontroler používá bezpečný zavaděč OS, ověřování podpisu SW komponent, kontrolu autentičnosti HW a mechanizmy pro ochranu SW a HW proti útokům	ANO	Kapitola 4.10.1

4.11 K.4 - Zavedení nástrojů ověřování zařízení přistupujících do počítačové sítě – 802.1x - Systém bezpečného přístupu do sítě 802.1x

4.11.1 Nabízené řešení

[redacted]

4.11.2 Způsob naplnění minimálních požadavků

Položka	Popis parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně uvedení výrobce, obchodního označení, konkrétní konfigurace, produktového čísla, případně uvede konkrétní parametry	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
Obecná charakteristika ověřovacího řešení	Centralizovaný systém pro ověřování uživatelů, klasifikaci zařízení, řízení přístupu k síti a guest přístup definující pravidla přístupu k síti v závislosti na kontextu připojení (uživatel, typ zařízení, stav zařízení, místo připojení apod.), dle standardu IEEE 802.1X	ANO	Kapitola 4.11.1
	Ve spolupráci s aktivními prvky (LAN přepínači, bezdrátovými AP nebo řídícími moduly, VPN branami) poskytuje ochranu před neoprávněným přístupem k pevné LAN síti, bezdrátové wifi síti (metodou 802.1x) a pro VPN přístup	ANO	Kapitola 4.11.1
	Poskytuje AAA funkce (viz níže)	ANO	Kapitola 4.11.1

	Podporuje klasifikaci připojených zařízení a řízení přístupu na základě této klasifikace (Network Admission Control)	ANO	Kapitola 4.11.1
	Podporuje centralizované nebo distribuované nasazení pro vysokou odolnost a rozšiřování kapacity	ANO	Kapitola 4.11.1
	Umožňuje snadné zálohování, rychlou a úplnou obnovu konfigurace	ANO	Kapitola 4.11.1
	Je dostupné ve formě virtuálního stroje pro stávající platformu Microsoft Hyper-V	ANO	Kapitola 4.11.1
AAA funkce - Podporované protokoly	RADIUS pro autentizaci, autorizaci a accounting	ANO	Kapitola 4.11.1
	Proxy funkce pro externí RADIUS	ANO	Kapitola 4.11.1
	PAP, MS-CHAP, MS-CHAPv2, EAP – MD5, Protected EAP (PEAP), EAP-TLS, EAP-TTLS, EAP-FAST, EAP-TEAP	ANO	Kapitola 4.11.1
	Podpora TACACS+ pro centrální řízení administrativního přístupu na zařízení	ANO	Kapitola 4.11.1
AAA funkce - Podporované databáze uživatelů (s možností definovat pořadí autentizace)	Interní databáze (pro uživatele i koncová zařízení)	ANO	Kapitola 4.11.1
	Active Directory – více nezávislých domén	ANO	Kapitola 4.11.1
	Azure Active Directory	ANO	Kapitola 4.11.1
	LDAP (RFC 2251)	ANO	Kapitola 4.11.1
	RADIUS Token indentity source (RFC 2865)	ANO	Kapitola 4.11.1
	RSA RADIUS token server	ANO	Kapitola 4.11.1
	Autentizace pomocí údajů obsažených v certifikátu	ANO	Kapitola 4.11.1
AAA funkce - Ověřování uživatelů a zařízení	Ověření uživatelů/zařízení heslem nebo certifikátem (různé kombinace)	ANO	Kapitola 4.11.1
	Ověření MAC adresou připojovaného zařízení	ANO	Kapitola 4.11.1
AAA funkce - Autorizace: pružný systém pro definici	Řízení přístupu k síti pomocí filtrů nebo přiřazením do VLAN sítě podle - uživatele (role, skupiny), - stavu a typu koncového zařízení (viz výše), - místa připojení, - historie připojení	ANO	Kapitola 4.11.1
	Omezení přístupu k síti pomocí filtrů aplikovaných na vstupu do sítě	ANO	Kapitola 4.11.1
	Omezení přístupu k síti pomocí filtrů aplikovaných na výstupu ze sítě	ANO	Kapitola 4.11.1

pravidel pro přístup k síti	Podpora Change of Authorization (CoA, RFC 3576) pro změny vynucovaných politik „za běhu“	ANO	Kapitola 4.11.1
	Možnost jednoduše identifikovat/označit přenášená data uživatele (rámce) v chráněné oblasti	ANO	Kapitola 4.11.1
	Řízení autentizace a založení důvěryhodné infrastruktury mezi jednotlivými prvky sítě, pro bezpečný a šifrovaný transport dat	ANO	Kapitola 4.11.1
AAA funkce - Accounting	Zaznamenávání aktivity uživatelů a zařízení připojených k síti	ANO	Kapitola 4.11.1
	Dotazovací systém, korelace záznamů, centralizované výkazy	ANO	Kapitola 4.11.1
	Systém pro sledování výstrah (úspěšná/neúspěšná přihlašování, neaktivita, stav systému AAA, dostupnost externích databází, aktivita filtrů)	ANO	Kapitola 4.11.1
AAA funkce - Funkce Guest serveru	Vytváření časově omezených oprávnění pro přístup k síti nebo do internetu pro hosty, externí spolupracovníky apod. ve fixních LAN i WiFi	ANO	Kapitola 4.11.1
	Oprávnění přidělovaná správcem přístupu přes portál pro snadné vytváření dočasných účtů	ANO	Kapitola 4.11.1
	Samoobslužný portál pro uživatele	ANO	Kapitola 4.11.1
	Ověření přes HTTP a HTTPS	ANO	Kapitola 4.11.1
	Rozhraní pro integraci s externími operátory pro zasílání SMS zpráv s autentizačními údaji	ANO	Kapitola 4.11.1
	Propojení s email serverem pro zasílání Guest účtu	ANO	Kapitola 4.11.1
AAA funkce - Rozpoznávání typu koncových zařízení a jejich stavu	Automatické rozpoznávání a klasifikace připojených zařízení (PC, telefonů, tabletů, mobilních telefonů apod.) ve spolupráci se síťovou infrastrukturou	ANO	Kapitola 4.11.1
	Předdefinované profily pro běžná mobilní zařízení (zařízení s OS Android, Apple, a další)	ANO	Kapitola 4.11.1
	Předdefinované profily pro síťová zařízení NAD od různých vendorů	ANO	Kapitola 4.11.1
	Podpora pro IPv6 koncová zařízení	ANO	Kapitola 4.11.1
AAA funkce - Podpora BYOD	Onboarding (registrace, provisioning, nastavení klientských zařízení)	ANO	Kapitola 4.11.1
	Onboarding/provisioning proces formou samoobsluhu	ANO	Kapitola 4.11.1
	Specifické politiky pro BYOD zařízení	ANO	Kapitola 4.11.1
	Možnost nastavení limitu BYOD zařízení pro jednoho uživatele	ANO	Kapitola 4.11.1
	Interní CA, pro vydávání certifikátů BYOD zařízením	ANO	Kapitola 4.11.1
	Interní CA lze řetězit jako subordinate pod firemní CA	ANO	Kapitola 4.11.1

AAA funkce - Podpora MDM	Workflow pro registrace do MDM	ANO	Kapitola 4.11.1
	Výměna informací z MDM platformy a využití v politikách (např. pokud zařízení je „compliant“)	ANO	Kapitola 4.11.1
	Ovládání MDM přímo z prostředků bezpečnostního managementu (zamykání, mazání, apod.) zařízení	ANO	Kapitola 4.11.1
	Uživatelská samoobsluha přes web portál (např. zamknutí přístupu pro ztracené zařízení)	ANO	Kapitola 4.11.1
AAA funkce - Rozpoznávání stavu koncových zařízení a jeho náprava	Ověření stavu koncových zařízení pomocí softwarového agenta nebo web agenta na koncovém zařízení. Systém musí rozpoznat: · instalovaný operační systém · opravy instalované v operačním systému · verze instalovaných programů · hodnoty položek v registry databázi systémů Windows · stav aplikací, zajména antivirů, antispyware, antimalware a firewall	ANO	Kapitola 4.11.1
	Ověření stavu koncových stanic pomocí skriptů PowerShell (WIN), nebo shell (MacOS, Linux)	ANO	Kapitola 4.11.1
	Spolupráce na uvedení stanic do požadovaného stavu (informací, odkazem,spuštěním programu, aktualizací antiviru, aktualizací OS, stažením souboru)	ANO	Kapitola 4.11.1
AAA funkce - Další vlastnosti	Aktivace šifrování MACSec (IEEE 802.1ae) pro připojená zařízení (pokud MACSec podporují)	ANO	Kapitola 4.11.1
	Možnost vyčítání informací o uživateli z Active Directory (Passive Fingerprint) nebo z logů jiných síťových zařízení	ANO	Kapitola 4.11.1
	Podpora SXP (Exchange Protocol) dle IETF	ANO	Kapitola 4.11.1
	Otevřené API pro podporu propojení se zařízeními třetích stran	ANO	Kapitola 4.11.1
Funkce pro správu ověřovacího systému	Centralizovaná správa	ANO	Kapitola 4.11.1
	Definice rolí administrátorů a úrovní přístupu k ověřovacímu systému	ANO	Kapitola 4.11.1
	Zjednodušení správy vytvářeními skupin uživatelů, koncových a síťových zařízení	ANO	Kapitola 4.11.1
	Grafické rozhraní pro definici pravidel přístupu k síti	ANO	Kapitola 4.11.1
	Grafické rozhraní pro monitorování, definici výkazů, řešení problémů	ANO	Kapitola 4.11.1
	Diagnostika problémů (systémová, údaje o chybách přihlašování, TCP dump, packet capture)	ANO	Kapitola 4.11.1
	Zaznamenávání událostí na externí syslog server	ANO	Kapitola 4.11.1
	Čtení monitoring dat pomoci analytických aplikací třetích stran (např. Microsoft PowerBI atp)	ANO	Kapitola 4.11.1
	Podpora SNMPv3	ANO	Kapitola 4.11.1

	NTP pro synchronizaci času	ANO	Kapitola 4.11.1
	SMTP pro zasílání zpráv a výstrah přes e-mail	ANO	Kapitola 4.11.1

4.12 K.5 - Systém pro centrální správu sítě

4.12.1 Nabízené řešení

[redacted]

4.12.2 Způsob naplnění minimálních požadavků

Položka	Popis parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně uvedení výrobce, obchodního označení, konkrétní konfigurace, produktového čísla, případně uvede konkrétní parametry	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
Základní vlastnosti	Řízení celého řešení - centrální kontrolér	ANO	Kapitola 4.12.1
	Funkce pro zcela automatické sestavení a konfiguraci fyzické infrastruktury	ANO	Kapitola 4.12.1
	Veškeré síťové politiky jsou implementovány prostřednictvím centrálního LAN kontroleru	ANO	Kapitola 4.12.1
	Podpora vytváření multi-tenant prostředí - členění koncových uživatelů a zařízení do oddělených virtuálních sítí	ANO	Kapitola 4.12.1
	Podpora mikrosegmentace - členění koncových uživatelů a zařízení do logických skupin podle jejich role, nezávisle na IP adresaci koncových zařízení a síťové topologii	ANO	Kapitola 4.12.1
	Podpora funkcionality distribuované default gateway na jednotlivých edge přepínačích	ANO	Kapitola 4.12.1

