SMLOUVA O DODÁVCE A IMPLEMENTACI SYSTÉMU OPATŘENÍ K POSÍLENÍ BEZPEČNOSTI A POSKYTOVÁNÍ SLUŽEB

Dnešního dne následující smluvní strany:

Objednatel:	**Vsetínská nemocnice a.s.**
zastoupen:	Ing. Martinem Pavlicou, MHA, předsedou představenstva
se sídlem:	Nemocniční 955, 755 01 Vsetín
IČO:	26871068
DIČ:	CZ26871068
bankovní spojení:	UniCredit Bank Czech Republic and Slovakia, a.s.
číslo účtu:	[redacted]
kontaktní osoba:	[redacted]
evidenční číslo smlouvy:	

(dále jen „***Objednatel***")

a

Poskytovatel:	**Aricoma Systems a.s.**
zastoupen:	[redacted], ředitel regionálního centra na základě plné moci
se sídlem:	Hornopolní 3322/34, 702 00 Ostrava
IČO:	04308697
DIČ:	CZ04308697
bankovní spojení:	Česká spořitelna a.s.
číslo účtu:	[redacted]

zapsaná v obchodním rejstříku vedeném u Krajského soudu v Ostravě, sp. zn. B 11012

kontaktní osoba:	[redacted] ředitel regionálního centra
evidenční číslo smlouvy:	RCS-240078

(dále jen „***Poskytovatel***")

(Objednatel a Poskytovatel dále jednotlivě též jen „***Smluvní strana***" nebo společně „***Smluvní strany***")

uzavírají v souladu s § 1746 odst. 2 zák. č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „***OZ***") s přihlédnutím k § 2586 a násl. OZ tuto

Smlouvu o dodávce a implementaci systému managementu bezpečnosti informací a poskytování služeb (dále jen „*Smlouva*“)

I. ÚVODNÍ USTANOVENÍ

1.1 Smlouva se mezi výše uvedenými Smluvními stranami uzavírá na základě výsledku otevřeného zadávacího řízení na veřejnou zakázku s názvem „*Kybernetická bezpečnost ve Vsetínské nemocnici a.s.*“, (dále jen „***Veřejná zakázka***“), zadávanou dle zákona č. 134/2016 Sb., o zadávání veřejných zakázkách, ve znění pozdějších předpisů (dále jen „***ZZVZ***“). Jednotlivá ujednání Smlouvy tak budou vykládána v souladu se zadávacími podmínkami Veřejné zakázky uvedenými v zadávací dokumentaci včetně jejich příloh a v souladu s nabídkou Poskytovatele podanou na Veřejnou zakázku.

1.2 Smluvní strany prohlašují, že osoby podepisující Smlouvu jsou k tomuto jednání oprávněny.

1.3 Poskytovatel prohlašuje, že se seznámil se zadávací dokumentací Veřejné zakázky, včetně všech jejích příloh (dále jen „***Zadávací dokumentace***“), že ji považuje za dostatečný podklad pro plnění Veřejné zakázky, a to zejména v rozsahu nezbytném pro plnění předmětu Smlouvy, přičemž mu nejsou známy žádné nejasnosti či pochybnosti, které by znemožňovaly řádné plnění jeho závazku dle Smlouvy.

1.4 Poskytovatel dále prohlašuje, že se detailně seznámil s rozsahem a povahou předmětu plnění Smlouvy, že jsou mu známy veškeré relevantní technické, kvalitativní a jiné podmínky nezbytné pro realizaci předmětu plnění Smlouvy, a že disponuje takovými kapacitami a odbornými znalostmi, které jsou nezbytné pro realizaci předmětu plnění Smlouvy za dohodnuté maximální smluvní ceny uvedené ve Smlouvě, a to rovněž ve vazbě na jím prokázanou kvalifikaci pro plnění Veřejné zakázky a informace doložené za účelem hodnocení nabídky dle kritéria hodnocení „Zkušenosti vybraných členů realizačního týmu“.

1.5 Poskytovatel dále prohlašuje, že jím poskytované plnění odpovídá všem požadavkům vyplývajícím z platných právních předpisů, které se na plnění vztahují.

1.6 Poskytovatel bere na vědomí, že se předpokládá, že Objednatel bude v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících předpisů, ve znění pozdějších předpisů (dále jen „***ZKB***“), resp. právní úpravou, která ZKB nahradí, určen jako provozovatel informačního systému základní služby, proto se Poskytovatel v průběhu plnění Smlouvy může stát významným dodavatelem dle § 2 písm. n) vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „***VKB***“), resp. právní úpravy, která VKB nahradí. Plnění předmětu Smlouvy, a to ve všech jeho fázích a ve všech jeho částech bude muset splňovat veškeré

podmínky dle ZKB a VKB, resp. právní úpravy, která ZKB a VKB nahradí. Poskytovatel se zavazuje informovat o těchto skutečnostech všechny své poddodavatele a další osoby, s jejichž pomocí či jejichž prostřednictvím bude Poskytovatel plnit předmět Smlouvy.

1.7 Objednatel předpokládá možnost kofinancování implementace předmětu plnění Veřejné zakázky z Integrovaného operačního programu (dále jen „***IROP***"), přičemž Poskytovatel je povinen postupovat tak, aby kofinancování z IROP nebylo ohroženo.

1.8 Pojmy s velkými počátečními písmeny definované ve Smlouvě budou mít význam, jenž je jim ve Smlouvě, včetně jejích příloh a dodatků, připisován. Pro vyloučení jakýchkoliv pochybností se Smluvní strany dále dohodly, že:

- v případě jakékoliv nejistoty ohledně výkladu ustanovení Smlouvy budou tato ustanovení vykládána tak, aby v co nejširší míře zohledňovala účel Veřejné zakázky vyjádřený Zadávací dokumentací;
- Poskytovatel je vázán svou nabídkou předloženou Objednateli v rámci zadávacího řízení Veřejné zakázky, která se pro úpravu vzájemných vztahů vyplývajících ze Smlouvy použije subsidiárně.

1.9 Není-li výslovně ve Smlouvě u lhůt či dob uvedeno, že příslušné dny jsou pracovní, jedná se o dny kalendářní.

II. ÚČEL SMLOUVY

2.1 Základním účelem, k jehož dosažení se Smlouva uzavírá, je zvýšení kybernetické bezpečnosti a celkové úrovně zabezpečení Objednatele a jeho systémů.

2.2 Konkrétně je účelem Smlouvy zásadní posílení ochrany informačních a komunikačních systémů Objednatele před kybernetickými útoky a únikem potencionálně vysoce citlivých dat, a to pomocí realizace vybraných technických bezpečnostních opatření.

III. PŘEDMĚT SMLOUVY

3.1 Předmětem Smlouvy je závazek Poskytovatele za podmínek Smlouvou dále stanovených poskytnout Objednateli plnění spočívající v zajištění komplexní dodávky a implementace systému managementu bezpečnosti informací, tedy řešení spočívající v posílení Systému kybernetické bezpečnosti (dále také jako „***SKB***") odpovídajícího požadavkům na funkcionality, výkonnost a dostupnost definovaných zejm. v příloze č. 1 a 6 Smlouvy, a dále zajištění veškerých dalších služeb a činností pro Objednatele specifikovaných ve Smlouvě (dále jen „***Plnění***").

3.2 Plnění předmětu Smlouvy je rozděleno do těchto základních fází:

- Fáze 1 (analytická fáze);

- Fáze 2 (implementační fáze);
- Fáze 3 (provozní fáze a služby rozvoje).

3.3 Fáze 1 – (analytická fáze) zahrnuje následující činnosti Poskytovatele:

- provedení detailní analýzy požadavků Objednatele, jejich detailní rozpracování a verifikace s Objednatelem určenými pracovníky za účelem standardizace a optimalizace implementace v prostředí Objednatele (implementační projekt jednotlivých opatření – může být zpracován jeden implementační projekt, ve kterém bude samostatná kapitola pro každé opatření); součástí implementačního projektu bude návrh akceptačních kritérií Fáze 2, tj. popis testování a ověřování pro účely akceptace a popis nezbytné součinnosti požadované po Objednateli; a
- zpracování harmonogramu realizace jednotlivých opatření (harmonogram projektu), který bude obsahovat časový plán prací a činností, které je nutné provést k úspěšné realizaci Plnění, a věcný popis všech fází realizace a vzájemných závislostí a vazeb jednotlivých opatření.

Výstupy: Implementační projekt a harmonogram projektu.
(dále jen „***Fáze 1***“)

3.4 Fáze 2 (implementační fáze) zahrnuje zejm. následující činnosti Poskytovatele:

- Dodávka, implementace a integrace SKB do prostředí Objednatele, přičemž SKB tvoří následující opatření (aktivity):
  - antivirová ochrana a EDR,
  - web aplikační firewall (AWAF),
  - Wi-fi AP,
  - dodávka a implementace systému PIM/PAM,
  - interní Firewall,
  - MFA / ochrana přístupu uživatelů,
  - Single Sign-On (SSO),
  - systém řízení přístupu do sítě 802.1x,
  - systém pro analýzu síťového provozu a bezpečnostní monitoring,
  - hardening,
  - Back Up Trezor - diskový úložný systém - dodávka a implementace,
  - servery a switche a záložní zdroje,
  - Backup server,

- Zálohovací SW,

- školení,
- testování,
- zajištění přípravy nasazení a vlastní nasazení SKB do produkčního provozu,

a to vše v rozsahu specifikace uvedené v příloze č. 1 Smlouvy a implementačním projektu. Dodané a naimplementované řešení SKB musí být kompatibilní a integrované se stávajícím prostředím Objednatele - zejména musí umožnovat zapojení do aktuální clusteru.

Výstupy: Funkční SKB odpovídající specifikaci řešení a veškerým požadavkům Objednatele, zejména detailní specifikaci uvedené ve výstupech Fáze 1, veškerá související uživatelská a technická dokumentace k SKB, včetně požadovaných licencí k SKB a protokoly o Poskytovatelem provedených, úspěšně zakončených testech SKB a o proškolení určených pracovníků Objednatele v rozsahu dle přílohy č. 1 Smlouvy a implementačního projektu.
(dále jen „***Fáze 2***")

3.5 Fáze 3 (provozní fáze a služby rozvoje) zahrnuje následující činnosti Poskytovatele:

- poskytování technické podpory, zahrnující služby maintenance licencí a podpory (full maintenance, SLA) SKB (společně dále jen „***Služby* podpory**"); Služby podpory musí být poskytovány v souladu s přílohou č. 6 Smlouvy tak, že bude zajištěna kvalitní údržba SKB po dobu trvání Smlouvy s aktualizací veškeré uživatelské a technické dokumentace k SKB minimálně jedenkrát ročně a ke dni ukončení Smlouvy; Poskytovatel je povinen aplikovat průběžné legislativní změny, a
- poskytování služeb rozvoje SKB dle požadavků Objednatele (dále jen „***Služby rozvoje***"); Služby rozvoje budou objednávány dle potřeb Objednatele v souladu s přílohou č. 6 Smlouvy, přičemž Objednatel není povinen odebrat jakýkoliv objem Služeb rozvoje. Maximální objem Služeb rozvoje činí 96 hodin za každé 4 roky poskytování Služeb rozvoje,

a to vše v rozsahu dle přílohy č. 1 a přílohy č. 6 Smlouvy.
(dále jen „***Fáze 3***").

3.6 Poskytovatel se zavazuje poskytovat Plnění v souladu s platnými právními předpisy, jakož i v souladu se všemi relevantními normami obsahujícími technické specifikace a technická řešení, technické a technologické postupy nebo jiná určující kritéria k zajištění, že materiály, výrobky, postupy a služby vyhovují předmětu Smlouvy a veškerým podmínkám uvedeným v Zadávací dokumentaci.

3.7 Poskytovatel prohlašuje, že předmět plnění dle Smlouvy není plněním nemožným, a že Smlouvu uzavírá po pečlivém zvážení všech možných důsledků. Poskytovatel dále

prohlašuje, že se seznámil s předmětem plnění dle Smlouvy, a že Plnění může být poskytnuto způsobem a v termínech stanovených ve Smlouvě.

3.8 Objednatel se zavazuje zaplatit Poskytovateli za řádně poskytnuté Plnění v souladu se všemi podmínkami Smlouvy sjednanou cenu dle Smlouvy.

IV. LHŮTA A MÍSTO PLNĚNÍ

4.1 Poskytovatel se zavazuje poskytovat Plnění v souladu s harmonogramem v následujících krocích (fázích):

Fáze	Zahájení Fáze	Ukončení (splnění) Fáze
Fáze 1	dnem nabytí účinnosti Smlouvy	do **3 měsíců** od účinnosti Smlouvy
Fáze 2	dnem nabytí účinnosti Smlouvy	do **6 měsíců** od účinnosti Smlouvy
Fáze 3	po dokončení (akceptaci) Fáze 2	po **dobu neurčitou** od zahájení Fáze 3

4.2 Místem plnění je sídlo Objednatele, není-li mezi Smluvními stranami výslovně dohodnuto jinak. Přípravné a programovací práce je Poskytovatel oprávněn realizovat na svém vlastním technickém vybavení, což však nezakládá jakýkoliv nárok Poskytovatele na navýšení ceny Plnění v souvislosti s převodem na cílovou infrastrukturu Objednatele.

4.3 Pokud to povaha plnění dle Smlouvy umožňuje, je Poskytovatel oprávněn poskytovat plnění dle Smlouvy také vzdáleným přístupem. Vzdálené připojení musí být vždy realizováno přes VPN a přístup musí být vždy na konkrétní osobu.

4.4 Veškeré písemné výstupy, které je podle Smlouvy Poskytovatel povinen vytvořit a/nebo které při plnění Smlouvy vzniknou, budou Poskytovatelem Objednateli předány v sídle Objednatele, nebude-li mezi Smluvními stranami v konkrétním případě dohodnuto jinak.

V. CENA PLNĚNÍ A PLATEBNÍ PODMÍNKY

5.1 Cena za poskytování Plnění je sjednána dohodou Smluvních stran následovně:

5.1.1 Cena za poskytnutí části Plnění odpovídající Fázi 1 a Fázi 2 dle Smlouvy činí [redacted] ve výši 21 %;

5.1.2 Cena za poskytování části Fáze 3 odpovídající Službám podpory bez full maintenance činí [redacted] **Kč bez DPH** za každé 3 po sobě následující kalendářní měsíce poskytovaného plnění dle Smlouvy, tj. [redacted] **Kč včetně DPH** ve výši 21 %.

5.1.3 Cena za poskytování části Fáze 3 odpovídající Službám podpory, konkrétně full maintenance včetně maintenance licencí, činí [redacted] **Kč bez DPH** za každých 12 po sobě následujících kalendářních měsíců poskytovaného plnění full maintenance dle Smlouvy, tj. [redacted] **Kč včetně DPH** ve výši 21 %.

5.1.4 Cena za poskytování části Fáze 3 odpovídající Službám rozvoje činí [redacted] **Kč bez DPH** za 1 hodinu poskytovaného plnění dle Smlouvy, tj. [redacted] **Kč včetně DPH** ve výši 21 %.

Podrobný rozpad ceny za jednotlivé části Plnění je uveden v příloze č. 5 Smlouvy – Ceník.

5.2 Součástí cen uvedených v tomto článku Smlouvy jsou i služby a dodávky nezbytné pro řádné a úplné poskytování předmětu Plnění. Poskytovatel nese veškeré náklady nutně nebo účelně vynaložené při plnění závazků ze Smlouvy včetně správních poplatků a nákladů souvisejících (zejména daně, pojištění, veškeré dopravní náklady, včetně nákladů souvisejících s provedením všech zkoušek a testů prokazujících dodržení předepsané kvality a parametrů předmětu Plnění dle Smlouvy, jakož nákladů souvisejících se zajištěním dalších podkladů, předpisů apod.).

5.3 Veškeré ceny uvedené v tomto článku Smlouvy jsou ceny v korunách českých (CZK). Stane-li se v průběhu trvání Smlouvy Česká republika členem Evropské měnové unie a bude-li v závazně stanoven koeficient pro přepočet CZK na EUR, budou ceny sjednané v CZK přepočteny do EUR na základě odpovídajícího koeficientu sjednaného v mezinárodních úmluvách, kterými bude Česká republika vázána, jakož i v souladu s případnou tomu odpovídající vnitrostátní právní úpravou České republiky.

5.4 Veškeré ceny uvedené v tomto článku Smlouvy jsou cenami maximálními, nejvýše přípustnými, nepřekročitelnými a jsou platné a konstantní po celou dobu platnosti Smlouvy, není-li uvedeno jinak. Cenu Plnění je možné změnit v případě změny výše sazby DPH v důsledku změny právních předpisů. V případě změny sazby DPH je Poskytovatel povinen k ceně bez DPH účtovat DPH v platné výši. Smluvní strany se dohodly, že v případě změny ceny v důsledku změny sazby DPH není nutno ke Smlouvě uzavírat dodatek. Poskytovatel odpovídá za to, že sazba daně z přidané hodnoty je stanovena v souladu s platnými právními předpisy.

5.5 Cenu Služeb podpory a Služeb rozvoje dle odst. 5.1.2, 5.1.3 a 5.1.4 Smlouvy lze v souvislosti s uplynutím čtvrtého výročí poskytování Služeb podpory ve Fázi 3 upravit z důvodu inflace za podmínek dále uvedených:

- Inflací se rozumí Průměrná roční míra inflace, kterou udává každým kalendářním rokem Český statistický úřad za rok předcházející vyjádřená v procentech.

- Počínaje pátým rokem zahájení poskytování Služeb podpory a dále do budoucna je Poskytovatel oprávněn zvýšit cenu Služeb podpory nebo Služeb rozvoje jednou ročně z důvodů inflace, a to o tolik procent, kolik procent činila Průměrná roční míra inflace za rok bezprostředně předcházející ; součástí (např. přílohou) daňového dokladu dle odst. 5.6 Smlouvy bude vymezení údajů o inflaci dle Smlouvy, přičemž Objednatel je oprávněn tuto fakturu před uplynutím lhůty splatnosti vrátit, pokud inflace nebude vyjádřena správně (vrácením vadné faktury Poskytovateli přestává běžet původní lhůta splatnosti, nová lhůta splatnosti běží ode dne vystavení nové faktury).
- Cena Služeb podpory nebo Služeb rozvoje upravená z důvodu inflace se považuje za sjednanou cenu, která nevyžaduje uzavření dodatku ke Smlouvě.

5.6 Ceny dle Smlouvy budou hrazeny na základě daňových dokladů vystavených Poskytovatelem (dále jen „***Faktura***" či „***Faktury***") následovně:

- právo fakturovat cenu za poskytnutí části Plnění odpovídající Fázi 1 a Fázi 2 dle odst. 5.1.1 Smlouvy vzniká Poskytovateli pouze po akceptaci odpovídajícího plnění (Fáze 1 a Fáze 2) dle Smlouvy Objednatelem na základě příslušného akceptačního protokolu ve smyslu čl. VI Smlouvy.
- cena za poskytování části Fáze 3 dle odst. 5.1.2 Smlouvy odpovídající Službám podpory bez full maintenance bude Objednatelem uhrazena čtvrtletně vždy po ukončení posledního měsíce příslušného kalendářního čtvrtletí (leden až březen, duben až červen, červenec až září, říjen až prosinec), v němž budou tyto Služby podpory poskytovány, přičemž Poskytovatel je oprávněn příslušnou Fakturu vystavit nejdříve 2 pracovní dny po ukončení příslušného období, v němž budou tyto Služby podpory poskytovány; s ohledem na nemožnost přesného určení počátku zahájení poskytování Služeb podpory Smluvní strany uvádí, že nezapočne-li poskytování Služeb podpory prvního dne kalendářního čtvrtletí, pak první Faktura za poskytování Služeb podpory bude vystavena na období od zahájení Služeb podpory do konce příslušného čtvrtletí, v němž poskytování Služeb podpory započalo, a to ve výši poměrné části ceny odpovídající tomuto období poskytování Služeb podpory;
- cena za poskytování části Fáze 3 dle odst. 5.1.3 Smlouvy odpovídající Službám podpory, konkrétně full maintenance (včetně licencí), bude Objednatelem uhrazena ročně vždy před zahájením prvního měsíce příslušného období (12 po sobě jdoucích kalendářních měsíců), v němž budou tyto Služby podpory, konkrétně full maintenance (včetně licencí), poskytovány, přičemž Poskytovatel je oprávněn příslušnou Fakturu vystavit nejdříve 2 pracovní dny před zahájením příslušného období (roku), v němž budou tyto Služby podpory poskytovány;
- cena za poskytování části Fáze 3 dle odst. 5.1.4 Smlouvy odpovídající Službám

rozvoje bude Objednatelem hrazena za skutečně poskytnuté Služby rozvoje na základě hodinové sazby podle počtu řádně poskytnutých hodin plnění Služeb rozvoje v souladu se Smlouvu a přílohou č. 6 Smlouvy čtvrtletně vždy po ukončení posledního měsíce příslušného kalendářního čtvrtletí (leden až březen, duben až červen, červenec až září, říjen až prosinec), v němž budou Služby rozvoje poskytovány, přičemž Poskytovatel je oprávněn příslušnou Fakturu vystavit nejdříve 2 pracovní dny po ukončení příslušného čtvrtletí, v němž budou Služby podpory poskytovány.

5.7 Kopie příslušných akceptačních protokolů podepsaných pověřenými zástupci obou Smluvních stran jsou povinnou náležitostí každé Faktury vystavené Poskytovatelem za poskytnutí Plnění (či jeho části) dle Smlouvy. V případě, že Plnění není akceptováno některým z uvedených způsobů, Poskytovatel není oprávněn vystavit příslušnou Fakturu, není-li výslovně uvedeno jinak.

5.8 Faktury musí obsahovat evidenční číslo Smlouvy a veškeré údaje vyžadované právními předpisy, zejména zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a § 435 OZ, obecné náležitosti účetních dokladů a současně požadavky poskytovatele dotace alespoň v rozsahu čísla projektu a rozlišení uznatelných a neuznatelných nákladů (dle pokynu Objednatele).

5.9 Splatnost Faktur je stanovena do 30 (třiceti) dnů ode dne doručení Faktury Objednateli. Cena za poskytnutí Plnění či jeho části se považuje za uhrazenou okamžikem odepsání fakturované ceny z bankovního účtu Objednatele ve prospěch účtu Poskytovatele. Uvedený bankovní účet musí být zveřejněn správcem daně způsobem umožňujícím dálkový přístup. V případě, že účet tímto způsobem zveřejněn nebude, je Objednatel oprávněn uhradit Poskytovateli cenu na úrovni bez DPH, DPH Objednatel poukáže správci daně. Stane-li se Poskytovatel nespolehlivým plátcem ve smyslu § 106a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, je povinen neprodleně o tomto písemně informovat Objednatele.

5.10 Nebude-li jakákoliv Faktura obsahovat některou povinnou nebo dohodnutou náležitost nebo bude-li chybně vyúčtována cena nebo DPH, je Objednatel oprávněn tuto fakturu před uplynutím lhůty splatnosti bez zaplacení vrátit Poskytovateli k provedení opravy s vyznačením důvodu vrácení. Poskytovatel provede opravu vystavením nové faktury. Vrácením vadné faktury Poskytovateli přestává běžet původní lhůta splatnosti. Nová lhůta splatnosti běží ode dne vystavení nové faktury.

5.11 Objednatel neposkytuje Poskytovateli na cenu předmětu Plnění jakékoliv zálohy.

5.12 Poskytovatel není oprávněn započíst jakékoliv pohledávky proti nárokům Objednatele. Pohledávky a nároky Poskytovatele vzniklé v souvislosti se Smlouvou nesmějí být postoupeny třetím osobám, zastaveny, nebo s nimi jinak disponováno. Jakýkoliv právní

úkon učiněný Poskytovatelem v rozporu s tímto ustanovením Smlouvy bude považován za příčící se dobrým mravům.

VI. PŘEDÁVÁNÍ A PŘEVZETÍ PLNĚNÍ

6.1 Fáze 1 bude Poskytovatelem předána a Objednatelem převzata na základě akceptace v rámci akceptační schůzky, která se bude konat na základě výzvy Poskytovatele, a to následovně:

6.1.1 Objednatel musí být Poskytovatelem ke schůzce písemně pozván nejpozději 7 dnů před termínem akceptační schůzky s tím, že nejpozději v této lhůtě je Poskytovatel rovněž povinen předat Objednateli výstup z Fáze 1 ve formě návrhu implementačního projektu a harmonogramu. Proces připomínkování a akceptace výstupů Fáze 1 proběhne v době plnění Fáze 1 dle odst. 4.1 Smlouvy, tj. nejpozději do 3 měsíců od účinnosti Smlouvy.

6.1.2 Objednatel je oprávněn ve lhůtě 3 dnů od doručení příslušného návrhu výstupu Fáze 1 písemně předložit Poskytovateli své připomínky. V takovém případě je Poskytovatel povinen upravit příslušný návrh v souladu s připomínkami Objednatele (zejména pokud nesplňuje požadavky na něj stanovené Objednatelem ve Smlouvě) a předá Objednateli konečnou verzi návrhu výstupu nejpozději 3 dny od doručení připomínek Objednatele, a to společně s protokolem o zapracování připomínek Objednatele. V případě, že Objednatel své připomínky k návrhu dle tohoto odst. Smlouvy nesdělí Poskytovateli ve lhůtě zde uvedené, má se za to, že s obsahem předloženého dokumentu souhlasí. Pro odstranění jakýchkoli pochybností Smluvní strany uvádějí, že Objednatel je oprávněn požadovat doplnění, aktualizaci či zpřesnění požadavků oproti požadavkům uvedeným ve Smlouvě a v příloze č. 1 Smlouvy v rámci zpracování implementačního projektu a harmonogramu (zejm. se zohledněním specifik postupu a procesního modelu Objednatele) a Poskytovatel je povinen takovým požadavkům vyhovět. Požadavky je Poskytovatel oprávněn uplatňovat průběžně v rámci plnění Fáze 1.

6.1.3 V rámci akceptační schůzky bude Objednatelem ověřeno, zda Fáze 1 byla dodána řádně dle příslušných ustanovení Smlouvy a pokud ano, je Objednatel povinen podepsat příslušný akceptační protokol. Podpis příslušného Akceptačního protokolu se závěrem „Akceptováno" je jednou z podmínek pro vznik oprávnění Poskytovatele vystavit Fakturu za poskytnutí příslušného plnění podle Smlouvy; Faktura za Plnění dle Fáze 1 a 2 bude vystavena najednou až po akceptaci Plnění dle obou Fází.

6.1.4 Výsledkem akceptačního řízení Fáze 1 mohou být stavy:

- **Akceptováno**, pokud Poskytovatel zpracuje implementační projekt a harmonogram v souladu se všemi podmínkami Smlouvy, zejm. v souladu s odst. 6.1.2 a 6.1.3 Smlouvy,
- **Neakceptováno**, pokud Poskytovatel řádně a včas nezpracuje implementační projekt a harmonogram v souladu se všemi podmínkami Smlouvy; v tomto případě Poskytovateli nevzniká nárok na zaplacení smluvní ceny.

6.2 Fáze 2 nebo její dílčí části (aktivity) budou Poskytovatelem předány a Objednatelem převzaty na základě dále popsaného akceptačního řízení:

6.2.1 Účelem akceptačního řízení je ověřit, zda SKB či jeho dílčí část odpovídá schváleným funkčním a technickým specifikacím a všem Objednatelem požadovaným parametrům (výkonnostním, provozním, bezpečnostní apod.), zejména technické specifikaci dle přílohy č. 1 Smlouvy a specifikaci uvedené ve výstupech Fáze 1. V rámci akceptačního řízení se bude předaný SKB či jeho dílčí část ověřovat a testovat podle vzájemně odsouhlasených akceptačních kritérií, které navrhne Poskytovatel ve Fázi 1 jakožto součást výstupů Fáze 1.

6.2.2 Poskytovatel vyzve Objednatele k zahájení akceptačního řízení pro příslušné plnění dle Smlouvy (Fáze 2 či její dílčí část) a předá takové plnění Objednateli na základě předávacího protokolu nejpozději 10 dní před termínem ukončení této fáze Smlouvy. Poskytovatel je oprávněn předávat průběžně jednotlivé dílčí části (aktivity) Fáze 2, avšak nárok na vystavení faktury za Fázi 1 a 2 vzniká až po dokončení a akceptaci kompletní Fáze 2.

6.2.3 Řízení o akceptaci Fáze 2 či její dílčí části je zahájeno dnem skutečného předání takového plnění a je ukončeno podpisem příslušného akceptačního protokolu Objednatelem (dále jen „***Akceptační protokol***"), který bude obsahovat minimálně:

- popis Plnění nebo jeho části, které byly předmětem akceptace;
- záznam průběhu akceptačního řízení;
- seznam akceptačních testů se záznamem jejich výsledků;
- seznam zjištěných vad s jejich klasifikací dle kategorií;
- výsledek akceptačního řízení.

6.2.4 Není-li výslovně ujednáno jinak, akceptační řízení za každou aktivitu Fáze 2 dle Smlouvy lze zahájit pouze na základě předání všech požadovaných plnění pro příslušnou aktivitu Fáze 2 dle Smlouvy. Objednatel provede oponentní řízení převzatého plnění a nejméně 3 dny před ukončením akceptačního řízení, které se koná v dohodnutém termínu, sdělí Poskytovateli výhrady k předanému plnění s

vyznačením jejich závažností. V akceptačním řízení budou projednány výhrady Objednatele a stanovena výsledná závažnost připomínek vad a nedodělků, včetně termínů jejich odstranění, přičemž Objednatel vezme do úvahy stanovisko Poskytovatele. Výsledky tohoto řízení budou uvedeny do Akceptačního protokolu.

6.2.5 Kategorizace vad předávaného plnění dle Smlouvy při akceptačním řízení, není-li ve výstupech Fáze 1 stanoveno jinak:

- Vada kategorie A

Popis vady: Vážné vady s nejvyšší prioritou, které mají kritický dopad do funkčnosti SKB nebo jeho části a dále vady, které znemožňují užívání SKB nebo jeho části Objednatelem nebo způsobují vážné provozní problémy.

- Vada kategorie B

Popis vady: Vada, která svým charakterem nespadá do kategorie A. Znamená vážné vady způsobující zhoršení výkonnosti a funkčnosti SKB nebo jeho části. SKB nebo jeho část má omezení nebo je částečně nefunkční. Jedná se o odstranitelné vady, které způsobují problémy při užívání a provozování SKB nebo jeho části Objednatelem, ale umožňují provoz.

- Vada kategorie C

Popis vady: Vada, která svým charakterem nespadá do kategorie A nebo kategorie B. Znamená snadno odstranitelné vady s minimálním dopadem na funkcionality či funkčnost SKB nebo jeho části.

6.2.6 Výsledkem akceptačních řízení Fáze 2 či její dílčí části mohou být dva stavy:

6.2.6.1 **Akceptováno.** V případě, že Objednatel v průběhu akceptačního řízení Fáze 2 nenalezne v předaném plnění dle Smlouvy žádné vady ani nedodělky (dle kategorizace vad stanovené Smlouvou, resp. výstupy Fáze 1), nebo budou v průběhu akceptačního řízení shledány v předaném plnění Objednatelem akceptovatelné vady nebo nedodělky kategorie C, avšak přes uvedené bude předvedena způsobilost Plnění sloužit svému účelu, uvede Objednatel do Akceptačního protokolu, že předané plnění bylo akceptováno a akceptační protokol potvrdí svým podpisem. V případě vad nebo nedodělků kategorie A nebo B nebude Objednatel plnění ve Fázi 2 akceptovat. Podpis Akceptačního protokolu Objednatelem s výsledkem „Akceptováno" nezbavuje Poskytovatele povinnosti odstranit případné vady a nedodělky (tj. výhrady Objednatele) uvedené v příslušném Akceptačním protokolu, a to ve lhůtách v akceptačním protokolu uvedených (nedohodnou-li se Smluvní strany jinak, resp. nebude-li ve výstupech Fáze 1 stanoveno jinak,

maximální lhůta na odstranění jakékoliv vady/nedodělku kategorie C nepřesáhne 15 dnů; vše od doručení Akceptačního protokolu se stavem „Akceptováno" v listinné či elektronické podobě Poskytovateli). Po odstranění všech případných vad a nedodělků podepíší Smluvní strany doklad prokazující odstranění všech případných vad a nedodělků. Vady kategorie C mohou být na základě dohody Smluvních stran převedeny do fáze poskytování Služeb podpory.

6.2.6.2 **Neakceptováno**. V případě, že budou v průběhu akceptačního řízení v předaném plnění dle Smlouvy Objednatelem shledány zásadní vady a nedodělky a nebude předvedena způsobilost Plnění sloužit svému účelu, není předané plnění akceptováno a není rovněž považováno za poskytnuté v souladu se Smlouvou. V Akceptačním protokolu bude Objednatelem uvedeno, že předané plnění nebylo akceptováno, včetně popisu zjištěných vad/nedostatků a Objednatel doručí Akceptační protokol Poskytovateli, který napraví tyto vady/nedostatky a předloží plnění k nové akceptaci. Tento proces se bude opakovat, dokud nebude možné ze strany Objednatele v Akceptačním protokolu zaznamenat výsledek „***Akceptováno***", a to v lhůtě dle čl. IV odst. 4.1. Smlouvy.

6.2.7 Kategorizaci vad předávaného plnění ve smyslu odst. 6.2.5 Smlouvy stanovuje při akceptačním řízení výhradně Objednatel. V případě změny, částečného řešení nebo vyřešení vady Objednatel může kategorii vady změnit dle závažnosti jejích dopadů.

6.2.8 Předání/převzetí Fáze 2 (implementační fáze) či její dílčí části je možné pouze na základě akceptačního řízení s výsledkem „Akceptováno", přičemž podpis příslušného Akceptačního protokolu Objednatelem pro všechna dokončená plnění Fáze 2 je podmínkou pro vznik oprávnění Poskytovatele vystavit Fakturu za poskytnutí části Plnění odpovídající Fázi 1 a 2. Tato skutečnost nezbavuje Poskytovatele jeho povinnosti odstranit případné vady zjištěné v rámci akceptačního řízení způsobem uvedeným v odst. 6.2.6.1 Smlouvy.

6.3 Nebude-li stanoveno jinak, Služby podpory a Služby rozvoje v rámci Fáze 3 budou Objednatelem přebírány na základě akceptace v rámci akceptačních schůzek, které se budou konat na základě výzvy Poskytovatele. Poskytovatel je povinen předat Objednateli doklady prokazující skutečný rozsah a kvalitu poskytovaného plnění. Před akceptací bude Objednatelem ověřeno, zda plnění bylo dodáno řádně dle příslušných ustanovení Smlouvy a pokud ano, je Objednatel povinen podepsat příslušný Akceptační protokol, jehož přílohou budou příslušné doklady o poskytovaném plnění.

6.4 Bližší podmínky poskytování Služeb podpory a Služeb rozvoje včetně procesu objednávání Služeb rozvoje jsou upraveny v příloze č. 6 Smlouvy.

VII. DALŠÍ PRÁVA A POVINNOSTI SMLUVNÍCH STRAN

7.1 Poskytovatel je povinen:

7.1.1 poskytovat řádně a včas Plnění podle Smlouvy bez faktických a právních vad;

7.1.2 postupovat při Plnění předmětu Smlouvy s odbornou péčí, podle nejlepších znalostí a schopností, sledovat a chránit oprávněné zájmy Objednatele a postupovat v souladu s jeho pokyny a interními předpisy souvisejícími s předmětem plnění Smlouvy (či jeho dílčí části), které Objednatel Poskytovateli poskytne, nebo s pokyny jím pověřených osob;

7.1.3 bez zbytečného odkladu oznámit Objednateli veškeré skutečnosti, které mohou mít vliv na povahu nebo na podmínky poskytování plnění dle Smlouvy. Zejména je povinen neprodleně písemně oznámit Objednateli změny svého majetkoprávního postavení, jako je např. přeměna společnosti, vstup do likvidace, úpadek či prohlášení konkurzu;

7.1.4 informovat bezodkladně Objednatele o jakýchkoliv zjištěných překážkách plnění, byť by za ně Poskytovatel neodpovídal, o vznesených požadavcích orgánů státního dozoru a o uplatněných nárocích třetích osob, které by mohly plnění dle Smlouvy ovlivnit;

7.1.5 poskytnout Objednateli veškerou nezbytnou součinnost k naplnění účelu Smlouvy;

7.1.6 na žádost Objednatele spolupracovat či poskytnout součinnost dalším dodavatelům Objednatele;

7.1.7 provádět svoje činnosti tak, aby nebyl v nadbytečném rozsahu omezen provoz dotčených pracovišť Objednatele;

7.1.8 dodržovat provozní řád v místě plnění a provádět svoje činnosti tak, aby nebyl v nadbytečném rozsahu omezen provoz na pracovištích Objednatele. Poskytovatel zajistí, aby všechny osoby, které se na jeho straně podílí na plnění předmětu Smlouvy, a které budou přítomny v prostorách Objednatele, dodržovaly všechny bezpečnostní a provozní předpisy tak, jak s nimi byly seznámeny Objednatelem;

7.1.9 informovat Objednatele na jeho žádost o průběhu plnění předmětu Smlouvy a akceptovat jeho pokyny a připomínky k plnění předmětu Smlouvy;

7.1.10 použít veškeré podklady předané mu Objednatelem pouze pro účely Smlouvy a zabezpečit jejich řádné vrácení Objednateli, bude-li to objektivně možné vzhledem k jejich povaze a způsobu použití;

7.1.11 Poskytovatel je povinen uchovávat veškerou dokumentaci související s realizací plnění dle Smlouvy včetně účetních dokladů v souladu s příslušnými Obecnými pravidly IROP minimálně do konce roku 2035. Pokud je v českých právních předpisech stanovena lhůta delší, musí ji Poskytovatel použít;

7.1.12 Poskytovatel je povinen v souladu s příslušnými Obecnými pravidly IROP minimálně do konce roku 2035 poskytovat požadované informace a dokumentaci související s realizací plnění dle Smlouvy zaměstnancům nebo zmocněncům pověřených orgánů (CRR, MMR ČR, MF ČR, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci plnění dle Smlouvy v rámci projektu kofinancovaného z IROP a poskytnout jim při provádění kontroly součinnost.

7.2 Objednatel se zavazuje poskytnout Poskytovateli součinnost potřebnou k řádné realizaci předmětu Smlouvy, kterou je po něm Poskytovatel jako osoba, která disponuje takovými kapacitami a odbornými znalostmi, které jsou nezbytné pro realizaci předmětu plnění Smlouvy, oprávněna požadovat.

7.3 Objednatel je v souvislosti s plněním předmětu Smlouvy oprávněn zejména udělovat Poskytovateli závazné pokyny pro výkon všech činností, ke kterým se Poskytovatel na základě Smlouvy zavázal; tyto pokyny jsou závazné, není tím však dotčena odpovědnost Poskytovatele za včasné upozornění Objednatele na jejich nevhodnou povahu.

7.4 Objednatel má právo přesvědčit se kdykoliv v průběhu realizace plnění Smlouvy o stavu realizace plnění a Poskytovatel mu k tomuto musí vytvořit přiměřené podmínky, případné náklady nese Poskytovatel.

7.5 Pokud se Smluvní strany nedohodnou jinak, součinnost zaměstnanců Objednatele dle Smlouvy bude poskytována pouze v pracovní době (od 8:00 do 16:00 hodin). Poskytovatel uvede v rámci Fáze 1 v implementačním projektu a harmonogramu předpokládané období a rozsah součinnosti, která bude potřebná ze strany Objednatele.

7.6 Objednatel požaduje, aby Poskytovatel a jeho případní poddodavatelé realizovali předmět Smlouvy v souladu s úmluvami Mezinárodní organizace práce (ILO) přijatými Českou republikou a právními předpisy. Poskytovatel a jeho případní poddodavatelé se zavazují dodržovat minimálně následující základní pracovní standardy:

- Úmluva č. 100 o stejném odměňování pracujících mužů a žen za práci stejné hodnoty,
- Úmluva č. 111 o diskriminaci (zaměstnání a povolání),
- Úmluva č. 138 o nejnižším věku pro vstup do zaměstnání,
- Úmluva č. 155 o bezpečnosti a zdraví pracovníků a o pracovním prostředí.

7.7 Poskytovatel a jeho případní poddodavatelé jsou povinni dodržovat rovněž povinnosti týkající se základních lidských práv, včetně dodržování Všeobecné deklarace lidských práv a evropské Úmluvy o ochraně lidských práv a základních svobod.

7.8 Poskytovatel a jeho případní poddodavatelé jsou odpovědní za zajištění, aby všichni zaměstnanci pracující při realizaci předmětu Smlouvy měli oprávnění k výkonu práce v České republice dle zákona č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, a že jejich pracovněprávní vztah bude v souladu se zákonem č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů, a prováděcími právními předpisy.

7.9 Poskytovatel a jeho případní poddodavatelé jsou povinni zajistit rovnost a spravedlivé a důstojné zacházení se všemi svými zaměstnanci, včetně spravedlivého a rovného odměňování za práci.

7.10 V případě, že Poskytovatel nebo jeho případní poddodavatelé poruší některou z výše uvedených povinností týkajících se dodržování výše uvedených základních pracovních standardů, mezinárodních úmluv a právních předpisů týkajících se zaměstnanců, je Poskytovatel či jeho poddodavatel povinen tyto nedostatky bezodkladně napravit a dokončit realizaci předmětu Smlouvy v souladu s těmito základními pracovními standardy, mezinárodními úmluvami a právními předpisy. Veškeré náklady vzniklé Poskytovateli či jeho poddodavateli a související s dodržováním povinností definovaných v tomto odstavci Smlouvy nese Poskytovatel, resp. jeho poddodavatel.

7.11 Objednatel je v přiměřené míře oprávněn v průběhu realizace předmětu Smlouvy kontrolovat dodržování výše uvedených základních pracovních standardů, mezinárodních úmluv a právních předpisů.

Sankce vůči Rusku a Bělorusku

7.12 Poskytovatel odpovídá za to, že platby poskytované Objednatelem dle této Smlouvy nebudou přímo nebo nepřímo ani jen zčásti poskytnuty osobám, vůči kterým platí tzv. individuální finanční sankce ve smyslu čl. 2 odst. 2 Nařízení Rady (EU) č. 208/2014 ze dne 5. 3. 2014 o omezujících opatřeních vůči některým osobám, subjektům a orgánům vzhledem k situaci na Ukrajině a Nařízení Rady (ES) č. 765/2006 ze dne 18. 5. 2006 o omezujících opatřeních vůči prezidentu Lukašenkovi a některým představitelům Běloruska a které jsou uvedeny na tzv. sankčních seznamech (dle příloh č. 1 obou nařízení); bude-li kterékoliv z nařízení v budoucnu nahrazeno jinou legislativou obdobného významu, uvedená povinnost se uplatní obdobně.

7.13 Poskytovatel odpovídá za to, že po dobu trvání Smlouvy nejsou naplněny podmínky uvedené v nařízení Rady (EU) č. 833/2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, tedy zejména, že Poskytovatel není:

- ruským státním příslušníkem, fyzickou nebo právnickou osobou se sídlem v Rusku,
- právnickou osobou, která je z více než 50 % přímo či nepřímo vlastněna některou z osob dle předešlé odrážky, nebo
- fyzickou nebo právnickou osobou, která jedná jménem nebo na pokyn některé z osob uvedených v předešlých odrážkách.

Poskytovatel odpovídá za to, že po dobu trvání Smlouvy žádná z výše uvedených podmínek není naplněna ani u jeho poddodavatele (nebo jiné osoby prokazující za Poskytovatele kvalifikaci), který se bude na plnění této Smlouvy podílet z více jak 10 % hodnoty Plnění.

7.14 Poskytovatel je povinen Objednatele bezodkladně informovat o jakýchkoliv skutečnostech, které mohou mít vliv na odpovědnost Poskytovatele dle odst. 7.12 nebo 7.13. tohoto článku Smlouvy. Poskytovatel je současně povinen kdykoliv poskytnout Objednateli bezodkladnou součinnost pro případné ověření pravdivosti informací dle odst. 7.12. nebo 7.13. tohoto článku Smlouvy.

7.15 Dojde-li k porušení pravidel dle odst. 7.12. nebo 7.13. tohoto článku Smlouvy, je Objednatel oprávněn odstoupit od této Smlouvy; odstoupení se však nedotýká povinností Poskytovatele vyplývajících ze záruky za jakost, odpovědnosti za vady, povinnosti zaplatit smluvní pokutu, povinnosti nahradit škodu a povinnosti zachovat důvěrnost informací souvisejících s plněním dle této Smlouvy.

7.16 Dojde-li k porušení pravidel dle odst. 7.12. nebo 7.13. tohoto článku Smlouvy, je Poskytovatel povinen zaplatit Objednateli smluvní pokutu ve výši 250.000 Kč, a to za každý jednotlivý případ porušení.