	Podpora mobility uživatelů a zařízení přes jednotnou infrastrukturou bez nutnosti vytvářet L2 broadcast domény	ANO	Kapitola 4.12.1
	Integrace WLAN infrastruktury s možností terminovat datový provoz od bezdrátově připojených uživatelů přímo na edge přepínačích	ANO	Kapitola 4.12.1
	Společné politiky pro pevně i bezdrátově připojené uživatele	ANO	Kapitola 4.12.1
	Centralizovaná definice pravidel pro řízení přístupu uživatelů a zařízení v síti	ANO	Kapitola 4.12.1
	Podpora real time telemetrie, schopnost monitorovat každý paket, každý datový tok procházející infrastrukturou	ANO	Kapitola 4.12.1
	Možnost exportovat monitorovaná data ve standartním formátu NetFlow v9 nebo IPFIX	ANO	Kapitola 4.12.1
Požadovaná funkcionalita centrálního kontroleru	Typ zařízení - SDN kontroler	ANO	Kapitola 4.12.1
	Redundantní nasazení	ANO	Kapitola 4.12.1
	Grafické uživatelské rozhraní	ANO	Kapitola 4.12.1
	Přístupová práva založená na uživatelských rolích	ANO	Kapitola 4.12.1
	Otevřené API rozhraní pro integraci s externími systémy	ANO	Kapitola 4.12.1
	Dokumentované API rozhraní pro volání všech dostupných funkcí kontroleru	ANO	Kapitola 4.12.1
	Pokročilá správa operačního systému síťových zařízení - Patching management - SW Image Rollback - Verifikace integrity SW image	ANO	Kapitola 4.12.1
	Inventarizace nasazeného HW	ANO	Kapitola 4.12.1
	Hierarchické zobrazení topologické mapy včetně jejího členění na jednotlivé lokality	ANO	Kapitola 4.12.1
	GUI rozhraní pro detailní přehled o výkonnosti a stavu celé komunikační infrastruktury včetně monitorování stavu jednotlivých zařízení (využití CPU, DRAM paměti, jednotlivých síťových rozhraní atd.)	ANO	Kapitola 4.12.1
	Konfigurace sítě a síťových politik prostřednictvím předefinovaných workflows	ANO	Kapitola 4.12.1
	Podpora mikrosegmentace - členění koncových uživatelů a zařízení do logických skupin podle jeho identity. Ke skupinám jsou pak definovány na abstraktní úrovni komunikační požadavky (bezpečnostní politiky) vůči jiným skupinám. Funkcionalita musí být kompatibilní s nabízenými přepínači	ANO	Kapitola 4.12.1

4.13 K.6 – Interní segmentační firewall

4.13.1 Nabízené řešení

[redacted]

4.13.2 Způsob naplnění minimálních požadavků

Položka	Popis parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně uvedení výrobce, obchodního označení, konkrétní konfigurace, produktového čísla, případně uvede konkrétní parametry	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
	Zařízení ve formě HW appliance o velikosti 1RU a veškeré příslušenství (montážní prvky) pro montáž do RACKu	ANO	Kapitola 4.13.1
	Možnost rozšíření platformy i další prvek typu NGFW jehož cílem bude zajišťování [redacted] sdílení telemetrických informací, vizualizace stavu sítě, zařízení a klientů	ANO – [redacted]	Kapitola 4.13.1
	Možnost o rozšíření platformy pro sběr logů a grafického reportingu včetně oboustranné komunikace (tím se rozumí minimálně odeslání a zpětné načítání logů pro účel vizualizace)	ANO – [redacted]	Kapitola 4.13.1
HW parametry	min 16x Počet síťových rozhraní copper RJ45 10/100/1000	ANO	Kapitola 4.13.1
	min. 8x Počet GE SFP	ANO	Kapitola 4.13.1
	min. 4x 10GE SFP	ANO	Kapitola 4.13.1
	min. 1x Konzolový port pro management	ANO	Kapitola 4.13.1
	min. 1x dedikovaný port RJ45 pro management	ANO	Kapitola 4.13.1
	minx 1x USB 3.0 port pro zálohu konfigurace, případně pro připojení USB 4G/5G modemu	ANO	Kapitola 4.13.1
	Redundantní napájecí zdroj	ANO	Kapitola 4.13.1

Výkonnostní parametry	Propustnost FW (stavové filtrování, UDP paket) paket o velikosti 1518 B, 512 B, 64 B- min 26000 Mbps, 26000 Mbps, 10000 Mbps, latence firewallu (64 B UDP paket) - max 5 mikro sec, počet naráz otevřených spojení – min 2,7 M, počet nových spojení za sekundu - min. 260 000, počet firewall pravidel až 10 000, podpora virtualizace (min 10 virtuálních kontextů), podpora funkce bezdrátový kontrolér - 128 AP, podpora funkce integrovaný switch controller – podpora až 64 switchů	ANO	Kapitola 4.13.1
Základní funkce	Podpora režimu vysoké dostupnosti, L2, Active Active, Active Passive, full mesh HA, VRRP, synchronizace stavové tabulky a IP-sec SAs mezi nódy v clusteru	ANO	Kapitola 4.13.1
	Režim fungování L2 – transparentní režim, L3 – NAT/Router	ANO	Kapitola 4.13.1
	Podpora VLAN	ANO	Kapitola 4.13.1
	Podopora multicast, vytváření politiky pro multicast routování	ANO	Kapitola 4.13.1
	Podpora 802.3ad link aggregation	ANO	Kapitola 4.13.1
	Funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora health check funkcí, podpora SSL offloading	ANO	Kapitola 4.13.1
	Podpora centrální NATovácí tabulky, stavová inspekce SCTP komunikace	ANO	Kapitola 4.13.1
	Podpora dynamických routovacích protokolů BGP, OSPF, ISIS, RIP	ANO	Kapitola 4.13.1
	Policy-based routing	ANO	Kapitola 4.13.1
	Funkce SD WAN – možnost rozkládání provozu mezi více linek na základě aplikačních signatur, IP adres a portů u známých aplikací, kvality linky včetně automatické detekce nefunkčnosti linky	ANO	Kapitola 4.13.1
VPN funkce	Funkce SSL VPN: podpora klientského i bezklientského (portálového) režimu, minimální počet současně navázaných SSL VPN tunelů 450, minimální propustnost SSL VPN 1900Mbps	ANO	Kapitola 4.13.1
	Funkce IPSEC VPN: podpora site-to-site VPN, podpora klientských VPN, dostupnost VPN klienta pro koncové stanice (Windows, MacOS), funkce klientských IP-Sec VPN nesmí být licencovaná na počet uživatel. V opačném případě požadujeme	ANO	Kapitola 4.13.1

	dodání neomezené licence, minimální počet IPSEC VPN tunelů typu lokalita-lokalita 2000, minimální počet klientských IPSEC VPN tunelů 15000, propustnost IPSec VPN min. 12,5 Gbps (měřeno při AES256-SHA256), podpora konfigurace redundatních IPSec VPN tunelů za pomoci statického směrování, podpora konfigurace redundatních IPSec VPN tunelů za pomoci dynamického směrování, podpora funkce dynamického navazování IPsec tunelů dle potřeby komunikace, podpora VXLAN, podpora L2TP, PPTP, GRE, podpora dynamických routovací protokolů OSPF, BGP ve VPN IPsec		
UTM	Funkce detekce aplikací na L7 (Application Control)	ANO	Kapitola 4.13.1
	Funkce detekce a potlačení narušení (IPS/IDS)	ANO	Kapitola 4.13.1
	Funkce antivirové kontroly	ANO	Kapitola 4.13.1
	Funkce kategorizace webových stránek	ANO	Kapitola 4.13.1
	Funkce DNS filtru	ANO	Kapitola 4.13.1
	Funkce ochrany před únikem citlivých informací (DLP)	ANO	Kapitola 4.13.1
Pokročilé funkcionality	Možnost nastavovat firewall politiku na základě geografických údajů	ANO	Kapitola 4.13.1
	Aplikace firewall policy na známé internetové služby, kde databáze těchto služeb je pravidelně aktualizována výrobcem	ANO	Kapitola 4.13.1
	Možnost snadné integrace cloudové služby. Minimálně na: MS Azure, Amazon Web Services, Google Cloud	ANO	Kapitola 4.13.1
	Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru	ANO	Kapitola 4.13.1
	Viditelnost do provozu na aplikační úrovni	ANO	Kapitola 4.13.1
	Možnost definice FW pravidel v tzv. NGFW režimu (tj. součástí základní definice FW pravidla je kromě zdroje/cíle také typ aplikace (definované v rámci funkce application control, nikoliv pouhý TCP/UDP port) resp. kategorie URL filter ANO ingu (nikoliv jako AppCtrl resp URL filtering profil aplikovaný na dané pravidlo)	ANO	Kapitola 4.13.1
	Ověřování uživatelů LDAP, Active Directory, Single Sign On, Radius, TACACS+, Ověřování na základě certifikátu	ANO	Kapitola 4.13.1

	Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření	ANO	Kapitola 4.13.1
	Traffic Shaping, QoS s podporou prioritizace provozu na základě DSCP markování a ToS, aplikace traffic shaping na konkrétní aplikaci nebo webovou kategorii	ANO	Kapitola 4.13.1
	Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu	ANO	Kapitola 4.13.1
	Podpora funkce reverzní proxy	ANO	Kapitola 4.13.1
	Podpora silné autentizace uživatelů – integrovaná podpora generátor jednorázových hesel (OTP) – pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů	ANO	Kapitola 4.13.1
Explicit proxy	podpora všech požadovaných ochranných profilů (AV, IPS, AppCtrl, DLP), podpora transparentního ověřování uživatel proti MS AD protokolem Kerberos, funkce transparentní proxy, kdy dochází k automatickému přesměrování provozu na proxy server bez nutnosti konfigurovat klienta, funkce transparentního ověřování uživatelů pomocí domény (MS Active Directory) včetně podpory autentizace uživatel na terminálovém serveru	ANO	Kapitola 4.13.1
Virtualizace	Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). Každý virtuální kontext musí být plnohodnotné řešení včetně odděleného GUI, management účtů, atp.	ANO	Kapitola 4.13.1
	Součástí dodávky musí být licence na min. 10 virtuálních kontextů (včetně licence na kompletní podporu požadovaných bezpečnostních funkcí v těchto virtuálních kontextech)	ANO	Kapitola 4.13.1
	Každý virtuální kontext je zároveň samostatným wifi controllerem	ANO	Kapitola 4.13.1
	Podporou izolovaných administrátorských účtů pro správu jednotlivých virtuálních kontextů (samostatný administrátor pro jeden či více virtuálních kontextů)	ANO	Kapitola 4.13.1
Management	FW cluster musí být možné plnohodnotně spravovat pomocí lokálního GUI a CLI, provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici	ANO	Kapitola 4.13.1

	Podpora SNMP včetně SMPB MIB souboru dodávaného výrobcem, možnost začlenění do stávajícího systému dohledu sítě	ANO	Kapitola 4.13.1
	Podpora otevřeného API (možnost integrace vybraných funkcí do stávající management infrastruktury)	ANO	Kapitola 4.13.1

4.14 K.7 – Správa privilegovaných účtů – SW pro správu privilegovaných účtů a přístupů

4.14.1 Nabízené řešení

[redacted]

4.14.2 Způsob naplnění minimálních požadavků

Položka	Popis parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně uvedení výrobce, obchodního označení, konkrétní konfigurace, produktového čísla, případně uvede konkrétní parametry	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
Striktní oddělení přístupových oprávnění	Uživatelské přístupy řízeny bezpečnostní politikou - vybraný uživatel má práva přístupu pouze k definovaným účtům a systémům	ANO	Kapitola 4.14.1
	Podpora multi-tenant prostředí	ANO	Kapitola 4.14.1
	Povolení přístupu uživatelům/skupinám uživatelů pouze k vybraným účtům, systémům, auditním záznamům, konfiguraci atp.	ANO	Kapitola 4.14.1
	Povolení přístupu správci/administrátorovi řešení pouze k vybraným složkám a konfiguraci	ANO	Kapitola 4.14.1

Víceúrovňové schvalování přístupů	Víceúrovňové schvalování správcovských přístupů k cílovým systémům	ANO	Kapitola 4.14.1
	Možnost omezení přístupů dle vybraného účtu nebo na daný časový úsek	ANO	Kapitola 4.14.1
	Schvalování přístupu odděleně pro přístup k přihlašovacím údajům privilegovaného účtu nebo pro připojení na koncový systém	ANO	Kapitola 4.14.1
	Upozornění emailem nebo vytvořením ticketu v helpdesk systému na novou žádost, schválení a zamítnutí	ANO	Kapitola 4.14.1
	Uložení informací, nahrávek a spravovaných přihlašovacích údajů v jedné centrální a vysoce zabezpečené databázi	ANO	Kapitola 4.14.1
Podpora MS Active Directory	Plná integrace s Microsoft Active Directory na úrovni informací o uživatelích, příslušnosti ke skupinám a emailech	ANO	Kapitola 4.14.1
	Mapování rolí v PAM řešení v návaznosti na skupiny v AD	ANO	Kapitola 4.14.1
	Přístup k uživatelskému rozhraní přes webový portál z prohlížečů v prostředí MS Windows a Apple MacOS	ANO	Kapitola 4.14.1
	Ověření přes LDAP/MS Active Directory a druhým faktorem (minimálně LDAP, Radius server, SAML)	ANO	Kapitola 4.14.1
Silná autentizace	Možnost vynucení silné autentizace uživatelů pro přístup k uloženým údajům a pro bezpečné vzdálené připojení	ANO	Kapitola 4.14.1
	Možnost kombinace jméno/heslo+druhý faktor (RADIUS, LDAP, SAML, atp…)	ANO	Kapitola 4.14.1
Šifrování a zabezpečení dat	Systém musí splňovat Standard FIPS 140-2	ANO	Kapitola 4.14.1
	Šifrovací algoritmy min. na úrovni AES-256 a RSA-2048	ANO	Kapitola 4.14.1
	Splnění compliance požadavků pro ZKB, GDPR, PCI-DSS, SOX, HIPAA, atd.	ANO	Kapitola 4.14.1
	Bezpečné uložení citlivých dat včetně šifrování hesel pomocí AES 256	ANO	Kapitola 4.14.1
	Definování komplexity generovaných čísel hesel dle počtu znaků, využití malých/velkých písmen a speciálních znaků	ANO	Kapitola 4.14.1
Řízení hesel a SSH klíčů	Automatická výměna hesel a SSH klíčů privilegovaných účtů po ukončení relace (jednorázové heslo) nebo v pravidelných intervalech dle bezpečnostní politiky	ANO	Kapitola 4.14.1
	Vynucená (manuálně i politikou) rotace hesla/SSH klíče správcem PIM/PAM řešení	ANO	Kapitola 4.14.1
	Výměna hesel a SSH klíče (bez nutnosti používat agenty)	ANO	Kapitola 4.14.1

	Možnost přizpůsobení password management modulu	ANO	Kapitola 4.14.1
SSH klíče	Bezpečné spravování a distribuce SSH klíče	ANO	Kapitola 4.14.1
	Automatická změna hesla a SSH klíče pro specifické systémy či skupiny účtů	ANO	Kapitola 4.14.1
	Definování výjimky pro zamezení automatických rotací hesel a SSH klíčů u určitých účtů	ANO	Kapitola 4.14.1
	Definování časových intervalů pro provádění automatizovaných změn hesel a SSH klíčů	ANO	Kapitola 4.14.1
	Iniciace změn hesel a SSH klíčů po každém odhlášení	ANO	Kapitola 4.14.1
	Změna hesel pomocí RESTI API	ANO	Kapitola 4.14.1
Izolace relací	Zprostředkování správcovského přístupu na cílový systém pomocí tzv. jump serveru prostřednictvým komunikačního protokolu, aplikace a příslušného privilegovaného účtu - koncový uživatel nemá přístup k přihlašovacím údajům	ANO	Kapitola 4.14.1
	Izolace přístupu až na úroveň aplikace (typu webový prohlížeč s konkrétní URL, MMC konzole s vybraným snap-in, konkrétní aplikace - např. MS SQL, Management Studio, WinSCP, atp.) - uživatel nemá možnost přistupovat k jiným službám a aplikacím v rámci dané relace	ANO	Kapitola 4.14.1
	Uzavření spojení celé relace po ukončení aplikace	ANO	Kapitola 4.14.1
	Navázání vzdáleného připojení k relaci přes vlastní GUI dodaného řešení nebo pomocí standardních protokolů RDP a SSH a standardních klientů typu putty a remote desktop manager	ANO	Kapitola 4.14.1
	Podpora vynucení silné autentizace (min. integrace s LDAP, RADIUS nebo SAML) u všech možností připojení ke vzdálené relaci	ANO	Kapitola 4.14.1
Autentizace privilegovaných uživatelů	Metody autentizace privilegovaných uživatelů na monitorovaných systémech, minimálně: 1.Autentizace privilegovaného uživatele na monitorovaném systému pomocí stejných přihlašovacích údajů, které byly využity pro autentizaci na PIM/PAM řešení.	ANO	Kapitola 4.14.1
	2.Autentizace privilegovaného uživatele na monitorovaném systému pomocí statických a bezpečně uložených přihlašovacích údajů. (např. root, admin, privilegovaný lokální účet).	ANO	Kapitola 4.14.1
	3.Vyzváním uživatele k opětovnému zadání přihlašovacích údajů k monitorovanému systému, bez jejich zaznamenání.	ANO	Kapitola 4.14.1
Připojení do webových relací	Zprostředkování uživateli bezpečné připojení na vybrané webové aplikace, přístup do cloudu a sociální sítě	ANO	Kapitola 4.14.1

	PIM/PAM řešení zprostředkuje přihlášení do koncové webové aplikace pomocí silného "privilegovaného" účtu	ANO	Kapitola 4.14.1
	Bez nutnosti uživatele znát hesla privilegovaných účtu	ANO	Kapitola 4.14.1
	Podpora transparentního SSO	ANO	Kapitola 4.14.1
Nahrávání relací	Monitoring a nahrávání celé relace a aktivit privilegovaných účtů ve video formátu s možností kontextového vyhledávání, bez nutnosti instalace agentů na koncový systém	ANO	Kapitola 4.14.1
	Záznam relace vytvářen kontinuálně (vytváření záznamu relace formou screenshotů není přípustné)	ANO	Kapitola 4.14.1
	Zpětné vyhledávání v záznamu ve formě metadat - min. u RDP spuštěné aplikace a události, u SSH relací jednotlivé příkazy, u Webových aplikací click na jednotlivé odkazy, u jiných typů relací alespoň stisky kláves	ANO	Kapitola 4.14.1
	Přehrávání nahrávek bez nutnosti instalace nástrojů třetích stran (flash, java, codec, atp…)	ANO	Kapitola 4.14.1
	Přehrávání nahrávek dostupné z GUI dodávaného řešení	ANO	Kapitola 4.14.1
	Aktivace/deaktivace zaznamenání relací dle jednotlivých uživatelských skupin	ANO	Kapitola 4.14.1
Relace	Automatická terminace potenciálně nebezpečných relací na základě definovaných procesů, příkazů nebo aplikací spouštěných uživatelem na spravovaném systému	ANO [redacted]	Kapitola 4.14.1
	Možnost nastavení pro různé uživatele nebo uživatelské skupiny	ANO	Kapitola 4.14.1
	Vyžadování schválení relace v určitých časových rámcích (např. pondělí-pátek, 9:00-16:00 bez potřeby schválení, v jiných časech pouze po schválení)	ANO	Kapitola 4.14.1
	Možnost sledování relací v reálném čase - sledování aktivních relací dalším uživatelem (např. auditor)	ANO	Kapitola 4.14.1
	Ukončení sledované relace v případě nutnosti, možnost převzetí relace oprávněnou osobou	ANO	Kapitola 4.14.1
Blokace procesů	Blokování vybraných procesů na systémech Windows.	ANO	Kapitola 4.14.1
Schvalování relací	Schvalování přístupu privilegovaného uživatele k určitým monitorovaným systémům	ANO	Kapitola 4.14.1
	Možnost definice workflow pro schvalování přístupu privilegovaných uživatelů	ANO	Kapitola 4.14.1

Kontrola relací	Centrální vyhledávání v nahrávkách podle data, uživatele a spuštěného příkazu pro autorizovaný personál	ANO	Kapitola 4.14.1
	Označování nahrávek relací pomocí skóre (nebo podobný systém) podle spuštěných aplikací, akcí a příkazů v dané relaci	ANO	Kapitola 4.14.1
Zobrazení aktivit uživatele	Možnost auditu jednotlivých akcí uživatelů s privilegovanými účty - zobrazení hesla, změny uložených údajů, vytvoření relace, kontrola změny hesla privilegovaného účtu	ANO	Kapitola 4.14.1
Audit administrátorských akcí	Zobrazení veškerých aktivit administrátora řešení.	ANO	Kapitola 4.14.1
Přístup k reportům	Nastavení přístupu k reportům pouze pro vybrané uživatele.	ANO	Kapitola 4.14.1
Export auditních dat	Export auditních záznamů včetně exportu ve formě video nahrávek a textového logu	ANO	Kapitola 4.14.1
Nezpochybnitelný auditní záznam	Zaručení nezpochybnitelné auditovatelnosti jednotlivých operací, možnosti reportování a textové logy.	ANO	Kapitola 4.14.1
Zabezpečení auditních záznamů	Nesmazatelnost logů po dobu minimálně 30 dní.	ANO	Kapitola 4.14.1
	Uložení auditních záznamů v zašifrované podobě - přístup pouze pro oprávněného uživatele	ANO	Kapitola 4.14.1
Monitoring pomocí RestAPI	Monitoring jednotlivých komponent pomocí RestAPI - integrace s monitoring systémy zadavatele.	ANO	Kapitola 4.14.1
Podpora systémů zadavatele	Možnost správy pro různé druhy koncových systémů - minimálně v prostředí zadavatele tzn. MS Windows 10,11, Windows Server 2016, 2019 a 2022.	ANO	Kapitola 4.14.1
MFA - multi factor autentizace	V rámci řešení bude součástí také řešení pro MFA privilegovaných účtů	ANO	Kapitola 4.14.1
	Minimálně na úrovni LDAP/S, RADIUS, SAML, apod.	ANO	Kapitola 4.14.1
SIEM integrace	Integrace s nástroji SIEM - přenos logovaných auditních záznamů, nejlépe v reálném čase pomocí Syslog.	ANO	Kapitola 4.14.1
Architektura řešení	Virtuální software appliance (obsahuje i OS) s podporou pro stávající virtuální prostředí Hyper-V	ANO	Kapitola 4.14.1
	Databáze dat součástí řešení - není nutné využívat nástroje třetích stran. Tento požadavek platí pro veškerá data v rámci řešení	ANO	Kapitola 4.14.1