VIII. PODDODAVATELÉ, REALIZAČNÍ TÝM, OPRÁVNĚNÉ OSOBY, CENTRÁLNÍ ZADAVATEL

8.1 Poddodavatelé

8.1.1 Poskytovatel se zavazuje plnění předmětu Smlouvy provést sám, nebo s využitím poddodavatelů, uvedených spolu s rozsahem jejich plnění v příloze č. 2 Smlouvy. Poskytovatel je povinen písemně informovat Objednatele o všech svých poddodavatelích (včetně jejich identifikačních a kontaktních údajů a o tom, které služby pro něj v rámci předmětu plnění každý se poddodavatelů poskytuje) a o jejich změně, a to ve smyslu ust. § 105 odst. 3 ZZVZ; Poskytovatel je povinen své poddodavatele smluvně zavázat tak, aby plnili veškeré povinnosti Poskytovatele uvedené v této smlouvě, ve stejném rozsahu jako je zavázán sám Poskytovatel. Poskytovatel je povinen kdykoliv na vyžádání Objednatele

předložit smlouvu uzavřenou mezi ním a poddodavatelem, ze které vyplývá tento závazek.

8.1.2 Poskytovatel je oprávněn změnit poddodavatele, pomocí něhož prokázal část splnění kvalifikace v rámci zadávacího řízení Veřejné zakázky, a/nebo jehož zkušenosti byly předmětem hodnocení v rámci hodnocení nabídek, jen s předchozím písemným souhlasem Objednatele, přičemž nový poddodavatel musí disponovat minimálně stejnou kvalifikací a zkušeností pro účely hodnocení, které původní poddodavatel prokázal za Poskytovatele. Objednatel nesmí souhlas se změnou poddodavatele bez objektivních důvodů odmítnout, pokud mu budou příslušné doklady ve stanovené lhůtě předloženy.

8.1.3 Zadání provedení části plnění dle Smlouvy poddodavateli Poskytovatelem nezbavuje Poskytovatele jeho výlučné odpovědnosti za řádné provedení plnění dle Smlouvy vůči Objednateli. Poskytovatel odpovídá Objednateli za plnění předmětu Smlouvy, které svěřil poddodavateli, ve stejném rozsahu, jako by jej poskytoval sám.

8.2 Realizační tým

8.2.1 Poskytovatel určuje k plnění předmětu Smlouvy realizační tým. Jmenné složení realizačního týmu je uvedeno v příloze č. 3 Smlouvy (dále jen „***Realizační tým***"). Poskytovatel se zavazuje zachovávat po celou dobu plnění předmětu Smlouvy profesionální složení Realizačního týmu v souladu s požadavky stanovenými ve Smlouvě.

8.2.2 Poskytovatel se zavazuje zabezpečovat plnění předmětu Smlouvy prostřednictvím osob, jejichž prostřednictvím prokázal v rámci zadávacího řízení na Veřejnou zakázku splnění kvalifikačních požadavků (technické kvalifikace) a které využil pro účely hodnocení své nabídky v zadávacím řízení. V případě změny těchto osob (členů Realizačního týmu) je Poskytovatel povinen vyžádat si předchozí písemný souhlas Objednatele, tento souhlas je oprávněna vydat oprávněná osoba Objednatele ve věcech smluvních. Nová osoba Poskytovatele musí splňovat příslušné požadavky na kvalifikaci stanovené v Zadávací dokumentaci, resp. mít alespoň takové zkušenosti, které byly relevantní pro účely hodnocení nabídek dle kritéria hodnocení „Zkušenosti vybraných členů realizačního týmu", což je Poskytovatel povinen Objednateli doložit odpovídajícími dokumenty.

8.2.3 Objednatel si vyhrazuje právo na odmítnutí významných změn ve složení Realizačního týmu v době plnění Smlouvy. Současně si Objednatel vyhrazuje právo požádat o výměnu člena Realizačního týmu pro opakovanou nespokojenost s kvalitou jím odváděné práce nebo pro nedostatečnou

komunikaci s Objednatelem. Veškeré případné náklady související s výměnou člena Realizačního týmu nese výlučně Poskytovatel.

8.3 Oprávněné osoby

8.3.1 Každá ze Smluvních stran dále jmenuje oprávněné osoby, které budou vystupovat jako zástupci Smluvních stran. Oprávněné osoby zastupují Smluvní stranu ve smluvních a technických záležitostech souvisejících s plněním předmětu Smlouvy, zejména podávají a přijímají informace o průběhu plnění Smlouvy a dále:

- osoby oprávněné ve věcech smluvních jsou oprávněny vést s druhou Smluvní stranou jednání obchodního charakteru, jednat v rámci akceptačních procedur při předávání a převzetí Plnění dle čl. 6 Smlouvy, zejména podepisovat příslušné akceptační či jiné protokoly dle Smlouvy.
- osoby oprávněné ve věcech technických jsou oprávněny vést jednání technického charakteru, poskytovat stanoviska v technických otázkách a jednat jménem Smluvních stran v rámci reklamace vad a při uplatňování záruky podle čl. 10 Smlouvy.

8.3.2 Oprávněné osoby budou oprávněny činit rozhodnutí závazná pro Smluvní strany ve vztahu ke Smlouvě v rámci své pravomoci. Oprávněné osoby, nejsou-li statutárními orgány, však nejsou oprávněny provádět změny ani zrušení Smlouvy, nebude-li jim udělena speciální plná moc.

8.3.3 Oprávněnými osobami za Objednatele jsou:

i) ve věcech smluvních: [redacted]

ii) ve věcech technických: [redacted]

8.3.4 Oprávněnými osobami za Poskytovatele jsou:

(i) ve věcech smluvních: [redacted]

(ii) ve věcech technických: [redacted]

8.3.5 Každá ze Smluvních stran má právo změnit jí jmenované oprávněné osoby, musí však o každé změně vyrozumět písemně druhou Smluvní stranu. Změna oprávněných osob je vůči druhé Smluvní straně účinná okamžikem, kdy o ní byla písemně vyrozuměna.

IX. VLASTNICKÉ PRÁVO, NEBEZPEČÍ ŠKODY NA VĚCI A PRÁVO UŽITÍ

9.1 Poskytovatel prohlašuje, že vlastnické právo a nebezpečí škody na věci ke všem hmotným součástem plnění předmětu Smlouvy předaným Poskytovatelem Objednateli v

souvislosti s plněním předmětu Smlouvy přechází na Objednatele dnem jejich předání Objednateli.

9.2 Vzhledem k tomu, že součástí Plnění dle Smlouvy je i plnění, které může naplňovat znaky autorského díla ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „**AZ**"), je k těmto součástem Plnění poskytována licence za podmínek sjednaných dále v tomto článku Smlouvy.

9.2.1 Objednatel je oprávněn veškeré součásti Plnění Poskytovatele považované za autorské dílo ve smyslu AZ (dále jen „***Autorské dílo***") užívat dle níže uvedených podmínek.

9.2.2 Objednatel je oprávněn Autorské dílo užívat dle níže uvedených licenčních podmínek (dále jen „***Licence***"), a to od okamžiku účinnosti poskytnutí Licence, přičemž Poskytovatel poskytuje Objednateli Licenci s účinností, která nastává okamžikem předání Plnění či jeho části, jehož je Autorské dílo součástí.

9.2.3 Nevyplývá-li z příloh Smlouvy jinak, je Licence udělena jako nevýhradní k užití Autorského díla Objednatelem k jakémukoliv účelu a v rozsahu, v jakém uzná za nezbytné, vhodné či přiměřené. Pro vyloučení všech pochybností to znamená, že:

- Licence je udělena jako neodvolatelná;
- Licence je dále udělena na dobu určitou, a to po celou dobu trvání majetkových práv autorských k Autorskému dílu, bez omezení územního rozsahu;
- v případě SW, který je součástí Plnění, se Licence vztahuje ve stejném rozsahu i na případné další verze tohoto SW upraveného na základě Smlouvy;
- Objednatel je bez potřeby jakéhokoliv dalšího svolení Poskytovatele oprávněn udělit třetí osobě podlicenci k užití Autorského díla nebo svoje oprávnění k jejímu užití třetí osobě postoupit;
- Licenci není Objednatel povinen využít, a to ani zčásti;
- Licence umožňující Objednateli SKB uživatelsky upravovat, pokud nebude nutné zasahovat do zdrojového kódu (tj. např. úprava formulářů, modifikace dle konkrétní činnosti/procesu apod.)

9.2.4 Současně Poskytovatel uděluje Objednateli souhlas ode dne účinnosti poskytnuté Licence dle Smlouvy provádět jakékoliv modifikace, úpravy, změny Autorského díla a dle svého uvážení do něj zasahovat, zapracovávat jej do dalších autorských děl, zařazovat jej do děl souborných či do databází apod., a to i prostřednictvím třetích osob;

9.2.5 V souvislosti s poskytnutou Licencí je Poskytovatel povinen, s výjimkami uvedenými v odst. 9.3 Smlouvy a 9.4 Smlouvy, nejpozději ke dni ukončení akceptace Plnění či jeho části předat Objednateli zdrojový kód každé jednotlivé části Autorského díla, která je počítačovým programem, a která je Objednateli poskytována na základě Plnění dle Smlouvy jako customizované plnění, aby s ním mohl Objednatel libovolně nakládat. Pro účely této Smlouvy se customizovaným plněním rozumí veškeré úpravy řešení dle požadavků Objednatele. Zdrojový kód musí být spustitelný v prostředí Objednatele a zaručovat možnost ověření, že je kompletní a ve správné verzi, tzn. umožňující kompilaci, instalaci, spuštění a ověření funkcionality, a to včetně podrobné dokumentace zdrojového kódu. Zdrojový kód bude Objednateli Poskytovatelem předán na nepřepisovatelném technickém nosiči dat s viditelně označeným názvem „Zdrojový kód" a označením počítačového programu či její části a jeho verze a dne předání zdrojového kódu. O předání technického nosiče dat bude oběma Smluvními stranami sepsán a podepsán písemný předávací protokol.

9.3 Je-li součástí Plnění tzv. proprietární software (dále jen „***Proprietární software***"), u kterého Poskytovatel nemůže poskytnout Objednateli oprávnění dle odst. 9.2.1 až 9.2.5 Smlouvy nebo to po něm nelze spravedlivě požadovat, postačí, aby Objednatel nabyl k takovému software nevýhradní oprávnění užít jej jakýmkoli způsobem nejméně po dobu trvání Smlouvy, bez územního omezení a v množstevním rozsahu, který je nezbytný pro pokrytí potřeb Objednatele ke dni uzavření Smlouvy. Smluvní strany výslovně uvádějí, že součástí takového nevýhradního oprávnění není právo provádět jakékoliv modifikace, úpravy či změny Proprietárního software či dle svého uvážení do něj zasahovat, zapracovávat ho do dalších autorských děl, zařazovat ho do děl souborných či do databází apod., a to i prostřednictvím třetích osob, ani se u Proprietárního software nevyžaduje poskytnutí zdrojových kódů k takovému software.

9.4 Je-li součástí Plnění tzv. open source software, u kterého Poskytovatel nemůže poskytnout Objednateli oprávnění dle odst. 9.2.1 až 9.2.5 Smlouvy nebo dle odst. 9.3 Smlouvy nebo to po něm nelze spravedlivě požadovat, je Poskytovatel povinen zajistit, aby se jednalo o open source software, který je veřejnosti poskytován zdarma, včetně zdrojových kódů, úplné původní uživatelské, provozní a administrátorské dokumentace a práva takový software měnit a zároveň možnost užití takového software Objednatelem k účelu sjednanému Smlouvou dle podmínek smlouvy.

9.5 Udělení veškerých práv uvedených v tomto článku Smlouvy nelze ze strany Poskytovatele vypovědět a na jejich udělení nemá vliv ukončení účinnosti Smlouvy.

9.6 Poskytovatel prohlašuje, že veškeré jím dodané plnění podle Smlouvy bude prosté právních vad a zavazuje se odškodnit v plné výši Objednatele v případě, že třetí osoba úspěšně uplatní autorskoprávní nebo jiný nárok plynoucí z právní vady poskytnutého

plnění dle Smlouvy. V případě, že by nárok třetí osoby vzniklý v souvislosti s plněním Poskytovatele podle Smlouvy, bez ohledu na jeho oprávněnost, vedl k dočasnému či trvalému soudnímu zákazu či omezení užívání SKB či jeho části, zavazuje se Poskytovatel zajistit náhradní řešení a minimalizovat dopady takovéto situace, a to bez dopadu na cenu plnění sjednanou podle Smlouvy, přičemž současně nebudou dotčeny ani nároky Objednatele na náhradu škody.

9.7 S nositeli chráněných práv duševního vlastnictví vzniklých v souvislosti s realizací Plnění dle Smlouvy je Poskytovatel povinen vždy smluvně zajistit možnost nakládání s těmito právy Objednatelem v rozsahu definovaném tímto článkem Smlouvy.

9.8 Poskytovatel podpisem Smlouvy výslovně prohlašuje, že odměna za veškerá oprávnění poskytnutá Objednateli dle tohoto článku Smlouvy je již zahrnuta v ceně za poskytování Plnění dle Smlouvy.

9.9 Poskytovatel je povinen Objednateli uhradit jakékoli majetkové a nemajetkové újmy, vzniklé v důsledku toho, že Objednatel nemohl předmět Plnění Smlouvy užívat řádně a nerušeně. Jestliže se jakékoliv prohlášení Poskytovatele v tomto článku ukáže nepravdivým nebo Poskytovatel poruší jinou povinnost dle tohoto článku Smlouvy, jde o podstatné porušení Smlouvy a Poskytovatel je povinen uhradit Objednateli smluvní pokutu ve výši 50.000,- Kč za každé jednotlivé porušení povinnosti. Zaplacením smluvní pokuty není nijak dotčeno ani omezeno právo Objednatele na náhradu škody, kterou lze vymáhat vedle smluvní pokuty v plné výši.

9.10 Poskytovatel poskytne Objednateli na jeho písemnou žádost veškerou nezbytně nutnou součinnost pro změnu poskytovatele, a to před ukončením této Smlouvy nebo její části, tj. v průběhu výpovědní doby i po jejím ukončení, případně bezodkladně po obdržení písemné žádosti Objednatele tak, aby byl zajištěn bezproblémový přechod k novému poskytovateli (dále jen „***Exit plán***"). Nezbytně nutná součinnost v rámci Exit plánu bude zahrnovat zejména:

- aktivní spolupráci Poskytovatele při migraci dat při přechodu k jinému poskytovateli, vč. zajištění exportu v dohodnutém či Objednatelem určeném formátu dat,
- poskytnutí úplné a aktuální provozní dokumentace k Plnění (dokumentace musí zahrnovat kompletní elektronickou kopii veškeré dokumentace, kterou Poskytovatel vytvořil v rámci Plnění s tím, že bude aktualizována tak, aby odrážela stav k datu ukončení Plnění),
- prokazatelné odstranění dat na HW prostředcích Poskytovatele,
- poskytnutí další konzultace Objednateli a případnému novému poskytovateli (nad rámec shora uvedených povinností) spojené zejména s přípravou nového dodavatele na výkon Služeb podpory či Služeb rozvoje; konzultace budou poskytovány na základě písemného vyžádání Objednatele.

Objednatel má právo žádost o součinnost učinit kdykoliv po dobu platnosti a účinnosti této Smlouvy a Poskytovatel je povinen tuto součinnost poskytnout ještě 3 další měsíce po ukončení platnosti této Smlouvy či její části. V souvislosti s poskytnutím součinnosti v rámci Exit plánu nenáleží Poskytovateli odměna za prvních 50 hodin, kdy tyto jsou zahrnuty v ceně Plnění. V souvislosti s poskytnutím součinnosti v rámci Exit plánu náleží Poskytovateli odměna za 51. a každou další Objednatelem odsouhlasenou hodinu součinnosti ve výši jednotkové ceny za hodinu Služeb rozvoje. Součinnost v rámci Exit plánu bude poskytována nejvýše v rozsahu 100 hodin. Exit plán bude dále upřesněn v implementačním projektu zpracovaném Poskytovatelem.

X. ODPOVĚDNOST ZA ŠKODU, ODPOVĚDNOST ZA VADY, ZÁRUKA

10.1 Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod. Smluvní strany nesou odpovědnost za škodu dle platných a účinných právních předpisů a Smlouvy. Poskytovatel odpovídá za škodu rovněž v případě, že část Plnění poskytuje prostřednictvím poddodavatele.

10.2 Žádná ze stran není odpovědná za škodu vzniklou porušením povinnosti ze Smlouvy, prokáže-li, že mu ve splnění povinnosti ze Smlouvy dočasně nebo trvale zabránila mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na jeho vůli. Překážka vzniklá ze škůdcových osobních poměrů nebo vzniklá až v době, kdy byl škůdce s plněním povinnosti ze Smlouvy v prodlení, ani překážka, kterou byl škůdce podle Smlouvy povinen překonat, ho však povinnosti k náhradě nezprostí. Smluvní strany se zavazují upozornit druhou stranu bez zbytečného odkladu na vzniklé překážky bránící řádnému plnění Smlouvy a dále se zavazují k vyvinutí maximálnímu úsilí k jejich odvrácení a překonání.

10.3 Škoda se hradí v penězích, nebo, je-li to možné nebo účelné, uvedením do předešlého stavu podle volby poškozené strany v konkrétním případě.

10.4 Poskytovatel se zavazuje, že po celou dobu účinnosti Smlouvy bude mít sjednánu pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za škodu způsobenou Poskytovatelem třetí osobě s limitem pojistného plnění minimálně 60.000.000,- Kč. Poskytovatel je povinen předložit kopii pojistné smlouvy na vyžádání Objednateli. V případě, že při činnosti prováděné Poskytovatelem dojde ke způsobení prokazatelné škody Objednateli nebo třetím osobám, která nebude kryta pojištěním sjednaným ve smyslu tohoto odst. Smlouvy, bude Poskytovatel povinen tyto škody uhradit z vlastních prostředků.

10.5 Poskytovatel přebírá závazek a odpovědnost za vady Plnění, jež bude mít Plnění (či jeho dílčí část) v době jeho předání Objednateli a dále za vady, které se na Plnění (či jeho dílčí

části) vyskytnou v průběhu záruční doby. Poskytovatel v souvislosti s odpovědností za vady Plnění poskytuje Objednateli níže specifikovanou záruku.

10.6 Nevyplývá-li z příloh Smlouvy jinak (zejm. v příloze č. 1 Smlouvy může být pro konkrétní zařízení požadována jiná min. délka záruky), poskytovatel poskytuje Objednateli ve smyslu § 2619 OZ záruku za jakost v délce 60 měsíců na to, že předané Plnění bude mít vlastnosti stanovené Smlouvou a výstupy Fáze 1 (u části plnění odpovídající Službám podpory nebo Službám rozvoje případně i vlastnosti stanovené příslušnou objednávkou), bude bez jakýchkoliv nedodělků či vad. Záruční doba počíná běžet u části Plnění odpovídajícího Fázi 1 a Fázi 2 ode dne předání a převzetí kompletní Fáze 2 Objednatelem, u části Fáze 3 odpovídající Službám rozvoje vždy ode dne předání a převzetí příslušného plnění.

10.7 Záruční doba neběží po dobu, po kterou Objednatel nemůže užívat Plnění či jeho část pro vady, za které odpovídá Poskytovatel. Veškeré činnosti nutné či související s vyřízením reklamací vad činí Poskytovatel sám na své náklady v součinnosti s Objednatelem a v jeho provozní době tak, aby svými činnostmi neohrozil nebo neomezil činnost Objednatele.

10.8 Není-li mezi Smluvními stranami sjednáno jinak, je Poskytovatel povinen jakékoliv vady Plnění či jeho části, které vzniknou v době trvání záruky odstraňovat na své náklady, a to v souladu s režimem SLA uvedeným v příloze č. 6 Smlouvy. Kategorii vady/chyby/incidentu určuje Objednatel; Poskytovatel je případně oprávněn se ke kategorizaci vyjádřit v souladu s přílohou č. 6 Smlouvy.

XI. SANKČNÍ UJEDNÁNÍ

11.1 Smluvní pokuty:

i) v případě prodlení Poskytovatele s poskytnutím plnění odpovídajícího Fázi 1 nebo Fázi 2 v termínu dle Smlouvy je Poskytovatel povinen uhradit Objednateli smluvní pokutu ve výši [redacted] Kč, a to za každý i započatý den prodlení, čímž není dotčeno oprávnění Objednatele požadovat náhradu škody, a to odpovídají také ztrátě či snížení dotace na předmět plnění Smlouvy;

ii) v případě jakéhokoliv nedodržení lhůt pro odstranění vad či nedodělků předaného (akceptovaného) plnění ve smyslu odst. 6.2.6.1 Smlouvy je Poskytovatel povinen Objednateli uhradit následující smluvní pokuty, není-li ve výstupech Fáze 1 stanoveno jinak:

- vada kategorie C: [redacted] Kč za každý i započatý den prodlení a jednotlivou vadu;

iii) v případě porušení povinnosti poskytování Služeb podpory, konkrétně SLA, v požadované kvalitě, tj. dle požadavků uvedených příloze č. 6 Smlouvy, je Poskytovatel povinen uhradit Objednateli následující smluvní pokuty:

- nedodržení lhůty odezvy (response time) u vady/chyby/incidentu kategorie A (kritická): [redacted] Kč za každých i započatých 60 minut prodlení a jednotlivou vadu/chybu/incident;
- nedodržení lhůty odezvy (response time) u vady/chyby/incidentu kategorie B (závažná): [redacted] Kč za každých i započatých 60 minut prodlení a jednotlivou vadu/chybu/incident;
- nedodržení lhůty odezvy (response time) u vady/chyby/incidentu kategorie C (běžná): [redacted] Kč za každý i započatý den prodlení a jednotlivou vadu/chybu/incident;
- nedodržení lhůty řešení (repair time) u vady/chyby/incidentu kategorie A (kritická): [redacted] Kč za každých i započatých 60 minut prodlení a jednotlivou vadu/chybu/incident;
- nedodržení lhůty řešení (repair time) u vady/chyby/incidentu kategorie B (závažná): [redacted] Kč za každých i započatých 60 minut prodlení a jednotlivou vadu/chybu/incident.
- nedodržení dostupnosti SKB dle přílohy č. 6 Smlouvy: [redacted] Kč za nedodržení každé desetiny % pod úrovní 99,95 % a [redacted] Kč za nedodržení každé desetiny % pod úrovní 99,00 %.

iv) v případě porušení povinnosti Poskytovatele udržovat v platnosti a účinnosti po celou dobu účinnosti Smlouvy pojistnou smlouvu dle odst. 10.4 Smlouvy je Poskytovatel povinen zaplatit Objednateli smluvní pokutu ve výši [redacted] Kč za každý i započatý měsíc, v němž nebude mít uzavřenou pojistnou smlouvu se stanovenými parametry;

v) v případě porušení povinností k ochraně důvěrných informací dle článku XII. Smlouvy je Poskytovatel povinen uhradit Objednateli smluvní pokutu ve výši [redacted] Kč za každý jednotlivý případ porušení;

vi) provede-li Poskytovatel změnu v realizačním týmu v rozporu s odst. 8.2.2 Smlouvy anebo neprovede změnu v realizačním týmu v souladu s požadavky Objednatele dle odst. 8.2.3 Smlouvy, má Objednatel právo na smluvní pokutu ve výši [redacted] Kč za každý jednotlivý případ porušení, a to i opakovaně pokud nedojde k nápravě do 14 dnů od předchozího zjištěného porušení;

vii) provede-li Poskytovatel změnu poddodavatele v rozporu s odst. 8.1.2. Smlouvy anebo nebude-li informovat Objednatele o všech svých poddodavatelích v rozporu s odst. 8.1.1. Smlouvy anebo nezaváže-li smluvně všechny své poddodavatele, aby plnili veškeré povinnosti Poskytovatele uvedené v této Smlouvě ve stejném rozsahu jako je zavázán sám Poskytovatel v rozporu s odst. 8.1.1. Smlouvy, je Poskytovatel povinen zaplatit Objednateli smluvní pokutu ve výši [redacted] Kč za každý jednotlivý

případ porušení, a to i opakovaně pokud nedojde k nápravě do 14 dnů od předchozího zjištěného porušení.

11.2 V případě prodlení kterékoliv Smluvní strany se zaplacením peněžité částky vzniká oprávněné Smluvní straně nárok na zákonný úrok z prodlení ve výši dle příslušných právních předpisů.

11.3 Zaplacením smluvní pokuty není jakkoliv dotčen nárok Objednatele na náhradu škody včetně případné újmy nemajetkové; nárok na náhradu škody je Objednatel oprávněn uplatnit vedle smluvní pokuty v plné výši. Zaplacením smluvní pokuty není dotčeno splnění povinnosti, která je prostřednictvím smluvní pokuty utvrzena.

11.4 Smluvní pokuta i úrok z prodlení jsou splatné do třiceti (30) dnů po obdržení jejich vyúčtování.

XII. OCHRANA DŮVĚRNÝCH INFORMACÍ A OCHRANA OSOBNÍCH ÚDAJŮ

12.1 Smluvní strany se dohodly, že veškeré informace, které si sdělily v rámci uzavírání a plnění Smlouvy, dále informace, které si sdělí nebo jinak vyplynou i z jejího plnění, stejně jako případné utajované informace ve smyslu zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti (dále jen „***Zákon o ochraně utaj. informací***“) jsou důvěrné (dále jen „***Důvěrné informace***“). Smluvní strany sjednávají, že Důvěrnými informacemi jsou veškeré Objednatelem poskytnuté informace, podklady a dokumenty, pokud nejsou běžně dostupné ve veřejných zdrojích.

12.2 Pro ochranu utajovaných informací dle Zákona o ochraně utaj. informací je Poskytovatel povinen dodržovat tento zákon. Smluvní strany se dohodly, že Důvěrné informace nikomu neprozradí a přijmou taková opatření, která znemožní jejich přístupnost třetím osobám. Ustanovení předchozí věty se nevztahuje na případy, kdy:

12.2.1 Smluvní strany mají povinnost stanovenou právním předpisem, a/nebo

12.2.2 takové informace sdělí osobám, které mají ze zákona stanovenou povinnost mlčenlivosti, a/nebo

12.2.3 se takové informace stanou veřejně známými či dostupnými jinak než porušením povinností vyplývajících z tohoto článku Smlouvy.

12.3 Vyjma výše uvedeného se Poskytovatel zavazuje, že bude chránit a utajovat před třetími osobami skutečnosti tvořící obchodní tajemství, Důvěrné informace a jiné skutečnosti, které mu byly poskytnuty v rámci smluvního vztahu s Objednatelem.

12.4 Pokud je sdělení Důvěrných informací třetí osobě nezbytné pro plnění závazků Poskytovatele vyplývajících mu ze Smlouvy, může Poskytovatel tyto Důvěrné informace poskytnout pouze s předchozím písemným souhlasem Objednatele a za předpokladu, že tato třetí osoba před započetím činnosti písemně potvrdí svůj závazek zachování

mlčenlivosti a ochrany Důvěrných informací, jinak je za toto porušení odpovědný v plném rozsahu Poskytovatel.

12.5 V případě uplatnění smluvních pokut a náhrady škody není dotčena hmotná a trestní odpovědnost fyzických osob, které za Poskytovatele jednaly a závazek mlčenlivosti a ochrany Důvěrných informací nedodržely.

12.6 Závazek k mlčenlivosti a ochrany Důvěrnosti informací je platný bez ohledu na ukončení účinnosti Smlouvy.

12.7 Vzhledem k veřejnoprávnímu charakteru Objednatele Poskytovatel výslovně prohlašuje, že je s touto skutečností obeznámen a souhlasí se zveřejněním smluvních podmínek obsažených ve Smlouvě v rozsahu a za podmínek vyplývajících z příslušných právních předpisů.

12.8 V případě, že bude při plnění Smlouvy docházet ke zpracování osobních údajů, Smluvní strany se zavazují uzavřít samostatnou smlouvu o zpracování osobních údajů, a to před zahájením zpracování.

XIII. DOBA TRVÁNÍ SMLOUVY, MOŽNOSTI UKONČENÍ SMLOUVY

13.1 Smlouva je v případě Fáze 3 (Služby podpory a Služby rozvoje) uzavřena na dobu neurčitou. Smlouva nabývá platnosti dnem jejího podpisu Objednatelem a Poskytovatelem a účinnosti dnem jejího uveřejnění prostřednictvím registru smluv ve smyslu zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv) ve znění pozdějších předpisů.

13.2 Smlouva může být ukončena písemnou dohodou Smluvních stran.

13.3 Objednatel je oprávněn od Smlouvy písemně odstoupit z důvodu jejího podstatného porušení Poskytovatelem, přičemž za podstatné porušení Smlouvy se bude považovat:

a) prodlení Poskytovatele s poskytováním Plnění či jeho části ve sjednaných termínech delší než 30 dnů, pokud Poskytovatel nezjedná nápravu ani v dodatečné přiměřené lhůtě, kterou mu k tomu Objednatel poskytne v písemné výzvě ke splnění povinnosti, přičemž tato lhůta nesmí být kratší než 10 dnů od doručení takovéto výzvy;

b) další případy, o kterých tak výslovně stanoví Smlouva.

13.4 Objednatel je rovněž oprávněn odstoupit od Smlouvy v případě, že:

a) v insolvenčním řízení bude zjištěn úpadek Poskytovatele nebo insolvenční návrh bude zamítnut pro nedostatek majetku Poskytovatele v souladu se zněním zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění

pozdějších předpisů. Objednatel je rovněž oprávněn odstoupit od Smlouvy v případě, že Poskytovatel vstoupí do likvidace; nebo

b) provede-li Poskytovatel změnu v realizačním týmu v rozporu s odst. 8.2.2 Smlouvy anebo neprovede změnu v realizačním týmu v souladu s požadavky Objednatele dle odst. 8.2.3 Smlouvy, nebo

c) dojde k významné změně kontroly nad dodavatelem nebo změny kontroly nad zásadními aktivy využívanými Poskytovatelem k plnění dle této Smlouvy ve smyslu písm. n) přílohy č. 7 VKB, nebo

d) proti Poskytovateli je zahájeno trestní stíhání pro trestný čin podle zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob, ve znění pozdějších předpisů.

13.5 Poskytovatel je oprávněn od Smlouvy písemně odstoupit z důvodu jejího podstatného porušení Objednatelem, za což se považuje prodlení Objednatele s úhradou ceny za plnění předmětu dle Smlouvy o více než 30 dní, pokud Objednatel nezjedná nápravu ani do 30 dnů od doručení písemného oznámení Poskytovatele o takovém prodlení s žádostí o jeho nápravu.

13.6 Odstoupení od Smlouvy ze strany Objednatele nesmí být spojeno s uložením jakékoliv sankce k tíži Objednatele.

13.7 Smluvní strany se dále dohodly, že odstoupení od Smlouvy musí být písemné, jinak je neplatné. Odstoupení je účinné ode dne, kdy bylo doručeno druhé Smluvní straně.

13.8 Objednatel i Poskytovatel jsou oprávněni Smlouvu vypovědět, a to i bez udání důvodu, a Smlouva skončí uplynutím příslušného roku (výročí) poskytování Služeb podpory ve Fázi 3, přičemž toto oprávnění může Objednatel uplatnit až v rámci Fáze 3 dle Smlouvy; Poskytovatel je oprávněn výpověď využít nejdříve po uplynutí 4 let od zahájení Fáze 3. V případě výpovědi Objednatele musí být písemná výpověď Poskytovateli doručena nejpozději 3 měsíce před uplynutím příslušného roku (výročí) poskytování Služeb podpory ve Fázi 3 dle Smlouvy, v případě výpovědi Poskytovatele musí být písemná výpověď Objednateli doručena nejpozději 6 měsíců před uplynutím příslušného roku (výročí) poskytování Služeb podpory ve Fázi 3 dle Smlouvy, jinak je výpověď neplatná, nedohodnou-li se Smluvní strany jinak.

13.9 Ukončením Smlouvy nejsou dotčena ustanovení o odpovědnosti za škodu, nároky na uplatnění smluvních pokut, ustanovení o ochraně důvěrných informací, jakož i ostatní práva a povinnosti založená Smlouvou, která mají podle zákona nebo Smlouvy trvat i po jejím zrušení.

XIV. SOUČINNOST A VZÁJEMNÁ KOMUNIKACE

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

14.2 Smluvní strany jsou povinny plnit své závazky vyplývající ze Smlouvy tak, aby nedocházelo k prodlení s plněním jednotlivých termínů a s prodlením splatnosti jednotlivých peněžních závazků.

14.3 Veškerá komunikace mezi smluvními stranami bude probíhat prostřednictvím oprávněných osob uvedených v čl. VIII Smlouvy nebo na jeho základě, pověřených pracovníků nebo statutárních zástupců Smluvních stran.

14.4 Veškerá oznámení, tj. jakákoliv komunikace na základě Smlouvy, bude probíhat v souladu s tímto článkem Smlouvy. Jakékoli oznámení, žádost či jiné sdělení, jež má být učiněno či dáno Smluvní straně dle Smlouvy, bude učiněno či dáno písemně. Kromě jiných způsobů komunikace dohodnutých mezi stranami se za účinné považují osobní doručování, doručování doporučenou poštou, kurýrní službou, datovou schránkou či elektronickou poštou, a to na adresy Smluvních stran uvedené v záhlaví Smlouvy, nebo na takové adresy, které si Smluvní strany vzájemně písemně oznámí.

14.5 Oznámení správně adresovaná se považují za doručená

- dnem, o němž tak stanoví zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů (dále jen „***ZDS***"), je-li oznámení zasíláno prostřednictvím datové zprávy do datové schránky ve smyslu ZDS; nebo
- dnem fyzického předání oznámení, je-li oznámení zasíláno prostřednictvím kurýra nebo doručováno osobně; nebo
- dnem doručení potvrzeným na doručence, je-li oznámení zasíláno doporučenou poštou; nebo
- dnem, kdy bude, v případě, že doručení výše uvedeným způsobem nebude z jakéhokoli důvodu možné, oznámení zasláno doporučenou poštou na adresu Smluvní strany, avšak k jeho převzetí z jakéhokoli důvodu nedojde, a to ani ve lhůtě tří (3) pracovních dnů od jeho uložení na příslušné pobočce pošty.

14.6 Informace a materiály, které obsahují osobní údaje či důvěrné informace, budou doručovány buď osobně, nebo zasílány elektronicky prostřednictvím šifrovaného distribučního kanálu určeného Objednatelem.

XV. ZÁVĚREČNÁ USTANOVENÍ

15.1 Smluvní strany si podpisem Smlouvy sjednávají (pokud Smlouva nestanoví jinak), že závazky Smlouvou založené budou vykládány výhradně podle obsahu Smlouvy, bez přihlédnutí k jakékoli skutečnosti, která nastala a/nebo byla sdělena, jednou stranou druhé straně před uzavřením Smlouvy. Ujednání dle odst. 1.1 Smlouvy tímto není dotčeno.

15.2 Smlouva představuje úplnou dohodu Smluvních stran o předmětu Smlouvy a všech náležitostech, které Smluvní strany měly a chtěly ve Smlouvě ujednat, a které považují za důležité pro závaznost Smlouvy. Žádný projev stran učiněný po uzavření Smlouvy nesmí být vykládán v rozporu s výslovnými ustanoveními Smlouvy a nezakládá žádný závazek žádné ze Smluvních stran. Smlouvu je možné měnit pouze písemnou dohodou Smluvních stran ve formě číslovaných dodatků Smlouvy, podepsaných oprávněnými zástupci obou Smluvních stran.

15.3 Smluvní strany se podpisem Smlouvy dohodly, že vylučují aplikaci ustanovení § 557 OZ.

15.4 Smluvní strany si nepřejí, aby nad rámec výslovných ustanovení Smlouvy byla jakákoliv práva a povinnosti dovozovány z dosavadní či budoucí praxe zavedené mezi smluvními stranami či zvyklostí zachovávaných obecně či v odvětví týkajícím se předmětu plnění Smlouvy, ledaže je ve Smlouvě výslovně sjednáno jinak.

15.5 Smluvní strany si sdělily všechny skutkové a právní okolnosti, o nichž k datu podpisu Smlouvy věděly nebo vědět musely, a které jsou relevantní ve vztahu k uzavření Smlouvy.

15.6 Pro vyloučení pochybností Poskytovatel výslovně potvrzuje, že je podnikatelem, uzavírá Smlouvu při svém podnikání, a na Smlouvu se tudíž neuplatní ustanovení § 1793 OZ.

15.7 Poskytovatel na sebe v souladu s ustanovením § 1765 odst. 2 OZ přebírá nebezpečí změny okolností. Tímto však nejsou nikterak dotčena práva Smluvních stran upravená ve Smlouvě.

15.8 Práva vyplývající ze Smlouvy či jejího porušení se promlčují ve lhůtě 4 let ode dne, kdy právo mohlo být uplatněno poprvé.

15.9 Není-li stanoveno jinak, jednacím jazykem mezi Objednatelem a Poskytovatelem bude pro veškerá plnění vyplývající ze Smlouvy výhradně jazyk český, případně slovenský, a to včetně veškeré dokumentace vztahující se k předmětu Smlouvy.

15.10 Stane-li se jakékoli ustanovení Smlouvy neplatným, nezákonným nebo nevynutitelným, netýká se tato neplatnost a nevynutitelnost zbývajících ustanovení Smlouvy. Smluvní strany se tímto zavazují nahradit do 5 pracovních dnů po doručení výzvy druhé Smluvní strany jakékoli takové neplatné, nezákonné nebo nevynutitelné ustanovení ustanovením, které je platné, zákonné a vynutitelné a má stejný nebo alespoň podobný obchodní a právní význam.

15.11 Vztahy Smluvních stran Smlouvou výslovně neupravené se řídí českým právním řádem, zejména OZ. Veškeré případné spory ze Smlouvy budou v prvé řadě řešeny smírem. Pokud smíru nebude dosaženo, všechny spory ze Smlouvy a v souvislosti s ní budou řešeny věcně a místně příslušným soudem v České republice podle právního řádu ČR.

15.12 Žádné ustanovení Smlouvy nesmí být vykládáno tak, aby omezovalo oprávnění Objednatele uvedená v Zadávací dokumentaci Veřejné zakázky.

15.13 Smlouva bude uzavřena v elektronické podobě, přičemž každá Smluvní strana obdrží její elektronický originál.

15.14 Pokud Smlouva podléhá uveřejnění v registru smluv dle zákona č. zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), Smluvní strany se dohodly, že Smlouvu zašle k uveřejnění v registru smluv Objednatel. Pokud Poskytovatel považuje některé informace v této Smlouvě či jejích přílohách za své obchodní tajemství, označí tyto části nejpozději při uzavření této Smlouvy, a to včetně podrobného odůvodnění, že tyto informace naplňují veškeré znaky dle § 504 OZ. Pokud Poskytovatel řádně prokáže, že určité informace naplňují znaky obchodního tajemství ve smyslu § 504 OZ, bude Objednatel postupovat v souladu s příslušnými právními předpisy.

15.15 Nedílnou součástí Smlouvy jsou následující přílohy:

- Příloha č. 1 – Technická specifikace
- Příloha č. 2 – Seznam poddodavatelů (vč. rozsahu jejich plnění);
- Příloha č. 3 – Realizační tým;
- Příloha č. 4 – Specifikace Proprietárního software
- Příloha č. 5 – Ceník
- Příloha č. 6 – SLA

Smluvní strany shodně prohlašují, že si Smlouvu před jejím podpisem přečetly a že byla uzavřena po podle jejich pravé a svobodné vůle, určitě, vážně a srozumitelně, což stvrzují svými podpisy.

Ve Vsetíně dne

za Objednatele:

[redacted] Digitálně podepsal [redacted]
Datum: 2024.05.23 [redacted]

Ing. Martin Pavlica, MHA
předseda představenstva

Ve Zlíně dne

za Poskytovatele:

[redacted] Digitálně podepsal [redacted]
Datum: 2024.05.20 [redacted]

[redacted]
ředitel regionálního centra
na základě plné moci

Příloha č. 1 – technická specifikace

1 Antivirová ochrana + EDR 2
2 Web aplikační firewall (AWAF) 8
3 Wi-fi AP 12
4 Dodávka a implementace systému PIM/PAM 22
5 Interní Firewall 33
6 MFA / ochrana přístupu uživatelů 47
7 Single Sign-On (SSO) 51
8 System řízení přístupu do sítě 802.1x 56
9 Systém pro analýzu síťového provozu a bezpečnostní monitoring 60
10 Hardening 77
11 Back Up Trezor - diskový úložný systém - dodávka a implementace 78
12 Servery a Switche a Záložní zdroje 86
13 Backup Server 90
14 Zálohovací SW 92

Příloha č. 1 – technická specifikace

1 Antivirová ochrana + EDR

[redacted]

Požadujeme tyto vlastnosti od End Point and server řešení:

1. Antivirové řešení pro [redacted]
2. Integrovaná cloudová analýza neznámých vzorků
3. Šifrování celých disků
4. EDR řešení
5. Management konzole pro správu všech řešení v rámci nabízeného balíku

1. Antivirové řešení pro koncové body a servery

- Podporované klientské platformy - OS: Windows, Linux, MacOS, Android, vše v českém jazyce
- Nativní podpora architektury pro platformy Windows a MacOS:
    - x86,
    - x64,
    - ARM64
- Antimalware, antiransomware, antispyware a anti-phishing pro aktivní ochranu před všemi typy hrozeb.
- Personální firewall pro zabránění neautorizovanému přístupu k zařízení se schopností automatického přebrání pravidel z brány Windows Firewall.
- Modul pro ochranu operačního systému a eliminaci aktivit ohrožující bezpečnost zařízení s možností definovat pravidla pro systémové registry, procesy, aplikace a soubory.
- Ochrana před neautorizovanou změnou nastavení / vyřazení z provozu / odinstalací antimalware řešení a kritických nastavení a souborů operačního systému
- Aktivní i pasivní heuristická analýza pro detekci dosud neznámých hrozeb.
- Systém pro blokaci exploitů zneužívajících zero-day zranitelností, jenž pokrývá nejpoužívanější vektory útoku:
    - síťové protokoly,
    - Flash Player,
    - Javu,
    - Microsoft Office,
    - webové prohlížeče,
    - e-mailové klienty,
    - PDF čtečky…
- Systém pro detekci malwaru již na síťové úrovni poskytující ochranu i před zneužitím zranitelností na síťové vrstvě.
- Kontrola šifrovaných spojení (SSL, TLS, HTTPS, IMAPS…).
- Anti-phishing se schopností detekce homoglyph útoků.
- Kontrola RAM paměti pro lepší detekci malwaru využívající silnou obfuskaci a šifrování.
- Cloud kontrola souborů pro urychlení skenování fungující na základě reputace souborů.

- Kontrola souborů v průběhu stahování pro snížení celkového času kontroly.
- Kontrola souborů při zapisování na disku a extrahování archivačních souborů
- Detekce s využitím strojového učení.
- Funkce ochrany proti zapojení do botnetu pracující s detekcí síťových signatur.
- Ochrana před síťovými útoky skenující síťovou komunikaci a blokující pokusy o zneužití zranitelností na síťové úrovni.
- Kontrola s podporou cloudu pro odesílání a online vyhodnocování neznámých a potenciálně škodlivých aplikací.
- Lokální sandbox
- Modul behaviorální analýzy pro detekce chování nových typů ransomwaru
- Systém reputace pro získání informací o závadnosti souborů a URL adres.
- Cloudový systém pro detekci nového malwaru ještě nezaneseného v aktualizacích signatur.
- Technologie pro detekci rootktitů obvykle se maskujících za součásti operačního systému.
- Skener firmwaru BIOSu a UEFI.
- Skenování souborů v cloudu OneDrive.
- Funkcionalita pro klienty MS Windows – Antimalware, Antispyware, Personal Firewall, Personal IPS, Application control, Device control, Security Memory (zabraňuje útokům na běžící aplikace), kontrola integrity systémových komponent
- Funkcionalita pro klienty MacOS – Personal Firewall, Device control, autoupgrade
- Možnost aplikování bezpečnostních politik i v offline režimu na základě definovaných podmínek
- Ochrana proti pokročilým hrozbám (APT) a 0-day zranitelnostem
- Podpora automatického vytváření dump souborů na stanici na základě nálezů
- Okamžité blokování/mazání napadených souborů na stanici (s možností stažení administrátorem k další analýze)
- Duální aktualizační profil pro možnost stahování aktualizací z mirroru v lokální síti a zároveň vzdálených serverů při nedostupnosti lokálního mirroru (pro cestující uživatele s notebooky).
- Možnost definovat webové stránky, které se spustí v chráněném režimu prohlížeče, pro bezpečnou práci s kritickými systémy nebo internetovým bankovnictví
- Aktivní ochrany před útoky hrubou silou na protokol SMB a RDP
- Možnost zablokování konkrétní IP adresy po sérii neúspěšných pokusů o přihlášení pro protokoly SMB a RDP s možností výjimek ve vnitřních sítích
- Automatické aktualizace bezpečnostního softwaru s možností odložení restartu stanice.
- „Zmražení“ na požadované verzi – produkt je možné nakonfigurovat tak, aby nedocházelo k automatickému povyšování majoritních a minoritních verzí zejména na stanicích, kde se vyžaduje vysoká stabilita

2. Integrovaná cloudová analýza neznámých vzorků

- Funkce cloudového sandboxu je integrována do produktu pro koncové a serverové zařízení, tzn. Cloudový sandbox nemá vlastního agenta, nevyžaduje instalaci další komponenty ať už v rámci produktu nebo implementace HW prvku do sítě
- Sandbox umožňující spuštění vzorků malwaru pro:
    - Windows,
    - Linux
- Možnost využití na koncových bodech a serverech pro aktivní detekci škodlivých souborů
- Analýza neznámých vzorků v řádu jednotek minut.
- Optimalizace pro znemožnění obejití anti-sandbox mechanismy.