Vyhledávání systémů	Vyhledávání systémů a privilegovaných účtů formou skenování RDP + SSH portů a importů z AD.	ANO	Kapitola 4.14.1
Onboarding systémů	Mechanismus pro plnou či částečnou automatizaci onboardingu nově nalezených zařízení / účtů.	ANO	Kapitola 4.14.1
Zálohování systému	Možnost bezpečného zálohování dat systému	ANO [redacted]	Kapitola 4.14.1
	Zálohy musí být šifrované	ANO	Kapitola 4.14.1
Úložiště	Ukládání zaznamenaných relací lokálně či na externí úložiště CIFS/NFS.	ANO	Kapitola 4.14.1

4.15 K.8a – Ochrana koncových zařízení – Pokročilá anti-X ochrana

4.15.1 Nabízené řešení

[redacted]

4.15.2 Způsob naplnění minimálních požadavků

Položka	Popis parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně uvedení výrobce, obchodního označení, konkrétní konfigurace, produktového čísla, případně uvede konkrétní parametry	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
Technické požadavky	Automatická detekce aplikací na koncových zařízeních – sken aplikací	ANO	Kapitola 4.15.1
	Samoučící mód pro detekci aplikací, které byly na koncových zařízení spuštěny	ANO	Kapitola 4.15.1

	Možnost odebrání práva lokálního správce – uživatel na koncovém zařízení, může pracovat pouze pod standardním neprivilegovaným uživatelským oprávněním. Veškeré požadavky na vyšší oprávnění jsou řízeny podle bezpečnostní politiky. Oprávnění jsou následně povyšována jednorázově pro vybrané aktivity.	ANO	Kapitola 4.15.1
	Zajištění běhu aplikací s nejnižším možným oprávněním	ANO	Kapitola 4.15.1
	Možnost definovat aplikaci nebo systémový proces pro běh s privilegovaným oprávněním	ANO	Kapitola 4.15.1
	Řízení privilegií na koncovém bodu umožňuje řízení oprávnění uživatelů na koncových systémech, tak aby bylo možné granulárně definovat, který příkaz, aplikaci a akci je uživatel schopný spustit a pod jakými oprávněními.	ANO	Kapitola 4.15.1
	Schvalování privilegovaných činností je schopné vynutit autorizaci (zadání důvodu, schvalování) pro každý úkon, který vyžaduje vyšší oprávnění, jako je spuštění aplikace vyžadující vyšší oprávnění, konfigurace systému, editace systémových nastavení atp.	ANO	Kapitola 4.15.1
	Automatizovaná kategorizace aplikace na základě:	ANO	Kapitola 4.15.1
	a. Certifikátu	ANO	Kapitola 4.15.1
	b. Chráněné sdílené složky	ANO	Kapitola 4.15.1
	c. Definovaného uživatele	ANO	Kapitola 4.15.1
	d. Distribučního SW – například SCCM	ANO	Kapitola 4.15.1
	Definice aplikačních politik pro:	ANO	Kapitola 4.15.1
	a. Běh aplikace se uživatelským oprávněním	ANO	Kapitola 4.15.1
	b. Běh aplikace s privilegovaným oprávněním	ANO	Kapitola 4.15.1
	c. Důvěryhodné aplikace – aplikace bude spouštěna s oprávněním, které požaduje	ANO	Kapitola 4.15.1
	d. Blokace spuštění aplikace	ANO	Kapitola 4.15.1
	Detekce a správa neznámých aplikací – grey zóna:	ANO	Kapitola 4.15.1
	a. Blokace neznámé aplikace	ANO	Kapitola 4.15.1
	b. Běh v restriktivním režimu – nedovolí aplikaci komunikovat	ANO	Kapitola 4.15.1

	I. Do intenetu	ANO	Kapitola 4.15.1
	II. Na intranet	ANO	Kapitola 4.15.1
	III. Na sdílené složky	ANO	Kapitola 4.15.1
	Detekce a blokace pokusů o krádež přihlašovacích údajů:	ANO	Kapitola 4.15.1
	a. systému Windows	ANO	Kapitola 4.15.1
	b. ve webových prohlížečích	ANO	Kapitola 4.15.1
	c. v nástrojích pro správu systému	ANO	Kapitola 4.15.1
	Ochrana před hrozbami ransomware – detekce a blokace ransomware hrozeb hned při jejich spuštění	ANO	Kapitola 4.15.1
	Povolení neznámým aplikacím bezpečné spouštění v omezeném režimu. Neznámé aplikace, které nejsou důvěryhodné ani systému známé, mohou běžet v „omezeném režimu“, který jim brání v přístupu k firemním zdrojům, citlivým datům nebo internetu.	ANO	Kapitola 4.15.1
	Kontrola reputace detekované aplikace – možnost napojení na reputační systém výrobce nebo jiný, například Virustotal.	ANO	Kapitola 4.15.1
	Ochrana před útoky typu Pass-the-Hash (PtH) a Pass-the-Ticket (PtT) - systém musí poskytovat ochranu proti útokům, které využívají ukradené heslo nebo jiné přihlašovací údaje, jako jsou PtH a PtT útoky. Ochrana proti útokům na úložiště hesel – Windows LSASS, Edge, Chrome, Putty	ANO	Kapitola 4.15.1
	Flexibilní správa založená na politikách – jednoduchá správa systému a nastavení aplikačních politik	ANO	Kapitola 4.15.1
	Řízení aplikací v Just-In-Time režimu – definice dočasného období, kdy uživatele bude mít privilegované oprávnění	ANO	Kapitola 4.15.1
	Sledování a auditování - EPM musí umožňovat sledování a auditování všech akcí uživatelů na koncových zařízeních, aby se v reálném čase mohly odhalit potenciální bezpečnostní hrozby a reagovat na ně.	ANO	Kapitola 4.15.1
	Správa a řízení aplikací - EPM musí umožňovat spravovat a řídit aplikace, které jsou instalovány na koncových zařízeních, aby se minimalizovalo riziko šíření malware a jiného škodlivého softwaru.	ANO	Kapitola 4.15.1
	Hromadná instalace SW klienta – GPO, SCCM	ANO	Kapitola 4.15.1

	Zabezpečená komunikace klienta s management konzolí	ANO	Kapitola 4.15.1
	Správa koncových zařízení, které jsou mimo interní síť	ANO	Kapitola 4.15.1
	Aktualizace klientského SW z management konzole	ANO	Kapitola 4.15.1
	Logování spuštěných povolených aplikací a přednastavené repoty s možností pravidelného rozesílání	ANO	Kapitola 4.15.1

4.16 K.8b – Ochrana koncových zařízení – Pokročilá ochrana koncových zařízení s rozšířenou detekční schopností

4.16.1 Nabízené řešení

[redacted]

4.16.2 Způsob naplnění minimálních požadavků

Položka	Popis parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně uvedení výrobce, obchodního označení, konkrétní konfigurace, produktového čísla, případně uvede konkrétní parametry	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
Základní technické požadavky	Pokročilá AV ochrana	ANO	Kapitola 4.16.1
	Ochrana před známými hrozbami	ANO	Kapitola 4.16.1
	Ochrana proti exploitům	ANO	Kapitola 4.16.1
	Ochrana proti bez souborovým útokům	ANO	Kapitola 4.16.1

	Ochrana proti síťovým útokům a hrozbám	ANO	Kapitola 4.16.1
	Monitorování škodlivých procesů	ANO	Kapitola 4.16.1
	Konfigurovatelný personální Firewall	ANO	Kapitola 4.16.1
	Sandbox	ANO	Kapitola 4.16.1
	Strojové učení	ANO	Kapitola 4.16.1
	Detekce anomálií	ANO	Kapitola 4.16.1
	Analýza hrozeb a anomálií	ANO	Kapitola 4.16.1
	Analýza rizik koncové stanice	ANO	Kapitola 4.16.1
	Integrace s Mitre modelem	ANO	Kapitola 4.16.1
	plná funkcionalita pro EDR/XDR	ANO, [redacted]	Kapitola 4.16.1
	Podpora integrace na stávající SIEM na úrovni zasílání Syslog zpráv	ANO	Kapitola 4.16.1
	Podpora API	ANO	Kapitola 4.16.1

4.17 K.9 – Monitorování práce s digitálními daty – SW pro monitorování práce s digitálními daty

4.17.1 Nabízené řešení

[redacted]

4.17.2 Způsob naplnění minimálních požadavků

Položka	Popis parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně uvedení výrobce, obchodního označení, konkrétní konfigurace, produktového čísla, případně uvede konkrétní parametry	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
DLP systém	Ochrana koncových zařízení uživatelů: PC, Notebooky, servery	[redacted]	Kapitola 4.17.1
	Ochrana koncových zařízení v Online / Offline režimu		Kapitola 4.17.1
	Ochrana rozhraní před únikem dat USB, CD, DVD a podobně		Kapitola 4.17.1
	Ochrana serverů souborového systému (CIFS, NCP a volitelně: NFS, SFTP, FTP)		Kapitola 4.17.1

	Ochrana přenášených dat do externích cloudových úložišť	[redacted]	Kapitola 4.17.1
	Ochrana interní emailové komunikace		Kapitola 4.17.1
	Ochrana před únikem dat cestou služeb Free mailů (např .: Gmail, Yahoo, Centrum, Seznam, podobně)		Kapitola 4.17.1
	Ochrana před únikem dat na internetová Webová úložiště (např .: Rapid Shere, Slunečnice a další)		Kapitola 4.17.1
	Ochrana tiskových služeb:		Kapitola 4.17.1
	a. lokální tiskárny		Kapitola 4.17.1
	b. síťové tiskárny		Kapitola 4.17.1
	Ochrana komunikace Instant Messaging (Icq, Yahoo, MSN Messenger		Kapitola 4.17.1
	Šifrování citlivých (klasifikovaných) dat kopírovaných na vyjímatelná média – USB flash disky	ANO	Kapitola 4.17.1
	Definice bezpečnostní politiky na zařízení, uživatelskou skupinu z AD nebo konkrétního uživatele	ANO	Kapitola 4.17.1
	Vyhledávání citlivých dat na lokálních discích – lokální discovery	ANO	Kapitola 4.17.1
	Vyhledávání citlivých dat na externích úložištích – Network Discovery pro:		Kapitola 4.17.1
	a. File servery – CIFS souborové systémy	ANO	Kapitola 4.17.1
	b. PST složky	ANO	Kapitola 4.17.1
	c. Microsoft Exchange	ANO	Kapitola 4.17.1
	d. Microsoft SharePoint	ANO	Kapitola 4.17.1
	e. Microsoft SQL server	ANO	Kapitola 4.17.1
	Nastavení reakčních pravidel podle závažnosti incidentu:		Kapitola 4.17.1
	a. Monitorování incidentu		Kapitola 4.17.1
	b. Justifikace incidentu – upozornění uživatele a možnost uživatele rozhodnout se o odeslání dat		Kapitola 4.17.1
	c. Blokace incidentu		Kapitola 4.17.1
	d. Šifrování dat na USB zařízení při detekci incidentu		Kapitola 4.17.1
	Možnost rozšíření funkcionality DLP o šifrování souborů a emailů, popřípadě podpora systémů, které tyto funkce nabízí.		Kapitola 4.17.1

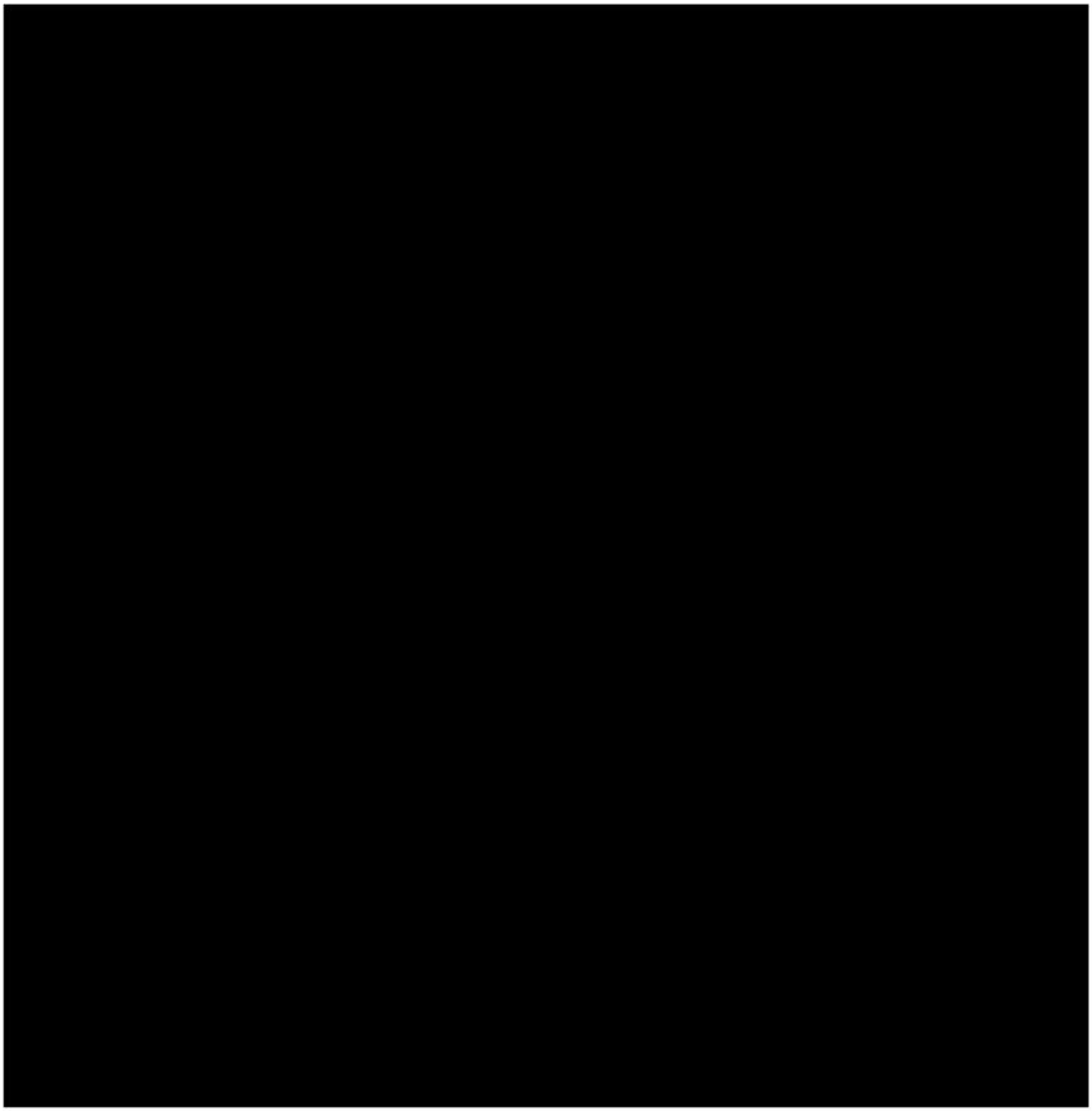
	Vynucení různé politiky DLP podle typu připojení NTB – Lokální síť, kavárna, hotel, letiště..	ANO [redacted]	Kapitola 4.17.1
	Vynucení různé politiky DLP pro uživatele nebo uživatelské skupiny z Microsoft AD	ANO [redacted]	Kapitola 4.17.1
Klasifikace dat v DLP systému	**Schopnost obsahové klasifikace dat - extrahovat a zkontrolovat textový obsah dat, souborů a příloh pomocí slov, frází a RegEx výrazů pro:**		Kapitola 4.17.1
	a. Emailovou komunikaci	ANO	Kapitola 4.17.1
	b. Webovou komunikaci včetně HTTPS	ANO	Kapitola 4.17.1
	c. Tisk dokumentů	ANO	Kapitola 4.17.1
	d. Kopírování na vyjímatelná média	ANO	Kapitola 4.17.1
	e. Odesílání na cloudové služby	ANO	Kapitola 4.17.1
	f. PrintScreen	ANO	Kapitola 4.17.1
	g. Copy/Paste	ANO	Kapitola 4.17.1
	h. Síťovou komunikaci	ANO	Kapitola 4.17.1
	Schopnost kontrolovat i metadata souborů při obsahové klasifikaci dat	ANO	Kapitola 4.17.1
	Schopnost detekovat klasifikátory třetích stran – Microsoft AIP	[redacted]	Kapitola 4.17.1
	Přednastavené bezpečnostní politiky, RegEx výrazy a slovníky pro nejčastěji kontrolované údaje (např. šifrované soubory, rodné číslo ČR, jména, příjmení, datum narození, typy souborů podle True Type apod.)	ANO, [redacted]	Kapitola 4.17.1
	Schopnost kontrolovat obsah komprimovaných (např. ZIP, TAR, RAR) archivů	ANO	Kapitola 4.17.1
	Detekce tzv. TrueType souboru - podpora detekce založené na skutečném typu dokumentu, i když uživatel změnil příponu	ANO	Kapitola 4.17.1
	Schopnost skládat více klasifikátorů v rámci klasifikačního pravidla - jak obsahové klasifikace dat, tak kontextové klasifikace dat a možnost definice thresholdu pro každý klasifikátor samostatně.	ANO, [redacted]	Kapitola 4.17.1
	Možnost definovat výjimky pro uživatele nebo uživatelské skupiny v rámci klasifikace dat	ANO, [redacted]	Kapitola 4.17.1
	Podpora Fingerprint klasifikace dat – vytvoření vlastní databáze hashů z konkrétních dat společnosti (např. z databáze) a následná kontrola výskytu těchto dat ve zpracovávaných datech uživatelem	ANO	Kapitola 4.17.1
Centrální správa DLP	Jednotný centrální management, který zajišťuje vymáhání nastavené bezpečnostní politiky (zaznamenávání, hlášení, notifikace)	ANO	Kapitola 4.17.1

	Centrální management bezpečnostní politiky zajišťuje přívětivé uživatelské prostředí, využívá se webová konzole pro správu celého systému	ANO	Kapitola 4.17.1
	Včasné oznámení na bezpečnostní incidenty úniku dat (SNMP trap, email, integrace se SIEM a podobně)	ANO	Kapitola 4.17.1
	Podpora konfigurovatelné vyhodnocování závažnosti incidentu	ANO, dle konfigurace	Kapitola 4.17.1
	Zobrazování událostí v graficky srozumitelné podobě	ANO	Kapitola 4.17.1
	Přehledné reporty, poskytnutí způsobu intuitivního reportování a používání Dashboard, pro management, bezpečnostního manažera, audit	ANO	Kapitola 4.17.1
	Podpora nasazení Endpoint agenta hromadnou instalací – například Microsoft SCCM, GPO.	ANO	Kapitola 4.17.1
	Změny bezpečnostní politiky, odesílání detekovaných incidentů řízena z centrální management konzole	ANO	Kapitola 4.17.1
Technické požadavky a prostředí určené pro implementaci DLP ochrany	Podpora stávající platformy zadavatele (Windows 10, 11 Windows server , 2016 a vyšší)	ANO	Kapitola 4.17.1
	Integrace do Active Directory	ANO	Kapitola 4.17.1
	Interně technické prostředí: emailový server, souborové servery, databáze interních aplikaci, koncová zařízení (osobní počítače, notebook)	ANO	Kapitola 4.17.1
	Provoz produktu s nevýznamným vlivem na výkon stávajícího informačního systému (např .: performance, systémové a související nároky v oblasti software / hardware)	ANO	Kapitola 4.17.1
Zabezpečení koncových bodů	Systém musí chránit agenta na koncovém zařízení proti manipulaci – zastavení, odinstalace SW, zastavení služby apod.	ANO	Kapitola 4.17.1
	Šifrovaná komunikace koncového zařízení s management serverem	ANO	Kapitola 4.17.1
Další požadavky	Možnost rozšířit v budoucnu systém o síťové sondy, tzv. Network DLP pro webovou a emailovou komunikaci	ANO	Kapitola 4.17.1
	Možnost rozšířit DLP systém v budoucnu o funkcionalitu UEBA – vyhodnocování chování uživatelů, automatické nastavení rizikovosti uživatelů a následná úprava DLP politiky.	ANO	Kapitola 4.17.1
	Kompatibilita se stávajícími ochrannými mechanismy (antivir, elektronická pošta, kontrola webu (Web Gateway)		Kapitola 4.17.1

	Podpora napojení na Microsoft Active directory a možnost využívat uživatele a skupiny definované v AD v politice DLP.		Kapitola 4.17.1
	Možnost napojení na systém SIEM pro vyhodnocování logů a incidentů		Kapitola 4.17.1

4.18 K.10a - Ochrana datové základny úřadu - Záložní server

4.18.1 Nabízené řešení



4.18.2 Způsob naplnění minimálních požadavků

Položka	Popis parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně uvedení výrobce, obchodního označení, konkrétní konfigurace, produktového čísla, případně uvede konkrétní parametry	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
Typ zařízení	Server v provedení k instalaci do 19" racku, maximálně 2U		Kapitola 4.18.1
	Zásuvné ližiny s managementem kabeláže		Kapitola 4.18.1
Procesor	1ks CPU - architektura **x86 s 32** plnohodnotnými jádry. Taktovací základní frekvence **min. 2,6 GHz**, FSB min. 3200 MHz, nebo v testu na cpubenchmark.net minimálně 59000 bodů. Max. počet CPU je omezen na 1 a počet jader je omezen na 32 core z důvodu licencování OS a aplikací. TDP max. 200W.		Kapitola 4.18.1
Paměť	**1536GB**, typu DDR4 s taktem 3200MT/s, Dual Rank		Kapitola 4.18.1
	Počet paměťových modulů a rozmístění musí být zvoleno pro optimální výkon s CPU		Kapitola 4.18.1
Pevné disk	Osaditelný min. **24** disků SAS nebo SATA SSD a **2** disky na instalaci OS. Veškeré potřebné komponenty (řadič, diskové pozice, kabeláž, napájecí zdroje apod.) musí být již nyní osazeny tak, aby server bylo možné funkčně osadit plným počtem SSD pouhým dodatečným vložením disků.		Kapitola 4.18.1