- Schopnost analýzy rootkitů a ransomwaru.
- Schopnost detekce a zastavení zneužití nebo pokusu o zneužití zero day zranitelnosti.
- Řešení pracuje s behaviorální analýzou.
- Kompletní výsledek o zanalyzovaném souboru včetně informace o nalezeném i nenalezeném škodlivém chování daného souboru
- Manuální odeslání vzorku do sandboxu.
- Možnost proaktivní ochrany, kdy je potenciální hrozba blokována, dokud není znám výsledek analýzy ze sandboxu.
- Neomezené množství odesílaných souborů.
- Veškerá komunikace probíhá šifrovaným kanálem.
- Okamžité odstranění souboru po dokončení analýzy v cloudovém sandboxu
- Možnost volby, jaké kategorie souborů do cloudového sandboxu budou odcházet (spustitelné soubory, archivy, skripty, pravděpodobný spam, dokumenty atp.)
- Velikost odeslaných souborů do cloudového sandboxu může dosahovat až 64MB.
- Výsledky analyzovaných souborů jsou dostupné a automatizovaně distribuované všem serverům a stanicím napříč organizací, tak aby nedocházelo k duplicitnímu testování

3. Šifrování celých disků

- Podpora platforem Windows a MacOS
- Správa skrze centrální management
- Unikátní technologie pro platformu Windows (je požadováno šifrování disků, avšak bez využití BitLocker)
- Podpora Pre-Boot autentizace
- Podpora TPM modulu
- Podpora Opal samošifrovacích disků
- Možnost definovat počet chybně zadaných pokusů
- Možnost definovat složitost a délku autentizačního hesla
- Možnost omezit platnost autentizačního hesla
- Podpora okamžitého smazání šifrovacího klíče a následné uzamčení počítače
- Recovery z centrální konzole

4. EDR řešení

- Možnost provozu centrálního serveru on-premise na platformě Windows Server
- Webová konzole pro správu a vyhodnocení
- Možnost provozu s databázemi:
  
- Možnost provozu v offline prostředí
- Autonomní chování se schopností vyhodnotit podezřelou/ škodlivou aktivitu a zareagovat na ni i bez aktuálně dostupného řídícího serveru nebo internetového připojení
- Logování činností administrátora (Audit Log)
- Podpora EDR pro systémy Windows, Windows server, MacOS a Linux
- Možnost autentizace do managementu EDR pomocí 2FA
- Možnost řízení managementu EDR prostřednictvím API, a to jak pro:
  - Přijímání informací z EDR serverů
  - Zasílání příkazů na EDR servery
- Integrovaný nástroj v EDR řešení pro vzdálené zasílání příkazů přímo z konzole

- Možnost izolace zařízení od sítě
- Možnost tvorby vlastních IoC.
- Možnost škálování množství historických dat vyhodnocených v EDR,
    - až 3 měsíce pro raw-data,
    - 3 roky pro detekované incidenty.
- „učící režim“ pro automatizované vytváření výjimek k detekčním pravidlům
- Indikátory útoku pracující s behaviorální detekcí.
- Indikátory útoku pracující s reputací.
- Řešení umožnuje analýzu vektorů útoku.
- Schopnost detekce:
    - škodlivých spustitelných souborů
        - skriptů,
        - exploitů,
        - rootkitů,
        - síťových útoků,
        - zneužití WMI nástrojů,
        - bezsouborového malwaru
        - škodlivých systémových ovladačů / kernel modulů.
    - Pokusů o dump přihlašovacích údajů uživatele
- Schopnost detekovat laterální pohyb útočníka.
- Analýza procesů, veškerých spustitelných souborů a DLL knihoven.
- Náhled na spuštěné skripty použité při detekované události
- Možnost zabezpečeného vzdáleného spojení přes servery výrobce do konzole EDR
- Schopnost automatizovaného response úkonu pro jednotlivá detekční pravidla v podobě:
    - izolace stanice,
    - blokace hash souboru,
    - blokace a vyčištění sítě od konkrétního souboru,
    - ukončení procesu,
    - restart počítače,
    - vypnutí počítače.
- Automatického vyřešení incidentu administrátorem
- Prioritizace vzniklých incidentů.
- Možnost stažení spustitelných souborů ze stanic pro bližší analýzu ve formátu archivu opatřeným heslem
- Integrace a zobrazení detekcí provedených antimalware produktem.
- Řešení je schopno generovat tzv. forest / full execution tree model.
- Vyhledávání pomocí nově vytvořených IoC nad historickými daty.
- Provázání s technikami popsanými v knowledge base MITRE ATT&CK (https://attack.mitre.org).
- Integrovaný vyhledávač VirusTotal s možnost rozšíření o vlastní vyhledávače

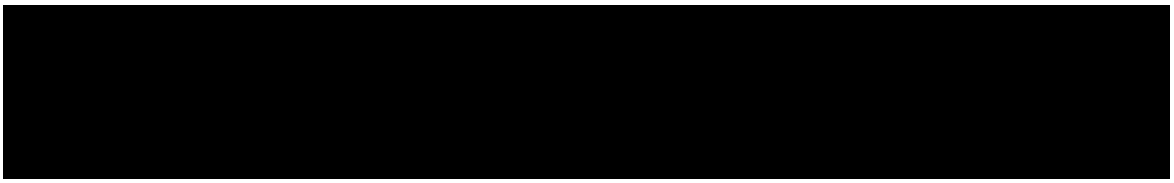
5. Management konzole pro správu všech řešení v rámci nabízeného balíku

- Webová konzole.
- Možnost instalace na Windows i Linux.
- Předpřipravená virtual appliance pro virtuální prostředí VMware, Microsoft Hyper-V a Microsoft Azure, Oracle Virtual Box.

Příloha č. 1 – technická specifikace

- Server/proxy architektura pro síťovou pružnost – snížení zátěže při stahování aktualizací detekčních modulů výrobce.
- Možnost probuzení klientů pomocí Wake On Lan.
- Vzdálené vypnutí, restart počítače nebo odhlášení všech uživatelů
- Možnost konfigurace virtual appliance přes uživatelsky přívětivé webové rozhraní Webmin.
- Nezávislí management agent pro platformy Windows, Linux a MacOS
- Management agent pro architektury na platformy Windows a MacOS:
    - x86,
    - x64,
    - ARM64
- Nezávislý agent (pracuje i offline) vzdálené správy pro zajištění komunikace a ovládání operačního systému klienta
- Offline uplatňování politik a spouštění úloh při výskytu definované události (například: odpojení od sítě při nalezení škodlivého kódu).
- Administrace v nejpoužívanějších jazycích včetně češtiny
- Široké možnosti konfigurace oprávnění administrátorů (například možnost správy pouze části infrastruktury, které konkrétnímu administrátorovi podléhá).
- Zabezpečení přístupu administrátorů do vzdálené správy pomocí 2FA.
- Podpora štítků/tagování pro snazší správu a vyhledávání
- Správa karantény s možností vzdáleného vymazání / obnovení / obnovení a vyloučení objektu z detekce.
- Vzdálené získání zachyceného škodlivého souboru z klienta.
- Detekce nespravovaných (rizikových) počítačů komunikujících na síti.
- Podpora pro instalace a odinstalace aplikací 3. stran.
- Vyčítání informací o verzích softwaru 3. stran.
- Možnost vyčítat informace o hardwaru na spravovaných zařízeních (CPU, RAM, diskové jednotky, grafické karty…).
- Možnost vyčíst sériové číslo zařízení
- Možnost vyčíst volné místo na disku
- Detekce aktivního šifrování BitLocker na spravované stanici
- Zobrazení časové informace o posledním bootu stanice
- Odeslání zprávy na počítač / mobilní zařízení, které se následně zobrazí uživateli na obrazovce.
- Vzdálená odinstalace antivirového řešení 3. strany.
- Vzdálené spuštění jakéhokoli příkazu na cílové stanici pomocí Příkazového řádku.
- Dynamické skupiny pro možnost definování podmínek, za kterých dojde k automatickému zařazení klienta do požadované skupiny a automatickému uplatnění klientské úlohy
- Automatické zasílání upozornění při dosažení definovaného počtu nebo procent ovlivněných klientů (například: 5 % všech počítačů / 50 klientů hlásí problémy).
- Podpora SNMP Trap, Syslogu a qRadar SIEM.
- Podpora formátů pro Syslog zprávy:
    - CEF
    - JSON
    - LEEF
- Podpora instalace skriptem - *.bat, *.sh, *.ini (GPO, SSCM…).
- Rychlé připojení na klienta pomocí RDP z konzole pro vzdálenou správu.

- Reportování stavu klientů chráněných jinými bezpečnostními programy.
- Schopnost zaslat reporty a upozornění na e-mail.
- Konzole podporuje multidoménové prostředí (schopnost pracovat s více AD strukturami)
- Konzole podporuje multitenantní prostředí (schopnost v jedné konzoli spravovat více počítačových struktur)
- Podpora VDI prostředí (podpora alespoň Citrix, VMware, SCCM)
- Podpora klonovaní počítačů za pomocí golden image
- Podpora instancích klonů
- Podpora obnovy identity počítače pro VDI prostředí na základě FQDN
- Možnost definovat vícero jmenných vzorů klonovaných počítačů pro VDI prostředí
- Přidání zařízení do vzdálené správy pomocí:
    - synchronizace s Active Directory,
    - ruční přidání pomocí dle IP adresy nebo názvu zařízení,
    - pomocí síťového skenu nechráněných zařízení v síti.
    - Import skrze csv soubor



2 Web aplikační firewall (AWAF)

[redacted]

Web aplikační firewall (AWAF) umožňuje ochranu webových aplikací (veškeré aplikace založené na http/https protokolu) před hrozbami zneužívající protokoly http/https/xml/json aj. Chránit nejen proti deseti nejčastějším hrozbám webu, jak je vyhodnotila skupina OWASP, ale je schopen ochránit i logiku aplikace (aplikační zranitelnost a útok typu zero-day) Špičkové obranné mechanismy proti DDoS na vrstvě 7, detekční a zmírňující metody, virtuální patchování a detailní informace o útocích zabraňují i těm nejsofistikovanějším hrozbám dostat se do vašich serverů.

Pomocí produktu AWAF také můžete zajistit soulad s klíčovými zákonnými normami, jako je HIPAA nebo PCI DSS.

S AWAF získávají organizace flexibilitu potřebnou k tomu, aby mohly implementovat služby WAF (Web Application Firewall) v těsné blízkosti daných aplikací. Tedy chránit aplikace tam, kde se provozují. V datových centrech, rámci virtuálního softwarově definovaného datového centra (SDDC), v prostředí privátního či veřejného cloudu.

Požadovaná funkcionalita/vlastnost
Zařízení dostupné ve formě virtuální edice pro [redacted]
Datová propustnost zařízení alespoň 1 Gbps či více na L4 a L7 [redacted]
Minimální propustnost HTTP požadavků: 180k za sekundu [redacted]
Minimální pocet novych L4 spojeni: 60k za sekundu [redacted]
Počet současných L4 spojení: 2M [redacted]
Počet SSL transakcí za sekundu min. 900 (při použití 2K klíče) [redacted]
Počet SSL transakcí za sekundu min. 5k (při použití ECC klíče) [redacted]
Počet současných SSL spojení min. 200k [redacted]
Propustnost SSL spojení (Bulk Encryption) RSA/ECC min. 820Mbps [redacted]
Plnohodnotná proxy architektura
Podpora NAT/SNAT/PAT
Podpora IPv6, IPv4/IPv6 gateway
Podpora IPSEC IKE v2
Podpora redundance dvou a více zařízení v režimech Active-Active/Active-Standby/N+1 s možností automatické i manuální synchronizacie konfigurace
Podpora IP směrování
Správa přes GUI a plnohodnotné CLI (SSH přístup s možností ověření uživatele heslem a certifikátem/klíčem) s ověřováním uživatelů a oprávnění proti externím službám (RADIUS/TACACS+, LDAP, AD, atd.)
Možnost přidat vlastní funkce pomocí skriptování – umožnění plnohodnotné manipulace a správy veškerého aplikačního provozu s cílem zachytit, zkontrolovat, transformovat a nasměrovat příchozí nebo odchozí provoz pomocí skriptovacího jazyka.
Možnost používat Node.js k úpravě a správě provozu
Podpora RBAC – různé uživatelské role
Podpora tvorby heterogenního clusteru (různé SW virtuální edice nebo kombinace SW edice a HW platformy)

Příloha č. 1 – technická specifikace

Možnost aktivovat následující funkce na jedné HW platformě: • L4-7 loadbalancing
Podpora filtrování paketů
Podpora QoS – markování, rate – limiting
TCP optimalizace síťových flows např. při přístupu k aplikaci z mobilu pomocí výrobcem dodaných, nebo vlastních profilů
Ukončení šifrovaného provozu SSL TLS 1.2 TLS 1.3
Dvoucestná SSL autentizace – serverový, klientský certifikát
Podpora SSL certifikátů s elektronickým podpisem dle standardu SHA-2 s podporou TLS
Podpora ECC a RSA certifikátů
Podpora minimálně těchto šifrovacích algoritmů: AES 256, SHA256, RSA klíče min. o velikosti 4096bit
Podpora validace intermediate certifikátu
Práce s CRL a jeho automatická obnova
Podpora vysokorychlostního granulárního logování / logování per aplikace na externí logovací systém
Možnost odeslání elektronické zprávy (e-mail) určené osobě při vzniku sledované události.
Podpora otevřeného API pro konfiguraci a automatizaci pro nástroje třetích stran
Podpora SW utilit na troubleshooting např. tcpdump
Podpora různých typů balančních metod (minimálně) • Kruhová metoda • Kruhová metoda s vážením
Zajištění “session persistence” na základě IP adresy, HTTP cookie, HTTP host
Podpora různých typů health monitoringu (min)– ICMP, HTTP/HTTPS.
Monitorování stavu a zátěže zdrojů/serverů: • Kontinuální monitorování nejen cílových serverů, ale i všech souvisejících aplikačních komponent • Možnost kombinace (AND/M of N) více metod (např., ICMP, HTTP, TCP port) • Možnost definování intervalu pro monitorování (samostatný interval pro oba stavy UP/DOWN)
Podpora modifikace provozu • Vložení/přepsání cookie • Vložení/přepsání http hlavičky • Modifikace URL • Možnost vložit zdrojovou IP do L7 hlavičky (XFF) • Modifikace http/html obsahu
Použití existující aplikační cookie k zajištění persistence spojení na server
Možnost směrovat požadavky z určitého subnetu jen na určité servery
Možnost mít v poolu nadefinované hot-standby servery ve skupinách s různou prioritou
Podpora cachování a komprese HTTP per služba
Podpora HTTP/2 směrem k uživateli i k serveru
SSL Session a SSL Connection mirroring napříč vícero uzly ADC
Podpora monitoringu o počtu připojených spojení, stavu poskytovaných služeb a připojených systémů
Podpora monitoringu per specifická služba
Podpora logování per aplikace na syslog server

Příloha č. 1 – technická specifikace

Webový aplikační firewall musí zajistit ochranu proti TOP 10 zranitelnostem dle metodiky OWASP dle https://owasp.org/www-project-top-ten/ včetně podpory pro AJAX/JSON XML/SOAP
Webový aplikační firewall s implementovaným negativním i positivním bezpečnostním modelem
Webový aplikační firewall s integrovaným XML firewallem
Zařízení musí podporovat logování přístupů k webovým službám
Základní aplikační firewall pro protokoly FTP a SMTP
Možnost konfigurace Webového aplikačního firewallu za využití učícího se módu
Automatické nahrávání a aplikování nových signatur od výrobce
Automatická korelace zranitelností do jednoho incidentu
Možnost vynucení vytvoření bezpečnostních politik způsobem hierarchie nadřízené a podřízené politiky.
Validace aplikačních flow pro webové aplikace
Validace log-on parametrů, ochrana přihlašovací stránky proti brutforce attack, ochrana vstupních polí jméno/heslo šifrováním na straně klienta bez nutnosti zásahu do aplikace
Podpora CAPTCHA
Detekce aktivity klávesnice a myši (rozlišení člověk/robot)
Možnost propojení WAF s externími skenery zranitelností webových aplikací pro automatickou tvorbu/úpravu bezpečnostních politik alespoň jeden z: • Cenzic Hailstorm • WhiteHat Sentinel • IBM Rational AppScan • QualysGuard Web Application Scanning
Možnost integrace s externí platformou [redacted]
Ochrana proti Session Highjackingu pomocí jednoznačné identifikace prohlížeče uživatele a v případě vyhodnocení rizika vynucení provedení nějakého úkolu dle vlastností prohlížeče (“challenge”).
Podpora standardu PCI DSS a možnost vytváření PCI reportů
Podpora PCI DSS 3.2
Podpora maskování/odstranění citlivých informací jako např. čísla kreditních karet
Filtrování WebSocket provozu
Podpora externí antivirové kontroly pomocí ICAP
DoS a DDoS detekce a ochrana na L7
Ochrana proti DDoS pomocí detekce stresu chráněné aplikace – zpoždění odpovědi a následné omezení počtu requestu, Captcha, TCP reset a podobně
Rozpoznání legitimního provozu na silně vytížených URL, odlišení od DoS nebo DDoS útoku a tím zamezení blokování legitimních uživatelů.
Automatické nebo ruční „blacklistování“ IP adres, které se opakovaně snaží překonat zabezpečení ochranu, nebo se vyznačují vysokou mírou nežádoucího provozu
Podpora nastavení konkrétních bezpečnostních politik podle IP adresy, doménového jména a URI
Podpora maskování/odstranění citlivých informací – čísla kreditních karet, aj. pomocí vlastních regulárních výrazů
Podpora visibility a reportingu per http request/response
Blokování útočníků podle geolokace
Automatické odlišení skutečných uživatelů od botnetů

Příloha č. 1 – technická specifikace

Možnost definovat bezpečnostní politiku WAF na základě kategorie Botu
Ochrana proti automatizovanému provozu/útokům (BotNetům) nejen pomocí signatur, ale také pomocí aktivního zjišťování, zda se jedná o browser vs. Bot (pomocí tzv. „challenge“, neboli úkolů, díky kterým WAF identifikuje Bot vs Uživatel), pokud umí bot simulovat chování skutečného prohlížeče a zamezení propuštění takové komunikace na aplikační server.
Průběžná analýza stresu aplikace, analýza nestandardního chování tzv. behaviorální analýzy a vylaďování ochrany aplikace za pomocí uplatňování dynamických signatur. WAF mapuje a zaznamenává standardní chování uživatelů vrámci aplikace. V případě zjištění odchylky se dynamicky vygeneruje signatura založená na těchto odchylkách, která jednoznačně identifikuje zdroje škodlivého provozu, který může být zablokován nebo zpomalen.
Ochrana proti Credential Stuffingu. Jedná se o rozšíření ochrany proti Bruteforce útokům, při kterých dochází k rozpoznání, že zadávaná uživatelská jména a hesla jsou součástí známých databází kompromitovaných identit a dojde k zablokování takových požadavků nebo notifikaci administrátora systému. Kompromitované identity, se kterými jsou požadavky na přístup k aplikaci porovnávány, jsou uloženy ve formě hashované a pravidelně aktualizované databáze v paměti web aplikačního FW.
Ochrana proti útoku typu Session Highjacking pomocí jednoznačné identifikace prohlížeče uživatele („fingerprintu“ webového prohlížeče).
Ochrana dat a přihlašovacích údajů proti malware během zadávání do citlivých polí formuláře na webové aplikaci šifrováním dat na aplikační vrstvě na straně klienta, jenž následně dekryptuje pouze WAF.
Ochrana proti útočným kampaním. Nejedná se o popis samotné zranitelnosti pomocí signatury WAF, ale schopnost detekovat probíhající útok konkrétní útočné skupiny s cílem zneužít známé zranitelnosti/exploitu, která je popsána ve známém CVE. Ochrana proti takovým útočným kampaním je realizována díky aktualizaci definicí aktuálních útoků, které jsou detekovány v globálním měřítku a v reálném čase přenášeny do WAF. Tak se maximalizuje ochrana aplikace v reálném čase a uspoří se také kapacita zařízení.
Podpora využití CI/CD pipeline pro nasazování security politik WAF na webových aplikacích
Podpora importu souboru Swagger pro definici security politiky pro ochranu API
Podpora importu souborů OpenAPI 3.0 za účelem vytvoření komplexní politiky WAF
Podpora mikroslužeb ve WAF politikách
Podpora integrace s nástroji chatu (Slack / Teams…) a hlášení stavu systému a logování pomocí těchto nástrojů

3 Wi-fi AP

[redacted]

Požadujeme Enterprise AP s pokročilým managementem a možností analýzy provozu, včetně řízení datového provozu aplikací a jeho kontroly – toto musí být v integrováno přímo v AP. Dále samo AP musí umět tunelovat veškerý provoz na centrální kontroler. Z důvodu budoucí implementace navazujících projektů požadujeme, aby AP mělo zabudovanou podporu technologie BT, ZigBee, IoT.

[redacted]

Požadavek na funkcionalitu	Minimální požadavek	Splňuje ANO/NE (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)
Třída zařízení: indoor přístupový bod	ANO	ANO
Uzavřená konstrukce bez ventilátorů	ANO	ANO
Podpora bezdrátových standardů: 802.11a/b/g/n, 802.11ac, 802.11ax	ANO	ANO
Plnohodnotná certifikace Wi-Fi Aliance: IEEE 802.11a/b/g/n/ac/ax	ANO	ANO
Plnohodnotná certifikace Wi-Fi Aliance: WPA3-CNSA, WPA3-SAE, WPA3-OWE	ANO	ANO
Pracovní režim AP bez kontroléru (autonomní)	ANO	ANO
Pracovní režim AP řízené kontrolérem (lightweight)	ANO	ANO
Pracovní režim AP v roli kontroléru s možností správy až 120 AP	ANO	ANO
Minimální počet portů ethernet LAN 10/100/1000 Mbps	1x GE RJ45	ANO
Podpora standardu IEEE 802.3af (PoE)	ANO	ANO
Podpora standardního PoE 15,4W bez nutnosti redukce výkonu 5GHz rádia	ANO	ANO
Podpora napájení z AC napájecího zdroje	ANO	ANO
Vestavěná interní anténa MIMO, omni down-tilt	ANO	ANO
Radiová část: dual band, současná podpora pásem 2,4GHz a 5GHz	ANO	ANO
MIMO a počet nezávislých streamů na 2,4GHz rádio: 2x2:2	ANO	ANO
MIMO a počet nezávislých streamů na 5GHz rádio: 2x2:2	ANO	ANO
Podpora šířky kanálu 80 MHz	ANO	ANO
HW podpora OFDMA	ANO	ANO
Automatické ladění kanálu a síly signálu v koordinaci s ostatními AP	ANO	ANO

Příloha č. 1 – technická specifikace

Možnost nastavení vysílacího výkonu s krokem 0.5 dBm	ANO	ANO
Minimální komunikační rychlost na fyzické vrstvě (Max data rate) pro 5GHz: 1200 Mbps	ANO	ANO
Integrovaný TPM pro bezpečné uložení certifikátů a klíčů	ANO	ANO
Podpora 802.11ac explicitního beamformingu	ANO	ANO
Podpora airtime fairness	ANO	ANO
Prioritizace jednotlivých SSID na základě vysílacího času	ANO	ANO
Vypínatelné indikační LED diody informující o stavu zařízení	ANO	ANO
Band Steering či obdobné (prioritizace 5GHz pásma v případě je-li podporováno)	ANO	ANO
Detekce Rogue AP	ANO	ANO
Minimální počet inzerovaných SSID (BSSID) na radio: 16	ANO	ANO
Nastavitelný DTIM interval pro jednotlivé SSID	ANO	ANO
Mapování SSID do různých VLAN podle IEEE 802.1Q	ANO	ANO
VLAN Pooling	ANO	ANO
Podpora wireless MESH funkcionality s protokolem pro optimální výběr cesty v rámci MESH stromu	ANO	ANO
Podpora Layer-2 izolace bezdrátových klientů	ANO	ANO
Podpora spektrální analýzy v pásmech 2,4GHz a 5GHz	ANO	ANO
Hardware filtry pro filtraci intermodulačního rušením pocházejícím z mobilních sítí (Advanced Cellular Coexistence nebo obdobné)	ANO	ANO
Detekce a monitorování problémů WLAN odchytáváním provozu na AP ve formátu PCAP a jeho zasíláním do Ethernetového analyzátoru, schopnost zachytávat rámce včetně 802.11 hlaviček	ANO	ANO
DHCP server, směrování a NAT pro bezdrátové klienty	ANO	ANO
AP v režimu IPSec VPN klient s možností tvorby L2 či L3 VPN	ANO	ANO
Automatická identifikace připojeného zařízení a jeho operačního systému	ANO	ANO
Předávání konektivity mezi AP při pohybu bez výpadku spojení – roaming	ANO	ANO
Dynamické vyvažování zátěže klientů mezi AP se zohledněním zátěže, počtu klientů, síly signálu v koordinaci s ostatními AP	ANO	ANO
Optimalizace provozu: multicast-to-unicast konverze	ANO	ANO
Možnost řízení QoS (šířky pásma) na základě aplikací (Office 365, Dropbox, Facebook, P2P sdílení, VoIP, video aplikace)	ANO	ANO
Filtrování přístupu na web	ANO	ANO
Podpora RadSec (RADIUS over TLS)	ANO	ANO
802.11w ochrana management rámců	ANO	ANO
Podpora Kensington lock	ANO	ANO
Podpora MAC ověřování a 802.1X ověřování s využitím lokální DB v AP	ANO	ANO
Podpora 802.1X suplicant, AP se ověřuje před připojením do LAN	ANO	ANO
Volitelně možnost spravovat AP cloud management nástrojem	ANO	ANO
CLI formou USB serial konsole port	ANO	ANO
SSHv2, SNMPv2c a SNMPv3	ANO	ANO
AP podporuje zero touch provisioning pomocí externího management SW jehož IP adresu získá z cloud aktivační služby poskytované výrobcem	ANO	ANO

Příloha č. 1 – technická specifikace

Součástí AP je příslušenství pro montáž na zeď nebo strop	ANO	ANO

[redacted]

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)
Třída zařízení: indoor přístupový bod	ANO	ANO
Uzavřená konstrukce bez ventilátorů	ANO	ANO
Podpora bezdrátových standardů: 802.11a/b/g/n, 802.11ac wave2, 802.11ax (Wifi 6)	ANO	ANO
Plnohodnotná certifikace Wi-Fi Aliance: IEEE 802.11a/b/g/n/ac	ANO	ANO
Plnohodnotná certifikace Wi-Fi Aliance: WPA3-CNSA, WPA3-SAE, WPA3-OWE	ANO	ANO
Pracovní režim AP bez kontroléru (autonomní)	ANO	ANO
Pracovní režim AP řízené kontrolérem (lightweight)	ANO	ANO
Pracovní režim AP v roli kontroléru s možností správy až 120 AP	ANO	ANO
Minimální počet portů ethernet LAN: 1x 100/1000 Mbit/s RJ45	ANO	ANO
Podpora standardů IEEE 802.3af (PoE) a IEEE 802.3at (PoE+)	ANO	ANO
Podpora standardního PoE 15,4W bez nutnosti redukce výkonu 5GHz rádia	ANO	ANO
Podpora napájení z AC napájecího zdroje	ANO	ANO
Vestavěná interní anténa MIMO, omni down-tilt	ANO	ANO
Radiová část: dual band, současná podpora pásem 2,4GHz a 5GHz	ANO	ANO
MIMO a počet nezávislých streamů na 2,4GHz rádio: 2x2:2	ANO	ANO
MIMO a počet nezávislých streamů na 5GHz rádio: 4x4:4	ANO	ANO

Příloha č. 1 – technická specifikace

Podpora DL-OFDMA, UL-OFDMA a DL-MU-MIMO	ANO	ANO
Automatické ladění kanálu a síly signálu v koordinaci s ostatními AP	ANO	ANO
Možnost nastavení vysílacího výkonu s krokem 0.5 dBm	ANO	ANO
Minimální komunikační rychlost na fyzické vrstvě (Max data rate) pro 5GHz: 4800 Mbps	ANO	ANO
Minimální komunikační rychlost na fyzické vrstvě (Max data rate) pro 2.4GHz: 300 Mbps	ANO	ANO
Integrovaný TPM pro bezpečné uložení certifikátů a klíčů	ANO	ANO
Podpora 802.11ac explicitního beamformingu	ANO	ANO
Podpora airtime fairness	ANO	ANO
Prioritizace jednotlivých SSID na základě vysílacího času	ANO	ANO
USB port s podporou 3G/4G USB modemu jako WAN uplink	ANO	ANO
Vypínatelné indikační LED diody informující o stavu zařízení	ANO	ANO
Band Steering či obdobné (prioritizace 5GHz pásma v případě je-li podporováno)	ANO	ANO
Detekce Rogue AP	ANO	ANO
Minimální počet inzerovaných SSID (BSSID) na radio: 16	ANO	ANO
Nastavitelný DTIM interval pro jednotlivé SSID	ANO	ANO
Mapování SSID do různých VLAN podle IEEE 802.1Q	ANO	ANO
VLAN Pooling	ANO	ANO
HW Podpora wireless MESH funkcionality s protokolem pro optimální výběr cesty v rámci MESH stromu	ANO	ANO
Podpora Layer-2 izolace bezdrátových klientů	ANO	ANO
HW Podpora spektrální analýzy v pásmech 2,4GHz a 5GHz	ANO	ANO
Hardware filtry pro filtraci intermodulačního rušením pocházejícím z mobilních sítí (Advanced Cellular Coexistence nebo obdobné)	ANO	ANO
Detekce a monitorování problémů WLAN odchytáváním provozu na AP ve formátu PCAP a jeho zasíláním do Ethernetového analyzátoru, schopnost zachytávat rámce včetně 802.11 hlaviček	ANO	ANO
DHCP server, směrování a NAT pro bezdrátové klienty	ANO	ANO
AP v režimu IPSec VPN klient s možností tvorby L2 či L3 VPN	ANO	ANO
Automatická identifikace připojeného zařízení a jeho operačního systému	ANO	ANO

Předávání konektivity mezi AP při pohybu bez výpadku spojení – roaming	ANO	ANO
Dynamické vyvažování zátěže klientů mezi AP se zohledněním zátěže, počtu klientů, síly signálu v koordinaci s ostatními AP	ANO	ANO
Optimalizace provozu: multicast-to-unicast konverze	ANO	ANO
Možnost řízení QoS (šířky pásma) na základě aplikací (Office 365, Dropbox, Facebook, P2P sdílení, VoIP, video aplikace)	ANO	ANO
Filtrování přístupu na web	ANO	ANO
Podpora RadSec (RADIUS over TLS)	ANO	ANO
802.11w ochrana management rámců	ANO	ANO
Podpora Kensington lock	ANO	ANO
Podpora MAC ověřování a 802.1X ověřování s využitím lokální DB v AP	ANO	ANO
Podpora 802.1X suplicant, AP se ověřuje před připojením do LAN	ANO	ANO
Volitelně možnost spravovat AP cloud management nástrojem	ANO	ANO
CLI formou serial konsole port a serial over bluetooth	ANO	ANO
SSHv2, SNMPv2c a SNMPv3	ANO	ANO
AP podporuje zero touch provisioning pomocí externího management SW jehož IP adresu získá z cloud aktivační služby poskytované výrobcem	ANO	ANO
Integrované Bluetooth 5.0 Low Energy (BLE) rádio	ANO	ANO
Integrované Zigbee 802.15.4 rádio	ANO	ANO
Podpora režimu SLEEP s max. spotřebou energie do 6W	ANO	ANO
Součástí AP je příslušenství pro montáž na zeď nebo strop	ANO	ANO

Ostatní podmínky:

- Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství).
- Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů.
- Je požadována záruka na hardware [redacted]. Tato záruka musí být garantovaná výrobcem zařízení.
- **Dodavatel je povinen doložit oficiální potvrzení lokálního zastoupení výrobce o všech dodávaných zařízeních pro český trh**; dodavatel doloží tuto skutečnost do nabídky; lze nahradit formou čestného prohlášení dodavatele.

[redacted]

Příloha č. 1 – technická specifikace

[redacted]

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)
Třída zařízení	kontrolér bezdrátové sítě	ANO
Virtuální appliance bez nutnosti dodatečných licencí např. pro OS nebo databáze	ANO	ANO
Podporované hypervisory: VMware, Hyper-V, KVM	ANO	ANO
Počet síťových rozhraní	1x 1000 Mbit/s	ANO
Podporovaný počet AP	250	ANO
Možnost rozšíření na 1000 AP v rámci jedné virtuální appliance kontroléru	ANO	ANO
Podporovaný počet současně připojených klientů	800	ANO
Sdílení licencí mezi více kontrolery	ANO	ANO
Podpora redundance (HA) kontrolerů v režimech: active-active a active-standby. Výpadek aktivního kontroleru v redundantním páru nemá dopad na provoz již připojených klientů (tj. bez potřeby opětovné autentizace)	ANO	ANO
Vzdálené lokality - možnost lokálního bridgování uživatelských dat per SSID přímo na příslušném AP, podpora roamingu přes AP na vzdálené lokalitě	ANO	ANO
Podpora VLAN podle IEEE 802.1Q	ano, 4000 aktivních VLAN	ANO
Podpora linkové agregace IEEE 802.3ad	ANO	ANO
IEEE 802.1w - Rapid spanning Tree	ANO	ANO
Podpora STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)	ANO	ANO
Detekce protilehlého zařízení LLDP	ANO	ANO
Statické směrování IPv4 a IPv6	ANO	ANO
Dynamické směrování OSPFv2 včetně podpory STUB a NSSA area	ANO	ANO
Podpora Multicast: IGMP a MLD	ANO	ANO
DHCP server pro IPv4 a IPv6	ANO	ANO
NTP včetně MD5 autentizace pro IPv4 a IPv6	ANO	ANO
Podpora překladu adres PAT/NAT	ANO	ANO
Podpora standardu 802.11ac Wave 2 a zpětná kompatibilita s 802.11a/b/g/n	ANO	ANO

Příloha č. 1 – technická specifikace

Tunelovaní uživatelských dat přes kontrolér včetně 802.11 hlaviček a bez 802.11 hlaviček	ANO	ANO
podpora IPv6: konfigurace, správa (SSH, SNMP, Syslog, DHCPv6,RADIUS), syst. komunikace mezi AP a kontrolérem. Kompatibilita s RFC 2460, RFC 3162, RFC 3736, RFC 6106	ANO	ANO
Typy autentizace: WPA3, WPA/WPA2-PSK, WPA/WPA2-Enterprise, 802.1X, MAC autentizace, “captive portal”, 802.1X ověření s následným ověřením MAC	ANO	ANO
Podporované autentizační/autorizační zdroje: RADIUS, LDAP, Active Directory, RFC 3576 Change of Authorization	ANO	ANO
Funkce řízení a ochrany rádioveho spektra s automatickou optimalizací sítě (přidělováni kanálů, fast roaming, rozdělení klientů na jednotlivá AP)	ANO	ANO
Aktivní scanování 802.11 kanálů pro výběr nejlepšího včetně automatického zastavení scanování v případě že probíhá časově senzitivní provoz (např. VoIP)	ANO	ANO
Klasifikace klientských zařízení do tříd na základě typu nebo OS zařízení a následné uplatnění definovaných politik pro danou třídu	ANO	ANO
Vestavěný “captive portal” pro hosty s podporou nativních IPv6 klientů. s možností úpravy vzhledu a přídáním vlastního loga s, včetně vestavěného rozhraní pro vytváření dočasných guest účtů.	ANO	ANO
Podpor 802.11u - Hotspot 2.0	ANO	ANO
Podpora pro 802.11r, 802.11v a 802.11k	ANO	ANO
Automatické dynamické rozpoznání a prioritizace hlasových protokolů jako SIP, SCCP, VOCERA a SVP pomocí funkce DPI a jejich SLA monitoring	ANO	ANO
Podporované úrovně oprávnění v administračním rozhraní: administrator, read-only, guest-provisoning, nework-operator	ANO	ANO
Podpora XML API pro management wifi klientů z externích zdrojů	ANO	ANO
Automatizovaná migrace klientů na optimální frekvenci, AP či rádio s využitím min. těchto parametrů: kategorie daného klienta, SNR, schopnosti klienta, kvalita signálu	ANO	ANO
Grafický uživatelský dashboard zobrazujicí kvalitu a obsazenost kanálů, jednotlivé klienty, náhledy na VoIP přes WiFi síť a zobrazující informace o MOS (mean opinion score) aktivních hovorů. Možnost realtime analýzy kvality prováděných hovorů	ANO	ANO
Podpora rozpoznáváni aplikací na 7. vrstvě (aplikace typu: Youtube, Facebook, Dropbox, BitTorrent, Skype, Office365, apod.). Možnost jejich povolování, zakazování, prioritizace nebo omezování možnosti vytvořit minimálně 20 souběžných aplikačních pravidel k omezení provozu konkrétních aplikací.	ANO	ANO
Centrální správa, aktualizace, konfigurace vč. bezpečnostních politik a QoS profilů pro všechna AP	ANO	ANO
Blacklist zařízení překračující nastavitelné prahy (opakovaná autentizace, porušení bezpečnostní politiky)	ANO	ANO
Podpora RadSec (RADIUS over TLS)	ANO	ANO
Podpora tvorby bezpečnostnich politik na zakladě časových pravidel.	ANO	ANO
Podpora Bonjour services gateway, zpracování mDNS paketů, možnost filtrování služeb mezi subnety	ANO	ANO
Podpora L2 a L3 roaming bez nutnosti speciálního SW na klientovi	ANO	ANO

Příloha č. 1 – technická specifikace

Podpora bezdrátových MESH sítí s protokolem pro výběr optimální cesty v rámci MESH stromu, podporovaná hloubka min. 8 hopů	ANO	ANO
Podpora Rogue Wireless detekce a containment	ANO	ANO
Podpora PKI	ANO	ANO
Možnost terminace vzdálených VPN klientů (podpora SSL i IPSec VPN)	ANO	ANO
Podpora WIPS pro detekci útoků na bezdrátovou síť	ANO	ANO
Podpora spektrální analýzy	ANO	ANO
Podpora ochrany pomocí IDS signatur	ANO	ANO
Ochrana řídících rámců - 802.11w	ANO	ANO
Podpora optimalizace WAN provozu formou komprese	ANO	ANO
Management	ANO	ANO
Dedikovany Ethernet port pro out-of-band management	ANO	ANO
Dual boot flash	ANO	ANO
Podpora SSHv2 a HTTPS web GUI	ANO	ANO
SNMPv2c, SNMPv3	ANO	ANO
Podpora IPFIX	ANO	ANO
Podpora OpenFlow v 1.3	ANO	ANO
Podpora parsování regulárních výrazů z externího syslogu (např. firewall) a následné reakce na ně.	ANO	ANO
Integrované nástroje na diagnostiku – ping, traceroute, tracepath, AAA test	ANO	ANO
Podpora JSON REST API pro konfiguraci a montoring	ANO	ANO
Podpora hierarchické konfigurace	ANO	ANO
Podpora upgrade firmware pomocí: TFTP, FTP, SCP	ANO	ANO
Plná kompatibilita s nabízenými přístupovými body	ANO	ANO

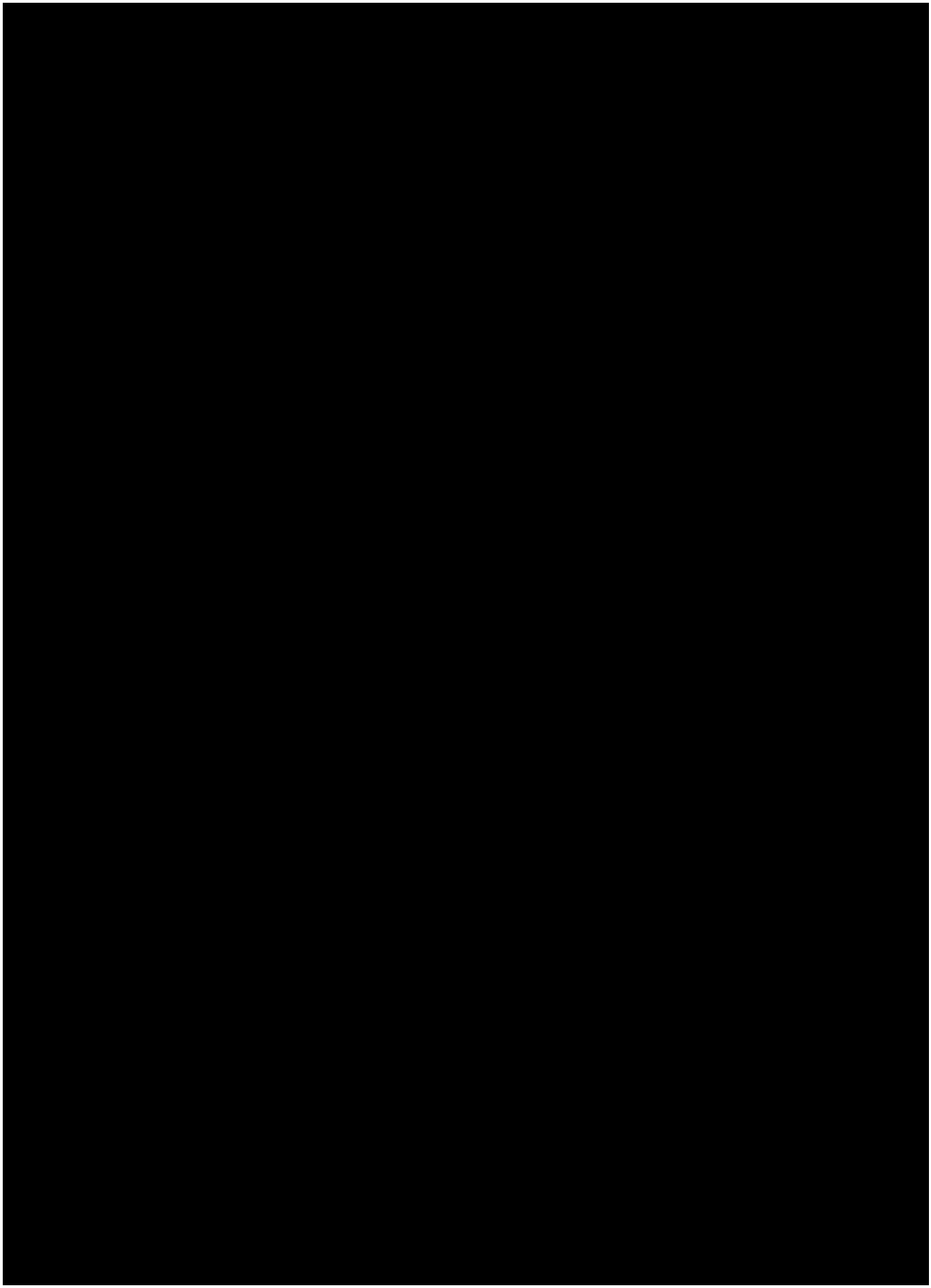
Ostatní podmínky:

- Software musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství)
- Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů.
- Je požadována podpora výrobce s možností otevření servisního požadavku 24x7 [redacted] přímo u výrobce zařízení.
- **Dodavatel je povinen v nabídce doložit oficiální potvrzení lokálního zastoupení výrobce o všech dodávaných zařízeních pro český trh**; lze nahradit formou čestného prohlášení dodavatele.
- Součástí dodávky jsou licence pro AP včetně supportu k nim ve shodné délce a úrovni jako u virtuálního kontroléru.

[redacted]

Přikládáme požadované potvrzení: Dodavatel je povinen doložit oficiální potvrzení lokálního zastoupení výrobce o všech dodávaných zařízeních pro český trh

Příloha č. 1 – technická specifikace



4 Dodávka a implementace systému PIM/PAM

[redacted]

1. Cíle projektu PIM/PAM technologie

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

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

Z hlediska bezpečnosti umožňují téměř neomezený přístup a manipulaci s informačními aktivy organizace, v případě kompromitace privilegovaného účtu je organizace vystavena velkému riziku zneužití nebo vyzrazení informací nebo jejich zneužití.

Požadavek řídit privilegované účty je hlavním požadavkem zákona o kybernetické bezpečnosti (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.

Cílem projektu je řešit:

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

2. Popis poptávaného řešení PIM/PAM technologie

Systém, který bude zajišťovat jednotnou správu a monitoring privilegovaných účtů Zadavatele. Systém bude dodán včetně analýzy stávajícího stavu, dodávky technologie (SW, licence), instalace,

konfigurace, uvedení do provozu, a následné zajištění technické podpory, zajištění záruky výrobce a zajištění dostupnosti softwarových aktualizací, a to na všechny části a komponenty dodaného Systému (SW i licence) [redacted]

[redacted]

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

[redacted]

3. Definice pojmů

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.

4. Požadavky na systémy a protokoly pro řízení hesel a bezpečné přístupy

Podpora musí být zajištěna pro následující typy zařízení:

- Windows 7, 8, 8.1, 10, 11, Windows Server 2012, 2016, 2019, 2022
- Linux Red Hat, Suse, Debian, Centos
- [redacted]
- [redacted]
- Databáze [redacted]
- Zařízení [redacted]

Podpora přihlášení bez nutnosti manuálně vkládat heslo a nahrávání relací pro následující aplikace a protokoly:

- protokoly: RDP, SSH, Telnet
- DB klienti: [redacted]
- Web GUI:Microsoft Edge, Chrome

5. Technické požadavky na PIM/PAM technologii

- Řešení bude poskytovat správcovský přístup na cílový systém prostřednictvím privilegovaných účtů, ke kterým má uživatel přístup dle bezpečnostní politiky. Účty a systémy, ke kterým nemá práva přístupu, nebudou pro uživatele viditelné.
- Řešení bude umožňovat víceúrovňové schvalování správcovských přístupů k cílovým systémům - přístupy lze omezit dle vybraného účtu, nebo na daný časový úsek. Schvalování přístupu lze vynutit odděleně pro přístup přihlašovacím údajům privilegovaného účtu, nebo pro připojení na koncový systém.
- Správcovský přístup na cílový systém bude zprostředkován pomocí jump serveru prostřednictvím zvoleného komunikačního protokolu, aplikace a příslušného privilegovaného účtu tak, aby koncový uživatel neměl přístup k přihlašovacím údajům. Izolace přístupu je možná až na úroveň aplikace (typu webový prohlížeč s konkrétní URL, MMC konzole s vybraným snap-in, konkrétní aplikace zadavatele [redacted]), kdy uživatel nemá možnost přistupovat k jiným službám, aplikacím v rámci dané relace. Po ukončení aplikace se uzavře spojení celé relace. Vzdálené připojení k relaci lze navázat jak přes vlastní GUI dodaného řešení, tak i pomocí standardních protokolů RDP a SSH a standardních klientů typu putty a remote desktop manager. U všech možností připojení ke vzdálené relaci musí být podporováno vynucení silné autentizace (minimálně integrace s LDAP, SAML a RADIUS).
- Řešení musí umožňovat silnou autentizaci přistupujících uživatelů pomocí multifaktorové autentizace - MFA. MFA musí být nedílnou součástí nabídky řešení, může se jednat jak o nativní nástroj PIM/PAM řešení, tak MFA nástroj třetí strany.
- Řešení musí umožňovat monitoring a nahrávání celé relace a aktivit privilegovaných účtů ve video formátu s možností kontextového vyhledávání, bez nutnosti instalace agentů na koncový systém. Záznam relace musí být vytvářen kontinuálně, nikoliv formou screenshotů. V záznamech je možné zpětně vyhledávat využitím metadat, které budou mimo jiné minimálně obsahovat:
    - u RDP relací spuštěné aplikace a události
    - u SSH relací jednotlivé příkazy
    - u Webových aplikací klik na jednotlivé odkazy,
    - u ostatních typů relací alespoň stisky kláves
- Pro přehrávání nahrávek není potřeba instalace nástrojů třetích stran (flash, java, codec, atp.) a je dostupné z GUI dodávaného řešení.
- Řešení umožňuje sledovat aktivní relace dalším uživatelem (například auditorem), který v případě potřeby má možnost sledovanou relaci ukončit.
- Systém umožňuje autorizovanému personálu centrálně vyhledávat v nahrávkách podle data pořízení, uživatele a spuštěného příkazu.
- Přístup k uživatelskému rozhraní je požadovaný přes webový portál s možností ověření přes LDAP/MS Active Directory a druhým faktorem (například LDAP, Radius server, SAML atp.).
- Řešení zaručuje vysokou bezpečnost přenášených a uložených informací (confidentiality, integrity, availability). Uložené informace, včetně nahrávek a spravovaným přihlašovacích údajů, jsou uloženy v jedné centrální a vysoce zabezpečené databázi.
- Řešení zaručuje nezpochybnitelnou auditovatelnost jednotlivých operací, možnosti reportování a textové logy. Auditní záznamy musí být bezpečně uloženy v zašifrované podobě tak, aby k nim měl přístup pouze oprávněný uživatel.
- Veškeré komponenty řešení musí splňovat nároky na vysoké zabezpečení a vynucovat tzv. hardening. Úložiště dat, kde jsou uloženy jednotlivé účty, přihlašovací údaje, nahrávky relací a auditní záznamy, je vysoce zabezpečeno a odděleno od ostatních komponent řešení. Databáze dat je součástí řešení a není nutné využívat nástroje třetích stran. Tento požadavek platí pro veškerá data v rámci řešení - i pro HA a DR.

- Řešení musí být dimenzované minimálně pro [redacted] neomezený počet přihlašovaných uživatelů ([redacted])

6. Analýza a rozsah nasazení

V rámci nasazení systému bude probíhat analýza, která popíše implementaci řešení včetně detailního návrhu harmonogramu realizace plnění.

Obsahem analýzy bude upřesnění instalace, parametrizace, definování workflow, popis realizace integrace s navazujícími systémy provozovanými v prostředí zadavatele.

Výsledkem bude popis způsobu a postup vlastní implementace v prostředí zadavatele v tomto rozsahu:

- Analýza stávajícího stavu privilegovaných účtů v infrastruktuře Zadavatele (servery, aktivní síťové prvky, management systémy, databáze)
- Vytvoření detailní harmonogramu realizace projektu
- Implementace technického řešení v rámci technické specifikace:
  - Dodávka a instalace komponent systému
  - Integrace s Active Directory (LDAP) a Email serverem Zadavatele
  - Nastavení dvoufaktorové autentizace
  - Nastavení politik, workflow, pro PIM/PAM (Nastavení skupin a oprávnění uživatelů a administrátorů PAM, nastavení a přiřazení přístupových politik skupinám uživatelů, nastavení politik hesel podle skupin zařízení).
  - Nastavení nahrávání privilegovaných relací, základní popis práce s relacemi, reporty a další.
  - Návrh zálohování a obnovy (popisem nastavení pravidelného zálohování a obnovou řešení ze záloh DRP).
  - Integrace s operačními systémy serverů provozovaných Zadavatelem:
    - RDP protokol pro Windows platformu
    - SSH protokol pro OS Linux/Unix platformu
    - Vytvoření účtů pro kmenové zaměstnance Zadavatele a přiřazení oprávnění k příslušným serverům.
    - Vytvoření účtů pro externí pracovníky a přiřazení oprávnění k příslušným serverům.
- Testování a ověření funkčnosti řešení:
  - Funkční testy ověří, že implementované řešení poskytuje bezchybně všechny požadované funkcionality uvedené v této Technické specifikaci, včetně požadovaných integrací.
  - Zátěžové testy budou simulovat práci uživatelů při obvyklých činnostech. Tím dojde k prověření vlastností PIM/PAM řešení na produkčním serveru s generovanou zátěží.
  - Akceptační testování bude vykonáno na základě připravených testovacích scénářů.

- Dokumentace
- Zaškolení obsluhy systému

7. Požadavky na licencování

Z pohledu licenční politiky jsou požadovány perpetuální licence s příslušnou maintenance v licenčním modelu.

Privilegovaným uživatelem je ten, který potřebuje účet a pověření s oprávněním ke správě/ administraci privilegovaným oprávněním, aby tak měl možnost vykonávat administraci v jednom nebo více systémech (například hesla databázového serveru, hesla bezpečnostních appliancí, popř. jiné pověření týkající se infrastruktury IT).

Níže uvedené informace popisují základní informace pro zvolení vhodného řešení a licenčního modelu

- Licence není omezena na počet přistupujících uživatelů nebo řízených privilegovaných účtů. Součástí licence je i řešení redundance a taktéž geo-redundance (active-active).
- Cena licence je stanovena pevně na celé období udržitelnosti, a to i pro nákup nových licencí nad rámec vysoutěžené dodávky
- Součástí dodávky musí být také všechny potřebné licence pro operační systémy, databáze a případné další potřebné komponenty systému.

Žádná z nabízených technologií nesmí být v okamžiku podání nabídky označena výrobcem jako končící = nesmí být označeny jako End of Sale nebo End of Support apod.

Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze dodávaného softwaru, funkce zařazené na tzv. roadmapu nebudou akceptovány.

8. Požadovaná dodávka prací (instalace, konfigurace, uvedení do provozu)

Práce	Předpokládaná pracnost v člověkodnech (čd)
1. Analýza stávajícího stavu privilegovaných účtů v infrastruktuře Zadavatele (servery, aktivní síťové prvky, management systémy, databáze) 2. Implementace technického řešení v rámci technické specifikace 3. Testování a ověření funkčnosti řešení 4. Dokumentace	20 čd

5. Zaškolení a podpora startu ostrého provozu v rozsahu min. 2 čd	

9. Podrobné technické požadavky na řešení

[redacted]

[redacted]

Správa privilegovaných přístupů - podrobné technické požadavky na systém			
Oblast	**Požadavky na řešení**	**Splňuje (vyplní účastník v rámci své nabídky ANO/NE; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)**	**Poznámka (doplní účastník tam, kde je relevantní)**
	Funkční požadavky		
Řízení přístupů	Řešení poskytuje nástroj pro správu privilegovaných účtů, řízení přístupu k těmto účtům a monitoring veškerých aktivit privilegovaných účtů. Uživatelské přístupy jsou řízeny bezpečnostní politikou, kdy má vybraný uživatel práva přístupu pouze k definovaným účtům a systémům. Účty a systémy, ke kterým nemá práva přístupu, nejsou pro uživatele viditelné.	ANO	
Striktní oddělení přístupových oprávnění	Systém plně podporuje multi-tenant prostředí. Uživatelé/skupiny uživatelů mají přístup pouze k vybraným účtům, systémům, auditním záznamům, konfiguraci atp. I správce/administrátor řešení má povolen přístup pouze k vybraným složkám a konfiguraci.	ANO	
Víceúrovňové schvalování přístupů	Řešení umožňuje víceúrovňové schvalování správcovských přístupů k cílovým systémům - přístupy lze omezit dle vybraného účtu, nebo na daný časový úsek. Schvalování přístupu lze vynutit odděleně pro přístup přihlašovacím údajům privilegovaného účtu, nebo pro připojení na koncový systém. O nových žádostech, schválení a zamítnutí budou uživatelé upozornění emailem nebo vytvořením ticketu v helpdesk systému.	ANO	

Bezpečnostní parametry	Řešení zaručuje vysokou bezpečnost přenášených a uložených informací (confidentiality, integrity, availability). Uložené informace, včetně nahrávek a spravovaným přihlašovacích údajů, jsou uloženy v jedné centrální a vysoce zabezpečené databázi.	ANO	
Jednotná centrální správa	Správa řešení je umožněna pomocí jednotné centrální správy.	ANO	
Podpora MS Active Directory	Řešení musí podporovat plnou integraci s Microsoft Active Directory na úrovni informací o uživatelích, příslušnosti ke skupinám a emailech. Integrace musí umožňovat mapování rolí v PAM řešení v návaznosti na skupiny v AD.	ANO	
Uživatelské rozhraní	Přístup k uživatelskému rozhraní je požadovaný přes webový portál s možností ověření přes LDAP/MS Active Directory a druhým faktorem (například LDAP, Radius server, SAML).	ANO	
Silná autentizace	Nástroj umožňuje vynutit silnou autentizaci uživatelů pro přístup k uloženým údajům i pro bezpečné vzdálené připojení. Silnou autentizací je míněna minimálně možnost kombinace jméno/heslo + druhý faktor (RADIUS, LDAP, SAML, atp...). Řešení nabízí vlastní MFA nástroj, nebo bude součástí nabídky MFA třetí strany.	ANO	
Šifrování a zabezpečení dat	Řešení musí splňovat standard FIPS 140-2 a šifrovací algoritmy minimálně na úrovni AES-256 a RSA-2048. Řešení umožňuje společnostem splnit compliance požadavky pro ZKB, GDPR, PCI-DSS, SOX, HIPAA, atd.	ANO	
	Password Management		
Řízení hesel a SSH klíčů	Řešení umožňuje automatickou výměnu hesel a SSH klíčů privilegovaných účtů po ukončení relace (jednorázové heslo), nebo v pravidelných intervalech dle bezpečnostní politiky. Rotaci hesla/SSH klíče lze vynutit i správcem PIM/PAM řešení. Hesla a SSH klíče se vyměňují bezagentsky. Řešení musí podporovat změnu přihlašovacích údajů minimálně pro typy systémů viz bod "Podpora řízení hesel a bezpečné přístupy pro systémy", zároveň řešení musí umožňovat tzv. customizaci password management modulu pro další systémy zadavatele.	ANO	
Ukládání hesel	Řešení bezpečně ukládá citlivá data včetně šifrování hesel pomocí AES 256.	ANO	
SSH klíče	Řešení bezpečně spravuje a distribuuje SSH klíče.	ANO	
Rotace hesel a klíčů	Řešení umožňuje automaticky měnit hesla a SSH klíče pro specifické systémy či skupiny účtů.	ANO	
Výjimky v rotaci hesel	Řešení umožňuje definovat výjimky pro zamezení automatických rotací hesel a SSH klíčů u určitých účtů.	ANO	
Časové intervaly rotace hesel	Řešení umožňuje definovat časové intervaly pro provádění automatizovaných změn hesel a SSH klíčů.	ANO	
Rotace hesel po každé relaci	Řešení umožňuje iniciovat změnu hesel a SSH klíčů po každém odhlášení.	ANO	

Komplexita generovaných hesel	Řešení umožňuje definovat komplexitu generovaných hesel dle počtu znaků, využití malých / velkých písmen a speciálních znaků.	ANO	
Rest API	Řešení musí umožňovat změnu hesel pomocí REST API.	ANO	
	Řízení vzdálených relací		
Izolace relací	Správcovský přístup na cílový systém bude zprostředkován pomocí tzv. jump serveru prostřednictvím zvoleného komunikačního protokolu, aplikace a příslušného privilegovaného účtu tak, aby koncový uživatel neměl přístup k přihlašovacím údajům. Izolace přístupu je možná až na úroveň aplikace (typu webový prohlížeč s konkrétní URL, MMC konzole s vybraným snap-in, konkrétní aplikace zadavatele [redacted]), kdy uživatel nemá možnost přistupovat k jiným službám, aplikacím v rámci dané relace. Po ukončení aplikace se uzavře spojení celé relace. Vzdálené připojení k relaci lze navázat jak přes vlastní GUI dodaného řešení, tak i pomocí standardních protokolů RDP a SSH a standardních klientů typu putty a remote desktop manager. U všech možností připojení ke vzdálené relaci musí být podporováno vynucení silné autentizace (minimálně integrace s LDAP, RADIUS nebo SAML).	ANO	
Autentizace privilegovaných uživatelů	Řešení poskytuje různé 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. 2.Autentizace privilegovaného uživatele na monitorovaném systému pomocí statických a bezpečně uložených přihlašovacích údajů. (např. root, admin, privilegovaný lokální účet). 3.Vyzváním uživatele k opětovnému zadání přihlašovacích údajů k monitorovanému systému, bez jejich zaznamenání.	ANO	
Připojení do webových relací	Řešení umožňuje zprostředkovat uživateli bezpečné připojení na vybrané webové aplikace, přístup do cloudu a sociální sítě. PIM/PAM řešení zprostředkuje přihlášení do koncové webové aplikace pomocí silného "privilegovaného" účtu. Uživatel nemusí znát hesla privilegovaných účtů a je mu umožněno transparentní SSO.	ANO	
Nahrávání relací	Řešení musí umožňovat monitoring a nahrávání celé relace a aktivit privilegovaných účtů ve video formátu s možností kontextového vyhledávání, bez nutnosti instalace agentů na koncový systém. Záznam relace musí být vytvářen kontinuálně, nikoliv formou screenshotů. V nahrávkách je možné zpětně vyhledávat v záznamu ve formě metadat - minimálně 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. Pro přehrávání nahrávek není potřeba instalace nástrojů třetích	ANO	

	stran (flash, java, codec, atp...) a je dostupné z GUI dodávaného řešení.		
Možnosti nahrávání relací	Řešení umožňuje aktivaci / deaktivaci zaznamenání relací dle jednotlivých uživatelských skupin.	ANO	
Terminace relací	Řešení nabízí možnost automatické terminace potenciálně nebezpečných relací na základě definovaných procesů, příkazů nebo aplikací, které uživatel spouští na spravovaném systému. Nastavení je možné provádět pro různé uživatele nebo uživatelské skupiny.	ANO	
Možnost sledování relací v reálném čase	Řešení umožňuje sledovat aktivní relace dalším uživatelem (například auditor) a v případě nutnosti ukončit sledovanou relaci.	ANO	
Časové rámce relací	Řešení umožňuje vyžadování schválení relace v určitých časových rámcích- Např. pondělí-pátek, 9:00-16:00 bez potřeby schválení, v jiných časech pouze po schválení.	ANO	
Blokace procesů	Řešení umožňuje blokování vybraných procesů na systémech Windows.	ANO	
Schvalování relací	Nástroj umožňuje schvalování přístupu privilegovaného uživatele k určitým monitorovaným systémům. Schvalování přístupu musí fungovat minimálně v následujícím rozsahu: 1. Privilegovaný uživatel požádá o přístup 2. Definovaní uživatelé obdrží žádost o schválení přístupu. 3. Minimální definovaný počet uživatelů schválí žádost. 4. Privilegovaný uživatel po schvalovacím procesu automaticky získá přístup k monitorovanému systému.	ANO	
Kontrola relací	Systém umožňuje autorizovanému personálu centrálně vyhledávat v nahrávkách podle data, uživatele a spuštěného příkazu.	ANO	
	Audit a reporting		
Zobrazení aktivit uživatele	Systém musí umožňovat audit jednotlivých akcí uživatelů s privilegovanými účty - zobrazení hesla, změny uložených údajů, vytvoření relace.	ANO	
Audit administrátorských akcí	Řešení musí umožňovat zobrazení veškerých aktivit administrátora řešení.	ANO	
Přístup k reportům	Řešení umožňuje nastavení přístupu k reportům pouze pro vybrané uživatele.	ANO	
Export auditních dat	Systém musí umožňovat export auditních záznamů	ANO	
Nezpochybnitelný auditní záznam	Řešení zaručuje nezpochybnitelnou auditovatelnost jednotlivých operací, možnosti reportování a textové logy.	ANO	

Zabezpečení auditních záznamů	Auditní záznamy musí být bezpečně uloženy v zašifrované podobě, tak aby k nim měl přístup pouze oprávněný uživatel.	ANO	
Monitoring pomocí RestAPI	Systém umožňuje monitoring jednotlivých komponent pomocí RestAPI - integrace s monitoring systémy zadavatele.	ANO	
	Integrace a Podporované platformy		
Podpora systémů zadavatele	Řešení musí umožňovat správu pro různé druhy koncových systémů - minimálně v rozsahu viz bod 4: "Požadavky na systémy a protokoly pro řízení hesel“	ANO	
Podpora řízení hesel	Řešení musí umožňovat správu privilegovaných účtů pro různé druhy koncových systémů - minimálně v rozsahu viz bod 4: " Požadavky na systémy a protokoly pro řízení hesel“	ANO	
MFA - multi factor autentizace	Řešení musí buď nativně nebo integrací nástroje třetí strany, vynucovat multi factor autentizaci. Minimálně na úrovní LDAP/S, RADIUS, SAML.. apod. MFA je vyžadována jako nedílná komponenta požadovaného řešení.	ANO	
SIEM integrace	Řešení musí umožňovat integraci s nástroji SIEM - přenos logovaných auditních záznamů, nejlépe v reálném čase pomocí Syslog.	ANO	
	Architektura		
Architektura řešení	Řešení je dodáváno jako virtuální software appliance (obsahuje i OS) s podporou pro virtuální prostředí Hyper-V/VMware.	ANO	
Architektura řešení	Veškeré komponenty řešení musí splňovat nároky na vysoké zabezpečení s hardeningem zajištěným výrobcem řešení. Úložiště dat, kde jsou uloženy jednotlivé účty, přihlašovací údaje, nahrávky relací a auditní záznamy, je vysoce zabezpečeno. Databáze dat je součástí řešení a není nutné využívat nástroje třetích stran. Tento požadavek platí pro veškerá data v rámci řešení - i pro HA a DR.	ANO	
Vyhledávání systémů	Řešení umožňuje vyhledávání systémů a privilegovaných účtů formou skenování RDP + SSH portů a importů z AD.	ANO	
Onboarding systémů	Řešení disponuje mechanismem pro plnou či částečnou automatizaci onboardingu nově nalezených zařízení / účtů.	ANO	
Zálohování systému	Řešení musí umožňovat bezpečné zálohování dat systému - zálohy musí být šifrované.	ANO	
Úložiště	Řešení umožňuje ukládání zaznamenaných relací lokálně či na externí úložiště CIFS/NFS.	ANO	
	Licenční model		

Druh licence	Licence musí být perperuální s pětiletou podporou. Licence není omezena na počet přistupujících uživatelů nebo řízených privilegovaných účtů.	ANO	
Licence počet zařízení	Licence je pro minimálně [redacted] nebo aplikací.	ANO	
Podpora řešení	Dodávka musí obsahovat podporu výrobce (maintenance) na období min. [redacted] Technická podpora musí být minimálně v rozsahu 8x5.	ANO	

[redacted]

5 Interní Firewall

[redacted]

[redacted]

Firewall

Požadované množství: [redacted]

Požadavky na Firewall

Základním požadavkem pro bezpečnostní zařízení typu firewall je, že musí být jako celek složen z komponent jednoho výrobce, včetně všech poskytovaných funkcionalit typu IPS, databází pro URL kategorizaci apod. Zároveň musí být tímto jedním výrobcem zajištěna podpora minimálně po dobu plánované životnosti FW. Záruční doba minimálně [redacted]

Požadované parametry	**Splňuje ANO/NE, hodnota (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)**
Firewall	[redacted]
Požadované funkcionality: Firewall, IPS, Aplikační kontrola, Malware, Botnet a Zero-day ochrana, HTTPs inspekce	ANO
Požadované funkcionality: Firewall, IPS, Aplikační kontrola, HTTPs inspekce	ANO
Propustnost Firewallu (dle RFC 3511, 2544, 2647, 1242), minimálně 30 Gbps	ANO
Propustnost IPS (Enterprise Mix), minimálně 6.5 Gbps	ANO

Příloha č. 1 – technická specifikace

Propustnost [redacted] (Firewall, IPS, Aplikační kontrola), minimálně 5.5 Gbps	ANO
Propustnost Threat ochrana (Firewall, IPS/IDS, Aplikační kontrola, Antivir, Botnet), minimálně 2.3 Gbps	ANO
Počet nových spojení za vteřinu (CPS) minimálně 90.000	ANO
Počet současných spojení, min. 4.000.000	ANO
Počet požadovaných fyzických síťových rozhraní, min. 8x 10/100/1000baseT	ANO
Počet požadovaných fyzických síťových rozhraní, min. 4x 10Gb SFP+ rozhraní	ANO
Lokální HDD, min 1x 240 GB SSD, v případě výpadku centrálního management log serveru	ANO
Dodávaná firewall platforma musí byt ve formě samostatné hardware appliance	ANO
Instalace do standardního 19" kabinetu s originálním rack mount kitem, velikost 1U	ANO
Podpora redundance dvou zařízení v režimu Active-Standby se stavovou synchronizací	ANO
Podpora agregace fyzických portů LACP	ANO
Podpora dual stack IPv4 a IPv6	ANO
Předefinované threat ochrany a profily pro IPS, Antivirus, Anti-botnet a Zero-day ochrana	ANO
Nové IPS signatury po aktualizaci musí být videlně označeny a být aktivovány jenom v detekčním režimu	ANO
Blokace SQL Injection a CSS útoků v celé URL a HTML body	ANO
Aplikační ochrana musí podporovat a rozeznat minimálně 10 000 aplikací	ANO
Detekce a řízení síťových aplikací. Minimální počet aplikací/pluginů pro sociální sítě, minimálně 250.000	ANO
Detekce a řízení datových souborů a typů na základě obsahu. Minimální počet již předefinovancýh datových typů. min 70	ANO
Možnost vytváření vlastních datových typů na základě klíčových slov, regex, souborových atributů a vážených slov	ANO
Podpora URL filteringu na základě kategorizace. Poskytované řešení musí pokrývat min. 85% Alexa top milion sites	ANO
Podpora explicitní HTTP/HTTPs proxy	ANO
Zobrazení uživatelské notifikace u přístupu pro protokoly HTTP a HTTPs (blokace a zeptání se uživatele)	ANO
Zobrazení uživatelské notifikace u blokovaní aplikací, které používají non-HTTP protokoly	ANO
Možnost získávání identit uživatelů z AD bez nutnosti instalace software na AD servery	ANO
Sdílení identit mezi jednotlivými firewally bez nutnosti externích komponent	ANO
Ochrana proti SNI spoofing v rámci HTTPs inspekce	ANO
Podpora S2S VPN, min. podpora algoritmů pro šifrování: AES-128, AES-256 a integritu: SHA-256 a AES-XCBC	ANO
Podpora IP komprese pro S2S VPN	ANO

Ochrana proti neznámým hrozbám: emulace soborů ve virtuálním sandbox prostředí, min. podporované typy souborů: powerpoint, word, excel, pdf, exe, archivy (zip, tar, 7z, rar)	ANO
Podporovaná velikost emulovaných souborů v sandbox, min. 80MB	ANO
Odstranění potenciálně škodlivého aktivního obsahu (makro, javascript...) ze souboru, případně konverze dokumentu do PDF. Podporované protokoly SMTP, SMTPs, HTTP a HTTPs.	ANO
Podporované typy souborů pro odstranění aktivního obsahu: MS Office, PDF, JPEG, BMP, PNG, TIFF, GIF	ANO
Zablokování prvního pokusu o stažení zero-day malware přes protokoly SMTP, SMTPs, HTTP a HTTPs.	ANO
Podpora MTA agenta za účelem skenování souborů pro Anti-virus a Zero-day ochranu	ANO
Přidávaní vlastních IOC indikátorů (IP, MD5, URL), manuálně nebo přes API	ANO
Integrovaný firewall performance analyzer, min. top 10 spojení a jejich % konzumace HW zdrojů/pro každé spojení/protokol	ANO
Podpora linux nástrojů (min. SCP, BASH, VI, TOP), spouštění linux skriptů a nástrojů třetích stran	ANO
Bezpečnostní logy musí být ukládány na fyzicky oddělenou management platformu.	ANO
Počet publikovaných zranitelností OS (na základě CVE) firewall za poslední 3 roky, max. 15; dodavatel doloží v nabídce	2
Řešení musí být uvedeno v Gartner Magic Quadrant for Enterprise Network Firewalls za roky 2017-2022 minimálně 3x v kvadrantu Leader; dodavatel doloží v nabídce	ANO
Automatické vypnutí IPS ochrany (pro konkrétní instanci virtuálního firewallu) v případě přetížení HW (využití CPU nebo fyzické paměti) nad definovanou prahovou hodnotu	ANO
Maximální spotřeba zdroje 150[W] a maximální tepelný tok 505BTU	ANO
Požadované parametry	
Management	
Management musí být fyzicky oddělený od firewall platformy	ANO
Jednotný centrální management: správa politik a analýza logů v na jedné konsolidované virtuální appliance (Hyper-V, ESXi) nebo hardware	ANO
Management musí ukládat a zpracovávat logy ze všech firewallů, objem logů za den min. 15 GB/den	ANO
Podpora administrátorských profilů pro delegaci oprávnění (čtení, zápis)	ANO
Možnost přidělení práv administrátorům nebo API účtu jen pro definovaný seznam přístupových firewall pravidel	ANO
Seskupování firewall pravidel do logických skupin a pod-skupin na základě zdroje, cíle, služby/aplikace pro dlouhodobou konzistenci pravidel	ANO
Ochrana vzájemného ovlivňovaní nebo kolize při současném připojení vícero administrátorů pomocí zamykání individuálních pravidel a objektů.	ANO
Policy Tracer - vyhledávaní firewall pravidla dle kombinace definovaných atributů (min. zdrojová IP, cílová IP, uživatel, služba, aplikace..)	ANO

Kontrola politik proti chybám a duplicitám	ANO
Vizualizace a prohledávaní logů přímo v politice na vybraném pravidle (min. zdroj, cíl, služba, aplikace, uživatel, čas)	ANO
Zobrazení historie a změn přímo v politice na vybraném pravidle (min. kdo, jaká změna a kdy byla na pravidle provedena)	ANO
Prohledávaní logů, min. podpora: "keyword" prohledávaní, "field" prohledávaní a "wildcard" prohledávaní	ANO
Práce s bezpečnostními logy – možnost prohledávaních všech typů logů (fw, ips, malware) v jedné záložce s definováním vlastních permanentních filtrů.	ANO
Rekonfigurace a ladění threat engine přímo z log výstupů firewallu	ANO
Logování a historické prohledávaní TCP stavových informací k jednotlivým spojením v rámci centrálního log serveru (min. SYN, SYN.ACK, Established, FIN, FIN.ACK, RST)	ANO
Integrovaný monitoring musí poskytovat grafické rozhraní pro sledování parametrů v reálnem čase a historii alespoň 30 dní (využití paměti, CPU, počet navázaných spojení, počet nově otevřených spojení za sekundu, propustnost, atd …).	ANO
Podpora služby vlastní certifikační autority pro vydávaní PKI certifikátů pro bezpečné přihlašovaní uživatelů a administrátorů a pro VPN klientský přístup	ANO
Kontrola politiky dle standardů, min. ISO 27000 a GDPR (může být dodané produktem třetí strany)	ANO
Možnost vytvářet bezpečnostní pravidla založená na identitě uživatelů - Integrace na [redacted] přes rozhraní [redacted]	ANO
Integrace na Vmware vSphere, min. dynamické získavaní VM objektů a jejich aplikace ve firewall politice	ANO
Je-li management licence omezena počtěm řízených objektů bezpečnostních bran, musí podporovat řízení min. 4 objektů bran	ANO
Je-li management licence omezena diskovou kapacitou, licence pro min. 16TB musí být součástí nabídky	ANO
Možnost upgrade/update software firewallu, bezpečnostních update (IPS signatury, geolokační databáze, apod.), konfigurací atd. z grafického rozhraní managementu	ANO
Možnost zasílat předdefinované reporty emailem. (podpora také autentizovaného SMTP pro komunikaci s mail relay)	ANO
Řešení poskytuje dynamické objekty se seznamem IP adres reprezentující externí služby typu Office365, Cloudové služby (AWS, Azure apod.), DropBox, ZOOM a další, a různé geografické lokality až na úrovni jednotlivých zemí	ANO
Možnost použít tyto dynamické objekty ve FW pravidlech, NAT pravidlech a definici HTTPS inspekce	ANO
Dynamické objekty se musí automaticky aktualizovat bez nutnosti zásahu administrátora	ANO
Možnost verzování politik a možnost generování rozdílových reportů mezi jednotlivými verzemi.	ANO

Požadavky na HW architekturu:

- Firewall musí být typu HW appliance
- Modul pro zpracování dat musí být v architektuře firewallu hardwarově oddělen od dalších podpůrných modulů (správa zařízení a řídící modul pro podpůrné síťové činnosti), aby nemohlo dojít k jejich vzájemnému ovlivnění
- Firewall musí obsahovat jeden dedikovaný port pro správu pomocí konzole pro přístup k CLI
- Firewall musí obsahovat minimálně 8 datových portů rychlosti 1Gbps
- Firewall musí obsahovat minimálně 4 datové porty rychlosti 10Gbps
- Součástí dodávky je příslušný počet optických modulů SFP a SFP+ a propojovacích kabelů k zajištění integrace do infrastruktury
- Firewall musí obsahovat alespoň jeden dedikovaný OOB management port pro plnohodnotnou správu FW
- Firewall musí být schopen ukládat logové údaje na interní storage o velikosti minimálně 100 GB

Požadavky na [redacted]:

- [redacted]
- [redacted]
- V obou typech [redacted] musejí být veškeré informace o probíhajícím provozu synchronizovány tak, aby při výpadku [redacted] nedošlo ke ztrátě informací NAT a k přerušení aktivních spojení provozu typu TCP i UDP procházejícího přes FW
- Firewall musí být schopen provést failover na základě stavu interface (up/down), nedostupnosti druhého FW v HA a přetížení CPU.

Obecné výkonové parametry:

- Propustnost firewallu při plné aplikační kontrole musí dosahovat hodnoty alespoň (690 Mbps of [redacted]
- Propustnost firewallu při plné aplikační kontrole a zapnutí všech dostupných signatur IPS a AV musí dosahovat hodnoty alespoň (395 Mbps of Threat Prevention)
- Minimální počet souběžných spojení musí dosahovat hodnoty alespoň 64000
- Minimální počet nových spojení za sekundu musí dosahovat hodnoty alespoň 4200

Síťová funkcionalita:

- Firewall musí plně podporovat IPv4 i IPv6
- Firewall musí podporovat zapojení v režimech L2 (s virtuálním L3 rozhraním), L3, transparent a TAP
- Firewall musí podporovat překlady adres typu Static NAT, Dynamic NAT, PAT, NAT64
- Firewall musí podporovat směrování typu Static route, RIP, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBF (Policy Based Forwarding)
- PBR musí být možno nakonfigurovat na základě všech dostupných metrik typu interface, IP adresa zdrojová, IP adresa cílová, služba, protokol.

VPN:

- Firewall musí podporovat site-to-site VPN pomocí protokolu IPSec.
- Firewall musí podporovat Remote Access VPN pomocí protokolů IPSec a SSL (TLS).
- Firewall musí podporovat Clientless Remote Access VPN.
- Počet současně připojených uživatelů musí být alespoň 1000.
- Propustnost IPSec musí být alespoň 100 Mbps.
- Firewall musí podporovat tzv. posture analýzu (kontrolu souladu stavu zařízení s předdefinovanými pravidly) pro připojovaná koncová zařízení.

- Firewall musí podporovat dvou-faktorovou autentizaci uživatelů např. pomocí SMS.

Management:

- Jednotlivé HW appliance musí obsahovat plnohodnotné grafické a textové rozhraní (GUI, CLI) pro správu, bez nutnosti používání centrálního management serveru. Připojení ke GUI, CLI musí podporovat šifrování.
- Firewall musí podporovat centrální management pro hromadnou správu bezpečnostních politik, hromadný upgrade OS a dynamického obsahu (signatury) i správu dalších parametrů.
- Firewall musí pro autentizaci a autorizaci administrátorů podporovat protokoly LDAP, Radius, TACACS+ a osobní certifikát.
- Firewall musí obsahovat nativní nástroje pro debugging problémových situací v úrovni L2 – L7 ISO/OSI modelu.
- Firewall musí podporovat nativní nástroj pro odchycení provozu.
- Firewall management musí podporovat práci více administrátorů ve stejném čase, včetně aplikace politik a nastavení vytvořených pouze konkrétním administrátorem
- Firewall musí mít možnost granulárně odlišit práva uživatelů na základě profilu jako IPS, TP a APCL politik.
- Firewall musí mít možnost granulárně odlišit práva uživatelů na základě pouze části politiky.
- **Management firewallu musí být označen jako „Gold standard“ v rámci hodnocení společnosti Gartner; dodavatel doloží v nabídce.**
- Centrální management server musí být součástí firewallu.

Aplikační kontrola:

- Firewall musí podporovat aplikační detekci a kontrolu jako svou nativní funkcionalitu
- Přiřazení povolené či zakázané aplikace musí být nativní součástí vytváření standardního bezpečnostního pravidla
- Firewall musí podporovat identifikaci aplikací napříč všemi porty/protokoly
- Identifikace aplikace musí probíhat přímo ve FW
- Firewall musí obsahovat databázi minimálně 5000 aplikací, pomocí kterých je možné filtrovat provoz.

Kontrola na úrovni uživatelských identit

- Firewall musí podporovat vytváření bezpečnostních pravidel na základě uživatelských identit
- Volba uživatelské identity musí být nativní součástí vytváření standardního bezpečnostního pravidla
- Firewall musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na doménový kontroler, na koncové zařízení či instalace dalších komponent mimo samotné HW appliance
- FW musí podporovat získávání vazby IP adresa-uživatelské jméno z Active Directory za pomoci doménového účtu s co nejnižšími možnými právy pro čtení Security logů, bez nutnosti disponovat rizikovými úrovněmi oprávnění (např. Domain Admins)
- FW musí podporovat získávání vazby IP adresa-uživatelské jméno z terminálových serverů MS a Citrix (možno za pomoci nainstalovaného agenta) či prostřednictvím načtení informace z logového záznamu, získaného pomocí zabezpečeného protokolu Syslog

Dekrypce

- Firewall musí podporovat dekrypci odchozího SSL/TLS provozu, za pomoci podvržení serverového certifikátu klientům či za pomoci naimportovaného privátního klíče interního serveru.

- Dekryptovaný provoz musí být možno definovat na základě URL kategorií, i všech dalších typických parametrů, jako jsou zdrojová a cílová IP adresa, port, uživatelská identita
- Firewall musí podporovat dekrypci za pomocí ECC (Elliptical Curve Cryptography), včetně DHE a ECDHE pro příchozí i odchozí provoz
- FW musí podporovat možnost zablokování útoků na známá C&C centra i v případě, že je provoz šifrován a není možné provádět SSL dekrypci

Sandboxing

- Firewall musí podporovat možnost odeslat do sandboxu k inspekci
- Sandbox systém musí být od stejného výrobce, jako je Firewall, ale HW nemusí být součástí Firewallu
- Sandbox systém musí mít možnost nasazení jako privátní cloud.
- Sandbox systém musí být schopen okamžitě automaticky vytvořit IPS/AV signatury pro FW, v případě, kdy je testovaný vzorek vyhodnocen jako škodlivý;
- Sandbox musí být schopen automaticky upravit kategorie používané URL databáze, pokud zjistí, že testovaný vzorek je škodlivý a komunikuje na konkrétní URL
- Sandboxing musí podporovat minimálně 40 typů souborů včetně známých typů archivů.
- U souborů pro emulaci musí být možnost nastavit velikost souboru větší než 10MB.
- Emulace souborů musí být dostupná pro všechna Windows 32/64 bit, Win7, Win8, Win10, Win11.
- Sandboxing musí být vždy v prevent módu, i v případě prvotního možného průniku tzv. Pacient zero.

Bezpečnostní funkcionality

- Firewall musí podporovat zavedení tzv. pozitivního bezpečnostního modelu – whitelisting pouze povolených aplikací a zákaz všeho ostatního, včetně neznámého provozu.
- Firewall musí obsahovat integrovaný systém ochrany proti zranitelnostem (virtual patching) a síťovým útokům (IPS). Databáze IPS signatur musí být uložena přímo ve FW. Aplikace IPS profilu musí být granulární, na úrovni bezpečnostního pravidla.
- Firewall musí umožňovat import IPS signatur z databáze SNORT.
- Firewall musí podporovat minimálně 10 virtuálních oddělených kontextů (firewalů)
- Firewall musí obsahovat integrovaný systém ochrany proti přítomnosti virů a škodlivého kódu. Databáze AV signatur musí být uložena přímo ve FW. Aplikace AV profilu musí být granulární, na úrovni bezpečnostního pravidla.
- Antivirus musí být schopen kontrolovat provoz v minimálně těchto aplikacích: SMTP, HTTP, HTTPS, FTP.
- Firewall musí poskytovat možnost zabránit odeslání doménových uživatelských přihlašovacích údajů do jiných než povolených URL kategorií, pro zabránění phishingu
- Firewall musí být schopen automaticky vytvářet C&C signatury a okamžitě je aplikovat je do bezpečnostní politiky.
- Firewall musí podporovat rozhraní API pro rozšířenou správu a vytváření objektů.
- Firewall musí poskytovat funkci ochrany, která edukuje uživatele o přístupu na Internetu do zakázaných kategorií a musí být pro uživatele interaktivní s možností volby akceptace rizika.
- Firewall musí být schopen detekce botnetů na základě behaviorální analýzy.
- **Firewall musí být vyhodnocen jako „LEADERS“ za posledních 5 let v rámci testu Gartner; dodavatel doloží v nabídce.**

Ochrana proti DoS

- Firewall musí obsahovat nativní službu pro ochranu proti útoku typu DoS pomocí limitace počtu spojení na úrovni zdrojová a cílová IP adresa
- QoS Firewall musí poskytovat možnost omezení využívané šířky pásma na základě zdrojové a cílové IP adresy, portu, uživatelské identity, aplikace a času (od – do, den v týdnu, čas apod.)
- Firewall musí podporovat prioritizaci provozu na základě IP adres či služby.
- Firewall musí podporovat systém váhy a garantovaní šířky pásma pro každé spojení.

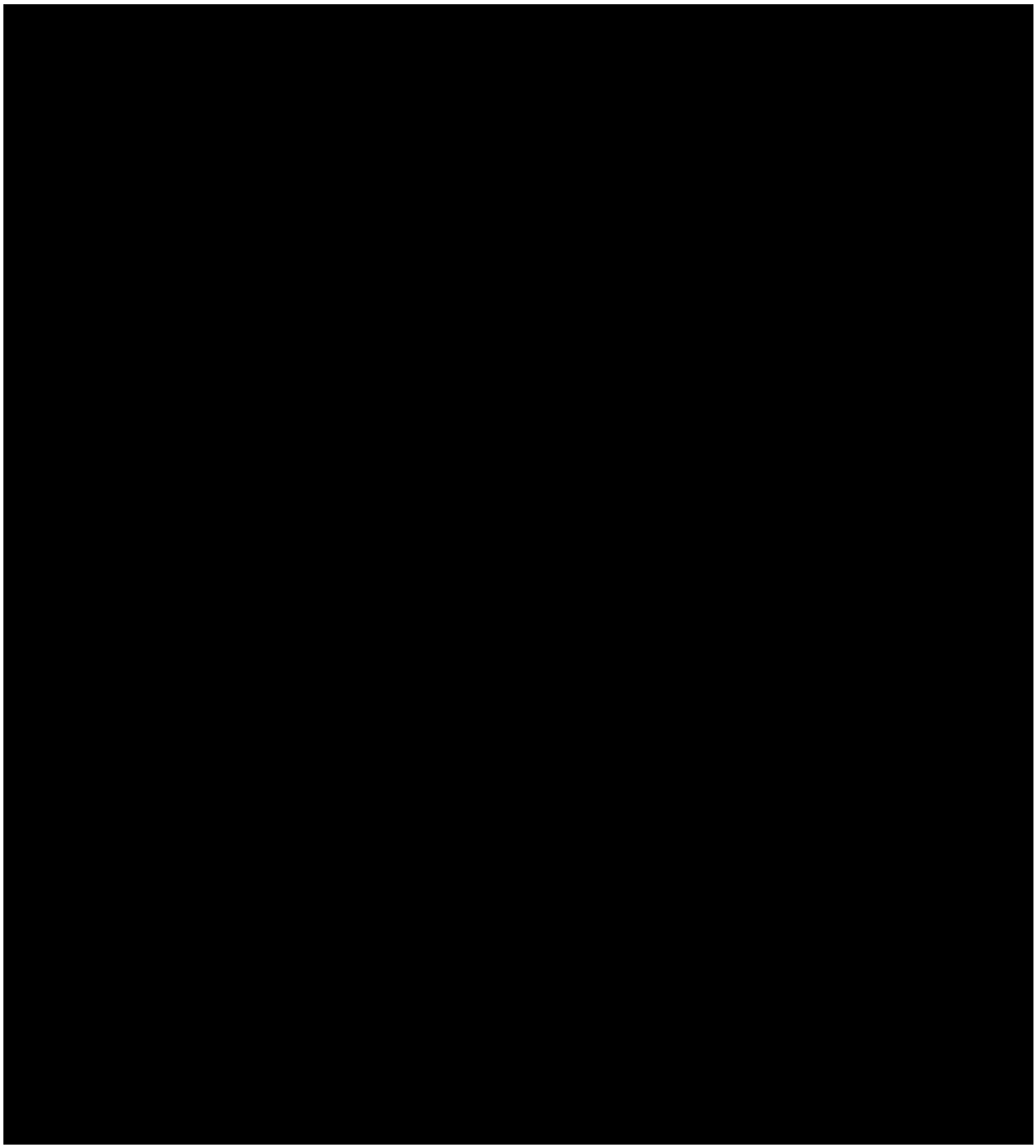
URL filtering

- Firewall musí obsahovat nativní podporu pro využívání databáze URL.
- URL databáze být od stejného výrobce, jako je FW.
- Firewall musí být schopen použít URL kategorii v definici bezpečnostního pravidla.
- Firewall musí podporovat vytváření uživatelsky definovaných kategorií, bez nutnosti využít externí nástroj a bez nutnosti zásahu výrobce/dodavatele.
- URL databáze musí být dynamicky aktualizovaná na základě nově zjištěných URL, vedoucích na škodlivý obsah, nebo C&C centra.
- Aplikace URL kategorie se musí vyhodnocovat oproti cloudové databáze, aby bylo vždy zaručeno co nejpřesnějších výsledků.