	Server musí podporovat Onboard SATA software RAID řadič pro SSD/HDD a také dvojici disků M.2, dále musí podporovat osazení nřadičem schopným pracovat v tzv. Mixed Mode jako RAID nebo HBA.	[redacted]	Kapitola 4.18.1
	12Gb/s SAS řadič s RAID 0/1/1+0/5/50/6/60/1 s 8GB battery backed write cache, onboard nebo osazený v PCI Express slotu.		Kapitola 4.18.1
OS Boot	Musí být zajištěn dvojicí SSD v **RAID1** a kapacitou min. **480GB**		Kapitola 4.18.1
LAN konektivita	1ks Ethernet adapter Dual Port 25GbE SFP28 Adapter včetně MM zářičů 10GbE a 2m kabelů LC/LC-LC/LC,		Kapitola 4.18.1
	1ks Ethernet adapter 2x1Gbps 1000BASE-T		Kapitola 4.18.1
FC konektivita	1x min. Single Port FC 16Gb/s HBA + kabel 2m, konektory LC		Kapitola 4.18.1
Napájení a chlazení	Server musí být vybaven redundantním napájením a chlazením, hot-plug vyměnitelné za provozu		Kapitola 4.18.1
	2ks hot-swap zdroje napájení dimenzované pro plné osazení serveru disky, CPU, RAM a PCIe zařízení, energetická účinnost min. Platinum (94%)		Kapitola 4.18.1
Podpora vzdálené správy	Disponování vyhrazeným Gb portem pro vzdálený management, port musí mít k dispozici úložiště pro firmware		Kapitola 4.18.1
	Úložiště konfigurovatelné pro vytváření firmware sad s možností rollback při pádu aktualizace		Kapitola 4.18.1
	Podpora bez agentového vzdáleného managementu		Kapitola 4.18.1
	Vzdálený management musí podporovat standardní webové prohlížeče pro grafickou vzdálenou konzoli spolu s tlačítkem pro Virtual Power a podporovat vzdálený boot z DVD/CD/USB zařízení a být schopen uchovávat historická data o sw upgradech a patchích		Kapitola 4.18.1
	Podpora vícefaktorové autentizace		Kapitola 4.18.1

	Monitorování změn v hw a systémové konfiguraci, podpora rychlé diagnostiky vzniklých problémů	[redacted]	Kapitola 4.18.1
	Podpora mobilního zařízení Android a Apple OS pro vzdálenou správu		Kapitola 4.18.1
	Vzdálená konzola musí umožnit současný přístup více uživatelů (min. 3) během pre-OS a OS runtime operací, musí existovat schopnost uchovat video z poslední zásadní poruchy a posledního bootovacího procesu, musí být podporována 128 bitové SSL enkrypce a Secure Shell Version 2, musí být podporovány AES a 3DES na prohlížeči a vzdálený firmware update a JAVA free pro vzdálenou konzoli.		Kapitola 4.18.1
	Podpora současné podpory většího množství serverů v následujících komponentách: Power Control, Power Caping, Firmware Update, konfigurace, Virtual Media, Licence Activation		Kapitola 4.18.1
	Podpora RESTFullAPI integrace a předávání hw událostí přímo na výrobce serveru		Kapitola 4.18.1
Funkční specifikace	Server musí být osazen TPM 2.0		Kapitola 4.18.1
	Možnost rychlého pohledu na spravované serverové zdroje		Kapitola 4.18.1
	Minimální zobrazované položky Dashboardu: Server Profiles, Server Hardware a Appliance Alerts		Kapitola 4.18.1
	Přístup do managementu řízen pomocí rolí		Kapitola 4.18.1
	Management sw musí být integrovatelný minimálně do VMware vCenter a Microsoft SCVMM		Kapitola 4.18.1
	Systém musí umožňovat proaktivní notifikaci o aktuálních nebo hrozících selháních kritických komponent jako jsou procesory, paměť a disky		Kapitola 4.18.1
	Schopnost systému upozornit na out-of-date BIOS, ovladače a agenty server managementu a umožnění vzdáleného update těchto komponent		Kapitola 4.18.1
	Server management sw musí být od stejného výrobce, jako je výrobce serveru		Kapitola 4.18.1

4.19 K.10b- Ochrana datové základny úřadu - Diskové úložiště

4.19.1 Nabízené řešení

[redacted]

[redacted]

4.19.2 Způsob naplnění minimálních požadavků

Položka	Popis parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně uvedení výrobce, obchodního označení, konkrétní konfigurace, produktového čísla, případně uvede konkrétní parametry	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
Minimální požadovaná hrubá kapacita a ochrana dat	Minimálně 45 TB na SSD / Flash ve variantě enterprise DWPD 2 a vyšší. Je požadována ochrana dat minimálně proti výpadku 2 disků/modulů současně	[redacted]	Kapitola 4.19.1
Konektivita k hostitelským serverům (front-end)	diskové pole musí být připojeno k záložnímu serveru redundantně a to minimální rychlostí každé linky 12Gb/s		Kapitola 4.19.1
Podpora operačních systémů a hypervizorů	VMware, 7.0 U3 a vyšší, Windows server 2016 a vyšší		Kapitola 4.19.1
Bezpečnost	diskové pole musí být schopno konfigurace pro různé. typy RAID ochrany, včetně spare disků (minimálně RAID v úrovní 0,1,5,10,50)		Kapitola 4.19.1
Správa diskového pole a další dostupné funkcionality	SW pro plnohodnotnou správu diskového pole a diskových subsystémů, možnost ovládání přes CLI, GUI (ze std. web browseru).		Kapitola 4.19.1
Příslušenství	Součástí dodávky bude potřebná kabeláž pro plné zapojení všech portů do instalovaného prostředí a napájecí kabeláž kompatibilní s napájecími lištami v RACK skříních.		Kapitola 4.19.1

4.20 K.10c - Ochrana datové základny úřadu - Zabezpečené úložiště záloh s řízenou retencí

4.20.1 Nabízené řešení

[redacted]

4.20.2 Způsob naplnění minimálních požadavků

Položka	Popis parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně uvedení výrobce, obchodního označení, konkrétní konfigurace, produktového čísla, případně uvede konkrétní parametry	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
Základní specifikace zařízení	Pásková knihovna v provedení k instalaci do 19" racku, maximálně 2U	[redacted]	Kapitola 4.20.1
	Uložiště pásek s automatickou výměnou pásek v páskových mechanikách		Kapitola 4.20.1
	Kapacita vyměnitelných médií: minimálně 24		Kapitola 4.20.1
	Počet paměťových modulů a rozmístění musí být zvoleno pro optimální výkon s CPU	ANO	Kapitola 4.20.1
	1 x Ethernet pro vzdálenou správu	ANO	Kapitola 4.20.1
	Součástí knihovny musí být integrovaná čtečka čárových kódů	ANO	Kapitola 4.20.1
	Podpora kazetových médií s páskami LTO Ultrium 8 a Ultrium 9	ANO	Kapitola 4.20.1
Specifikace páskové mechaniky	Mechanika plně kompatibilní s dodávanou páskovou knihovnou a se zálohovacím SW zadavatele (Veeam)	ANO	Kapitola 4.20.1
	Standard záznamu: LTO Ultrium 9	[redacted]	Kapitola 4.20.1

	Typ rozhraní: minimálně 8Gb Fibre Channel	[redacted]	Kapitola 4.20.1
Ostatní požadavky	Součástí dodávky je minimálně 40ks pásek LTO-9 a 1ks čistící pásky		Kapitola 4.20.1

4.21 K.10d - Ochrana datové základny úřadu - SW licence operačních systémů záložního serveru

4.21.1 Nabízené řešení

[redacted]

4.21.2 Způsob naplnění minimálních požadavků

Položka	Popis parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně uvedení výrobce, obchodního označení, konkrétní konfigurace, produktového čísla, případně uvede konkrétní parametry	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
OS záložního serveru	Zadavatel požaduje dodání OS v aktuální verzi (s možností downgrade), který je plně kompatibilní s OS používáným ve stávajícím MS Hyper-V clusteru. Je požadováno dodání verze, umožňující spuštění neomezného množství virtuálních serverů. Licence musí pokrývat všechna CPU jádra, dodaná v rámci Záložního serveru.	[redacted]	Kapitola 4.21.1
Databázový server	Součásí dodávky musí být také licence databázového serveru Microsoft SQL v aktuální verzi (použití tohoto typu databázového serveru je přímo určeno aplikacemi provozovanými v IT prostředí úřadu). Licence musí být určena pro provoz ve virtualizovaném prostředí a musí být schopna migrace mezi nody Hyper-V clusteru dle provozních okolností zadavatele bez dalšího omezení. Licenčně musí být pokryto minimálně 8 CPU jader		Kapitola 4.21.1

4.22 K.10e - Ochrana datové základny úřadu - SW licence zabezpečeného úložiště

4.22.1 Nabízené řešení

[redacted]

4.22.2 Způsob naplnění minimálních požadavků

Položka	Popis parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně uvedení výrobce, obchodního označení, konkrétní konfigurace, produktového čísla, případně uvede konkrétní parametry	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
Základní specifikace zařízení	Disaster recovery na úrovni virtuálních strojů bez negativního ovlivňování výkonu prostředí, kompatibilní s provozovanou serverovou virtualizací (MS Hyper-V) (např. pokud by dodavatelem zvolený způsob využíval snapshot technologii, jejich četnost nesmí negativně ovlivnit odezvu provozovaných VM).	ANO	Kapitola 4.22.1
	Možnost nedestruktivního testování obnovy v oddělené, izolované LAN.	ANO	Kapitola 4.22.1
	Automatické obnovení replikace v opačném směru po obnovení provozuschopnosti hlavní lokality (re-protect funkcionalita) s důrazem na minimální součinnost administrátora (tzv. One-Click Recovery).	ANO	Kapitola 4.22.1
	Možnost ze zálohy jednoduchým způsobem obnovit jednotlivé soubory virtuálního serveru. Podpora plné automatizované orchestrace DR scénářů	ANO	Kapitola 4.22.1
	Zaručená konzistence dat na souborové úrovni pomocí technologie VSS pro OS Windows.	ANO	Kapitola 4.22.1

	Monitorování alertů replikace v management nástroji virtuálního prostředí.	ANO	Kapitola 4.22.1
	Možnost využití cloudu jako úložiště replikací, tak jako provozní infrastruktury pro obnovu.	ANO	Kapitola 4.22.1
	Podpora Consistency Group pro společnou ochranu skupin VM kritických aplikací.	ANO	Kapitola 4.22.1
Výkonové požadavky	Reálná a akceptačními testy prověřená hodnota parametru RPO (Recovery Point Objective) lepší jak 30 vteřin.	ANO	Kapitola 4.22.1
	Reálná a akceptačními testy prověřená hodnota parametru RTO (Recovery Time Objective) nesmí překročit 5 minut.	ANO	Kapitola 4.22.1

4.23 K.10f - Ochrana datové základny úřadu - Datové rozvaděče 19" vč. non IT technologií

4.23.1 Nabízené řešení

4.23.1.1 Datový stojanový rozvaděč pro umístění UPS, aktivních prvků a pasivních optických komponent

[redacted]