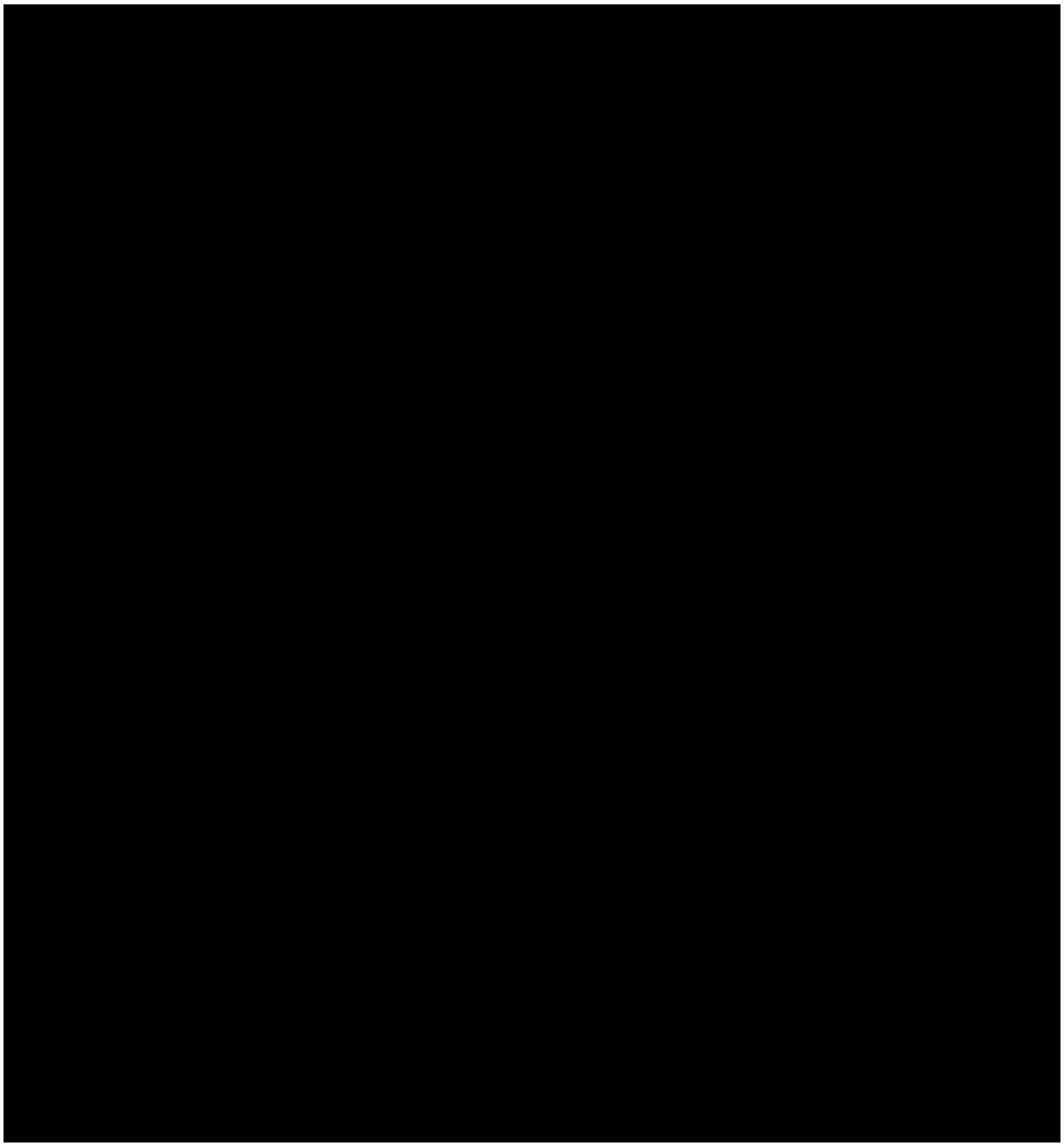
Logování

- Firewall musí obsahovat lokální úložiště logů.
- Firewall musí obsahovat nástroj pro analýzu logů bez nutnosti využití dalšího systému mimo GUI.
- Firewall musí podporovat agregované zobrazení logů na základě jednoho filtrovacího pravidla, napříč jednotlivými typy logů, jako jsou provozní logy, logy bezpečnostních incidentů a logy přístupů na URL.
- Firewall musí podporovat přeposílání logů na zařízení třetích stran.
- Management musí obsahovat vlastní nativní nástroj pro vyhodnocování logů a vypracování událostí, ze kterých se následně mohou dělat reporty.
- Reportování musí podporovat klíčové funkce jako FW, URL, APP, IPS, Sandboxing.
- Vyhledávání v log souborech musí být fulltextové a intuitivní s možností použití předdefinovaných filtrů a BOOLEAN operátorů.

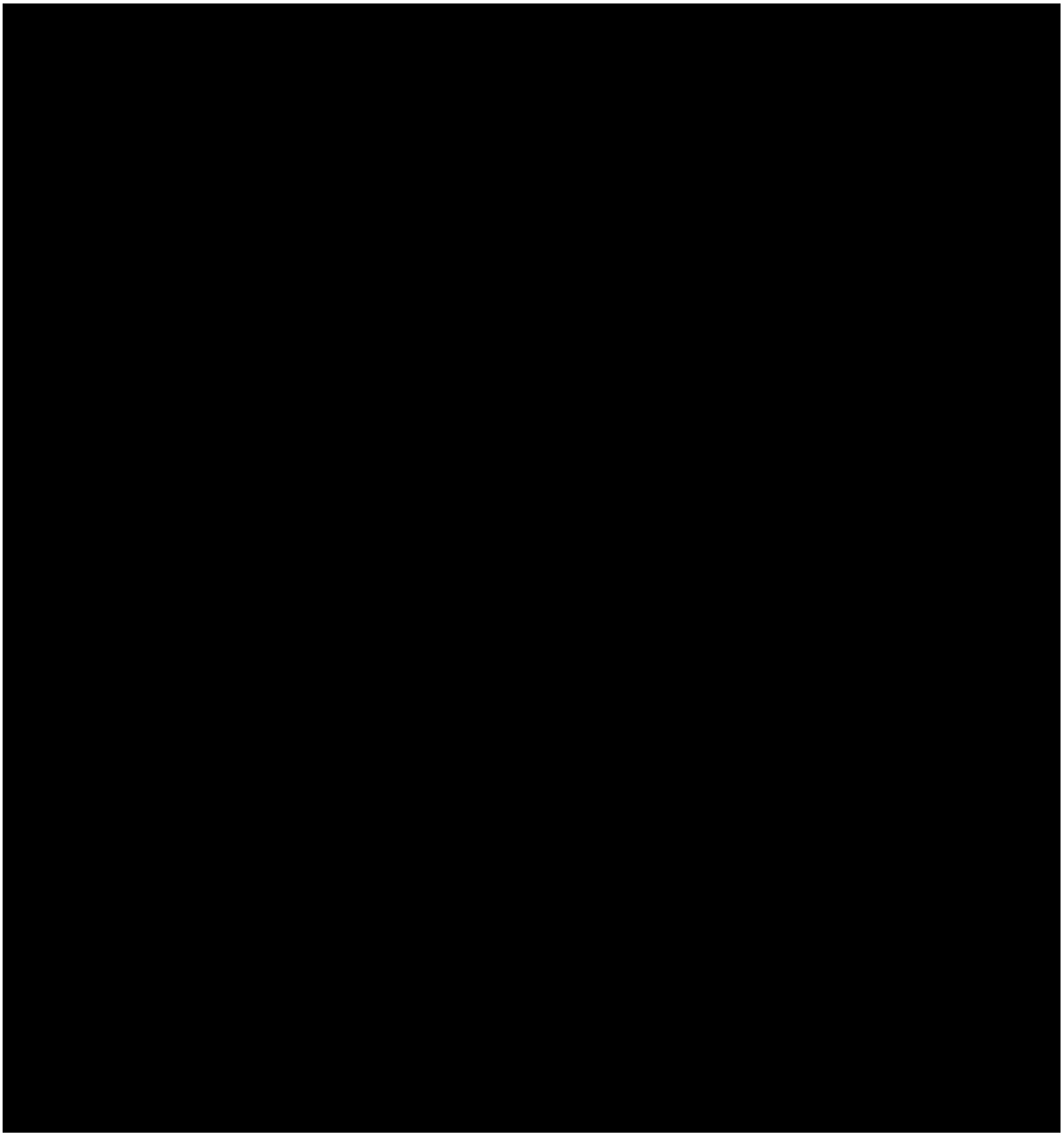
Příloha č. 1 – technická specifikace



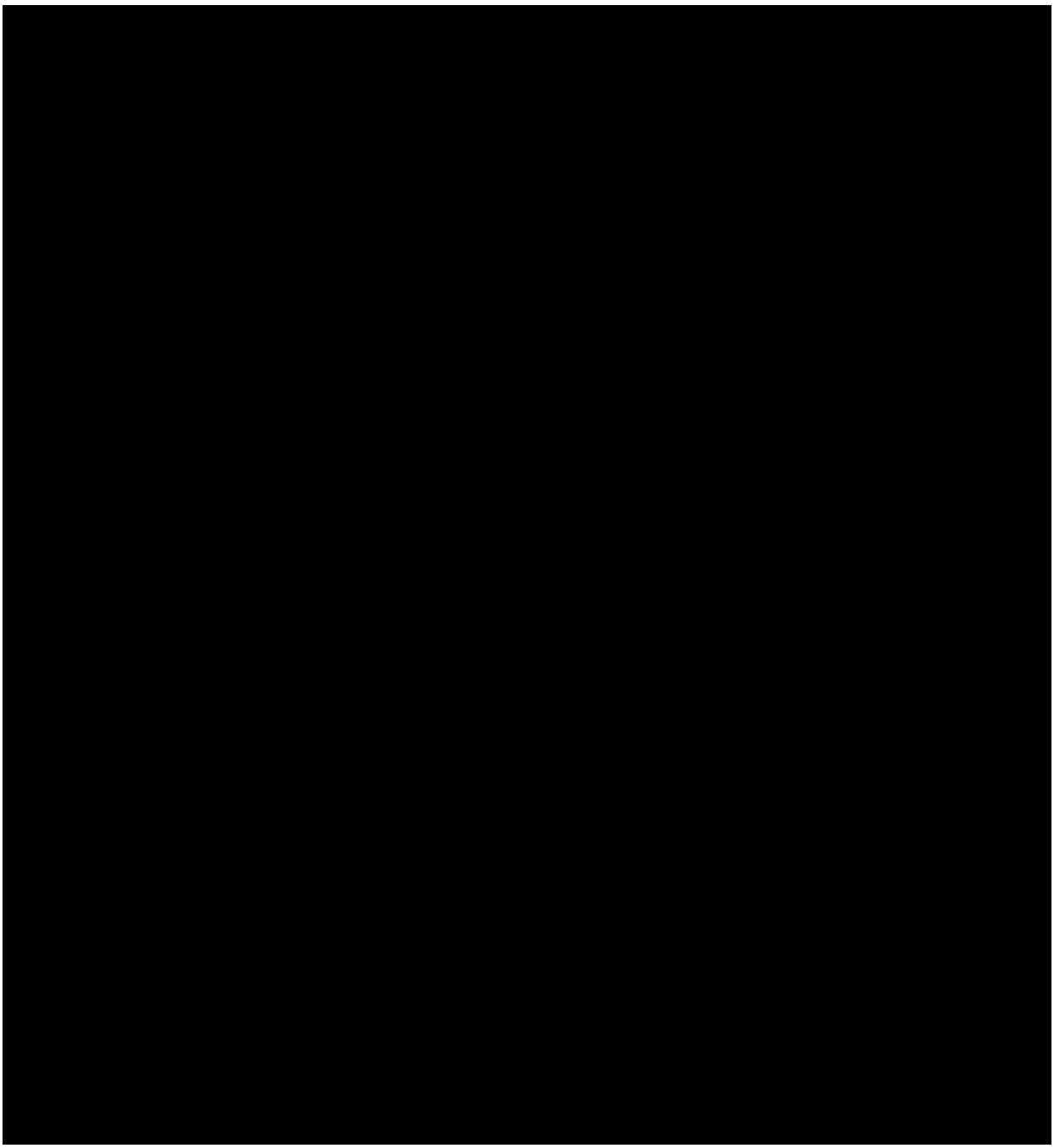
Příloha č. 1 – technická specifikace



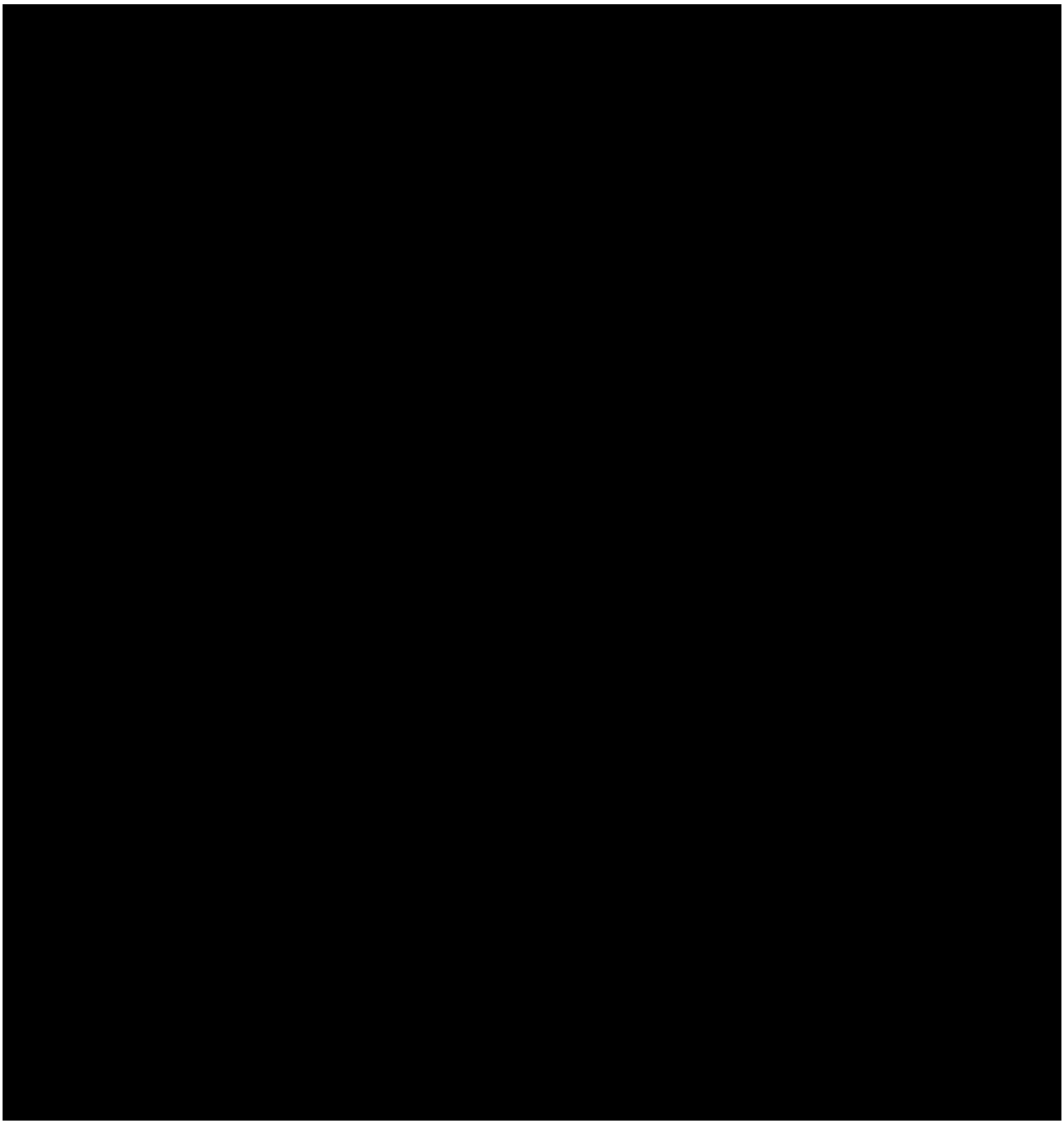
Příloha č. 1 – technická specifikace



Příloha č. 1 – technická specifikace



Příloha č. 1 – technická specifikace



Příloha č. 1 – technická specifikace

6 MFA / ochrana přístupu uživatelů

[redacted]

Specifikace potřeb

- Dodat [redacted] hybridních čipových karet ve formátu ID-1 (velikost bankovní karty). Kontaktní čipy a aplikace nahraná do kontaktního čipu umožňuje správu kryptografických klíčů určených k vytváření kvalifikovaného elektronického podpisu. Možnost garantovaného dokoupení dalších kontaktních karet stejného typu nejméně po dobu 5 let.
- Dodané karty budou obsahovat i bezkontaktní čip, který Zadavatel ve svém prostředí provozuje a to [redacted].
- Dodat SW aplikace pro správu hybridních čipových karet a certifikátů s licencí na dobu neurčitou pro [redacted] uživatelů.
- Pomocí hybridních čipových karet zajistit 2faktorovou autentizaci uživatelů, tak aby byly naplněny podmínky ZKB.
- Implementace dodaných systémů.
- Poskytovat servisní podporu pro plnou funkčnost dodaného zboží a SW aplikací. Servisní podpora zahrnuje upgrade a update zboží a software.
- Dodat čtečky karet stejného typu, který již zadavatel používá – [redacted] Požadovaný počet kusů uveden v kapitole 7 Single Sign-On.
- Dodat čtečky [redacted] funkční na HW stanicích zadavatele s připojením ke stanici přes USB. Požadovaný počet kusů uveden v kapitole 7 Single Sing-On.

Technické opatření

a) Cílovým požadavkem je:

Umožnit zaměstnancům vytvářet kvalifikovaný elektronický podpis podle nařízení eIDAS pomocí kryptografických klíčů bezpečně chráněných v hardwarovém prostředku – hybridní čipové kartě.

Karta musí také umožňovat společné uložení certifikátu z interní certifikační autority založené na produktech Microsoft. Pomocí tohoto certifikátu se držitel karty bude moci v budoucnu přihlásit do doménových počítačů (technologie Smartcard Logon).

b) Základní požadavky na zařízení:

Hybridní čipové karta a ovladače:

Pro uložení elektronických certifikátů X.509 (a generování / uložení příslušných kryptografických klíčů)

budou dodány hybridní čipové karty ve formátu ID-1 (velikost bankovní karty):

- kontaktní čip na bázi GlobalPlatform/JavaCard s personalizovanou PKI aplikací.

Certifikované karty musí být v souladu:

- s normou ČSN EN ISO 7816, část 1-4 a
- standardem EN 419 211 a profily:
    - BSI-CC-PP-0059
    - BSI-CC-PP-0075
    - BSI-CC-PP-0071
    - BSI-CC-PP-0072
    - BSI-CC-PP-0076

Vlastnosti kontaktního čipu a PKI aplikace:

- Všechny operace s privátním klíčem probíhají uvnitř čipu – klíč neopustí prostředí karty
- Privátní klíč uložený na kartě nelze z karty vyexportovat
- Vytváření kvalifikovaného elektronického podpisu splňující nařízení eIDAS
- Klíče pro kvalifikovaný elektronický podpis jsou generovány v čipu.
- Klíče, které nejsou určeny pro kvalifikovaný elektronický podpis, mohou být generovány v čipu anebo mohou být na kartu importovány
- Generování RSA i ECC klíčů v čipu i import klíčů s certifikáty do čipu, ze souboru formátu PKCS#12
- Archivaci privátních klíčů v procesech vydávání šifrovacích certifikátů
- Podporované jsou minimálně kryptografické algoritmy:
    - Symetrické: 3DES, AES
    - Hash: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512.
    - RSA: 1024, 2048 bitů
    - Eliptické křivky: P-224, P-256, P-384, P-521
- Zablokování bezpečnostního kódu PIN, QPIN resp. PUK po opakovaném chybném zadání PIN, QPIN resp. PUK
- Podpora odblokování bezpečnostního kódu PIN pomocí PIN nebo PUK, podpora odblokování bezpečnostního kódu QPIN pomocí QPIN nebo PUK.
- Zabezpečení komunikace na bázi e-mailů (S/MIME, elektronický podpis a šifrování e-mailů)
- Dvoufaktorovou autentizaci na bázi certifikátů X.509 (do PC v prostředí Microsoft AD, webových služeb, VPN, aplikací atd.)
- Vytváření elektronického podpisu na bázi certifikátů ve formě:
    - kvalifikovaného elektronického podpisu,
    - zaručeného elektronického podpisu,
    - uznávaného elektronického podpisu a
    - jiné formy elektronického podpisu.
- Generování a práce s RSA a ECC klíči v čipu
- Hybridní čipová karta podporuje získání následného certifikátu prostřednictvím aplikace pro automatizovanou obnovu certifikátů.

Ovládací software karty:

Příloha č. 1 – technická specifikace

Čipové karty budou dodány s ovládacím software, pro integraci kontaktního čipu karty do operačního systému. Vlastnosti ovládacího software:

- podléhá specifikaci Microsoft Smart Card minidriver for Windows Base CSP V5.07 nebo vyšší
- podpora Microsoft CryptoAPI, Microsoft CNG i PKCS#11
- použití na O MS Windows 8 nebo vyšších verzích;
- případné použití i na Linux – LTS (Long Term Support) verze pro Ubuntu a RHEL (PKCS#11) OS X (PKCS#11)
- instalace z MSI balíčků (podpora obslužné a bezobslužné instalace), RPM, DEB

Stav dodané karty:

- Inicializovaná PKI aplikace s PIN, QPIN a PUK.
- Předání seznamu personalizovaných karet, pro import [redacted]. U každé karty uvedeno číslo kontaktního, případně i bezkontaktního čipu.
- Inicializovaná PKI aplikace výchozími hodnotami PIN, QPIN a PUK. Technickými prostředky bude vynuceno, aby si uživatel po přijetí karty změnil hodnotu bezpečnostních kódů.

1. **Požadavky na aplikace pro správu a podporu čipových karet a certifikátů:**

a) Zjednodušení životního cyklu karet a certifikátů
b) Software umožňuje evidenci uživatelů přes AD i v rámci vlastní databáze. Uživatelům evidovaných v rámci vlastní databáze není možné vystavit certifikát pro autentizaci do AD.
c) Automatizovaná obnova kvalifikovaných i komerčních certifikátů od externího poskytovatele. Automatizovaná obnova interních certifikátů z doménové CA
d) Implementace aplikace pro kvalifikované elektronické pečetění dokumentů prostřednictvím čipové karty
e) Implementace aplikace, která prostřednictvím e-mailové notifikace upozorní uživatele na blížící se konec platnosti certifikátu
f) Implementace aplikace pro podporu činností spojených se správou životního cyklu čipových karet a certifikátů, zastřešení registračního místa doménové CA.
g) Implementace webové aplikace, určené správcům certifikátů. Možnost vyhledávat a prohlížet informace o certifikátech, odvolávat certifikáty, generovat a prohlížet reporty.

2. **Implementace PKI Zadavatele**

Zadavatel požaduje ve své infrastruktuře vybudovat bezpečnostní vrstvu na bázi PKI MS Windows, která je primárně určena pro vydávání klientských karetních a infrastrukturních certifikátů.
Nově se plánuje z doménového PKI vydávat uživatelské certifikáty na čipové karty za účelem zavedení primárně 2-faktorové autentizace (náhrada autentizace jménem/heslem). Mimo přihlášení do PC budou z interní CA vydávány případně certifikáty pro přihlášení do VPN a interní elektronický podpis. Interní PKI bude také poskytovat infrastrukturní certifikáty pro interní použití, např. certifikáty pro web servery a DC.
V rámci dodávky je Zadavatelem požadované:

- Provést a předat návrh PKI
- Implementace PKI dle návrhu, součástí minimálně bude:
    - Implementace zvolené architektury PKI, zprovoznění PKI v prostředí zákazníka
    - Předat podklady na implementaci šablon pro vydání certifikátů pro autentizaci uživatelů do domény, případně další uživatelské akce.

- Předat podklady na implementaci šablon pro vydání technologických certifikátů
- Implementace šablon uživatelských a technologických certifikátů
- Definici distribučních bodů CRL
- Ochrana a uložení klíče CA
- Dodání havarijní a provozní dokumentace k vybudované vrstvě PKI
- Kompletní napojení dodávaného řešení na AD zadavatele

Servisní podpora:

Základní servis nabízeného řešení musí zahrnovat podporu po dobu udržitelnosti (delší podpora je volitelná a zadavatel ji nemusí využít):

- operačních systémů na klientských stanicích Windows 8 až Windows 11
- serverových operačních systémů Windows Server 2016 a vyšších
- čipových karet do konce životnosti
- čteček pro práci s kartou
- instalovaných aplikací pro správu životního cyklu karet a certifikátů
- formou Service Desku v režimu 5 x 8, jehož provozní doba musí být min. od 8:00 do 16:00 v pracovní dny.

Požadované reakční doby:

- Přijetí požadavku do 2 hodin od nahlášení.
- Dočasné řešení do 1 pracovního dne od přijetí požadavku.
- Vyřešení požadavku do 5 pracovních dnů od dodání dočasného řešení.
- Reakční doby musí být garantovány pro serverové komponenty řešení.

7 Single Sign-On (SSO)

[redacted]

Požadavek na HW, SW	Minimální požadavky	Splňuje ano/ne (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)
Požadavky na HW		
[redacted]	600 ks	600
[redacted]	200 ks	200
Požadavky na SW licence		
MFA a SSO licence	700	700
Samoobslužný reset hesla	25	25
Mobilní aplikace MFA	25	25
Licence pro tablety Android	16	16
MFA a SSO serverová strana	2	2
Požadavek na funkcionalitu	**Minimální požadavky**	**Splňuje ano/ne (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku**

Příloha č. 1 – technická specifikace

		představuje nesplnění zadávacích podmínek)
Obecné požadavky		
Klientská část řešení musí podporovat Windows Desktop OS (Windows 10 a novější), Linuxové OS tenkých klientů a v případě mobilních klientských zařízení minimálně operační systémy Windows a Android.		ANO
Řešení bude ve výchozím stavu navrženo a dodáno jako vysoce dostupné, s odolností vůči výpadku jednoho serverového prvku, s minimálně dvěma vzájemně zastupitelnými prvky. Při výpadku jednoho prvku zůstává řešení plně funkční, zbylý funkční prvek/prvky nadále poskytují plnou funkčnost. K překlopení na funkční prvek/prvky musí dojít automaticky, bez nutnosti ručního zásahu, maximálně v jednotkách sekund. Všechny prvky si vzájemně replikují nastavení a data, v případě výpadku prvku tedy nedojde ke ztrátě nastavení či dat. Všechny prvky řešení musí být spravovány jako jeden celek, jednotnou správou z webové konzoly, napříč datovými centry případně cloudy.		ANO
Serverová část řešení bude nasazena ve formě virtuálních strojů (podpora minimálně VMware vSphere, Microsoft Hyper-V). Virtuální stroje musí být možné, a ze strany výrobce podporované, provozovat v cloudu (podpora minimálně Microsoft Azure). Řešení musí být možné nasadit také v hybridním režimu, kdy jeden nebo více virtuálních strojů je provozováno v datovém centru on premises a další virtuální stroj nebo stroje v cloudu, formou SaaS.		ANO
Řešení musí umožnovat definovat práva na činnosti ve správcovských nástrojích na základě členství v Active Directory skupinách. Řešení musí být schopno definovat různé úrovně administrátorských přístupů – delegování administrativních oprávnění – vytvořením kombinací (sad) oprávnění.		ANO
Řešení musí být integrováno na adresářovou službu Microsoft Active Directory Directory Services (AD DS), identita – uživatelský účet – uživatele dodaného řešení musí odpovídat identitě v AD DS. Změny v AD DS (změny stavu účtu, atributů, členství ve skupinách) musí být automaticky synchronizovány s dodaným řešením. Řešení nesmí modifikovat schéma Active Directory. Dodané řešení musí být možné integrovat na další adresářové (LDAP) služby.		ANO
Komunikace mezi jednotlivými komponentami řešení v rámci HTTPS komunikace musí být šifrována TLS protokolem minimálně verze 1.2, uložená citlivá data – zejména přihlašovací údaje uživatelů – musí být chráněna FIPS 140-2 validovaným šifrováním AES 256.		ANO
Více-faktorová autentizace		
Řešení musí umožňovat používání různých autentizačních předmětů pro více-faktorovou autentizaci, minimálně: kontaktní čipové karty (smart karty), bezkontaktní karty včetně karet Mifare DesFire, FIDO bezpečnostní klíče, USB tokeny, bezkontaktní RFID předměty, biometrické prvky (otisk prstu), login/heslo (s vazbou i bez vazby na adresářovou službu), a jejich vzájemné kombinace. Vyžádání druhého faktoru musí být možné definovat dynamicky, na základě splnění podmínky (např. uplynutí časového intervalu).		ANO
Řešení musí pro vybrané uživatele poskytnout funkci tzv. „Push“ autentizace a/nebo autentizace pomocí OTP (One-Time Password) pro přihlášení ke koncovým zařízením s Windows OS a do VPN prostřednictvím mobilní aplikace (podporované mobilní OS: minimálně Android a iOS).		ANO

Řešení musí umožnit volbu parametrů autentizačního PIN kódu pro více-faktorové ověřování (podobně, jako u hesla např. v Active Directory). Délku PINu v rozmezí alespoň od 4 do alespoň 16 znaků, musí umožnit exspiraci PIN kódu po definovaném časovém intervalu, musí umožnit použití jak čistě numerického PINu, tak PINu obsahujícího čísla a písmena a speciální znaky. Řešení dále musí umožnit vynucení historie PINu a zamezit uživateli, aby si při obnově PINu zvolil dříve jím použitý PIN kód (je požadováno, aby si systém pamatoval alespoň 8 posledních PINů). Řešení musí umožnit vynutit nastavení, které uživateli zamezí nastavit si snadno uhodnutelný PIN (minimálně nedovolit opakování stejných po sobě jdoucích znaků, jako např. „1111“ a jednoduchou číselnou řadu, jako např. „1234“).		ANO
Řešení musí obsahovat technologii pro automatizaci přihlašovacího procesu, která uživateli umožní přihlášení do vzdálené plochy s využitím již zadaných přihlašovacích pověření, bez nutnosti opakovaně zadávat přihlašovací údaje, potvrzovat připojovací dialogy, znovu použít autentizační předmět, znovu zadávat PIN kód. Tato technologie musí podporovat nejběžnější produkty pro virtualizaci aplikací a desktopů (Microsoft Remote Desktop Services, Citrix Virtual Apps and Desktops, VMware Horizon).		ANO
Řešení musí umožňovat režim redukovaného uživatelského rozhraní, tzv. "appliance mode", na tenkých klientech. V tomto režimu je běžné uživatelské rozhraní tenkého klienta nahrazeno přihlašovací obrazovkou pro více-faktorovou autentizaci.		ANO
Řešení musí umožnit nastavení různých kombinací přihlašovacích faktorů pomocí politik, a tyto politiky aplikovat na skupiny uživatelů, skupiny koncových zařízení, typy koncových zařízení s rozlišením alespoň fyzická stanice/virtuální desktop/server vzdálené plochy.		ANO
Řešení musí zajistit funkčnost více-faktorové autentizace pomocí bezkontaktních karet i v případě, kdy klientské zařízení není připojeno k síti (je offline) nebo není dostupná serverová strana řešení.		ANO
Řešení musí poskytnout funkce více-faktorové autentizace na koncových (klientských) zařízeních používaných jedním uživatelem, používaných více uživateli, a dále na sdílených koncových stanicích s častým střídáním uživatelů v průběhu pracovní doby. Řešení musí poskytnout funkce více-faktorové autentizace na koncovém (klientském) zařízení přihlášeném pomocí jmenného účtu, pomocí obecného (skupinového) Active Directory účtu a pomocí obecného (skupinového) lokálního účtu. Ve všech případech musí být více-faktorové ověření provedeno jménem konkrétního uživatele, tedy přihlašování musí být prováděno uživatelským Active Directory účtem reprezentujícím konkrétní přihlašovanou osobu. Výše uvedené funkce musí být dostupné také na koncových stanicích, které nejsou členy Active Directory domény.		ANO
Single Sign-On (SSO)		
Řešení musí poskytovat funkci automatického přihlášení SSO (Single Sign-On) alespoň do následujících aplikací: [redacted] V případě webových aplikací musí být pro funkci SSO podporovány minimálně tyto prohlížeče: Microsoft Edge Chromium verze 110 a vyšší, Google Chrome verze 110 a vyšší. Dále musí být pro webové aplikace podporována autentizace pomocí protokolů SAML a OpenID Connect.		ANO

Řešení musí poskytovat funkci Single Sign-On do aplikací (popsaných v předchozím bodu) z koncových (klientských) zařízení používaných jedním uživatelem, používaných více uživateli, a dále na sdílených koncových stanicích s častým střídáním uživatelů v průběhu pracovní doby. Řešení musí poskytnout funkce SSO do aplikací (popsaných v předchozím bodu) na koncovém zařízení přihlášeném pomocí jmenného účtu, pomocí obecného (skupinového) Active Directory účtu a pomocí obecného (skupinového) lokálního účtu. Ve všech případech musí být funkce SSO poskytovány jménem konkrétního uživatele, tedy přihlašování do aplikací musí být prováděno uživatelským účtem reprezentujícím konkrétní přihlašovanou osobu. Výše uvedené funkce musí být dostupné také na koncových stanicích, které nejsou členy Active Directory domény.		ANO
Řešení musí zajišťovat funkčnost SSO pro aplikace, jejichž klientská strana běží jak na fyzických stanicích, tak ve virtuální ploše – VDI, virtualizované aplikace, server vzdálené plochy. Řešení musí poskytnout plnou funkčnost SSO pro nejběžnější technologie virtualizace aplikací a desktopů na trhu (Microsoft Remote Desktop Services, Citrix Virtual Apps and Desktops, VMware Horizon).		ANO
Přihlašovací údaje do jednotlivých aplikací musí být dostupné jen příslušnému uživateli. Přihlašovací údaje do jednotlivých aplikací a systémů jsou šifrovány, a musí být ukládány na serverovou stranu řešení, aby byly dostupné na každé koncové stanici, ke které se uživatel přihlašuje. Systém musí umožnit, aby pro kritické aplikace bylo přihlášení pomocí SSO vynucováno.		ANO
Řešení musí umožnit funkci SSO přihlašování do aplikací jak identitou (účtem) z Active Directory, tak účtem spravovaným danou aplikací. Řešení musí dále poskytovat funkcionalitu Identity Provider (IdP), kdy neuchovává přihlašovací údaje uživatelů.		ANO
Řešení bude obsahovat integrovaný správce hesel (Password Manager) pro všechny uživatele, s možností uživatelské správy. IT správce musí mít možnost nastavit, zda uživatel může přihlašovací údaje editovat nebo jen zobrazit, a dále, zda může zobrazit heslo v čitelné podobě. Funkce zobrazení hesla v čitelné podobě musí být možné dodatečně zabezpečit (např. vyžádáním hesla, PINu apod.).		ANO
Řešení musí obsahovat grafické uživatelské rozhraní pro vytváření, editaci a správu Single Sign-On napojení (konektorů/profilů). Toto prostředí musí být intuitivní a uživatelsky přívětivé, bez nutnosti psát kód, programovat, používat řádkové příkazy a umožnit zadavateli vytvářet vlastní napojení (konektory/profily) na další aplikace uživatelsky, vlastními silami, bez nutnosti objednávání nových napojení u dodavatele a bez nutnosti úprav kódu těchto aplikací.		ANO
Samoobslužný reset hesla		
Řešení musí poskytnout integraci na funkci samoobslužného resetu hesla Active Directory účtu a musí umožnit vyvolání této funkce z přihlašovací obrazovky klientské stanice, bez nutnosti se předem přihlásit.		ANO

Čtečky karet		
Požadované parametry stacionárních čteček bezkontaktních karet resp. tokenů, které v současnosti nemocnice používá: • [redacted] • Rozhraní: připojitelná přes USB • Typ: externí		ANO

• Napájení: přes USB rozhraní • Formát: stolní • Přenos dat: zabezpečený, přes API (nesmí simulovat klávesnici) • Kompatibilita OS: Windows 10 a vyšší		

8 System řízení přístupu do sítě 802.1x

[redacted]

Požadujeme velmi pokročilé řešení pro definici přístupových politik s velkou sadou připravených šablon pro různá nasazení. Kromě lokální báze uživatelů požadujeme napojení na Active Directory, klasický LDAP, libovolný ODBC databázový backend, token server nebo Kerberos či SQL, soubor nebo externí SSO řešení. Systém musí umožňovat reagovat v zásadě na cokoli jakkoli – pokud je třeba, je možné nastavit si svoje reakce na jakékoli atributy v RADIUS a TACACS+ protokolech, mapovat role na různá pole v externím systému (třeba atributy Active Directory) a vynucovat politiku přidáním jakýchkoli i nestandardních atributů. To vše pomocí jednoduchého ovládání, díky přednastaveným šablonám a průvodcům. Musí spolupracovat s infrastrukturou nezávisle na výrobci a je tedy z tohoto pohledu multiplatformní. Musí fungovat i se staršími přepínači, které 802.1x přímo nepodporují! Konfigurace takových přepínačů zabezpečuje modul, který pak přepínače řídí pomocí zápisů SNMP.

Schopnosti technologie musí jít daleko za obecné požadavky spojené s implementací 802.1x. Technologie v sobě musí integrovat hostovský a profiler modul. To znamená, že pod jedinou licencí zadavatel může konfigurovat 802.1x pro přístup zaměstnanců a svých zařízení a zároveň realizovat pokročilý portálový přístup hosta k sítí (drátové/bezdrátové). Technologie musí poskytovat skrze modul hosta vysoce pokročilý a škálovatelný přístup hosta na bázi prakticky jakéhokoli myslitelného druhu přístupu, od prostého odsouhlasení podmínek, přes tzv. vlastní registrace účtů přímo hostem, vouchery a předzaložené účty až např. po sponzorem aktivovaný přístup.

Profiler modul pak musí poskytovat především druhý faktor autentizace pro ta zařízení, které .1x nesplňují (tiskárny, terminály, projektory …) a přesto musí být připojena bezpečně k síti. Standardní ověření pomocí MAC adresy nelze považovat za bezpečné. Profiler musí každé přistupující zařízení prozkoumat, jak žádá o DHCP, na jaké porty se spojuje, na jakých naslouchá, co o sobě říkají protokoly (SNMP, LLDP, CDP …) a tento jedinečný „síťový otisk“ použít jako druhou autentizaci spolu s MAC.

PKI infrastruktura

V síti musí existovat hierarchie certifikačních úřadů, musí být funkční publikace odvolaných certifikátů (CRL) a v případě uvažovaného použití pro autentizaci klientského přístupu, pak musí jít i o publikaci do Internetu. Zařízení musí být vždy schopno získat aktuální seznam odvolaných certifikátů nehledě na polohu.

Pro ověření do VPN se předpokládá klientský certifikát vázaný na uživatele, naopak pro ověřování přístupu do vnitřních sítí musí být možno použít certifikát vázaný na zařízení. Auto-entrollement procesy za pomoci AD a potažmo GP objektů musí zajistí vystavení a aktualizaci certifikátů všem kompatibilním zařízením bez zásahu uživatele či administrátora. O vystavení svého uživatelského certifikátu musí uživatelé sami být schopni požádat skrze k tomu určený webový portál s příslušnou šablonou certifikátu.

[redacted]

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE/

Příloha č. 1 – technická specifikace

		hodnota (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)
Podpora 802.1X autentizace pro bezdrátové sítě, Ethernet LAN sítě a VPN připojení	ANO	ANO
Forma dodání: virtuální appliance pro [redacted]	ANO	ANO
Minimální celková kapacita řešení pro autentizaci unikátních koncových zařízení	1000 v redundantním clusteru	ANO
Řešení musí poskytovat vysokou dostupnost tak aby v případě výpadku primárního serveru převzal jeho roli sekundární server.	ANO	ANO
Možnost vytváření clusteru více virtuálních appliance. Minimální počet podporovaných appliance v clusteru.	ANO	ANO
Cluster musí poskytovat vysokou dostupnost pro všechny funkcionality řešení a zároveň možnost navýšení počtu podporovaných uživatelů přidáním další instance.	ANO	ANO
Podpora minimálně 20ti předních světových výrobců síťových zařízení (LAN switche, WiFi řešení, obecně přístupové datové sítě)	ANO	ANO
Požadované metody autentizace uživatelů a zařízení	PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, MAC autentizace	ANO
Podpora RADIUS CoA	ano – dle RFC3576	ANO
Podpora autorizace zařízení a uživatelů na základě kontextových informací jako čas, místo připojení, osobní profil či skupina v AD	ANO	ANO
Možnost autorizace uživatelů na základě jejich vlastních accounting informací z předchozích připojení – např. za účelem omezení celkového času online či objemu přenesených dat za delší časové období	ANO	ANO
Možnost TACACS+ autentizace správců síťových zařízení	ANO	ANO
Další požadované autentizační a autorizační zdroje a metody.	LDAP, MS AD, Token, MAC, generická SQL databáze, Kerberos,	ANO

	HTTPS web autentizace, Single Sign-On (minimálně SAML 2+ IdP a SP, OAuth, Shibboleth a Okta)	
Možnost integrace s MDM (Mobile Device Management) platformami třetích stran	minimálně AirWatch, Citrix, MobileIron, JAMF, InTune	ANO
Podpora REST API pro většinu základních úkonů AAA platformy	ANO	ANO
Podpora REST volání vyvolaného autentizační či autorizační událostí (minimálně pro předání informací o klientovi jinému systému, automatického založení support ticketu atp.)	ANO	ANO
Zpracovávání syslog hlášení z externích zdrojů, vyhledávání klíčových událostí a automatizovaná reakce na ně. Minimálně v rozsahu přijmutí bezpečnostního hlášení z firewallu a izolace konkrétního klienta na základě tohoto hlášení.	ANO	ANO
Administrátor systému musí mít možnost vlastní tvorby parseru/integrace syslog hlášení pro možnost uživatelské integrace s libovolnými systémy třetích stran.	ANO	ANO
Sběr dodatečných informací o připojených zařízeních (“profiling”) jako jsou DHCP volby klienta, HTTP uživatelský agent či předvolba MAC adresy. Tyto informace musí být možné využít pro doplňkové ověření přístupu zařízení do sítě.	ANO	ANO
LAN a WLAN Guest portál. Portál musí podporovat možnost přihlašování přes účty minimálně těchto sociálních sítí – Linkedln, Facebook, Twitter, Google+. Portál musí umožňovat bohatou grafickou úpravu včetně možnosti přidávání videí a dalšího dynamického obsahu. Možnost samoobslužné registrace hosta do sítě s SMS, email ověřením nebo na elektronickou notifikaci a schválení pověřených pracovníků.	ANO	ANO
Možnost licenčního rozšíření o bezpečnou registraci soukromých zařízení do interní sítě na základě uživatelských údajů z AD či LDAP. Uživatel musí být schopen jednoduchým uživatelským wizardem instalovat osobní certifikát a síťový profil na své soukromé zařízení (BYOD systém).	ANO	ANO
Možnost licenčního rozšíření o certifikační autoritu pro vydávání certifikátů na soukromá zařízení musí být součástí AAA platformy.	ANO	ANO
Možnost licenčního rozšíření o samoobslužný portál pro hosty či interní uživatele s možností správy svých vlastních registrací.	ANO	ANO

Možnost licenčního rozšíření o systém pro bezpečnostní kontrolu přistupujících zařízení před jejich vpuštěním do sítě pomocí software agenta na koncová zařízení.	ANO	ANO
Možnost licenčního rozšíření o kontroly stavu registrů, spuštěných procesů, stavu síťových zařízení, nastavení firewallu, aktualizace antivirů, instalované VM, stav enkrypce disku.	ANO	ANO
Možnost licenčního rozšíření o podporu jednorázového i permanentního klienta pro kontroly na koncových zařízeních. Podpora klienta pro kontrolu koncových zařízení na OS Windows, MAC OS a Linux	ANO	ANO
Možnost licenčního rozšíření o integraci tohoto koncového klienta s VPN klientem	ANO	ANO
Jakékoliv funkční rozšíření systému musí být vždy v rámci stejné virtuální appliance jako je AAA systém.	ANO	ANO
Servisní podpora na [redacted] garantovaná přímo výrobcem zařízení v režimu 24x7. Možnost otevírat servisní požadavky přímo u výrobce.	ANO	ANO

[redacted]

9 Systém pro analýzu síťového provozu a bezpečnostní monitoring

[redacted]

TECHNICKÁ SPECIFIKACE :

Systém pro analýzu síťového provozu a bezpečnostní monitoring, který okamžitě identifikuje bezpečnostní rizika a události a který splňuje klíčové požadavky uvedené níže.
Nabízená technologie musí být určená pro český trh. Podpora na licence ve všech úrovních musí být zajištěna přímo jejich výrobcem, kterého může zadavatel přímo kontaktovat.
Při definici technických požadavků jsou všechny uvedené požadavky závazné. Je-li definice požadavku „umožňuje, lze, je možné, možnost, …“ je uvedený parametr závazný a požadovaná funkcionalita musí být v rámci Systému dodána/naimplementována a případně licencována. Tyto technické požadavky jsou minimální možné, dodavatel může nabídnout charakteristiky (funkce) lepší.

Řešení musí splňovat **VŠECHNY** níže uvedené požadavky:

Požadované funkcionality/vlastnosti	**Nabízené řešení splňuje/nesplňuje,** vč. vysvětlení jak je požadavek splněn, je-li vysvětlení relevantní (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)
Systém pro analýzu síťového provozu	
Systém složený z hardwarových zařízení musí monitorovat síťovou aktivitu v reálném čase a identifikovat potenciální kybernetické hrozby, bezpečnostní rizika a anomální chování a musí o nich v reálném čase vytvářet upozornění.	**Nabízené řešení postavené na kombinaci příslušné SW licence a HW monitoruje síťovou aktivitu v reálném čase, identifikuje hrozby, bezpečnostní rizika i anomální chování a vytváří upozornění o těchto událostech v reálném čase. Upozornění je odesláno okamžitě dle nastavení správce.**
Dodaný systém musí analyzovat síť na základě zrcadleného síťového provozu ze SPAN portů nebo TAPů (nikoliv jen na základě statistických protokolů typu NetFlow) a zároveň	**Nabízené řešení analyzuje síť na základě zrcadleného síťového provozu ze SPAN portů nebo TAPů a nevyžaduje instalaci agentů na jakákoliv další zařízení**

bez potřeby nasazovat agenty na koncové stanice nebo další zařízení v síti.	**v síti. V případě potřeby zadavatele dokáže analyzovat také statistické protokoly.**
Systém musí analyzovat obsah datových paketů v reálném čase a detekovat protokol nebo aplikaci na základě obsahu provozu prostřednictvím DPI (Deep Packet Inspection), nikoli pouze čísla portu.	**Nabízené řešení analyzuje obsah datových paketů v reálném čase a prostřednictvím Deep Packet Inspection.**
Dodaný systém musí být schopen analyzovat síť také na základě zpracování statistických protokolů typu NetFlow, IPFIX, NetStream, Cisco NSEL a případně dalších obdobných.	**Nabízené řešení umožňuje analyzovat síť také na základě zpracování protokolů typu NetFlow, IPFIX, NetStream, Cisco NSEL a dalších dle potřeby zadavatele.**
Systém musí být plně funkční v offline prostředí objednatele bez využití cloudového prostředí pro sběr, ukládání a zpracování dat a veškeré konfigurace a reporting jsou k dispozici přímo v systému.	**Nabízené řešení lze provozovat zcela v offline prostředí zadavatele, konfiguraci může provést obsluha přímo v systému, stejně jako vytváření požadovaných reportů. Sběr, ukládání a zpracování dat může probíhat lokálně v offline režimu.**
Aktualizace systému musí být možné provádět uživatelsky v offline režimu.	**Aktualizaci nabízeného řešení je možné provádět v offline režimu, tento postup je běžně využíván pro bezpečnostní složky, kde není povolen přímý přístup ze sítě k veřejnému internetu. Nové verze SW i aktualizace signatur hrozeb a zranitelností v takovém případě získává zadavatel jiným způsobem, například přes proxy.**
Zpracování a ukládání síťových toků	
Systém ukládá síťové toky ve formátu, který umožní analýzu síťové komunikace na úrovni jednotlivých toků, včetně dohledání informací o aplikačních transakcích a jejich metadatech z L2 až L7, obsažených v daném síťovém toku.	**Nabízené řešení ukládá síťové toky ve formátu, který umožňuje analýzu síťové komunikace na úrovni jednotlivých toků, včetně dohledání informací o aplikačních transakcích a jejich metadatech z L2 až L7, obsažených v daném síťovém toku. Data jsou uložena v softwarově akcelerovaných databázích pro okamžitý přístup k datům. U všech toků jsou obsaženy volumetrické, statické a dynamické vlastnosti toku, a dále dle protokolu obsah**

	aplikačních metadat nebo plný obsah protokolu. Nabízené řešení detailně (aplikační detail) zpracovává asi 70 protokolů, šifrovaných i nešifrovaných a uchovává až 2000 parametrů pro jeden síťový tok. Dále uživatel může nechat zaznamenávat definovanou velikost aplikačního obsahu nebo i celý aplikační obsah u každého toku.
Požadované protokoly pro ukládání aplikačních metadat z jednotlivých transakcí jsou: DHCP, DNS, SMB, HTTP, HTTPS, SMTP, SMTPS, POP3, IMAP, SSH, LDAP, LDAPS, KERBEROS, SNMP, CIFS, MSSQL, RDP, SIP, TELNET, FTP, FTP-DATA, TFTP, TFTP-DATA, NFS, ARP, SSL/TLS zapouzdření.	**Nabízené řešení využívá pro ukládání aplikačních metadat z jednotlivých transakcí následující protokoly: DHCP, DNS, SMB , HTTP, HTTPS, SMTP, SMTPS, POP3, IMAP, SSH, LDAP, LDAPS, KERBEROS, SNMP, CIFS, MSSQL, RDP, SIP, TELNET, FTP, FTP-DATA, TFTP, TFTP-DATA, SSL/TLS zapouzdření**
Je požadováno vysokorychlostní úložiště pro uchování historie datových toků minimálně 3 TB.	**Nabízené řešení zahrnuje vysokorychlostní úložiště pro uchování datových toků 2x1,92 TB SSD SATA, tj, celkem 3,8 TB úložiště.**
Analýza aplikačních a systémových logů Systém musí být schopen sbírat a analyzovat aplikační a systémové logy ve formátu syslog z dohledovaných zařízení a identifikovat nebezpečné nebo potenciálně škodlivé aktivity.	**Nabízené řešení z dohledovaných zařízení sbírá a analyzuje aplikační a systémové logy ve formátu syslog, detekuje nebezpečné a potenciálně škodlivé aktivity využitím všech aplikovaných metod identifikace uvedených dále ve specifikaci.**
Uživatelské rozhraní	
Systém musí poskytovat jednotné grafické uživatelské rozhraní pro veškerou práci uživatelů, včetně všech detekcí, analýzy síťových statistik, nastavení systému, konfiguraci alertů, reportů a dashboardů.	**Nabízené řešení poskytuje jednotné grafické rozhraní pro uživatele a veškerou jejich práci se systémem; uživatel si může nastavit rozhraní se světlou nebo tmavou grafikou dle svých preferencí.**
Systém musí být schopen vytváření profilů a skupin uživatelů pro omezení funkcionality produktu a viditelnosti uložených dat s podporou minimálně:	**Administrátor nabízeného řešení má možnost vytvářet profily jednotlivých uživatelů a jejich skupin s definovanými oprávněními k funkcionalitám řešení a omezeným přístupem**

	k datům. Administrátor nastavuje:
· granulárního nastavení přístupu k analytickým i konfiguračním/administrativním komponentám systému s definovanými úrovněmi přístupu (alespoň read, write, execute),	**- přístupy a omezení k analytickým a konfiguračním komponentám s požadovanou úrovní přístupu R/W/Execute**
· granulárního nastavení přístupu k datům z různých segmentů sítě organizace s definovanými úrovněmi přístupu (alespoň read, write, execute),	**- granulární přístupy k datům z jednotlivých segmentů sítě s požadovanými úrovněmi R/W/E**
· vytváření vlastních filtrů veškerých dat a jejich sdílení mezi uživateli a skupinami uživatelů,	**- filtry dat a jejich sdílení mezi jednotlivými uživateli a/nebo jejich skupinami**
· vytváření vlastních uživatelských pohledů, reportů, dashboardů apod.	**Uživatelé mohou vytvářet vlastní dashboardy, filtry a reporty v rámci svých oprávnění.**
Automatické hlášení (alerty) a reporting	
Systém musí být schopen upozorňovat uživatele prostřednictvím minimálně emailu a logu o všech identifikovaných událostech a dále o událostech filtrovaných minimálně dle IP a MAC adresy, podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu.	**Nabízené řešení upozorňuje uživatele prostřednictvím přednastaveného typu komunikace, např. mailem na zvolené adresy a logy o všech identifikovaných událostech i o událostech filtrovaných dle IP a MAC adresy, podsítě, závažnosti a kategorie události, země, uživatele, síťové služby, čísla portu, provozu z a do internetu.**
Tyto alerty musí být systém schopen dodávat i ve strojově čitelném formátu pro vyžití v nástrojích typu SIEM a musí obsahovat minimálně kompletní informace o detekované události včetně URL odkazu na danou událost v reportovaném období do grafického rozhraní systému.	**Nabízené řešení dodává tyto aletry i ve strojově čitelném formátu pro využití v produktech třetích stran, například SIEM, obsahuje kompletní informace o detekované události včetně URL odkazu na událost v reportovaném období do grafického rozhraní.**
Systém musí mít možnost vytváření automatizovaných manažerských reportů o stavu kybernetické bezpečnosti z pohledu zprávy kybernetických incidentů ideálně dle oblastí jejich vzniků (např.: doména, web, email apod.).	**Nabízené řešení umožňuje vytvářet automatizované manažerské reporty o stavu kybernetické bezpečnosti z pohledu správy kybernetických incidentů dle oblasti jejich vzniku (doména, web, e-mail apod.)**

Je požadováno vytváření automatizovaných reportů v českém jazyce.	**Reporty lze vytvářet v českém jazyce.**
Integrace systému	
Systém musí poskytovat hotové nástroje umožňující integraci se softwarem třetích stran bez použití API systému, a to minimálně:	**Nabízené řešení disponuje hotovými nástroji pro integraci se SW třetích stran bez použití API, včetně:**
· syslog, CEF a LEEF pro export událostí včetně plné podpory filtrů (exportování pouze požadovaných dat)	**Syslog, CEF a LEEF pro export událostí včetně podpory filtrů**
· přímé url odkazy na libovolnou obrazovku grafického uživatelského rozhraní a filtrovaná zobrazení v grafickém uživatelském rozhraní	**Přímé URL odkazy na jakoukoliv obrazovku GUI a filtrovaná zobrazení v GUI**
· export informací o toku ve formátu IPFIX nebo podobném formátu včetně plné podpory filtrů (exportovat lze pouze požadovaná data)	**Export informací o toku ve formátu IPFIX a jemu podobných včetně podpory filtrů**
· integrace se službami identity uživatelů bez nutnosti konfigurace zasílání logů do systému Microsoft Active Directory	**Integraci se službami identity uživatelů bez nutnosti konfigurace zasílání logů, např. Cisco ISE, Microsoft Active Directory**
· integrace s firewally pro automatické a manuální reakce vyvolané systémem	**Integraci s firewally Palo Alto, Fortigate, Checkpoint a dalšími pro aktivní automatický i manuální response**
· integrace s nástroji pro řízení přístupu k síti, pro automatickou a manuální reakci systému.	**Integraci s nástroji pro řízení přístupu k síti, např. Cisco ISE, pro automatický i manuální response**
Podpora EDR	
Systém musí poskytovat nástroje umožňující přímou integraci se softwarem EDR třetích stran pro získání informací a zkvalitnění detekce.	**Nabízené řešení umožňuje přímou integraci s EDR nástroji třetích stran pro získání informací a zkvalitnění detekce událostí.**

Požadavky na architekturu nasazení

Požadované funkcionality/vlastnosti	**Nabízené řešení splňuje/nesplňuje,** vč. vysvětlení jak je požadavek splněn, je-li vysvětlení relevantní (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku

	představuje nesplnění zadávacích podmínek)
Obecné požadavky pro nasazení	
Pro všechny HW komponenty senzor a kolektor je požadován formát 1U nebo 2U server o velikosti 19“.	**Všechny navržené HW komponenty senzor, kolektor i all-in-one jsou dodávány jako server formátu 1U nebo 2U o velikosti 19“.**
Pro všechny HW komponenty senzor a kolektor je požadován duální zdroj napájení se schopností hot-swap.	**Všechny HW servery jsou dodávány s duálním zdrojem napájení se schopností hot-swap.**
Pro všechny HW komponenty senzor a kolektor je požadováno samostatné síťové rozhraní pro vzdálenou správu serveru v případě výpadku systému typu IPMI, IDRAC, ILO apod.	**Veškeré HW servery (senzory, kolektory i all-in-one) jsou dodávány se samostatným síťovým rozhraním pro vzdálenou správu serveru pro případ výpadku nabízeného řešení typu IPMI, IDRAC, ILO apod.**
Požadavky pro pokrytí IT prostředí	

[redacted]

Požadavky na schopnost detekce bezpečnostních událostí

Požadované funkcionality/vlastnosti	**Nabízené řešení splňuje/nesplňuje,** vč. vysvětlení jak je požadavek splněn, je-li vysvětlení relevantní (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)
Monitorování zařízení, segmentů sítě a využívaných síťových služeb	

Dodaný systém musí identifikovat všechna zařízení připojená do sítě včetně koncových zařízení, serverů, IoT zařízení apod. Zároveň musí být systém schopen identifikovat změny v síti – minimálně:	**Nabízené řešení identifikuje všechna zařízení připojená do sítě (koncových zařízení, serverů, IoT zařízení apod.) a identifikuje následující změny v síti:**
· změna IP/MAC adresy hosta,	**Změnu IP/MAC adresy hosta**
· duplicitní IP/MAC adresa,	**Duplicitní IP/MAC adresu**
· změna VLAN,	**Změnu VLAN**
· vytvoření nové podsítě,	**Vytvoření nové podsítě**
· připojení nového zařízení,	**Připojení nového zařízení**
· použití nebo vznik nové služby,	**Použití nebo vznik nové služby**
· nedostupnost dříve dostupné a komunikující služby nebo dříve dostupného a komunikujícího zařízení,	**Nedostupnost dříve dostupné a komunikující služby a dříve dostupného a komunikujícího zařízení**
· přístup nového zařízení ke službě či zařízení	**Přístupy novách zařízení ke službám a/nebo zařízením**
· ověřování platnosti interních certifikátu pro validní TLS šifrování u HTTPS a upozornění před datem jejich vypršení.	**Ověřování platnosti interních certifikátů pro validní TLS šifrování u HTTPS a upozornění před datem jejich vypršení.**
Systém musí uživateli umožnit pomocí těchto detekčních metod nastavovat bezpečnostní politiky pro různé segmenty sítě a pro různá zařízení a na porušení těchto politik reagovat upozorněním.	**Nabízené řešení umožňuje uživateli pomocí detekčních metod nastavovat bezpečnostní politiky pro různé segmenty sítě a různá zařízení a upozornit na jejich porušení.**
Samostatné učení behaviorálních aktivit a detekce anomálií	
Systém musí používat matematické metody samostatného učení pro analýzu síťové aktivity, vytvářet a v čase automaticky modifikovat modely chování na základě běžného chování jednotlivých zařízení a na nich provozovaných služeb v rámci celé organizace.	**Nabízené řešení používá matematické metody samostatného učení pro analýzu síťových aktivit, vytváří a automaticky v čase modifikuje modely chování na základě chování jednotlivých zařízení a provozovaných služeb v rámci celé organizace.**
Systém musí mít schopnost na základě matematického modelu daného zařízení a jeho služeb identifikovat nestandardní síťové chování, a to zejména odchylky od modelu normálního chování pro:	**Nabízené řešení identifikuje nestandardní síťové chování na základě matematického modelu daného zařízení a jeho služeb. Zejména detekuje následující**

	odchylky od normálního chování:
· odchylku od modelu pro přenos dat, toků a paketů,	**Odchylky pro přenos dat, toků a paketů**
· odchylku od modelu pro počet komunikačních partnerů,	**Odchylky pro počet komunikačních partnerů**
· odchylku od modelu entropie na komunikačních portech,	**Odchylky od modelu entropie na komunikačních portech**
· odchylku od modelu pro počet síťových toků a využitých síťových služeb,	**Odchylky od modelu pro počet síťových toků a využitých síťových služeb**
· odchylku od modelu výkonnosti sítě (rychlost přenosu) a aplikací (doba odezvy).	**Odchylky od modelu výkonnosti sítě a aplikací, tedy rychlosti přenosu a doby odezvy**
Samostatné učení je požadováno na všech síťových zařízeních a na nich provozovaných službách (port číslo 0 až 65535 u TCP i UDP) na IPv4 a IPv6 a dalších protokolech L3 a L4 síťové vrstvy.	**Nabízené řešení využívá metodu samostatného učení na všech síťových zařízeních a na nich provozovaných službách – porty 0 – 65535 u TCP a UDP, na IPv4 a IPv6, na dalších protokolech L3 a L4**
Identifikace neznámých hrozeb a podezřelých chování	
Systém musí být schopen detekovat neznámé hrozby, které nelze identifikovat prostřednictvím detekčních signatur, jako jsou trojské koně, botnety apod. Zejména musí být identifikovány tyto příznaky potenciálně škodlivého chování:	**Nabízené řešení detekuje neznámé hrozby, které není možné odhalit pomocí detekčních signatur – trojské koně, botnety apod, zejména následující příznaky škodlivého chování:**
· průzkumné aktivity v síti,	**Průzkumné aktivity v síti**
· detekce podezřelého strojového chování, které nevytvářejí lidští uživatelé sítě,	**Podezřelé strojové chování, které neodpovídá aktivitě lidských uživatelů sítě**
· detekce repetitivních vzorců chování na síti,	**Repetitivní vzorce chování v síti**
· detekce botnetů a ovládání kompromitované stanice,	**Botnety a ovládání kompromitované stanice**
· detekce příznaků těžení kryptoměn,	**Příznaky těžby kryptoměn**
· útoky hrubou silou a enumerace dat,	**Útoky hrubou silou a enumerace dat**

· rozpoznání tunelovaného síťového provozu – alespoň IPv4 prostřednictvím IPv6 a DNS tunely.	**Tunelovaný síťový provoz IPv4 prostřednictvím IPv6 a DNS tunely**
Detekce na základě databáze známých hrozeb	
Systém musí být schopen identifikovat hrozby a reportovat události na základě	**Nabízené řešení identifikuje hrozby a reportuje události na základě:**
· detekční databáze známých hrozeb, tj. malware (trojské koně, viry, červy, rootkity, apod.), známých útoků (exploity) a zranitelností, porušení bezpečnostních pravidel a „best practices“ a dalších rizik,	**Detekční databáze známých hrozeb – malware, známých útoků a zranitelností, porušení bezpečnostních pravidel a best practices a dalších hrozeb**
· reputační databáze známých škodlivých IP adres, TLS certifikátů, záznamů DNS a hostname, URL adres a hashů souborů.	**Reputační databáze známých škodlivých IP adres, TLS certifikátů, záznamů DNS a hostname, URL adres a hashů souborů**
Tyto databáze musí být aktualizované minimálně na hodinové bázi. Nesmí se jednat pouze o volně dostupné/open-source databáze, ale musí se jednat o komerční databázi renomovaného vendora nebo poskytovatele těchto služeb.	**Nabízené řešení využívá profesionální licencovanou reputační databázi ProofPoint, která je aktualizovaná každou hodinu.**
Uživatel musí být schopen importovat vlastní záznamy.	**Nabízené řešení umožňuje uživateli importovat vlastní záznamy**
Systém musí využívat tuto detekci pro veškerý monitorovaný provoz (na perimetru i v interní síti mezi všemi segmenty), nikoliv pouze pro omezený segment nebo podmnožinu celkové komunikace.	**Nabízené řešení využívá tuto metodu detekce pro veškerý monitorovaný provoz v interní síti mezi všemi segmenty i na perimetru sítě.**
Databáze detekčních pravidel (signatur) musí být založena na pokročilých regulárních výrazech pro zpracování řetězců, které dokáží provádět inspekci veškeré síťové komunikace od L2 (Ethernet apod.) po L7. Systém musí detekovat události na základě vysokého počtu signaturních pravidel (minimálně několik desítek tisíc).	**Databáze detekčních pravidel v nabízeném řešení je založena na pokročilých regulárních výrazech pro zpracování řetězců, které provádí inspekci veškeré síťové komunikace od L2 po L7. Řešení detekuje události na základě více než 90 tisíc signaturních pravidel.**
Uživatel musí být schopen přidávat vlastní detekční pravidla v praktickém a obecně využívaném formátu. Příklad možné syntaxe detekčního pravidla:	**Nabízené řešení umožňuje uživateli přidávat vlastní detekční pravidla v běžně**

alert tcp $HOME_NET any -> any any (msg:"Command Shell Access"; *content:"C:\\Users\\Administrator\\Desktop\\hfs2.3b";* *sid:1000001; rev:1;)*	**využívaném formátu, jako je uvedený příklad.**
Analýza šifrované komunikace Vedle samostatného učení musí systém používat další metody pro analýzu šifrované komunikace, minimálně TLS fingerprinting a s ní spojenou detekci známých hrozeb.	**Nabízené řešení používá pro analýzu šifrované komunikace rovněž TLS fingerprinting a s tím spojenou detekci známých hrozeb.**
Asistované učení	
Je požadován uživatelsky přívětivý proces vytváření pravidel pro zpřesnění detekce a eliminaci falešně pozitivní detekce, a to na základě minimálně následujících parametrů:	**Nabízené řešení umožňuje uživatelsky snadné vytváření pravidel pro zpřesnění detekce a eliminaci falešně pozitivní detekce na základě následujících parametrů:**
· IP adresa,	**IP adresy**
· MAC adresa,	**MAC adresa**
· hostname,	**Hostname**
· segment sítě / podsíť,	**Segment sítě / podsíť**
· lokalita – ASN, země, apod.	**Lokalita – ASN, země apod.**
· směr komunikace – určení klienta, nebo serveru,	**Směr komunikace, určení klienta a serveru**
· detekovaná událost – kategorie, název apod.	**Kategorie události, název apod.**
· použité služby, protokolu, portu,	**Služba, protokol, port…**
· libovolné kombinaci výše popsaných.	**Kombinace uvedených parametrů**
Systém musí být schopen eliminovat falešné alarmy i pro události detekované v historii.	**Nabízené řešení umí eliminovat falešné alarmy také pro události, které byly detekované v minulosti.**

Požadavky na zajištění síťové viditelnosti

Požadované funkcionality/vlastnosti	**Nabízené řešení splňuje/nesplňuje,** vč. vysvětlení jak je požadavek splněn, je-li vysvětlení relevantní (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku

	představuje nesplnění zadávacích podmínek)
Vyhledávání, filtrování a vizualizace dat	
Systém musí být schopen okamžitého (v řádu vteřin) vyhledávání a vizualizace pro forenzní analýzu a podporu threat hunting bez zvláštního dotazovacího jazyka.	**Nabízené řešení vyhledává a vizualizuje výsledky pro forenzní analýzu a podporu threat hunting bez speciálního dotazovacího jazyka v řádu vteřin.**
Jedná se o možnost okamžitě filtrovat a vyhledávat v plné historii všech uložených dat, tj. bezpečnostních událostí, síťových toků a agregovaných síťových statistikách (tabulky a grafy), a to minimálně:	**Nabízení řešení bez časového zpoždění filtruje a vyhledává údaje v plné historii všech uložených dat (bezpečnostních událostí, síťových toků a agregovaných statistikách – tabulkách a grafech) podle následujících parametrů:**
· podle parametrů IP a MAC adresa, hostname, username (identita uživatele), příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (služba z pohledu klient nebo server), číslo portu, VLAN, země, ASN,	**IP a MAC adresa, hostname, identita uživatele, příchozí/odchozí provoz, síťová služba, lokální/vzdálená služba (z pohledu klinet/server), číslo portu, VLAN, země, ASN**
· prostřednictvím full-textového vyhledávání v datech a vyhledávání na základě definice směru (zdroj, cíl) a logických výrazů and, or, not.	**Full-text vyhledávvání v datech a na základě definice zdroje/cíle a logických výrazů (AND/OR/NOT).**
Systém musí pro vyhledávání poskytovat již předpočítané hodnoty výkonnostních a behaviorálních charakteristik pro každé zařízení v síti a pro všechny na něm provozované služby, bez nutnosti zpracování surových dat ze síťových logů.	**Nabízené řešení poskytuje pro vyhledávání předpočítané hodnoty výkonnostních a behaviorálních charakteristik pro jednotlivá zařízení v síti a pro všechny na nich provozované služby bez nutnosti zpracování surových dat ze síťových logů.**
Systém musí být schopen filtrovat a vizualizovat výsledky v grafech, výčtových tabulkách s možností řazení a TOP N statistikách.	**Nabízené řešení filtruje a vizualizuje výsledky v grafech, výpočtových tabulkách a možností řazení a TOP N statistikách.**
Systém musí být schopen ukládat a následně vyhledávat aplikační metadata (vždy dotaz i odpověď všech transakcí v toku) minimálně z následujících protokolů, které jsou nebo mohou být využívány ve vnitřní síti organizace: FTP, FTP-DATA, TFTP, TFTP-DATA, SSH, Telnet, SMTP, SMTPS, DNS, DHCP,	**Nabízené řešení ukládá a vyhledává aplikační metadata (dotaz i odpověď všech transakcí v toku) z protokolů: FTP, FTP-DATA, TFTP, TFTP-DATA, SSH,**

HTTP, HTTPS, NTP, SMB, SNMP, LDAP, NFS, RDP, ARP, MS-SQL, SIP, Kerberos, SSL/TLS. Metadata jsou v tomto případě chápána jako přenášená aplikační metadata nebo vlastní data servisních protokolů. U protokolu HTTP například http hlavička s metodou, URI, host, user-agent, cookies apod. V odpovědi pak návratový kód a další http parametry.	**Telnet, SMTP, SMTPS, DNS, DHCP, HTTP, HTTPS, NTP, SMB, SNMP, LDAP, NFS, RDP, ARP, MS-SQL, SIP, Kerberos, SSL/TLS**
Systém umožnuje provádět uživatelsky jednoduché a okamžité vizualizace síťových prostupů mezi zařízeními a podsítěmi. Využitím uživatelského datového filtru lze vizualizační pohledy libovolně modifikovat.	**Nabízené řešení poskytuje uživateli možnost jednoduše a okamžitě vizualizovat síťové prostupy mezi zařízeními a podsítěmi, tyto vizualizační pohledy může uživatel libovolně upravovat díky uživatelskému datovému filtru dle vlastních potřeb.**
Kontextuální informace	
Systém musí být schopen pro každé zařízení získávat, vizualizovat a v jednom grafickém pohledu zobrazovat kontextuální informace:	**Nabízené řešení získává, vizualizuje a v jednom grafickém pohledu zobrazuje pro každé zařízení následující kontextuální informace:**
· jméno uživatele a další jeho parametry z doménového řadiče (MS Active Directory), včetně její historie	**Jméno uživatele a další parametry doménového řadiče – MS AD včetně historie**
· hostname zařízení a jeho historie na základě zpracování relevantních dat z DNS a DHCP provozu	**Hostname zařízení a jeho historii na základě zpracování relevantních dat z DNS a DHCP provozu**
· IP geolokace	**IPO geolokaci**
· IP reputace, vč. údaje, jestli je IP adresa na blacklistu nebo podezřelá	**IP reputaci včetně informaí, zda je IP adresa na blacklistu / podezřelá**
· historie použitých MAC adresa a výrobce zařízení	**Historii použitých MAC adres a výrobce zařízení**
· operační systém a jeho historie na zařízení	**Operační systém a jeho historii na zařízení**
· uživatelem zadané poznámky a informace k zařízení	**Uživatelsky zadané poznámky a informace o zařízení**
· automaticky přiřazené značky/tagy zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna,	**Automaticky přiřazené tagy zařízení popisující jejich účel a chování: server doménového řadiče, webový server, poštovní**

administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy.	**server, DNS, SSH, DB server, tiskárna, admin. zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy.**
· seznam provozovaných a využívaných služeb (klient a server) u daného zařízení a množství na nich přenesených dat.	**Seznam provozovaných a využívaných služeb klient/server u zařízení a množství na nich přenesených dat.**
· seznam detekovaných bezpečnostních a provozních událostí daného zařízení.	**Seznam detekovaných bezpečnostních a provozních událostí daného zařízení.**
Zaznamenávání a ukládání plného provozu Je požadováno volitelné nahrávání plného síťového provozu (full packet capture) ve formátu PCAP na všech dodaných zařízeních minimálně na základě parametrů: cílová a zdrojová IP/MAC adresa, podsíť, využitý protokol, IPv4 nebo IPv6. Zaznamenávání je možno zapínat automaticky dle detekovaných událostí, nebo uživatelskou aktivací.	**Nabízené řešení umožňuje volitelné nahrávání plného síťového provozu – full packet capture ve formátu PCAP na všech dodaných zařízeních na základě parametrů: cílová a zdrojová IP/MAC adresa, podsíť, využitý protokol, IPv4 /IPv6. Zaznamenávání lze zapínat automaticky na základě detekovaných událostí nebo uživatelskou aktivací.**

Další požadované oblasti využití

Požadované funkcionality/vlastnosti	**Nabízené řešení splňuje/nesplňuje,** vč. vysvětlení jak je požadavek splněn, je-li vysvětlení relevantní (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)
Monitorování politik kybernetické bezpečnosti	
Systém musí umožňovat vytváření komplexních komunikačních a bezpečnostních politik, a to minimálně:	**Nabízené řešení umožňuje vytváření komplexních komunikačních a bezpečnostních politik s následujícími parametry:**

· monitorovat definovanou komunikační matici a detekovat, kdy jsou tyto matice porušeny – alespoň jaké zařízení smí komunikovat s jakým zařízením, přes jaký protokol, v jakém čase.	**Monitorování definované komunikační matice a detekování v případě porušení – jaké zařízení má povoleno komunikovat s jakých zařízením, přes jaký protokol a v jakém čase**
· detekce změn v síti – přinejmenším nové komunikační vektory, nová nebo změněná zařízení a podsítě, obcházení perimetru.	**Detekci změn v síti – komunikační vektory, nová/změněná zařízení a podsítě, obcházení perimetru.**
Pro účely monitorování politik kybernetické bezpečnosti musí systém poskytovat uživatelský rámec pro definování pravidel pomocí:	**Nabízené řešení poskytuje pro monitorování politik KB uživatelské prostředí pro definování pravidel pomocí následujících parametrů:**
· uživatelem definované podsítě na základě rozsahů IP adres	**Uživatelem definované podsítě na základě rozsahů IP adres**
· uživatelsky libovolně definovaných skupin zařízení	**Uživatelsky libovolně definovaných skupin zařízení**
· automaticky přiřazené značky/tagu zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy.	**Automaticky přiřazených tagů zařízení popisujících jejich účel a chování – server doménového řadiče, webový server, poštovní server, DNS, SSH, DB server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy.**
Management bezpečnostních událostí a incidentů	
Systém musí poskytovat funkcionalitu pro reporting bezpečnostních incidentů (prohlášení identifikované události za bezpečnostní incident), včetně:	**Nabízené řešení umožňuje reporting bezpečnostních incidentů (označení události za bezpečnostní incident) s následujícími parametry:**
· spolupráci a sdílení informací při analýze identifikovaných bezpečnostních incidentů včetně potřebného workflow mezi jednotlivými uživateli s podporou automatizovaných oznámení o změně stavu události či přiřazení řešitele,	**Sdílení informací při analýze identifikovaných incidentů včetně souvisejícího workflow mezi uživateli s podporou automatizovaných oznámení o změně stavu události a přiřazení řešitele**
· jednoduché sdílení informací o bezpečnostních incidentech, včetně uživatelem zadaných komentářů,	**Sdílení informací o bezpečnostních incidentech**

	včetně uživatelsky vložených komentářů
· možnost vyhledávání a filtrování nad všemi událostmi z pohledu workflow bezpečnostního incidentů (reportovaná událost, událost v řešení, vyřešená událost, události v řešení daného uživatele apod.),	**Vyhledávání a filtrování nad všemi událostmi z pohledu workflow incidentu – report/ v řešení / vyřešená událost / událost v řešení zadaného uživatele atd.**
· možnost exportování dat do emailu, csv, pdf, syslogu a podobně,	**Exportování dat do e-mailu, csv, pdf, syslog**
· možnost exportu bezpečnostních událostí a incidentů do systémů typu ticket management třetích stran.	**Exportování bezpečnostních událostí a incidentů do ticketovacích systémů třetích stran**
Detekce úniku dat	
Systém musí být schopen detekovat přenosy citlivých souborů a dat definovaných pomocí jejich názvů, hashů, specifického binárního obsahu (vodoznaku) nebo regulárních výrazů (např. rodné číslo).	**Nabízené řešení detekuje přenosy citlivých souborů a dat definovaných jejich názvem, hashem, binárním obsahem nebo regulárními výrazy**
Systém musí být schopen detekovat přenosy citlivých souborů a dat alespoň u následujících protokolů: HTTP, FTP, SMTP, SMB, NFS.	**Nabízené řešení detekuje přenosy citlivých souborů a dat u protokolů HTTP, FTP, SMTP, SMB, NFS.**
V rámci historických metadat u HTTP, FTP, SMTP, SMB a NFS je požadováno ukládání informací o všech po síti přenášených souborech alespoň v rozsahu:	**Pro historická metadata u protokolů HTTP, FTP, SMTP, SMB a NFS jsou ukládány informace o všech přenášených souborech v síti v rozsahu:**
· název souboru,	**Název souboru**
· velikost souboru,	**Velikost souboru**
· HASH souboru.	**Hash souboru**
Monitoring výkonu aplikací a sítě	
Systém v celé monitorované síti, mezi všemi zařízeními a na všech službách měří a vytváří automaticky (bez nutnosti nastavovat manuálně limitní hodnoty) model normálního chování pro výkonnostní parametry minimálně:	**Nabízené řešení měří a automaticky vytváří model normálního chování v celé monitorované síti, mezi všemi zařízeními a na všech službách pro následující výkonnostní parametry:**
· přenosová rychlost sítě,	**Přenosová rychlost sítě**

· rychlost odezvy aplikace,	**Rychlost odezvy aplikace**
· odezva systému z pohledu uživatele.	**Odezva z pohledu uživatele**
Výpočet uvedených výkonnostních parametrů a automatické detekce anomálií na základě odchylky od modelu normálního chování musí být prováděna pro:	**Nabízené řešení provádí výpočet výše uvedených výkonnostních parametrů a automatické detekce anomálií na základě odchylky od modelu normálního chování pro všechny:**
· všechny porty a služby TCP,	**Porty a služby TCP**
· pro všechny kombinace služeb a zařízení.	**Kombinace služeb a zařízení**
Systém musí v celé monitorované síti, mezi všemi zařízeními a na všech službách měřit informace o retransmission paketech, out of order paketech, TTL, QoS a komunikaci blokované firewally.	**Nabízené řešení měří informace o retransmission / out-of-order paketech, TTL, QoS a komunikacích blokovaných firewally v celé monitorované síti mezi všemi zařízeními a na všech službách.**
Monitoring cloudových služeb	
Systém musí být schopen monitorovat přístupy zařízení a uživatelů ke cloudovým službám, a to minimálně Google Workspace a Microsoft Office 365, vč. monitoringu operací se soubory, změn oprávnění a nastavení a neúspěšných přístupů.	**Nabízené řešení monitoruje přístupy zařízení a uživatelů je cloud službám Google Workspace a MS Office 365 včetně monitorování operací se soubory, změn oprávnění / nastavení a neúspěšných pokusů o přístup.**
Systém musí být schopen tyto informace autonomně a průběžně získávat z aplikačních rozhraní těchto cloudových služeb bez nutnosti využití řešení třetích stran.	**Nabízené řešení výše uvedené informace autonomně a průběžně získává z aplikačního rozhraní těchto cloud služeb bez potřeby využití řešení třetích stran**
Inventarizace sítě a grafický vizualizace topologie	
Systém musí být schopen zobrazit celý inventář monitorované sítě s počtem zařízení v jednotlivých lokalitách, segmentech, nebo podsítích. Včetně detailního přehledu zařízení.	**Nabízené řešení umožňuje zobrazit celý inventář monitorované sítě, počty zařízení v jednotlivých lokalitách, segmentech a podsítích včetně detailního přehledu zařízení.**
Systém musí být schopen graficky vykreslit celou topologii sítě, dle zaznamenané komunikace.	**Nabízené řešení umožňuje graficky vykreslit celou topologii sítě podle zaznamenané komunikace.**

Systém musí být schopen zobrazit inventář jednotlivých lokalit, přehledy zařízení, přehledy výrobců, tagy zřízení, uživatele.	**Nabízené řešení umožňuje zobrazit celý inventář jednotlivých lokalit s přehledy zařízení, výrobců, tagy a uživateli zařízení.**
Systém umožnuje všechny inventory informace řadit dle různých parametrů.	**Nabízené řešení umožňuje řadit veškeré inventarizační informace podle různých parametrů dle potřeby uživatele.**

Implementační služby

Všechna dodavatelem instalovaná zařízení budou zabezpečena a nebudou obsahovat zjevná rizika a zranitelnosti, a to po celou dobu provozu služby.

Dodavatel zajistí vyladění a nastavení detekce všech dodávaných systémů tak, aby nebyly detekováné nežádoucí a falešně pozitivní události. Tato činnost bude provedena ve spolupraci s kompetenními osobami zadavatele. Dodavatel zajistí integraci nástroje s aktuálním log managementem zadavatele, dále pak nastavení aktivních alertů a reportů dle potřeb zadavatele.

Produktová podpora výrobce

Dodavatel musí zajistit:

- softwarovou produktovou podporu řešení v délce [redacted] od podepsání akceptačního protokolu po předáním monitorovacího systému.
- [redacted]

Administrátorské školení

V rámci realizace je požadováno administrátorské a uživatelské školení pro zaměstnance zadavatele v rozsahu nezbytném pro kvalifikovanou obsluhu včetně videozáznamu pro zpětné použití, který bude dostupný online na zabezpečeném úložišti dodavatele.

Dále je požadováno opakované proškolení uživatelů jednou ročně v rozsahu minimálně 1MD, včetně revize analýzy bezpečnostních událostí ve všech lokalitách.

Termín plnění

Dle smlouvy na plnění veřejné zakázky.

[redacted]

10 Hardening

Zadavatel požaduje [redacted] Předpokládaný rozsah 2 čd.

Zadavatel požaduje centralizaci správy pravidel [redacted] Centralizace správy firewallových pravidel bude obsahovat analýzu prostředí ve spolupráci se zadavatelem, doporučení a vytvoření globálních pravidel pro celou organizaci, vytvoření specifických pravidel dle provozních podmínek, potřeb organizačních složek, požadavků pro provoz používaných aplikací a podle druhu zařízení (endpoint/server), dle principu Least privilege, tam kde to bude možné. Předpokládaný rozsah 10 čd.

[redacted]

[redacted]

11 Back Up Trezor - diskový úložný systém - dodávka a implementace

[redacted]

Popis

Požadavkem je dodávka [redacted] nového deduplikačního diskového úložiště určeného pro zálohování, dodávka programového vybavení pro zálohování, implementace celého řešení a jeho následná podpora [redacted]

Technická specifikace

Dodávka nového deduplikačního úložiště

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

Výkon a škálovatelnost

Požadovaný parametr	ANO/NE a popis naplnění požadavku, je-li popis relevantní (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)
[redacted] deduplikačního diskového úložiště	ANO
diskové úložiště musí disponovat alespoň 64TB čisté využitelné kapacity (kapacita, která je dostupná pro uložení dat a lze ji zkontrolovat prostřednictvím management nástrojů). Nabízené uložiště musí umožňovat licenční rozšíření kapacity po 4TB krocích.	ANO Čistá využitelní kapacita 64TB Licenční krok 4TB
diskové úložiště musí umožnit rozšiřování minimálně do 170TB čisté kapacity	ANO Až 172TB
minimální propustnost pro zápis 12 TB/h,	ANO Až 12.7 TB/h
Interní cache SSD 1,92TB	ANO 1,92TB
minimální propustnost pro čtení 3 TB/h,	ANO
každé úložiště musí být osazeno minimálně: • 4x 10Gbps ETH Base-T, • 2x 25Gbps ETH optical SFP28 • součástí dodávky musí být potřebné moduly a kabely pro připojení	ANO 4x 10GbE a 2x 25 GbE SFP28
podpora až 270 konkurenčních zálohovacích úloh per fyzický systém,	ANO
zařízení musí při ukládání dat využívat princip in-line deduplikace na cíli na principu variabilní délky bloku,	ANO
architektura diskové úložiště musí pro deduplikace využívat procesorový výkon a nesmí být závislá na počtu a typu backendových disků,	ANO

Příloha č. 1 – technická specifikace

Požadovaný parametr	ANO/NE a popis naplnění požadavku, je-li popis relevantní (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)
zálohovací diskové úložiště musí konsolidovat a centralizovat zálohovací prostředí (lokální i vzdálené) – všechna data budou deduplikována v rámci jednoho boxu (žádné separátní množiny deduplikovaných úložišť)	ANO

Integrace a interoperabilita

Požadovaný parametr	ANO/NE a popis naplnění požadavku, je-li popis relevantní (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)
zařízení musí podporovat minimálně následující protokoly: CIFS, NFS, VTL, FC; a musí umožnit jejich současné použití,	ANO
zařízení musí umožňovat integraci s různými typy zálohovacích SW (minimálně Microfocus Data Protector, VEEAM, IBM TSM, Veritas NetBackup, Dell EMC Data Protection Suite, Quest, Microsoft DPM, Oracle RMAN, MS SQL Studio),	ANO
zálohovací diskové úložiště musí být univerzální z hlediska podpory datových typů zálohovaných dat, musí podporovat všechny datové typy, používané v produkčním prostředí – soubor a tisk, databáze, emaily, VMware, Oracle, MS Exchange,	ANO
deduplikace musí být prováděna přes celé zálohovací prostředí – jak přes všechny aplikace, tak přes cílová úložiště,	ANO
zařízení musí umožnit současnou podporu standardních aplikací, platforem a protokolů bez nutnosti změny instalované infrastruktury (např. nutnost výměny zálohovacího SW, změny topologie sítě, apod.),	ANO
diskové úložiště musí být kompatibilní se standardem OpenStorage,	ANO
diskové úložiště musí umožnit ukládat data i pro archivní účely s funkcionalitou nastavení retenčních politik,	ANO
diskové úložiště musí být certifikováno podle SEC 17a-4f nebo ekvivalentní evropské nebo české normy,	ANO
diskové úložiště musí umožnit případnou distribuci deduplikačního algoritmu z cílového (deduplikačního úložiště) na zdrojové zařízení (backup klienta nebo backup server) z důvodu výkonu a škálovatelnosti prostředí a z důvodu úspor na slabých datových linkách,	ANO

Příloha č. 1 – technická specifikace

Požadovaný parametr	ANO/NE a popis naplnění požadavku, je-li popis relevantní (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)
diskové úložiště musí disponovat funkcí multitenancy (umožnit logické dělení diskového prostoru pro různé skupiny uživatelů s právy pouze na tyto logické jednotky s možností definice tenant administrator)	ANO
diskové úložiště musí poskytovat stejné výsledky deduplikace zálohy Oracle prostředí bez ohledu na Oracle multiplexing,	ANO

Replikace
je vyžadována dodávka licencí pro replikaci.