4.23.1.2 Datový rozvaděč pro umístění UPS, aktivních prvků a pasivních optických komponent

[redacted]

4.23.2 Způsob naplnění minimálních požadavků

4.23.2.1 Datový stojanový rozvaděč pro umístění UPS, aktivních prvků a pasivních optických komponent

Položka	Popis parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně uvedení výrobce, obchodního označení, konkrétní konfigurace, produktového čísla, případně uvede konkrétní parametry	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
Datový stojanový rozvaděč pro umístění UPS, aktivních prvků a pasivních optických komponent	Šířka 800mm	ANO	Kapitola 4.23.1.1
	Hloubka 1000mm	ANO	Kapitola 4.23.1.1
	Výška 42U	ANO	Kapitola 4.23.1.1
	Nosnost min. 800kg	ANO	Kapitola 4.23.1.1
	Přední dveře jednokřídlé	ANO	Kapitola 4.23.1.1
	Zadní dveře jednokřídlé	ANO	Kapitola 4.23.1.1
	Uzamykatelný	ANO	Kapitola 4.23.1.1

	Přední dveře perforované	ANO	Kapitola 4.23.1.1
	Zadní dveře perforované	ANO	Kapitola 4.23.1.1
	2 páry posuvných 19" lišt L	ANO	Kapitola 4.23.1.1
	IP krytí IP30	ANO	Kapitola 4.23.1.1
	Míra perforace 80-88%	ANO,[redacted]	Kapitola 4.23.1.1
	Možnost spodního vstupu kabelů	ANO	Kapitola 4.23.1.1
	Možnost horního vstupu kabelů	ANO	Kapitola 4.23.1.1
	Odnímatelné boční panely	ANO	Kapitola 4.23.1.1

4.23.2.2 Datový rozvaděč pro umístění UPS, aktivních prvků a pasivních optických komponent

Položka	Popis parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně uvedení výrobce, obchodního označení, konkrétní konfigurace, produktového čísla, případně uvede konkrétní parametry	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
Datový rozvaděč pro umístění UPS, aktivních prvků a pasivních optických komponent	Šířka 600mm	ANO	Kapitola 4.23.1.2
	Hloubka 600mm	ANO	Kapitola 4.23.1.2
	Výška 42U	ANO	Kapitola 4.23.1.2
	Max. zátěž min. 80kg	ANO,[redacted]	Kapitola 4.23.1.2
	Přední dveře jednokřídlé	ANO	Kapitola 4.23.1.2
	Uzamykatelný	ANO	Kapitola 4.23.1.2
	Posuvné 19" lišty L	ANO	Kapitola 4.23.1.2
	IP krytí IP20	ANO,[redacted]	Kapitola 4.23.1.2
	Možnost spodního vstupu kabelů	ANO	Kapitola 4.23.1.2
	Možnost horního vstupu kabelů	ANO	Kapitola 4.23.1.2
	Odnímatelné boční panely	ANO	Kapitola 4.23.1.2

4.24 K.10g - Ochrana datové základny úřadu - Tenký klient

4.24.1 Nabízené řešení

[redacted]

4.24.2 Způsob naplnění minimálních požadavků

Položka	Popis parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně uvedení výrobce, obchodního označení, konkrétní konfigurace, produktového čísla, případně uvede konkrétní parametry	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
Centrální správa	Pro centrální řízení terminálových stanic bude dodán a implementován systém pro jejich centrální správu.	ANO	Kapitola 4.24.1
Provedení	Pasivní provedení bez rotačních dílů (HDD, ventilátor apod.), možnost umístění "nastojato" i "naležato" (umístění v kancelářích)	ANO	Kapitola 4.24.1
Rozměry	Z důvodu instalace do stávajícího nábytku, případně do držáku na monitorech je požadována maximální velikost tenkého klienta 20 x 20 x 4 cm	ANO[redacted]	Kapitola 4.24.1
Porty	Min. 6x USB, z toho min 4x USB 3.1 a min. 2x USB na čelním panelu, 2x display port 1.2, audio - mikrofon, sluchátka, LAN RJ-45 1 Gb s podporou WoL (wake on line)	ANO	Kapitola 4.24.1
Výkon	64 bit CPU, HD grafický čip, RAM min. 4 GB, interní flash úložiště min. 32 GB	ANO,[redacted]	Kapitola 4.24.1
Grafika	Rozlišení min. 4k (3840x2160), podpora dvoumonitorového provozu	ANO	Kapitola 4.24.1
Kompatibilita	Microsoft RDP 8.1; Remote FX; Citrix ICA, Citrix HDX, VMware PCoIP, podpora nabízených verzí virtualizačního software	ANO	Kapitola 4.24.1
Bezpečnost	Podpora 802.1X	ANO	Kapitola 4.24.1
Šifrování	Integrovaný TPM chip	ANO	Kapitola 4.24.1
Operační systém	Windows 10 IoT a vyšší	ANO	Kapitola 4.24.1
VESA	Podpora standardu VESA pro montáž na monitor, zeď apod.	ANO	Kapitola 4.24.1
Rozšiřitelnost	Sériový port, WiFi včetně antény. Vše interní nebo pevně spojené se šasi - ochrana proti odcizení	ANO	Kapitola 4.24.1
Spotřeba	Z důvodu snížení provozních nákladů je požadována spotřeba max. 10 W	ANO[redacted]	Kapitola 4.24.1
Zabezpečení	Slot pro Kensington lock nebo kompatibilní	ANO	Kapitola 4.24.1
Periferie	Včetně bezdrátové klávesnice s CZ rozložením kláves a bezdrátové optické myši	ANO	Kapitola 4.24.1
Licence	Pro všechny nabízené tenké klienty	ANO	Kapitola 4.24.1
Rozhraní	Grafické, funkčnost v prostředí zadavatele	ANO	Kapitola 4.24.1

Funkce	Vzdálené zapnutí a vypnutí klientů, konfigurace klientů, nahrání image operačního systému, řízení aktualizací a rozšíření klientů, vzdálený přístup k OS klienta (shadowing), správa konfiguračních šablon, automatické vyhledání klientů	ANO	Kapitola 4.24.1
Dálkové řízení	Podpora WoL	ANO	Kapitola 4.24.1
Integrace	Integrace s Active Directory	ANO	Kapitola 4.24.1

4.25 K.11a - Centrální komunikační systém úřadu - Hlasová brána

4.25.1 Nabízené řešení

4.25.2 Způsob naplnění minimálních požadavků

Položka	Popis parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně uvedení výrobce, obchodního označení, konkrétní konfigurace, produktového čísla, případně uvede konkrétní parametry	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
Určení	Propojení IP telefonního systému s veřejnou telefonní sítí na centrální úrovni musí být možné realizovat rovněž pomocí IP trunků.	ANO	Kapitola 4.25.1

hlasové brány/IP PBX	IP telefonní systém musí v případě potřeby umožnit snadné připojení externích telefonních sítí (hlasových bran/IP PBX) pomocí IP trunků, které zajistí oddělení externí a interní telefonní komunikace, normalizaci a překlad signalizačního protokolu H.323, resp. SIP a překlad (transkodování) hlasového kanálu.	ANO	Kapitola 4.25.1
Technické požadavky	Typ zařízení - Směrovač	ANO	Kapitola 4.25.1
	Formát zařízení modulární	ANO	Kapitola 4.25.1
	Požadovaný počet portů GigabitEthernet 3x10/100/100Base-TX	ANO	Kapitola 4.25.1
	Interní AC napájecí zdroj	ANO	Kapitola 4.25.1
	Min. 3 volné sloty pro rozšiřující moduly	ANO	Kapitola 4.25.1
	Směrování IPv4	ANO	Kapitola 4.25.1
	Směrování IPv6	ANO	Kapitola 4.25.1
	OSPFv2	ANO	Kapitola 4.25.1
	BGPv4	ANO	Kapitola 4.25.1
	Podpora 4 byte AS numbers in BGP	ANO	Kapitola 4.25.1
	Možnost směrování provozu dle dynamicky měřených metrik (zatížení linky, zpoždění, ztrátovost paketů, jitter)	ANO	Kapitola 4.25.1
	First Hop Redundancy Protokol (např. VRRP, HSRP)	ANO	Kapitola 4.25.1
	GRE (Generic Routing Encapsulation)	ANO	Kapitola 4.25.1
	Policy-based routing podle ACL	ANO	Kapitola 4.25.1
	IP Multicast (PIM SSM, PIM SM)	ANO	Kapitola 4.25.1
	IGMPv2, IGMPv3	ANO	Kapitola 4.25.1
	uRPF	ANO	Kapitola 4.25.1
	DHCP relay	ANO	Kapitola 4.25.1
	First Hop Redundancy Protokol pro IPv6	ANO	Kapitola 4.25.1
	OSPFv3	ANO	Kapitola 4.25.1
	MP BGP	ANO	Kapitola 4.25.1
	IPv6 Multicast (MLDv1 & v2)	ANO	Kapitola 4.25.1
	IPv6 Multicast (PIM SM, PIM SSM)	ANO	Kapitola 4.25.1
	IPv6 SLA nebo ekvivalentní technologie	ANO	Kapitola 4.25.1
	uRPF pro IPv6	ANO	Kapitola 4.25.1
	IPv6 Tunneling: IPv6 over IPv4 GRE Tunnels	ANO	Kapitola 4.25.1
	IPv6 over IPv4 Multipoint VPN nebo ekvivalentní technologie	ANO	Kapitola 4.25.1
	DHCPv6 Relay	ANO	Kapitola 4.25.1
	QoS classification – ACL, DSCP, CoS based	ANO	Kapitola 4.25.1
	QoS marking - DSCP, CoS	ANO	Kapitola 4.25.1
	QoS Shaping and Policing	ANO	Kapitola 4.25.1

	Class Based and Priority queuing	ANO	Kapitola 4.25.1
	Rate Limiting	ANO	Kapitola 4.25.1
	Hierarchical QoS min. 3 úrovně	ANO	Kapitola 4.25.1
	RSVP	ANO	Kapitola 4.25.1
	Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)	ANO	Kapitola 4.25.1
	Minimálně 20 oddělených (nezávislých) směrovacích tabulek	ANO	Kapitola 4.25.1
	QoS pre-classification for IPSec	ANO	Kapitola 4.25.1
	VRF aware IPSec	ANO	Kapitola 4.25.1
	Vytváření šifrovaných Hub&Spoke VPN s možností dynamicky sestavovat tunely mezi „spoke“ lokalitami (např. pro IPT provoz)	ANO	Kapitola 4.25.1
	Vytváření šifrovaných VPN bez potřeby tunelů dle RFC 3547 (GDOI based VPN) s centrální správou šifrovacích klíčů	ANO	Kapitola 4.25.1
	Podpora Suite-B šifrovacích algoritmů (RFC 6379) ve spojení s GDOI based VPN	ANO	Kapitola 4.25.1
	VRF aware GDOI group member (selektivní šifrování provozu per IP VPN)	ANO	Kapitola 4.25.1
	Měření statistik a výkonnostních charakteristik přenášených multimediálních, realtimových a aplikačních toků - využívané pásmo	ANO	Kapitola 4.25.1
	Měření statistik a výkonnostních charakteristik přenášených multimediálních, realtimových a aplikačních toků - odezvy aplikací	ANO	Kapitola 4.25.1
	Vynucení QoS parametrů pro takto rozpoznané aplikace a skupiny aplikací - marking, garance šířky pásma pro jednotlivé aplikace, shaping, policing	ANO	Kapitola 4.25.1
	Sběr a vyhodnocování statistik a výkonnostních charakteristik multimediálních toků: využívané pásmo, odezvy aplikací, RTP statistiky	ANO	Kapitola 4.25.1
	Application Visibility - Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)	ANO	Kapitola 4.25.1
	Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	Kapitola 4.25.1
	Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type	ANO	Kapitola 4.25.1