Požadovaný parametr	ANO/NE a popis naplnění požadavku, je-li popis relevantní (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)
diskové úložiště musí obsahovat licenci pro replikaci do záložní lokality,	ANO
diskové úložiště musí posílat pouze deduplikovaná zkomprimovaná data,	ANO
diskové úložiště musí podporovat alespoň následující scénáře pro replikaci: 1:1, M:1 a kaskádovou replikaci,	ANO
replikaci musí být možno spustit ve stejném čase jako zálohu bez dopadu na výkon zálohy,	ANO
diskové úložiště musí umožnit řízení replikace v prostředí zálohovacího SW,	ANO
diskové úložiště musí umožnit funkcionalitu šifrování replikačního toku data-in-flight,	ANO

Spolehlivost, ochrana a obnova

Požadovaný parametr	ANO/NE a popis naplnění požadavku, je-li popis relevantní (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)
zařízení musí disponovat interním algoritmem pro neustálou kontrolu zdraví uložených dat a v případě poškození jejich automatickou obnovu tak, aby bylo možno zálohy kdykoliv obnovit k jakémukoliv okamžiku,	ANO

Požadovaný parametr	ANO/NE a popis naplnění požadavku, je-li popis relevantní (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)
zařízení musí obnovovat data vždy z deduplikovaného a komprimovaného stavu, není přípustný mezikrok (např. externí disková cache),	ANO
zařízení musí disponovat funkcionalitou pro šifrování ukládaných data metodou data-at-rest,	ANO
zařízení je možné osadit HotSpare diskem,	ANO
zařízení musí obsahovat kompletní verifikace dat – okamžitá verifikace záloh a kontrola integrity právě ukládaných dat	ANO

Pokročilá ochrana dat (ochrana proti ransomware)

Požadovaný parametr	ANO/NE a popis naplnění požadavku, je-li popis relevantní (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)
Nabízené zařízení musí umožňovat šifrovat data a musí disponovat i nástroji pro správu klíčů.	ANO
Úložiště musí umožňovat nastavit retenční lhůty uložených data, granulárně podle definovaných politik řízených zálohovacím SW.	ANO
Retenční zámek úložiště musí ochránit data před změnou, nebo smazáním před vypršením retenční lhůty.	ANO
Úložiště musí disponovat mechanismem ochrany dat a samotného úložiště před napadením útočníkem z prostředí zadavatele i mimo toto prostředí (např. hackerský útok, ransomware, apod.).	ANO
Úložiště musí umožnit tzv. HW hardening – tedy takové nastavení, aby nebylo možno jedním uživatelem s dostatečnými právy manipulovat s uloženými daty nebo systémovým nastavením (např. princip čtyř očí).	ANO
Řešení musí podporovat automatickou kontrolu zdraví ukládaných dat (zda neobsahují např. škodlivý ransomware, zda nejsou šifrována útočníkem, apod.) a musí být schopno automatizovat kontrolu obnovitelnosti těchto dat ve fyzicky odděleném prostředí od produkčního prostředí zadavatele.	ANO
Řešení musí být schopno zajistit sadu dat k obnově tak, aby v případě úspěšného hackerského útoku na prostředí zadavatele, nebyla data uložená v tomto zařízení kompromitována a mohla být použita – řešení musí disponovat centrální konzolí (rozhraním) pro tuto obnovu, které je nezávislé na SW pro zálohování.	ANO
Diskové úložiště musí být možno instalovat na separátním segmentu sítě, který je určen pouze pro replikaci dat pro	ANO

Příloha č. 1 – technická specifikace

Požadovaný parametr	ANO/NE a popis naplnění požadavku, je-li popis relevantní (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)
ochranu proti ransomware. Tento segment musí být možno automaticky zpřístupnit pouze pro potřeby replikace dat a řízení tohoto přístupu bude probíhat nezávisle na zbytku běžné infrastruktury pro zálohování a obnovu z bezpečného místa prostřednictvím speciální management konzole.	
Diskové úložiště musí být certifikováno podle SEC 17a-4f nebo ekvivalentní evropské nebo české normy; doklad o certifikaci účastník předloží v nabídce.	ANO, [redacted]

Správa (management)

Požadovaný parametr	ANO/NE a popis naplnění požadavku, je-li popis relevantní (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)
diskové úložiště musí umožnit správu prostřednictvím jednotného webového rozhraní,	ANO
diskové úložiště musí poskytovat funkcionalitu automatického reportingu, automatický call-home,	ANO
diskové úložiště musí umožnit správu na principu rolí s různými typy oprávnění.	ANO
zařízení musí být plně kompatibilní se stávajícím či nabízeným zálohovacím systémem objednatele (podpora jednotné správy se stávajícími prvky).	ANO
diskové úložiště musí umožnit přímou správu z managementu aktuálně poptávaného SW řešení pro zálohování (řízení replikací, nastavení multitenancy, využití funkcionalit jako jsou change block tracking backup pro prostředí VMware, souborových systémů Windows a Linux, MS Exchange, Oracle VM, a další)	ANO

Další související služby

Zadavatel požaduje, aby součástí dodávky byly následující služby.

Příloha č. 1 – technická specifikace

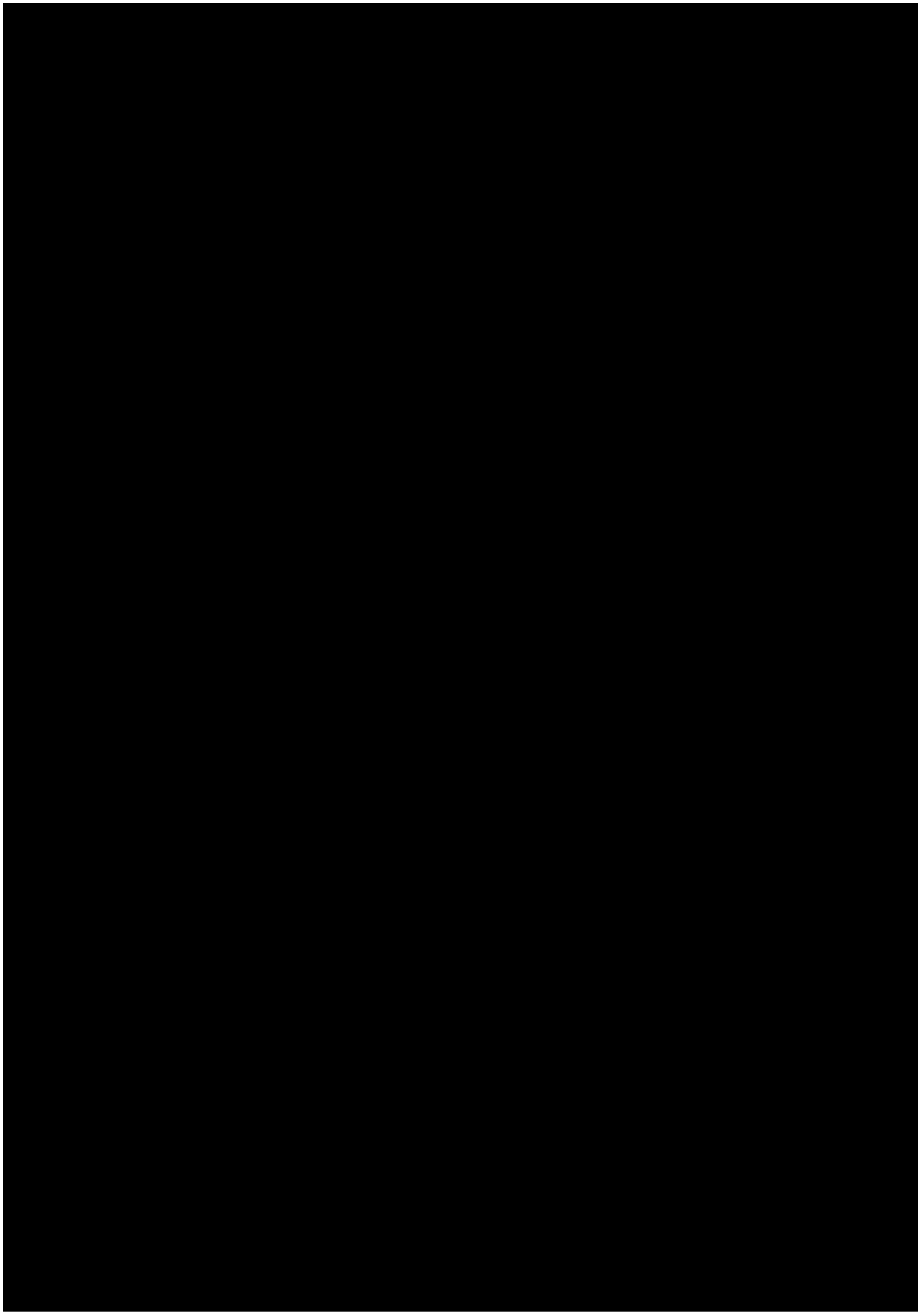
Požadovaný parametr	ANO/NE a popis naplnění požadavku, je-li popis relevantní (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)
Doprava zboží, likvidace obalů	ANO
Instalace a konfigurace HW a SW vybavení	ANO
Implementace a integrace HW a SW vybavení a předání do rutinního provozu včetně roční správy předaného prostředí.	ANO
Migrace stávajících záloh do nového prostředí	ANO
Seznámení s obsluhou formou školení v prostorách zadavatele pro minimálně 3 účastníků	ANO
Dodání dokumentace pro obsluhu	ANO

Technická podpora

Požadovaný parametr	ANO/NE a popis naplnění požadavku, je-li popis relevantní (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)
Záruka na HW a SW [redacted]	ANO
Podpora a maintenance řešení [redacted]	ANO
HW Úroveň podpory 24x7 s reakcí nejpozději do následujícího pracovního dne onsite od nahlášení pro úroveň požadavku „Kritický“ (tedy chyba, která znemožňuje chod systému a má dopad na fungování zadavatele)	následujícího pracovního dne
SW Úroveň podpory 24x7 s reakcí nejpozději do následujícího pracovního dne od nahlášení pro úroveň požadavku „Kritický“ (tedy chyba, která znemožňuje chod systému a má dopad na fungování zadavatele)	ANO

[redacted]

Příloha č. 1 – technická specifikace



Příloha č. 1 – technická specifikace

12 Servery a Switche a Záložní zdroje

Je-li kdekoliv v ZD uveden konkrétní model zařízení konkrétního výrobce je v rámci zadávacího řízení toto považováno pouze jako indikativní (minimální) parametr. Jedinou výjimku tvoří případy, kdy se jedná o rozšíření stávající infrastruktury a je z důvodu kompatibility a ochrany v minulosti již učiněných investic požadováno zachování stávajícího stavu nebo systému.

Pokud dodavatelem navržené řešení vyžaduje využití konkrétních softwarových produktů, které nejsou uvedeny v ZD a nejsou výslovně uvedeny jako součinnost, ale dodavatelem zvolené řešení zadání je na takových konkrétních softwarových produktech závislé, musí dodavatel do své nabídkové ceny zahrnout všechny náklady na jejich pořízení, instalaci, konfiguraci a další služby potřebné pro uvedení do provozu a podpora (support) po dobu udržitelnosti.

Výsledkem musí být nový HW, který rozšiřuje stávající infrastrukturu. Požadované propojení dodávané infrastruktury včetně instalace operačních systémů na servery a její integraci do prostředí Zadavatele provede Dodavatel.

[redacted]

Požadovaná specifikace nabízeného HW

Položka	**Počet ks**	**Označení výrobku a výrobce**
[redacted] **(server)**	[redacted]	
Minimální požadavky každého HCI nod (serveru)	**Splňuje (ANO / NE)** (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)	**Naplnění požadavku – upřesnění dodavatele (upřesnění povinné pouze o položek, u kterých zadavatel výslovně požaduje uvedení parametrů apod.)**
Provedení max. 2U.	ANO / NE	ANO 2U
Server osazený 1x CPU, s výkonem ve výkonovém testu uvedeným na stránkách https://xmrig.com/benchmark/, minimálně 11.030 bodů v testu HASHRATE pro jednoprocesorové systémy při maximálním TDP procesoru 270 W, s možností doplnění druhého CPU.	ANO / NE (uveďte parametry CPU)	ANO 11036,19 bodů TDP 270W
RAM 512 GB, rovnoměrně obsazené paměťové kanály CPU.	ANO / NE (uveďte typ a počet modulů)	ANO 8x 64GB RDIMM, 4800MT/s Dual Rank
LAN min. 4x 25Gbit SFP28.	ANO / NE	ANO
LAN min. 2x 1Gbit	ANO / NE	ANO

Min. dvě diskové skupiny, každá s min. 5ks datových ssd o min. velikosti 3.84TB (celkem tedy min. 10ks 3.84TB SSD vSAS disků) Read Intensive 12Gbps 512e 2.5in Hot-Plug, 1 DWPD.	ANO / NE (uveďte popis nabízených disků)	ANO 10x 3.84TB SSD vSAS, Read Intensive, up to 24Gbps FIPS-140 512e 2.5in Hot-Plug, AG Drive
1 ks FC karta, Dual Port 32Gb Fibre Channel HBA.	ANO / NE	ANO
Trusted Platform Module 2.0.	ANO / NE	ANO
[redacted]	ANO / NE	ANO
Licence serverového OS Windows, verze datacentrum s pokrytím všech jader nabízeného CPU.	ANO / NE	ANO
1.6TB Enterprise NVMe Mixed Use AG Drive U.2 Gen4, 2 kusy	ANO / NE	ANO
BOSS card 2 M.2 960GB (RAID 1)	ANO / NE	ANO
DAC kabel SFP28 to SFP28, 25GbE, délka 5m , 4 kusy	ANO / NE	ANO
HW pro instalaci do RACKU včetně kabelového ramena.	ANO / NE	ANO
Redundantní Hot-Plug ventilátory a zdroje 2x 2400W	ANO / NE	ANO
Záruka a technická podpora: • v délce minimálně 5 let, • reakční doba max. 4 hodiny, • garantovaná lhůta odstranění vady 5 pracovních dnů, • možnost automatického generování chybového hlášení přímo k výrobci hardware (resp. Poskytovateli) – např. automaticky generovaná emailová notifikace, • technická podpora je poskytována výrobcem, resp. autorizovaným partnerem výrobce v českém nebo slovenském jazyce.	ANO / NE	ANO

LAN Switch

Položka	Počet ks	Označení výrobku a výrobce
LAN switch	**2 ks**	
Minimální požadavky	**Splňuje (ANO / NE)** (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění	**Naplnění požadavku – upřesnění dodavatele (upřesnění povinné pouze o položek, u kterých zadavatel výslovně požaduje uvedení parametrů apod.)**

	zadávacích podmínek)	
Rack mount max. 1U, redundantní napájení.	ANO / NE	ANO 1U
Min. 24 portů 10/25GbE SFP28.	ANO / NE	ANO 24x 10/25GbE SFP28.
Min. 4x 100GbE QSFP28+.	ANO / NE	ANO 4x 100GbE QSFP28+.
Velikost packet bufferu min. 30 MB.	ANO / NE	ANO 30 MB
Switching kapacita min. 1.08 Tbps.	ANO / NE	ANO 2.16 Tbps
Propustnost min. 950 Mpps.	ANO / NE	ANO 1420 Mpps
Veškerá potřebná kabeláž na propojení serverů, členů clusteru, na rychlosti 25Gbps, napojení na stávající LAN.	ANO / NE	ANO
[redacted]		
Záruka a technická podpora: • v délce min. 5 let, • reakční doba do 4 hodin, • garantovaná doba odstranění vady do 5 pracovních dnů, • technická podpora je poskytována výrobcem, resp. autorizovaným partnerem výrobce.	ANO / NE	ANO

SAN Switch - doplnění

Položka	**Počet ks**	**Označení výrobku a výrobce**
SAN switch – doplnění	**2 ks**	**Doplnění stávajících Connectrix DS-6610B**
Minimální požadavky	**Splňuje (ANO / NE)** (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)	**Naplnění požadavku – upřesnění dodavatele (upřesnění povinné pouze o položek, u kterých zadavatel výslovně požaduje uvedení parametrů apod.)**
[redacted]	ANO / NE	ANO
Záruka a technická podpora	ANO / NE	ANO

• v délce minimálně 2 let, • reakční doba do 4 hodin, • garantovaná doba odstranění kritické vady následující pracovní den, • technická podpora je poskytována výrobcem, případně autorizovaným partnerem výrobce.		

Záložní zdroj – UPS

Položka	**Počet ks**	**Označení výrobku a výrobce**
Záložní zdroj – UPS	**2 ks**	
Minimální požadavky	**Splňuje (ANO / NE)** (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)	**Naplnění požadavku – upřesnění dodavatele (upřesnění povinné pouze o položek, u kterých zadavatel výslovně požaduje uvedení parametrů apod.)**
Provedení Rack mount	ANO / NE	ANO
Topologie online s dvojí konverzí	ANO / NE	ANO
Kapacita min. 5kVA	ANO / NE	ANO 5kVA
Rozsah vstupního napětí pro napájení z rozvodné sítě min. 160 – 275 V	ANO / NE	ANO 160 – 275 V
SNMP včetně TRAPů, IPv4	ANO / NE	ANO
Zkreslení vstupního napětí méně než 2%	ANO / NE	ANO
Management přes prohlížeč bez nutnosti instalovat klienta	ANO / NE	ANO
Porty: 1x Ethernet, 1x sériová linka	ANO / NE	ANO
Baterie vyměnitelné za chodu Automatické testování kapacity Upozorňování e-mailem Minimálně 5 let podpora výrobcem	ANO / NE	ANO

[redacted]

13 Backup Server

[redacted]

Backup server

Položka	Počet ks	Označení výrobku a výrobce
Backup server	**1 ks**	
Minimální požadavky	**Splňuje (ANO / NE)** (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)	**Naplnění požadavku – upřesnění dodavatele (upřesnění povinné pouze o položek, u kterých zadavatel výslovně požaduje uvedení parametrů apod.)**
Provedení max. 2U.	ANO / NE	ANO 2U
Server osazený 1x CPU, s výkonem ve výkonovém testu uvedeným na stránkách https://www.cpubenchmark.net/, minimálně 36.390 bodů v testu pro jednoprocesorové systémy při maximálním TDP procesoru 150 W, s možností doplnění druhého CPU.	ANO / NE (uveďte parametry CPU)	ANO 36735 bodů TDP 150W
RAM 128 GB, rovnoměrně obsazené paměťové kanály CPU.	ANO / NE (uveďte typ a počet modulů)	ANO 8x 16GB RDIMM, 4800MT/s Single Rank
LAN min. 4x 25Gbit SFP28.	ANO / NE	ANO
LAN min. 2x 1Gbit	ANO / NE	ANO
SSD o min. velikosti 3.84TB (min. 4ks 3.84TB SSD disků) Read Intensive 6Gbps 512 2.5in Hot-Plug, 6Gbps 512 AG Drive, 3.5in HYB CARR, 1 DWPD.	ANO / NE (uveďte popis nabízených disků)	ANO 4x 3.84TB SSD SATA Read Intensive 6Gbps 512 2.5in Hot-plug AG Drive,3.5in HYB CARR, 1 DWPD
HDD o min. velikosti 20TB Hard Drive SAS 12Gbps 7.2K 512e 3.5in Hot-Plug, AG Drive 14 kusů	ANO / NE (uveďte popis nabízených disků)	ANO 14x 20TB Hard Drive SAS 12Gbps 7.2K 512e 3.5in Hot-Plug, AG

Příloha č. 1 – technická specifikace

1 ks FC karta, Dual Port 32Gb Fibre Channel HBA.	ANO / NE	ANO
SFP+ SR Optic 10GbE 850nm 2 kusy	ANO / NE	ANO
Licence serverového OS Windows, verze standard s pokrytím všech jader nabízeného CPU.	ANO / NE	ANO
BOSS card 2 M.2 960GB (RAID 1)	ANO / NE	ANO
DAC kabel SFP28 to SFP28, 25GbE, délka 3m, 2 kusy	ANO / NE	ANO
HW pro instalaci do RACKU včetně kabelového ramena.	ANO / NE	ANO
Redundantní Hot-Plug zdroje 2x 1100W	ANO / NE	ANO
Záruka a technická podpora: • v délce minimálně 5 let, • reakční doba max. 4 hodiny, • garantovaná lhůta odstranění vady 5 pracovních dnů, • možnost automatického generování chybového hlášení přímo k výrobci hardware (resp. Poskytovateli) – např. automaticky generovaná emailová notifikace, • technická podpora je poskytována výrobcem, resp. autorizovaným partnerem výrobce v českém nebo slovenském jazyce.	ANO / NE	ANO

[redacted]

14 Zálohovací SW

[redacted]

Požadavek	Splňuje ANO / NE (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)	Popis plnění (upřesnění povinné pouze o položek, u kterých zadavatel výslovně požaduje uvedení parametrů apod.)
Obecné požadavky		
Požadujeme dodání [redacted]	ANO	[redacted]
Zálohovací řešení musí podporovat infrastrukturu VMware ve verzích 6.x, 7.x a 8.0, včetně VMware Cloud Foundation, VMware Cloud on AWS, VMware cloud on Dell a Azure VMware Solution	ANO	
Řešení musí podporovat hostitele spravované serverem VMware vCenter ve verzích 6.x, 7.x a 8.0 i samostatné ESXi hostitele.	ANO	
Zálohovací řešení musí podporovat Windows Server Hyper-V 2012 až 2022 včetně Server Core, Azure Stack HCI i Microsoft Hyper-V Server	ANO	
Řešení musí podporovat hostitele spravované pomocí Microsoft System Center Virtual Machine Manager 2012 R2 až 2019, klastrové i samostatné hostitele Hyper-V	ANO	
Řešení musí podporovat zálohování všech operačních systémů, které jsou podporovány pro provoz na těchto hypervizorech	ANO	
Řešení musí podporovat zálohování platformy Red Hat Virtualization 4.4 SP1	ANO	
Řešení musí podporovat zálohování celých zařízení NAS, jednotlivých sdílených složek SMB a NFS a souborových serverů Windows a Linux.	ANO	
Software musí být možné licencovat pomocí trvalé licence i formou časově omezené subscripce.	ANO	
TCO		

Řešení nesmí být závislé na jednom poskytovateli HW, virtualizační, nebo cloudové platformy a to jak pro výpočetní část, tak pro část ukládání dat.	ANO	
Licence musí být přenositelná mezi různými fyzickými, virtuálními a cloudovými chráněnými objekty	ANO	
Všechny součásti řešení musí plně podporovat komunikaci po IPv6	ANO	
Řešení musí mít mechanismy k úspoře objemu úložného prostoru pro ukládání záloh. Jejich využití musí být volitelné a nesmí omezit žádné funkcionality zálohování a obnovy dat.	ANO	
Řešení musí poskytovat jednotnou konzoli pro přehled o zálohách fyzických, virtuálních, cloudových, NAS i Kubernetes prostředí	ANO	
Řešení musí umožnit vytvoření jednoho logického úložiště pro ukládání záloh z neomezeného počtu různorodých diskových úložišť	ANO	
Řešení musí umožňovat ukládání záloh do různých diskových úložišť, souborových systémů, objektových úložišť, nebo deduplikačních diskových zařízení.	ANO	
Řešení musí umožňovat rozšíření logického úložiště o vrstvy pro automatické vytváření sekundární a archivní kopie záloh, zajišťující soulad s pravidlem 3-2-1 ukládání záloh.	ANO	
Řešení musí umožňovat "single pass backup“ s možností vyloučit zpracování jednotlivých souborů a složek. „Jednoprůchodová záloha“ je vyžadována pro všechny druhy obnovení včetně granulárních obnov na úrovni aplikačních položek	ANO	
Řešení musí umožňovat připojování a spouštění jakéhokoli skriptu pro zálohování před nebo po spuštěním zálohovací úlohy, nebo před a po snapshotu VM	ANO	
Řešení musí podporovat technologie klonování datových bloků u souborových systémů pro Windows i Linux pro zajištění dalších úspor konzumované kapacity	ANO	
Řešení musí nabízet samoobslužný portál, prostřednictvím kterého si uživatelé mohou obnovit soubory z GuestOS, nebo virtuální počítače, včetně jejich okamžitého spuštění ze souboru zálohy, či objekty MS Exchange a databází MS SQL, Oracle a PosgreSQL (včetně obnovení k zvolenému bodu v čase)	ANO	
Řešení musí disponovat technologií pro snadnou migraci a kopírování záloh mezi jednotlivými úložnými zařízeními, při zachování datových úspor	ANO	
Řešení musí umožňovat kopírovat body obnovení a replikovat virtuální počítače do vzdáleného umístění pomocí technologie založené na vestavěné WAN akceleraci	ANO	
Řešení musí být schopen integrace s jinými systémy pomocí zabudovaného rozhraní REST API	ANO	
Řešení musí umožňovat samostatně škálovat výkonově i geograficky výpočetní, úložné i administrativní komponenty	ANO	
Požadavky na RPO		
Řešení musí využívat mechanismus sledování změn bloku. Pro všechny podporované hypervizory musí být implementace CBT certifikována výrobcem hypervizoru; dodavatel doloží v nabídce	ANO	[redacted]
Výše uvedená funkce musí být konfigurovatelná na úrovni datastore virtualizační platformy	ANO	

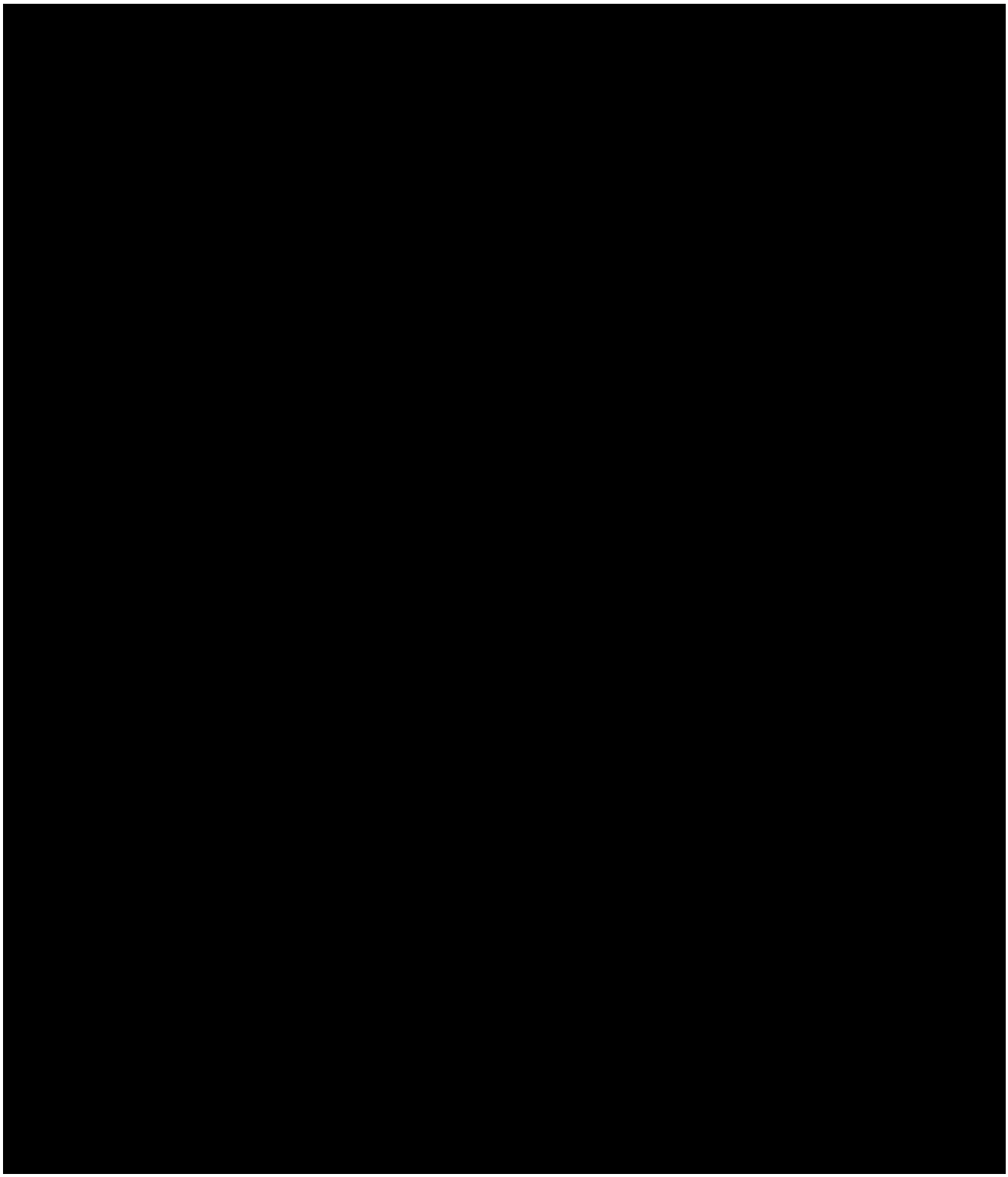
Řešení musí umožňovat vytváření záloh integrací se snímky úložiště. Dále musí umožnit obnovu jednotlivých VM, souborů a položek aplikace z těchto snímků. Proces zálohy nemůže k připojení snímku použít dočasného hostitele. Popsaná funkce musí fungovat pro prostředí VMware vSphere a musí podporovat následující pole: Dell, NetApp, HPE, HITACHI VANTARA, IBM, Lenovo, Fujitsu, Pure Storage, CISCO, DataCore	ANO	
Řešení musí umožňovat integraci se zařízeními Netapp FAS a EMC Isilon pro zálohování NAS prostředí s využitím vytváření snapshotů na diskovém poli.	ANO	
Řešení musí mít oficiální podporu pro VMware vSAN certifikovanou společností VMware	ANO	
Řešení musí podporovat NDMP protokol pro zálohování NAS zařízení	ANO	
Řešení musí využívat protokol DD BOOST [redacted] To musí být podporováno pomocí připojení k síti LAN nebo FC	ANO	
Řešení musí využívat protokol Catalyst (včetně Catalyst Copy) pokud je HPE StoreOnce používán jako záložní úložiště. To musí být podporováno pomocí připojení k síti LAN nebo FC	ANO	
Řešení musí mít replikaci produkčních VM přímo z infrastruktury VMware vSphere, mezi hostiteli ESXi, včetně asynchronní nepřetržité replikace. Řešení musí navíc umožnit jako zdroj replikačních úloh využít soubory záloh	ANO	
Řešení musí umožňovat „seeding“ replik ze stávajícího virtuálního počítače	ANO	
Řešení musí mít stejné funkce replikace pro Hyper-V	ANO	
Řešení musí umožňovat technologii replikace VM v prostředí Vmware založené na VAIO filtru (CDP, Continuous Data Protection).	ANO	
Řešení musí využívat všechny režimy přenosu zálohy podporované hypervizorem (network, hotadd, direct SAN a direct NFS)	ANO	
Řešení musí být schopen vytvořit zálohu „ad-hoc“ pomocí nativní konzole nebo webového klienta vSphere	ANO	
Řešení musí umožňovat paralelní zpracování virtuálních disků a jejich disků, včetně paralelní obnovy virtuálních disků v úplném režimu obnovy VM	ANO	
Požadavky na RTO		
Řešení musí umožňovat okamžitou obnovu více virtuálních strojů současně, přímo ze záložních souborů z libovolného bodu obnovení (vestavěný NFS server). Tato funkce musí být podporována pro prostředí VMware a Hyper-V a musí fungovat bez ohledu na hardware používaný k ukládání záložních souborů VM	ANO	
Uvedená funkce musí umožňovat spuštění zálohy vytvořené z různých platforem (různých virtuálních, fyzických a veřejných cloudových virtuálních strojů)	ANO	
Řešení musí umožňovat online migraci virtuálních počítačů, zpuštěných z úložiště záloh, do produkčního úložiště pomocí funkcí hypervizoru. Řešení musí také poskytovat svou vlastní funkci, která takové schopnosti poskytne.	ANO	
Řešení musí umožňovat prezentaci disků přímo ze záložního souboru do spuštěné VMware VM	ANO	
Řešení musí umožňovat úplné obnovení VM, obnovu souborů VM nebo disků VM	ANO	

Řešení musí umožňovat úplné obnovení VM přímo do Microsoft Azure, Azure Stack, Amazon EC2, Google Cloud Platform	ANO	
Řešení musí umožňovat přímou obnovu ze záloh uložených v S3-kompatibilním objektovém úložišti, bez nutnosti mezikroku a to jak pro obnovi jednotlivých VM, souborů, aplikačních položek, nebo okamžitého spuštění GuestOS, databází, či NAS z úložiště záloh	ANO	
Řešení musí umožňovat vytvářet aplikačně konzistentní snímky VM na úrovni diskových polí s možností granulární obnovy přímo z těchto snímků na úrovni celých VM, jednotlivých souborů, nebo položek aplikací, či okamžitého spuštění VM ze zvoleného snímku.	ANO	
Řešení musí umožňovat okamžitou dostupnost NAS ze zvoleného bodu v čase pro čtení i zápis přímo z úložiště záloh se souběžnou obnovou do původní, nebo nové lokality	ANO	
Řešení musí umožňovat obnovu souborů na stroj operátora nebo přímo do produkční VM bez potřeby agenta nainstalovaného uvnitř VM. Během obnovy bez agentů nesmí existovat žádné omezení na velikost souboru ani omezení počtu souborů	ANO	
Řešení musí umožňovat obnovu souborů přímo do virtuálního počítače pomocí síťového připojení a rozhraní VIX API v prostředích VMware a PowerShell Direct v prostředích Hyper-V	ANO	
Řešení musí podporovat obnovu souborů z Linux LVM a Windows Storage Spaces	ANO	
Řešení musí umožňovat při obnově na úrovni souborů zobrazení změněných souborů od zvoleného bodu obnovy v produkčním prostředí	ANO	
Řešení musí umožňovat rychlou a podrobnou obnovu aplikačních objektů bez použití jakéhokoli agenta nainstalovaného uvnitř virtuálních počítačů	ANO	
Řešení musí podporovat granulární obnovení libovolného objektu a všech atributů tohoto objektu včetně hesla, GPO, AD configuration partition, AD integrovaných záznamů DNS, Microsoft System Objects, informací o certifikátu CA a AD Sites subnet	ANO	
Řešení musí podporovat Microsoft Exchange 2013 a novější, granulární obnovení jakéhokoli objektu včetně objektů ve složce „Permanently deleted objects“	ANO	
Řešení musí podporovat granulární obnovení Microsoft SQL 2008 a novějších, včetně databází s možností obnovení v čase (PiT), obnovy na úrovni tabulky, schéma	ANO	
Řešení musí podporovat podrobné obnovení Microsoft Sharepoint Server 2013 a novějších. Možnost obnovit položky, weby, oprávnění	ANO	
Řešení musí podporovat granulární obnovu databází Oracle s obnovou v čase (PiT) a podporou Oracle DataGuard. Toto musí být nabídnuto pro databáze spuštěné v operačních systémech Windows a Linux	ANO	
Řešení musí umožňovat publikování MS SQL a Oracle DB přímo ze záložního souboru na spuštěný databázový server	ANO	
Řešení musí umožňovat okamžitou obnovu databází MS SQL a Oracle v režimu Instant Recovery do libovolného umístění.	ANO	
Řešení musí umožňovat integraci nativního pluginu pro zálohování Oracle RMAN	ANO	

Řešení musí umožňovat integraci nativního pluginu pro zálohování SAP HANA	ANO	
Řešení musí umožňovat integraci nativního pluginu pro zálohování [redacted]	ANO	
Řešení musí umožňovat „reverzní CBT“ a obnovu pomocí Direct SAN	ANO	
Předcházení rizik		
Přístup do řídící konzole musí být chráněný vícefaktorovou autentizací bez nutnosti přístupu k internetu.	ANO	
Řešení musí umožňovat vytváření záloh odolných vůči náhodnému, či úmyslnému smazání, nebo ransomware útokům na komoditním serverovém HW, nebo jakémkoliv S3-kompatibilním objektovém úložišti	ANO	
Řešení musí podporovat gMSA účty pro zajištění aplikačně-konzistentních záloh v GuestOS bez nutnosti ukládání přístupových oprávnění na úrovni administrátora pro daný GuestOS.	ANO	
Řešení nesmí použít centrální databázi pro ukládání jakýchkoli metadat deduplikace. Ztráta databáze nemůže způsobit, že záložní soubory budou nestabilní. Metadata deduplikace musí být uložena v záložních souborech	ANO	
Řešení musí umožňovat pravidelné automatické testování obnovitelnosti záloh, včetně funkčnosi jednotlivých služeb a kontrolou obsahu na kybernetické hrozby pomocí řešení třetích stran.	ANO	
Řešení musí umožnit přiřadit jednotlivým komponentám zálohovací infrastruktury geografické identifikátory	ANO	
Řešení musí disponovat mechanizmem řízení životního cyklu šifrovacích klíčů	ANO	
Řešení musí disponovat nástrojem pro analýzu konfigurace z pohledu bezpečnostních "Best Practices" doporučení.	ANO	
Řešení musí umožňovat v průběhu obnovy dat ověřovat obsah obnovovaných dat na kybernetické hrozby pomocí produktů třetích stran	ANO	
Řešení musí disponovat API pro zpřístupnění obsahu záloh aplikacím třetích stran	ANO	
Řešení musí umožňovat vytvářet a spouštět izolované "Sandbox" prostředí pro provoz skupin VM ze záloh, replik i snímků diskových polí	ANO	
Řešení musí nabízet šifrování celého síťového provozu mezi všemi komponentami a také šifrování souborů záloh "na cíli" na diskovém, cloudovém nebo páskovém úložišti.	ANO	
Řešení musí nabízet způsoby, jak omezit stres na úložišti zdrojových dat během zálohování tak, aby záloha kontrolovatelným způsobem ovlivňovala latenci produkčního úložiště.	ANO	
Zálohování NAS zařízení musí podporovat přímé ukládání záloh do S3-kompatibilních objektových úložišť s podporou ObjectLock funkce	ANO	
Řešení musí podporovat vytváření sekundárních kopií záloh z S3-kompatibilních objektových úložišť na datové pásky pro zajištění "off-line", či "air-gapped" sady záloh	ANO	
Součástí záloh musí být všechny informace, potřebné pro zajištění obnovy i v případě nedostupnosti původního zálohovacího serveru, nebo databáze s katalogem záloh.	ANO	
Řešení musí nabízet automatickou detekci "orphaned snapshots" a musí provést jejich konsolidaci automaticky bez zásahu uživatele	ANO	

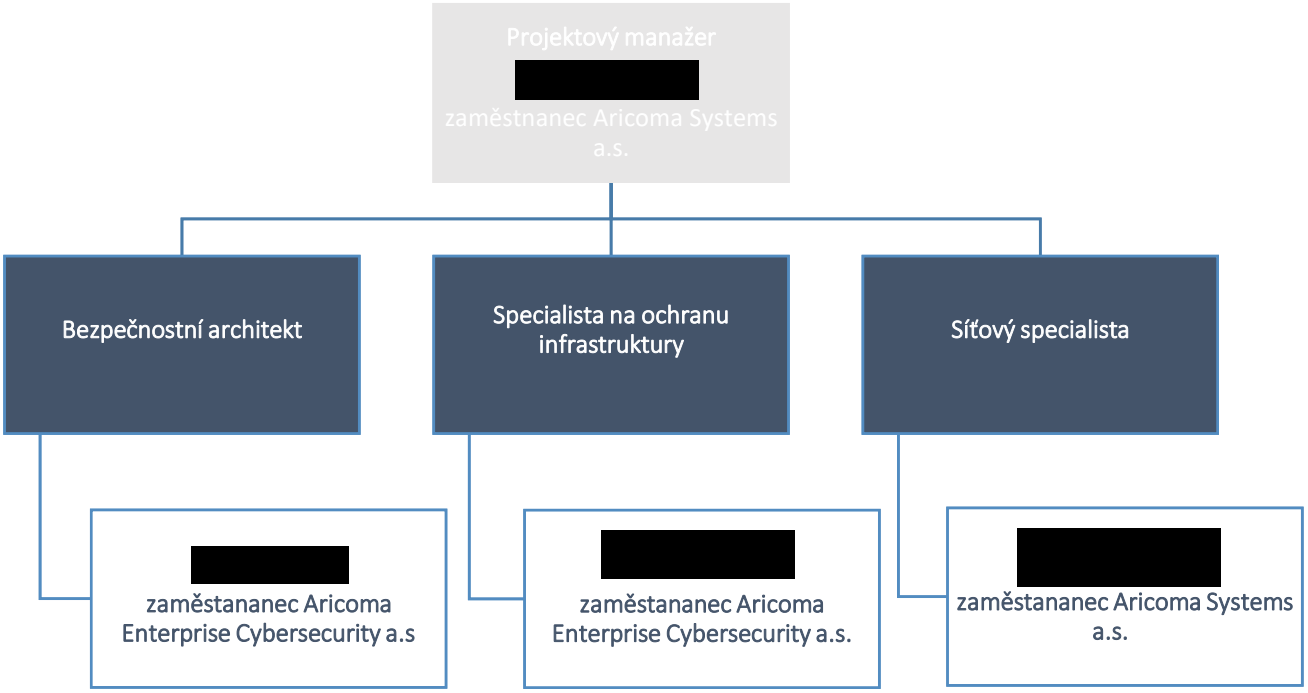
Řešení musí umožňovat automatizovanou dvoustupňovou obnovu virtuálních strojů, což umožňuje vložení vlastních skriptů za účelem změny dat před obnovením do produkčního prostředí.	ANO	

[redacted]



1.1 Realizační tým

Dle plánované organizace projektu uvádíme níže seznam našich pracovníků s konkrétními rolemi, které budou pravděpodobně v rámci projektu vykonávat. Zaměstnanci mají zkušenosti s obdobnou zakázkou. Alokace zaměstnanců se může změnit, primárně je ale plánována tato alokace. Dodávka řešení bude realizována naším projektovým týmem, který bude zahrnovat následující role obsazené vhodnými specialisty a konzultanty:



1.2 Profesní způsobilost

1.2.1 [redacted]

Vedoucí realizačního týmu (Projektový manažer)	
Požadovaný údaj	Naplnění požadovaného údaje
Jméno a příjmení	[redacted]
min. vysokoškolské vzdělání v oblasti ICT	ANO
min. 10 let praxe v oboru shodném s předmětem plnění na pracovní pozici shodné/obdobné vedoucího projektu	ANO
je držitelem certifikace pro projektovou metodiku na úrovni min. PRINCE2 nebo obdobné	ANO
vedl (byl v pozici vedoucího) v posledních 5 letech před zahájením zadávacího řízení minimálně 3 zakázky v oblasti kybernetické bezpečnosti5 ve finančním objemu zakázky min. 10 mil. Kč bez DPH/každá zakázka.	ANO
komunikace v českém nebo slovenském jazyce slovem i písmem.	ANO
Nejvyšší dosažené vzdělání (konkretizovat název vzdělávací instituce a vystudovaný obor aj.)	Informace je obsažena v přiloženém CV
Dosavadní praxe v oboru (pracovní pozice, pracovní náplň apod.), který souvisí s předmětem plnění	Informace je obsažena v přiloženém CV
Délka praxe v oboru, který souvisí s předmětem plnění	Informace je obsažena v přiloženém CV
Upřesnění vztahu, ve kterém je uvedená osoba k účastníkovi výběrového řízení (např. pracovněprávní vztah, smluvní – poddodavatelský vztah apod. – konkretizovat)	Zaměstnanec - Název zaměstnavatele (IČO): Aricoma systems a.s. Hornopolní 3322/34, 702 00 Ostrava, Ičo 04308697
Specifikace druhu a typu certifikace (osvědčení/potvrzení) (je-li relevantní pro konkrétní pracovní pozici)	Certifikáty a osvědčení od výrobců jsou přiloženy u každého specialisty
Datum podpisu a vlastnoruční podpis	23.1.2024 [redacted]

Profesní životopis

[redacted]

Aricoma Systems a.s.

Adresa [redacted]

Telefon

E-mail

VZDĚLÁNÍ

• Období (od – do)	2006 – 2009
• Název a typ organizace	Vysoké Učení Technické, Fakulta Podnikatelská
• Získaný titul	**Bc.**
•Obor	**Systémové inženýrství a informatika**

• Období (od – do)	2009 – 2011
• Název a typ organizace	Vysoké Učení Technické, Fakulta Podnikatelská
• Získaný titul	**Ing.**
•Obor	**Řízení a ekonomika podniku**

• Období (od – do)	2009 – 2011
• Název a typ organizace	Nottingham Trent University, Nottingham, Velká Británie
• Získaný titul	**MSc.**
•Obor	**MSc in Business and Informatics**

PROFESNÍ PRAXE

• Dosažená pozice	**Projektový manažer**
• Období (od – do)	2011 – doposud
• Jméno a adresa zaměstnavatele	**Aricoma Systems a.s.** Hornopolní 3322, Ostrava
• Hlavní pracovní náplň	Vedení komplexních projektů v oblastech systémové infrastruktury, informačních systémů a aplikační vrstvy. Realizace projektů pro st. správu a samosprávu a významné privátní zákazníky. Projekty s působností po celé ČR na Slovensku, Polsku i mimo EU. **Významní zákazníci v privátním sektoru:** ArcelorMittal, SGI corp, Třinecké železárny, ČEZ, Kofola, ABB, Catterpilar, Dalkia, UPC, Shimano, PZU PL, Brembo, Home Credit International, Linaset, Avenier, Romotop **Významní zákazníci ve státním sektoru:** Ministerstvo vnitra, Moravskoslezský kraj, Zlínský kraj, Jihomoravský kraj, Národní Banka Slovensko, Vysoka škola báňská, Univerzita Tomáše Bati, Psychiatrická nemocnice v Opavě, Městská nemocnice v Ostravě, Krajské nemocnice MSK a ZLK, SM Ostrava, MM Opavy, MM Karviná, MM Bruntál a další.
• Další funkce	**Vedoucí projektové kanceláře divize Mid Market** Zodpovědný za vedení a výsledky týmu projektových manažerů skrz celou ČR. Tvorba metodiky práce a aplikace metod projektového managementu.