	Application Visibility – Schopnost detekce bezpečnostních hrozeb v šifrovaném provozu, např. v HTTPS, bez nutnosti dešifrování paketů	ANO	Kapitola 4.25.1
	Export NetFlow dat dle formátu NetFlow v9 nebo IPFIX	ANO	Kapitola 4.25.1
	Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní	ANO	Kapitola 4.25.1
	Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů	ANO	Kapitola 4.25.1
	Podpora Secure Unique Device Identity (IEEE 802.1AR) pro ověření autentičnosti HW prostředků zařízení	ANO	Kapitola 4.25.1
	SSHv2	ANO	Kapitola 4.25.1
	CLI rozhraní	ANO	Kapitola 4.25.1
	Programovatelnost prostřednictvím NETCONF/YANG	ANO	Kapitola 4.25.1
	Python scripting	ANO	Kapitola 4.25.1
	Software patching	ANO	Kapitola 4.25.1
	Model-driven telemetrie pro real-time streaming informací o stavu zařízení	ANO	Kapitola 4.25.1
	SNMPv2/v3	ANO	Kapitola 4.25.1
	TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	Kapitola 4.25.1
	NTPv3 server	ANO	Kapitola 4.25.1
	Protokol H.323v4	ANO	Kapitola 4.25.1
	Protokol SIPv2 (RFC3261 a návazné)	ANO	Kapitola 4.25.1
	Funkce T.38 Fax Gateway	ANO	Kapitola 4.25.1
	Podpora protokolů a služeb per VRF (VoIP gateway)	ANO	Kapitola 4.25.1
	Podpora hlasových rozhraní ISDN PRI	ANO	Kapitola 4.25.1
	Podpora G.711 kanálů realizovatelných instalovanými DSP procesory	ANO	Kapitola 4.25.1
	Signalizační protokol Q.SIG (BC a GF/SS) dle standardů ECMA pro spojení s pobočkovými ústřednami Alcatel	ANO	Kapitola 4.25.1
	Kodeky G.722 a G.711	ANO	Kapitola 4.25.1
	Počet souběžných SIP trunk hovorů k operátorovi min. 30	ANO	Kapitola 4.25.1

	Kodek iLBC	ANO	Kapitola 4.25.1
	Kodek G.729	ANO	Kapitola 4.25.1
	Podpora hlasových rozhraní ISDN BRI	ANO	Kapitola 4.25.1
	DTMF relay přes IP - in-band podle RFC2833	ANO	Kapitola 4.25.1
	Možnost modifikace algoritmu zpracování signalizace (například pomocí skriptů)	ANO	Kapitola 4.25.1
	Podpora protokolů SRTP a TLS pro šifrovaný přenos hlasu	ANO	Kapitola 4.25.1

4.26 K.11b - Centrální komunikační systém úřadu

4.26.1 Nabízené řešení

4.26.2 Způsob naplnění minimálních požadavků

Položka	Popis parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně uvedení výrobce, obchodního označení, konkrétní konfigurace, produktového čísla, případně uvede konkrétní parametry	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru

	Centralizovaný model hlasových služeb, včetně správy celého systému pomocí webového rozhraní.	ANO	Kapitola 4.26.1
	Maximální dostupnost řešení (redundance klíčových prvků infrastruktury).	ANO	Kapitola 4.26.1
	Geografické rozmístění virt. serverů, včetně neustálé synchronizace databáze.	ANO	Kapitola 4.26.1
	Signalizace SIP, H.323, MGCP.	ANO	Kapitola 4.26.1
	Podpora aplikací http, XML, SOAP, SIPT, TAPI, JTAPI.	ANO	Kapitola 4.26.1
	Podpora virtuální prostředí	ANO	Kapitola 4.26.1
	Podpora protokolů IPv4 a IPv6.	ANO	Kapitola 4.26.1
	Správa pomocí webového rozhraní.	ANO	Kapitola 4.26.1
	Podpora HTTPS od koncových zařízení přes hlasovou bránu až po samotnou ústřednu.	ANO	Kapitola 4.26.1
	Všechny konfigurační parametry IP telefonů budou uloženy na řídících serverech ústředny. Telefony si konfigurační soubory stahují z ústředny pomocí protokolu TFTP.	ANO	Kapitola 4.26.1
	Konfigurace a dohled IP telefonů je nedílnou součástí administrace.	ANO	Kapitola 4.26.1
Technické požadavky	Podpora SIP podle RFC 3261 a navazujících standardů	ANO	Kapitola 4.26.1
	Podpora základních VoIP kodeků - G.711 A-law, G.711 µ-law a G.729 a, b, a.	ANO	Kapitola 4.26.1
	Podpora rozšířených VoIP kodeků - G.722, iLBC.	ANO	Kapitola 4.26.1
	Podpora H.323v2 podle specifikace ITU-T.	ANO	Kapitola 4.26.1
	Podpora Q.sig	ANO	Kapitola 4.26.1
	Podpora šifrované signalizace mezi IP PBX a klienty (TLS mode).	ANO	Kapitola 4.26.1
	Podpora šifrované signalizace mezi IP PBX a externími systémy (jiná IP PBX, hlasová brána, apod.) (TLS).	ANO	Kapitola 4.26.1
	Podpora pro šifrovaný přenos hlasu protokolem SRTP (Secure RTP).	ANO	Kapitola 4.26.1
	CTI rozhraní JTAPI.	ANO	Kapitola 4.26.1
	Podpora zařízeních třetích stran (SIP).	ANO	Kapitola 4.26.1
	Podpora připojení min. 5 000 uživatelů a 5 000 koncových zařízení s možností dalšího rozšíření bez nutnosti investic do virtualizační platformy provozovaného DC	ANO	Kapitola 4.26.1
	Řešení musí umožnit nasazení videokonferenčních prostředků s možností více bodového spojení.	ANO	Kapitola 4.26.1

	Je požadováno licencování na uživatele systému, cílem je maximální transparentnost.	ANO	Kapitola 4.26.1
	Konfigurace/nastavení telefonů. Je vyžadováno využití funkcionalit na stávajících telefonech Zadavatele - Cisco 7821 a Cisco 7861.	ANO	Kapitola 4.26.1
	Sestavení a přijetí hovoru.	ANO	Kapitola 4.26.1
Minimální seznam služeb pro každého uživatele	Opakované vytáčení posledního čísla.	ANO	Kapitola 4.26.1
	Vytvoření zrychlené volby.	ANO	Kapitola 4.26.1
	Volání druhého účastníka (zpětný dotaz, střídání mezi hovory).	ANO	Kapitola 4.26.1
	Variabilní přesměrování volání – každé (off net a on-net), zaneprázdněn, bez odpovědi.	ANO	Kapitola 4.26.1
	Přidržení hovoru a pokračování.	ANO	Kapitola 4.26.1
	Připojení k hovoru.	ANO	Kapitola 4.26.1
	Parkování a vyzvednutí hovoru.	ANO	Kapitola 4.26.1
	Skupinové převzetí hovoru.	ANO	Kapitola 4.26.1
	Možnost vytváření přímých linek – volba bez vytáčení, pouze zvednutím sluchátka.	ANO	Kapitola 4.26.1
	Zpětné volání.	ANO	Kapitola 4.26.1
	Čekání a vyzvednutí hovoru (s konfigurovatelnou zvukovou výstrahou).	ANO	Kapitola 4.26.1
	Identifikace volajícího – CLIP (identifikace volajícího linky CLID – Calling Line Identification, identifikace jména volajícího CNID – Calling Party Name Identification).	ANO	Kapitola 4.26.1
	Možnost nastavování oprávnění pro externí hovory.	ANO	Kapitola 4.26.1
	Vytvoření konferenčního hovoru.	ANO	Kapitola 4.26.1
	Odmítnutí hovoru.	ANO	Kapitola 4.26.1
	Adresářové služby – resortní i osobní telefonní seznamy.	ANO	Kapitola 4.26.1
	Přidělení a přenositelnost uživatelského profilu v prostředí společnosti.	ANO	Kapitola 4.26.1
	Rozšíření hlasových služeb o službu o video složku přidáním USB kamery.	ANO	Kapitola 4.26.1
	Hudba při čekání – Music on Hold (MoH).	ANO	Kapitola 4.26.1
	Přiřazení práv volání jednotlivým účastníkům - nastavení pravidel pro odchozí volání.	ANO	Kapitola 4.26.1

4.27 Implementační služby

4.27.1 Obecné požadavky

V rámci dodávky provedeme implementační práce na dodaných komponentech a případně dalších výše uvedených zařízeních. V naší nabídce jsou zahrnuty veškeré další činnosti a prostředky, které jsou nezbytné pro provedení díla v rozsahu doporučeném výrobci a dle tzv. nejlepších praktik, i v případě, pokud nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné. Implementační služby budou zahrnovat:

- Zajištění projektového vedení realizace předmětu plnění.
- Zpracování prováděcí dokumentace, která představuje projektovou dokumentaci, podle které se projekt bude realizovat. Součástí zpracování prováděcí dokumentace je mj. provedení předimplementační analýzy a zpracování finálního návrhu cílového stavu. Prováděcí dokumentace musí respektovat a využívat osvědčené praktiky (tzv. Best Practice) a doporučení výrobců nabízených technologií.
- Dodávku nabízených prvků a kompletní implementaci řešení provedenou podle prováděcí dokumentace a splňující povinné parametry technického řešení,
- Provedení školení,
- Zajištění zkušebního provozu,
- Provedení akceptačních testů,
- Zpracování provozní dokumentace v rozsahu detailního popisu skutečného provedení a popisu činností běžné údržby a administrace systémů a činností pro spolehlivé zajištění provozu.
- Předání do ostrého provozu,

Součástí naší nabídky jsou dále veškeré služby, požadované v Příloze 3a ZD, kapitole č. 4.

4.28 Podpora provozu

Pro hlášení servisních požadavků zajistíme Zadavateli přístup ke svému helpdeskovému systému s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení. Detailní popis helpdeskového systému a jeho obsluhy je součástí nabídky č. 55.
Provozní doba helpdeskového systému je v době 8-17 hod. v pracovních dnech.
Běžná pracovní doba zadavatele je období mezi 8:00 a 17:00 v pracovní dny.

- Neplánované zásahy do systému, které mohou ovlivnit uživatelské prostředí, jsou uživatelům oznámeny minimálně 1 hodinu před zahájením poskytování služby nebo činnosti.
- Plánované zásahy do systému, které mohou ovlivnit uživatelské prostředí, jsou uživatelům oznámeny minimálně 24 hodin před zahájením poskytování služby nebo činnosti

V naší nabídce jsou zahrnuty veškeré služby podpory provozu tak, jak jsou specifikovány v příloze č. 3 ZD, kapitole č. 5.