Mentor

Spolupráce se začleněním nových členů do prostředí společnosti, skupiny, týmu. Předávání informací, životních i profesních zkušeností, podpora při rozvoji odborných i měkkých dovedností.

• Dosažená pozice	**Projektový manažer**
• Období	2005 – 2011
• Jméno a adresa zaměstnavatele	**Klub Stypendystów fundacji Semper Polonia (nezisková organizace)** Český Těšín
• Hlavní pracovní náplň	Příprava a realizace projektů v oblastech personálního rozvoje a vzdělávání studentů. Zajišťování možnosti zahraničních studentských stáží po střední a východní Evropě, získávání financí z prostředků EU a realizace konferencí s mezinárodní účastí.

REALIZOVANÉ PROJEKTY
(PROJEKTOVÝ MANAŽER)

• Období (od – do)	Q2 2021
• Název projektu	**Dodávka nástroje pro logmanagement**
• Zadavatel projektu	Statutární město Frýdek Místek
• Popis projektu	Dodávka nástroje pro LogManagement Log Manager – analýza, implementace, servisní podpora

• Období (od – do)	Q1 2021
• Název projektu	**Dodávka, implementace a technická podpora nástroje typu DLP**
• Zadavatel projektu	Statutární město Ostrava
• Popis projektu	Dodávka, implementace a technická podpora nástroje typu DLP (Data Loss Prevention) zajišťující ochranu dat před různými vektory potenciálních úniků informací v ICT prostředí města Ostravy a monitoring koncových stanic.

• Období (od – do)	Q4 2021 – Q2 2022
• Název projektu	**Dodávka systému pro správu digitálních identit**
• Zadavatel projektu	Statutární město Ostrava
• Popis projektu	Dodávka identity managera AC Identita vč napojení na klíčové IS.

• Období (od – do)	Q3/2021 – 34/2021
• Název projektu	**Modernizace serverové IT infrastruktury**
• Zadavatel projektu	Linaset, a.s. Československé armády 362 747 87 Budišov nad Budišovkou, ***IČ:*** 47674687 **Kontaktní údaje:** **Vedoucí ICT oddělení:** [redacted]
• Popis projektu	Implementace a začlenění hyperkonvergované infrastruktury do existující infrastruktury zákazníka. Použití server/storage hyperkonvergované infrastruktury DELL VxRail. Vybudování storage i serverové virtualizace vč DR site a zálohování. Vybudování nové páteřní a přístupové síťové infrastruktury ARUBA. Migrace HW i VM do nové serverovny v lokalitě Bruntál.
• Rozsah	Nad 6M Kč

• Období (od – do)	Q3-Q4 2021
• Název projektu	**Sloučení programových platforem REUIP II**
• Zadavatel projektu	ČR - Státní úřad inspekce práce
• Popis projektu	Dodávka analýzy, serverové, storage a síťové infrastruktury v rámci dodávky nového ERP MS Dynamisc 365 Customer Engagement. Vybudování DR site v datovém centru zadavatele.

Dodávka bezpečností dokumentace.

• Období (od – do)	Q3-Q4 2020
• Název projektu	**Zvýšení zabezpečení informačních systémů, výpočetních středisek a síťové komunikace v nemocnici**
• Zadavatel projektu	Nem ve Frýdku-Místku, Nemocnice Třinec, Nemocnice s pol. Karviná, Nemocnice s pol. Havířov, Slezská nemocnice v Opavě
• Popis projektu	Dodávka identity managera AC Identita vč napojení na klíčové IS.

• Období (od – do)	Q1-Q3 2020
• Název projektu	**Implementace systémů managementu bezpečnosti informací a poskytovaných služeb**
• Zadavatel projektu	Krajská nem. T.Bati Zlín, Uherskohradišťská nem., Vsetínská nem., Kroměřížská nem **Kontaktní údaje:** **Oddělení ICT VSN:** [redacted] **Oddělení ICT KNTB** **Oddělení ICT UHN** **Oddělení ICT KMN**
• Popis projektu	Implementace a začlenění hyperkonvergované infrastruktury do existující infrastruktury. Realizace hyperkonvergované server/storage infrastruktury na technologiích DELL VxRail. Dodávka identity managera AC Identita vč napojení na klíčové IS zadavatele. Vybudování MS Active Directory infrastruktury pro Uherskohradišťskou nemocnici.
• Rozsah	Nad 13M Kč

• Období (od – do)	Q3-Q4 2019
• Název projektu	Bezpečnost informačních systémů
• Zadavatel projektu	Psychiatrická nemocnice v Opavě
• Popis projektu	Rozšíření technologické infrastruktury, prostředků pro bezpečnou komunikaci, sdílení dokumentů, možnosti základní manažerské kontroly hospodaření pomocí společného datového skladu, prvků pro elektronické zpracování interních procesů a zvýšení komfortu uživatelů informačních systémů a zvýšení bezpečnosti prostředí v souvislosti s naplněním požadavků zákona a vyhlášky o kybernetické bezpečnosti. Realizace projektu zahrnovala tyto oblasti: • Řízení uživatelských identit (IdM), • Dvoufaktorové (dvoufázové) ověřování uživatelů a Single Sign-On (SSO), • Monitorování privilegovaných účtů (PAM), • Správa servisních požadavků (ServiceDesk, Asset Management), • Správa bezpečnostních informací a událostí (SIEM), • Řízení oběhu dokumentů vč. silného šifrování (DMS), • Zabezpečení přístupu k síti dle standardu 802.1x, • Aplikační bezpečnost a vysoká dostupnosti infrastruktury, • Centralizace komunikačních kanálů (e-mail, IM, videokonference).
• Ocenění	Projekt roku CACIO, Citrix awards

• Období (od – do)	Q1 2019
• Název projektu	Vybudování nové VI infrastruktury včetně DR lokality
• Zadavatel projektu	Sungwoo Hitech s.r.o.
• Popis projektu	Vybudování primární i DR serverovny ve vysoké dostupnosti s důrazem na minimálním RTO/RPO. Obměna páteřní sítové infrastruktury.

• Období (od – do)	Q2 2018 – Q1 2019
• Název projektu	Zálohování dat krajské korporace
• Zadavatel projektu	**Moravskoslezský kraj**

• Popis projektu	Vypracování analýzy, metodiky a projektu nasazení nové služby krajského úřadu zajišťující pravidelnou zálohu dat kritických systémů v rámci krajské korporace (více než 220 PO) do centrálního úložiště provozovaného v rámci Technologického centra Moravskoslezského kraje. Implementace zálohovacího řešení na platformě DELL EMC Networker a Avamar. Zvýšení zabezpečení dat krajské korporace, zálohování služeb poskytovaných Technologickým centrem kraje, centralizace zálohování lokálních provozních systémů vybraných příspěvkových organizací Moravskoslezského kraje, sjednocení metodiky a kategorizace dat.
• Období (od – do)	Q4 2018 – Q1 2019
• Název projektu	Migrace do nové domény
• Zadavatel projektu	**ArcelorMittal Ostrava a.s.**
• Popis projektu	Vývoj migračního nástroje a vypracování migračních postupů. Migrace více než 3000 stanic, uživatelů a souvisejících objektů do nové domény. Realizace více než 30 migračních vln včetně VIP uživatelů. Analýza a následná migrace 12 vybraných aplikací do nové domény. Zajištění L3 podpory během celého procesu migrace.
• Období (od – do)	Q1 – Q4 2018
• Název projektu	28 Specifické informační a komunikační systémy a infrastruktura II, Výzva č. 28.
• Zadavatel projektu	**Statutární město Karviná, Město Bruntál, Město Hlučín, Město Bohumín, Město Petřvald, Obec Ludgeřovice**
• Popis projektu	Dodávka, nasazení, implementace a následná podpora informačních a komunikačních systému pro veřejnou správu. Integrace systému mezi sebou a jejich konsolidace na společné nově dodané infrastruktuře. **Implementované SW:** Identity management AC Identita a integrace na cca 20 systémů třetích stran, Systém pro monitoring privilegovaných uživatelů ObserveIT, IS pro finanční řízení PO Croseus, Digitální úřední desky Kivi a Spojmont, IP pro městskou policií MP Manager, Rozvoj spisových služeb spol. Geovap, VERA, Docházkový systém PowerKey, Systém pro monitoring stavů ICT infrastruktury PRTG, Systém pro monitoring datových toků INVEA, Objednávkový a vyvolávací systém.
• Období (od – do)	Q1 – Q4 2018
• Název projektu	Realizace bezpečnostních opatření podle zákona o kybernetické bezpečnosti, Výzva č. 10
• Zadavatel projektu	K2 atmitec s.r.o.
• Koncový zákazník	**Moravskoslezský kraj**
• Popis projektu	Dodávka a konfigurace nástroje SIEM McAfee pokrývajícího funkcionalitu pro audit logů za účelem zvýšení bezpečnosti prostředí Krajského úřadu Moravskoslezského kraje (dále též „KÚ MSK“) v souvislosti s naplněním požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti a vyhlášky č. 316/2014 Sb., o kybernetické bezpečnosti.
• Období (od – do)	Q2- Q3 2017
• Název projektu	Upgrade na Microsoft Windows Server 2016
• Zadavatel projektu	**TŘINECKÉ ŽELEZÁRNY a.s.**
• Popis projektu	Provedení generační obměny Microsoft Windows Server 2016 včetně optimalizace služeb MS AD, DHCP, DNS, FS, DFS a nasazení MS CA pro dvě domény. Zlepšení užitné hodnoty řešení: efektivita správy, bezpečnost a celkové zvýšení kvality služeb
• Období (od – do)	Q3 2016
• Název projektu	Serverovna Kvasiny, Serverová a desktopová virtualizace
• Zadavatel projektu	**EVEKTOR spol. s r. o.**
• Popis projektu	Vybudování kompletní serverové a síťové infrastruktury včetně dodávky, implementace a následné podpory diskového pole. Vybudování serverové a

desktopové vitalizační vrstvy VMware a VMware Horizon View (VDI) pro účely grafický výkonných aplikací (CAD).

• Období (od – do)	Q1 2016
• Název projektu	Systém pro monitoring aktivity privilegovaných uživatelů
• Zadavatel projektu	**Krajský úřad Moravskoslezského kraje**
• Popis projektu	Dodávka systému na sledování privilegovaných účtů. Pomocí tohoto nástroje je naplňován jeden z požadavků ZKB. Systém ObserveIT funguje jako tzv. session rekordér.

• Období (od – do)	Q4 2015
• Název projektu	**Analýza a konsolidace DB MS SQL, Konsolidace serverové MS AD infrastruktury**
• Zadavatel projektu	**Kofola a.s.**
• Popis projektu	Analýza a následná migrace a konsolidace databázového prostředí na platformě MS SQL, provedení konsolidace MS Windows serverové infrastruktury do jednotné adresářové struktury vybudované na platformě MS Active Directory.

• Období (od – do)	Q3 – Q4 2015
• Název projektu	**MNO Rekonstrukce IT infrastruktury - nové vyhlášení**
• Zadavatel projektu	**Městská nemocnice Ostrava**
• Popis projektu	Provedení práci ve všech oblastech IT infrastruktury, vybudování optické, metalické i bezdrátové sítě. Modernizace síťové i serverové infrastruktury včetně migrací služeb na nové technologie FW, IPS, MS Exchange, MS AD.

• Období (od – do)	Q2 – Q3 2015
• Název projektu	**IT4Innovations – Supercomputer Salamon**
• Zadavatel projektu	**Silicon Graphics International Corp**
• Popis projektu	Vybudování kompletní podpůrné infrastruktury pro 6tý nejrychlejší superpočítač Evropy Salomon. Realizace virtualizační platformy VMware pro chod klíčových management serverů obsluhujících výpočetní výkon 1,46 PFLOPS.

• Období (od – do)	Q1 – Q3 2015
• Název projektu	**Digitalizace a ukládání dat (PACS a krajské digitální úložiště)**
• Zadavatel projektu	**Krajský úřad Moravskoslezského kraje**
• Popis projektu	Vybudování centrálního datového úložiště (diskového pole) pro účely ukládání elektronické dokumentace pro potřeby Moravskoslezského kraje a jím zřizovaným organizacím. Realizace včetně implementace a zajištění technické podpory.

• Období (od – do)	Q2 – Q4 2015
• Název projektu	**Zavádění ICT v územní veřejné správě – IOP výzva č. 22**
• Zadavatel projektu	**Město Hlučín, Magistrát města Kravaře, Magistrát města Karviná**
• Popis projektu	Dodávka a implementace vybraných způsobilých oblastí v rámci dotačního titulu: **Hardware:** výměna telefonní ústředny, realizace skenovací linky, rozšíření diskových polí, dodávka nových serverů, dodávka páteřních i přístupových switchů včetně IRF konfigurace, HW pro zálohování dat, UPS, rozšíření městské sítě MAN, kamerový systém, protipožární systém, výměna zastaralé klimatizační jednotky **Software:** implementace nových informačních systémů, pořízení nového MS Office, centrální evidence smluv, implementace nových modulů do stávajících IS, redakční systémy, zavedení online formulářů, systém pro elektronizaci procesu jednání městského zastupitelstva, zavedení Portál úředníka, zavedení Portál občana, SW pro vedení agendy rady a zastupitelstva města, Uživatelské školení

• Období (od – do)	Q1 2014 – Q1 2015
• Název projektu	**Implementace bezpečnostní infrastruktury pro krajské technologické centra**

- Zadavatel projektu **Zlínský kraj, Moravskoslezský kraj, Jihomoravský kraj**
  - Popis projektu Implementace LoadBalancerů, webaplikačního firewallu a acces policy manageru - F5 BIG IP, systému pro zajištění redundance z více internetových připojení, systému pro analýzu datových toků – INVEA a systému pro korelační analýzu – SIEM McAfee.

- Období (od – do) Q4 2014 – Q1 2015, Q4 2016 – Q1 2017
  - Název projektu **Digitalizace a archivace faktur**
- Zadavatel projektu **Brembo Czech s.r.o., Linaset a.s.**
  - Popis projektu Tvorba analýzy a prováděcího projektu, implementace scanovací linky včetně nástroje pro datamining IBM datacup, tvorba serveru pro archivaci faktur včetně časových razítek – O2 archiv, provázanost dodávaného řešení se systémy dodavatele, zejména s MS AX, dokumentace a školení koncových uživatelů.

- Období (od – do) Q3 2014 – Q2 2015
  - Název projektu **Dodávka AC privátního cloudu**
- Zadavatel projektu **Shimano, ArcelorMittal Karviná, Město Opava**
  - Popis projektu Implementace AC privátního cloudu, dodávka server-storage konvergované infrastruktury včetně migrace provozních serverů do nového prostředí. Vybudování DR lokalit.

- Období (od – do) Q1 2014 – Q4 2014
  - Název projektu **Migrace z WinXP na Win7**
- Zadavatel projektu **Národná banka Slovenska**
  - Popis projektu Migrace operačního systému v prostředí Národné banky Slovenska na všech pracovních stanicích z Microsoft Windows XP na Windows 7, příprava, řešení logistiky, náročné testování aplikací, zabezpečení a optimalizace operačního systému.

- Období (od – do) Q3 2014
  - Název projektu **MS Global architecture for Home Credit Int.**
    Pilotní migrace 4 národních poboček do technologií Microsoft
- Zadavatel projektu **Homecredit CZ a.s.**
  - Popis projektu Globální návrh architektury MS prostředí pro všech 11 zemí HCI International.
    Implementace systémové infrastruktury MS prostředí AD, Exchange, Lync, BlackBerry
    Migrace poštovních služeb v 4 pilotních zemích (Indie, Indonésie, Filipíny, Hong Kong)

- Období (od – do) Q3 2014
  - Název projektu **Zpracování strategického přístupu ICT v rámci investičních akcí a v rámci provozu ICT**
- Zadavatel projektu **Teplárny Brno a.s.**
  - Popis projektu Vyhodnocení ICT prostředí zákazníka a vypracování nové ICT strategie pro další roky, včetně vypracování konkrétních investičních plánů.

- Období (od – do) Q4 2013 – Q1 2014
  - Název projektu **Analýza platformy FileNet**
- Zadavatel projektu **PZU – Powszechny Zaklad Ubezpieczeń (Warszawa)**
  - Popis projektu Provedení performance analýzy platformy FileNet včetně aplikacedoporučení.
    Vypracování migračního projektu pro upgrade platformy na nejnovější verzi.

- Období (od – do) Q1 2012 – Q4 2014
  - Název projektu **Zvýšení kvality a dostupnosti veřejných služeb – IOP výzva č. 18**
- Zadavatel projektu **Město Hlučín, Město Rychnov nad Kněžnou, Město Kravaře, Město Frýdlant, Město Rožnov pod Radhoštěm, Město Vsetín**
  - Popis projektu Dodávka a implementace vybraných způsobilých oblastí v rámci dotačního titulu.
    Vybudování technologických center, vybavení serveroven, implementace server-storage architektury ve vysoké dostupnosti, virtualizační platforma VMware/hyper-v,

páteřní LAN infrastruktura, motorgenerátory, UPS, zálohování, monitoring, dohled.

• Období (od – do)	Q3 2012
• Název projektu	**Modernizace hlasových systémů**
• Zadavatel projektu	**AT Computers a.s.**
• Popis projektu	Dodávka a implementace IP telefonie Inovaphone napříč celou firmou, včetně zahraničních poboček, komunikačního rozhraní MS Lync 2010, integrace do stávajících systémů, vybudování call-centra na technologii MS Lync 2010.
• Ocenění	**Vítěz Microsoft Awards 2013 v kategorii Komunikace a telefonie**

• Období (od – do)	Q1-Q4 2012
• Název projektu	**Informační systém základních registrů**
• Zadavatel projektu	**Česká republika – Ministerstvo vnitra**
• Role na projektu	Projektový vedoucí – část administrace
• Popis projektu	Informační Systém Základních Registrů - vytvoření komplexního informačního systému (včetně vyvinutého aplikačního software) včetně ICT infrastruktury s vysokou dostupností (2 datová centra). Ověření funkcionality, naplnění relevantními daty, verifikace dat, pilotní provoz podle zákona č.111/2009 Sb., o základních registrech a nasazení Informačního systému základních registrů do ostrého provozu.

ŠKOLENÍ A CERTIFIKACE

• Certifikace	Certifikace Projektový manažer **PRINCE 2 PRACTITIONER (expirace 2027)** Certifikace Projektový manažer **IPMA level D (expirace 2016)** Certifikace **ITIL® V3**
• Profesní školení	**Měkké dovednosti** Školení lídrů – Caritas Školení emoční inteligence – Scott&Hagget Czech Školení vyjednávání pro projektové manažery – princonsult.cz Školení negociace – princonsult.cz Řízení diskuse pro PM- facilitace – Scott&Hagget Czech **Odborné dovednosti** Školení ITIL® V3 Foundation – AutoCont CZ Školení projektového managementu dle standardu IPMA – Shine Consulting Školení řízení Programu – SPŘ Školení řízení rozsahu projektu dle metody WBS – IT Cluster Školení nástrojů MS Project Professional, MS Project server – AutoCont CZ

JAZYKOVÉ ZNALOSTI

MATEŘSKÝ JAZYK	**Český jazyk, Polský jazyk**
OSTATNÍ JAZYKY	
	Anglický jazyk
• Úroveň	Upper-intermediate (vyšší)
	Německý jazyk
• Úroveň	Pre-intermediate (mírně pokročilý)

PODPIS

[redacted]

V Ostravě dne 27.6.2022

[redacted]

PeopleCert®
All talents, certified.

AXELOS
GLOBAL BEST PRACTICE

This is to certify that

[redacted]

Has achieved the

PRINCE2® Practitioner Certificate in Project Management

Effective from **23 Jun 2022**

Expiry date **23 Jun 2027**

Certificate number **GR634063360FJ**

Candidate number **9980052983990591**

[redacted]

[redacted]

PRINCE2 5th edition

Printed on 27 June 2022

1.2.1.1 Referenční zakázky – projektový manažer Filip Junga

	IMPLEMENTACE SYSTÉMU MANAGEMENTU BEZPEČNOSTI INFORMACÍ PRO NEMOCNICE ZLÍNSKÉHO KRAJE
Místo	Zlín
Identifikace klienta	Krajská nemocnice T. Bati, a. s., Havlíčkovo nábřeží 600, Zlín, 762 75, ičo 27661989
Rozsah projektu	Zajištění dostupnosti a integrity informací, servery, UPS, FW, SW, switche, Zlín, Dodávka hyper-konvergované serverové infrastruktury, instalace, konfigurace, zprovoznění, zaškolení administrátorů, zajištění technické podpory
Kontaktní osoba	jméno: [redacted] tel.: [redacted] e-mail: [redacted]
Počátek	1/2020
Konec	9/2020
Hodnota zakázky	Více než 16 mil Kč bez DPH

	IMPLEMENTACE SYSTÉMU MANAGEMENTU BEZPEČNOSTI INFORMACÍ PRO NEMOCNICE ZLÍNSKÉHO KRAJE
Místo	Uherské Hradiště
Identifikace klienta	Uherskohradišťská nemocnice a.s. J. E. Purkyně 365, 686 06 Uherské Hradiště, ičo 27660915,
Rozsah projektu	Zajištění dostupnosti a integrity informací, servery, UPS, FW, SW, switche, Zlín, Dodávka hyper-konvergované serverové infrastruktury, instalace, konfigurace, zprovoznění, zaškolení administrátorů, zajištění technické podpory
Kontaktní osoba	jméno: [redacted] tel.: [redacted] e-mail: [redacted]
Počátek	1/2020
Konec	9/2020
Hodnota zakázky	Více než 18 mil Kč bez DPH

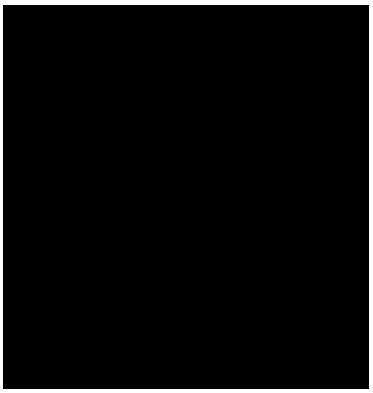
IMPLEMENTACE SYSTÉMU MANAGEMENTU BEZPEČNOSTI INFORMACÍ PRO NEMOCNICE ZLÍNSKÉHO KRAJE

Místo	Kroměříž
Identifikace klienta	Kroměřížská nemocnice a.s. Havlíčkova 660/69, 767 01 Kroměříž, ičo 27660532,
Rozsah projektu	Zajištění dostupnosti a integrity informací, servery, UPS, FW, SW, switche, Zlín, Dodávka hyper-konvergované serverové infrastruktury, instalace, konfigurace, zprovoznění, zaškolení administrátorů, zajištění technické podpory
Kontaktní osoba	jméno: [redacted] tel.: [redacted] e-mail: [redacted]
Počátek	1/2020
Konec	9/2020
Hodnota zakázky	Více než 13 mil Kč bez DPH

IMPLEMENTACE SYSTÉMU MANAGEMENTU BEZPEČNOSTI INFORMACÍ PRO NEMOCNICE ZLÍNSKÉHO KRAJE

Místo	Vsetín
Identifikace klienta	Vsetínská nemocnice a.s. Nemocniční 955, 755 01 Vsetín, ičo 26871068
Rozsah projektu	Zajištění dostupnosti a integrity informací, servery, UPS, FW, SW, switche, Zlín, Dodávka hyper-konvergované serverové infrastruktury, instalace, konfigurace, zprovoznění, zaškolení administrátorů, zajištění technické podpory
Kontaktní osoba	jméno: [redacted] tel.: +[redacted] e-mail: [redacted]
Počátek	1/2020
Konec	9/2020
Hodnota zakázky	Více než 13 mil Kč bez DPH

1.2.2 [redacted]



[redacted]

Senior IT Security Specialist | Aricoma Enterprise Cybersecurity a.s.

Zkušenosti v oblasti ICT bezpečnosti: 15 let

V Aricoma Enterprise Cybersecurity zaměstnán/a: od roku 2007

- Klíčové dovednosti

Zavádění systému řízení informační bezpečnosti, bezpečnostní audity, analýzy rizik, znalost bezpečnostních norem, tvorba bezpečnostní dokumentace, řízení kontinuity, řízení penetračních testů, bezpečnostní technologie, implementace bezpečnostních opatření a jejich zavádění do praxe, zavádění bezpečnosti do procesu vývoje SW, analytické práce pro vývoj SW, vedení týmu, projektové řízení.

- Vybrané projekty

- **Fakultní nemocnice Plzeň**

  Příprava společnosti k certifikaci dle ISO/IEC 27001 včetně vypracování bezpečnostní dokumentace v souladu se ZoKB, zpracování analýzy rizik a realizace školení.

- **Symbiosy s.r.o. (SK)**

  Příprava společnosti k certifikaci dle ISO/IEC 27001 včetně vypracování bezpečnostní dokumentace, zpracování analýzy rizik a realizace školení.

- **KBC Group NV (CZ, SK, BE, IE, FR)**

  Více než 80 projektů – řízení projektů, penetrační testy, procesní audity, analytické práce pro vývoj SW

- **Česká spořitelna, a.s.**

  Více než 30 projektů – řízení projektů, penetrační testy, procesní audity

- **Krajská nem. T.Bati Zlín, Uherskohradišťská nem., Vestínská nem., Kroměřížská nem**

Implementace systémů managementu bezpečnosti informací a poskytovaných služeb

- **Českomoravská stavební spořitelna, a.s.**

Více projektů – řízení projektů, penetrační testy, procesní audity, tvorba bezpečnostní dokumentace

- **Operátor trhu s elektřinou, a.s.**

Více projektů – řízení projektů, penetrační testy, procesní audity, testy metodami sociálního inženýrství

- **T-Systems Slovakia s.r.o.**

Více projektů – tvorba bezpečnostní dokumentace, procesní audity

- **Mountfield, a.s.**

Více projektů – řízení projektů, penetrační testy, procesní audity

- Pracovní zkušenosti

- **Aricoma Enterprise Cybersecurity a.s.**

Senior IT Security Specialist, 2020 – dosud

- **AEC, a.s.**

Head of Risk & Compliance Division, 2016 – 2020

- **AEC, spol. s r.o.**

IT Security consultant, 2007 – 2016

- **ecommerce.cz, a.s.**

Analytik vývoje SW, 2006 – 2007

- **Vojenský technický ústav letectva, s. p.**

Programátor, analytik, vedoucí projektu 2002 – 2006

- Vzdělání

- **Vojenská akademie Brno, fakulta letectva a PVO**

  Ing., Automatizované systémy letectva a PVO, 1995 – 2001

- **Střední průmyslová škola Šumperk**

  Maturita, obor Doprava a přeprava, 1991 – 1995

- Školení & Certifikáty

- CISA, 2020, ISACA, ID 20168676

  CISM, 2020, ISACA, ID 2052344

  CISSP, 2018, (ISC)², ID 681592

  Manažer kybernetické bezpečnosti dle zák. 181/2014 Sb., 2020, Taylor & Cox

  Data Privacy Officer, 2017, Taylor & Cox

  ITIL v3, 2009, GOPAS, a.s.

- Nástroje & Standardy

Řada norem ISO/IEC 27001-5 Information Security Management Systems

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti + navazující vyhlášky

Zákon č. 110/2019 Sb. o zpracování osobních údajů

GDPR (General Data Protection Regulation)

OWASP Testing Guide v4

International Information System Security Certification Consortium

The (ISC)² Board of Directors hereby awards

[redacted]

the credential of

Certified Information Systems Security Professional

having met all of the certification requirements, which include the professional experience prerequisite, adoption of the (ISC)² Code of Ethics, and successful performance on the required competency examination, subject to recertification every three years, this individual is entitled to all of the rights and privileges associated with this designation, as defined in the (ISC)² Bylaws.

[redacted]

CISSP

ANSI ISO/IEC 17024

681592
Certification Number

Sep 1, 2021 - Aug 31, 2024
Certification Cycle

Certified Since: 2018

(ISC)²

Verify Member is in good standing at:www.isc2.org/verify

Printed On: 11/29/2022

CISM Certified Information Security Manager.
An ISACA® Certification

ISACA hereby certifies that

[redacted]

has successfully met all requirements and is qualified as a Certified Information Security Manager; in witness whereof, we have subscribed our signatures to this certificate.

Requirements include prerequisite professional experience; adherence to the ISACA Code of Professional Ethics and the CISM continuing professional education policy; and passage of the CISM exam.

2052344	16 July 2020	31 January 2024
Certificate Number	Date of Certification	Expiration Date

ISACA

[redacted]

CISA Certified Information Systems Auditor
An ISACA® Certification

ISACA hereby certifies that

[redacted]

has successfully met all requirements and is qualified as a Certified Information Systems Auditor;
in witness whereof, we have subscribed our signatures to this certificate.

Requirements include prerequisite professional experience; adherence to the ISACA Code of Professional Ethics and the CISA continuing professional education policy; and passage of the CISA exam.

20168676	10 September 2020	31 January 2024
Certificate Number	Date of Certification	Expiration Date

ISACA

[redacted]

1.2.2.1 Referenční zakázky – bezpečnostní architekt Jan Poduška

	IMPLEMENTACE SYSTÉMU MANAGEMENTU BEZPEČNOSTI INFORMACÍ PRO NEMOCNICE ZLÍNSKÉHO KRAJE
Místo	Zlín
Identifikace klienta	Krajská nemocnice T. Bati, a. s., Havlíčkovo nábřeží 600, Zlín, 762 75, ičo 27661989
Rozsah projektu	Zajištění dostupnosti a integrity informací, servery, UPS, FW, SW, switche, Zlín, Dodávka hyper-konvergované serverové infrastruktury, instalace, konfigurace, zprovoznění, zaškolení administrátorů, zajištění technické podpory
Kontaktní osoba	jméno: [redacted] tel.: [redacted] e-mail: [redacted]
Počátek	1/2020
Konec	9/2020
Hodnota zakázky	Více než 16 mil Kč bez DPH

	IMPLEMENTACE SYSTÉMU MANAGEMENTU BEZPEČNOSTI INFORMACÍ PRO NEMOCNICE ZLÍNSKÉHO KRAJE
Místo	Uherské Hradiště
Identifikace klienta	Uherskohradišťská nemocnice a.s. J. E. Purkyně 365, 686 06 Uherské Hradiště, ičo 27660915,
Rozsah projektu	Zajištění dostupnosti a integrity informací, servery, UPS, FW, SW, switche, Zlín, Dodávka hyper-konvergované serverové infrastruktury, instalace, konfigurace, zprovoznění, zaškolení administrátorů, zajištění technické podpory
Kontaktní osoba	jméno: [redacted] tel.: [redacted] e-mail: [redacted]
Počátek	1/2020
Konec	9/2020
Hodnota zakázky	Více než 18 mil Kč bez DPH

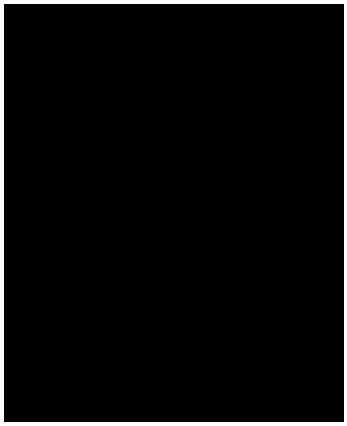
IMPLEMENTACE SYSTÉMU MANAGEMENTU BEZPEČNOSTI INFORMACÍ PRO NEMOCNICE ZLÍNSKÉHO KRAJE

Místo	Kroměříž
Identifikace klienta	Kroměřížská nemocnice a.s. Havlíčkova 660/69, 767 01 Kroměříž, ičo 27660532,
Rozsah projektu	Zajištění dostupnosti a integrity informací, servery, UPS, FW, SW, switche, Zlín, Dodávka hyper-konvergované serverové infrastruktury, instalace, konfigurace, zprovoznění, zaškolení administrátorů, zajištění technické podpory
Kontaktní osoba	jméno: [redacted] tel.: [redacted] e-mail: [redacted]
Počátek	1/2020
Konec	9/2020
Hodnota zakázky	Více než 13 mil Kč bez DPH

IMPLEMENTACE SYSTÉMU MANAGEMENTU BEZPEČNOSTI INFORMACÍ PRO NEMOCNICE ZLÍNSKÉHO KRAJE

Místo	Vsetín
Identifikace klienta	Vsetínská nemocnice a.s. Nemocniční 955, 755 01 Vsetín, ičo 26871068
Rozsah projektu	Zajištění dostupnosti a integrity informací, servery, UPS, FW, SW, switche, Zlín, Dodávka hyper-konvergované serverové infrastruktury, instalace, konfigurace, zprovoznění, zaškolení administrátorů, zajištění technické podpory
Kontaktní osoba	jméno: [redacted] tel.: [redacted] e-mail: [redacted]
Počátek	1/2020
Konec	9/2020
Hodnota zakázky	Více než 13 mil Kč bez DPH

1.2.3 [redacted]



[redacted]

Senior Security Specialist | AEC a.s.

Pozice na projektu: Senior Security Specialist

Zkušenosti v oblasti ICT bezpečnosti: 10 let

V AEC zaměstnán/a: od roku 2017

- Klíčové dovednosti

Networking Security, Internal and External Penetration Tests, Networking, Security event monitoring, Security assessment, Network Behaviour Analysis, Security Standards and Technologies, Operating systems

- Vybrané projekty

- **Českomoravská stavební spořitelna - Implementace Firewallu**

  Implementace a konfigurace technologie Check Point

- **Home Credit - Implementace Firewallu**

  Implementace a konfigurace technologie Check Point

- **Povodí Moravy – Detekce a odstranění následků průniku do počítačové sítě**

  Analýza útoků na společnost

- **Vice zakazníků – Implementace klasifikace informací a systému pro značkování dokumentů**

  Zavedení klasifikace dokumentů

- **Webnode – penetrační testy**

  Penetrační testy webové aplikace a externí penetrační testy infrastruktury

- **Krajský úřad Zlínského kraje – Datacentrum**

  Vybudování Technologického centra a krajská komunikační infrastruktury

- **Pro-Line comp – NBA a hardering**

  Implementace NBA technologie a hardering metrolopolitní sítě

- **Krajský úřad Zlínského kraje – Bezpečnostní infrastruktura**

  Implementace bezpečnostní infrastruktury a rozvoj služeb Technologického centra kraje

- **Nemocnice Zlínského kraje - Implementace systémů managementu bezpečnosti informací a poskytovaných služeb**

  Krajská nem. T.Bati Zlín, Uherskohradišťská nem., Vestínská nem., Kroměřížská nem

  Implementace Firewallu

- **Fakultní nemocnice Plzeň - KOMPLEXNÍ OCHRANA CELONEMOCNIČNÍHO INFORMAČNÍHO SYSTÉMU FN PLZEŇ VŮČI KYBERNETICKÝM HROZBÁM - BEZPEČNOSTNÍ INFRASTRUKTURA A MONITORING**

  Komplexní ochrana celonemocničního informačního systému FN Plzeň vůči kybernetickým hrozbám - Bezpečnostní infrastruktura a monitoring

- **Nemocenice Rokycany - Implementace Active Directory**

  Implementace a konfigurace technologie Check Point

- **Nemocnice Pardubice – Rekonfigurace emailové ochrany**

  Implementace a konfigurace emailové ochrany

- Pracovní zkušenosti

- **AEC, a.s.**

Senior Security Specialist, březen 2017 - současnost

- **Krajský úřad Zlínského kraje**

System and Security Administrator, 2011 – 2017

- **Pro-line s.r.o. Software Engineer**

Head of Technical Support. 2010 – 2011

- **Westcom s.r.o.**

IT Network Administrator, 2004 – 2010

- Vzdělání

- **Vysoké učení technické v Brně, fakulta informačních technologií**
- Bc., Informační technologie, 2002 – 2004

- Školení & Certifikáty

Certified Ethical Hackers, 2016, EC Council, certificate

Check Point Certified Security Expert, 2021, certificate

Check Point Certified Security Administrator R80, 2018, certificate

FireEye Partner Sales Certification, 2019, certificate

FireEye Systems Engineer (FSE) , 2019, certificate

Flowmon Networsk - Solution Consultant, 2018, certificate

Configuring Windows Server 2008/2008 R2 Active Directory Domain Services, 2015

Designing, Optimizing and Maintaining a Database Administrative Solution for Microsoft SQL Server, 2014

- Nástroje & Standardy

OWASP, PTES standard, CIS


CHECK POINT™

CHECK POINT SOFTWARE TECHNOLOGIES LTD.

THIS CERTIFIES THAT

[redacted]

HAS DEMONSTRATED THE KNOWLEDGE TO BE A

Check Point Certified Security Expert R80

This 26 day of July 2022

Expiration Date: July 26, 2024

[redacted]

Vice President, Learning and Training

Check Point mind Learn from the masters!

CHECK POINT CERTIFIED · CHECK POINT · CHECK POINT CERTIFIED

Validate this certificate's authenticity at www.credly.com/org/checkpoint/verify

1.2.3.1 Referenční zakázky – specialista na ochranu infrastruktury Josef Gottwald

	IMPLEMENTACE SYSTÉMU MANAGEMENTU BEZPEČNOSTI INFORMACÍ PRO NEMOCNICE ZLÍNSKÉHO KRAJE
Místo	Zlín
Identifikace klienta	Krajská nemocnice T. Bati, a. s., Havlíčkovo nábřeží 600, Zlín, 762 75, ičo 27661989
Rozsah projektu	Zajištění dostupnosti a integrity informací, servery, UPS, FW, SW, switche, Zlín, Dodávka hyper-konvergované serverové infrastruktury, instalace, konfigurace, zprovoznění, zaškolení administrátorů, zajištění technické podpory

Kontaktní osoba	jméno: [redacted] tel.: [redacted] e-mail: [redacted]
Počátek	1/2020
Konec	9/2020
Hodnota zakázky	Více než 16 mil Kč bez DPH

IMPLEMENTACE SYSTÉMU MANAGEMENTU BEZPEČNOSTI INFORMACÍ PRO NEMOCNICE ZLÍNSKÉHO KRAJE

Místo	Uherské Hradiště
Identifikace klienta	Uherskohradišťská nemocnice a.s. J. E. Purkyně 365, 686 06 Uherské Hradiště, ičo 27660915,
Rozsah projektu	Zajištění dostupnosti a integrity informací, servery, UPS, FW, SW, switche, Zlín, Dodávka hyper-konvergované serverové infrastruktury, instalace, konfigurace, zprovoznění, zaškolení administrátorů, zajištění technické podpory
Kontaktní osoba	jméno: [redacted] tel.: [redacted] e-mail: [redacted]
Počátek	1/2020
Konec	9/2020
Hodnota zakázky	Více než 18 mil Kč bez DPH

IMPLEMENTACE SYSTÉMU MANAGEMENTU BEZPEČNOSTI INFORMACÍ PRO NEMOCNICE ZLÍNSKÉHO KRAJE

Místo	Kroměříž
Identifikace klienta	Kroměřížská nemocnice a.s. Havlíčkova 660/69, 767 01 Kroměříž, ičo 27660532,
Rozsah projektu	Zajištění dostupnosti a integrity informací, servery, UPS, FW, SW, switche, Zlín, Dodávka hyper-konvergované serverové infrastruktury, instalace, konfigurace, zprovoznění, zaškolení administrátorů, zajištění technické podpory
Kontaktní osoba	jméno: [redacted] tel.: [redacted]

	e-mail: [redacted]
Počátek	1/2020
Konec	9/2020
Hodnota zakázky	Více než 13 mil Kč bez DPH

IMPLEMENTACE SYSTÉMU MANAGEMENTU BEZPEČNOSTI INFORMACÍ PRO NEMOCNICE ZLÍNSKÉHO KRAJE

Místo	Vsetín
Identifikace klienta	Vsetínská nemocnice a.s. Nemocniční 955, 755 01 Vsetín, ičo 26871068
Rozsah projektu	Zajištění dostupnosti a integrity informací, servery, UPS, FW, SW, switche, Zlín, Dodávka hyper-konvergované serverové infrastruktury, instalace, konfigurace, zprovoznění, zaškolení administrátorů, zajištění technické podpory
Kontaktní osoba	jméno: [redacted] tel.: [redacted] e-mail: [redacted]
Počátek	1/2020
Konec	9/2020
Hodnota zakázky	Více než 13 mil Kč bez DPH

KOMPLEXNÍ OCHRANA CELONEMOCNIČNÍHO INFORMAČNÍHO SYSTÉMU FN PLZEŇ VŮČI KYBERNETICKÝM HROZBÁM - BEZPEČNOSTNÍ INFRASTRUKTURA A MONITORING

Místo	Plzeň
Identifikace klienta	Fakultní nemocnice Plzeň, Edvarda Beneše 1128/13 301 00 Plzeň-Bory, ičo 00669806
Rozsah projektu	Komplexní ochrana celonemocničního informačního systému FN Plzeň vůči kybernetickým hrozbám - Bezpečnostní infrastruktura a monitoring
Kontaktní osoba	jméno: [redacted] tel.: [redacted] e-mail: [redacted]
Počátek	1/2020
Konec	1/2021

Hodnota zakázky	Více než 129 mil Kč bez DPH

1.2.4 [redacted]

PROFESNÍ ŽIVOTOPIS

Jméno Příjmení [redacted]

Pracovní pozice Systémový specialista / Konzultant

Zaměstnavatel ARICOMA SYSTEMS a.s.

Adresa [redacted]

Telefon

E-mail

NEJVYŠŠÍ DOSAŽENÉ VZDĚLÁNÍ

Období (od – do) 1983 - 1987

Název a typ organizace Střední odborné učiliště spojů, Ostrava-Poruba

studijní obor mechanik telekomunikačních a přenosových zařízení

Úroveň vzdělání Úplné střední odborné

Profesní praxe

Období (od – do) 1.7. 2016 – doposud ARICOMA SYSTEMS A.S. (původně AUTOCONT a.s., v roce 2016 dochází ke sloučení části AG COM, a.s. s Autocont CZ a.s.)

Jméno a adresa zaměstnavatele ARICOMA SYSTEMS a.s., Hornopolní 3322/34, 702 00 Ostrava

Dnem 1.7.2016 nabylo účinnosti rozdělení společnosti AG COM, a.s. realizované podle Projektu rozdělení odštěpení sloučením,

vypracovaným ve smyslu zákona č. 125/2008 Sb.. Nástupnickou společností je AutoCont CZ a.s.. V důsledku realizace přeměny

přešlo na nástupnickou společnost všech 40 zaměstnanců IT Divize rozdělované společnosti. Certifikace a pracovní dovednosti

získané jednotlivými pracovníky ve společnosti AG COM jsou platné i ve společnosti AutoCont CZ.

Na nástupnickou společnost přešla rovněž veškerá práva a povinnosti ze smluv o dílo, kupních smluv a ze servisních smluv,

jejichž seznam a bližší specifikace jsou uvedeny v Projektu přeměny. Zakázky realizované společností AG COM před 30.6.2016

jsou tedy referenčními zakázkami nástupnické společnosti AutoCont CZ.

Období (od – do) 11/2004 – 06/2016

Jméno a adresa zaměstnavatele AG COM, a.s. (v roce 2016 dochází ke sloučení části AG COM, a.s. s Autocont CZ a.s.)

Dosažená pozice Servisní technik – specialista LAN / WAN sítí

Hlavní pracovní náplň a odpovědnost Návrh, příprava a realizace síťových zakázek

Instalace, konfigurace a správa LAN, MAN, WAN

Zabezpečení počítačových sítí

Servisní činnost, servisní dostupnost

Systémová podpora zákazníkům a pracovníkům společnosti

Období (od – do) 06/1987 – 11/2004

Jméno a adresa zaměstnavatele ČESKÝ TELECOM, a.s. a jeho právní předchůdci

Dosažená pozice Specialista infrastruktury IT – 1997 - 2004

Hlavní pracovní náplň a odpovědnost Instalace, konfigurace a správa interní datové sítě ČT

Mechanik telekomunikačních a přenosových zařízení

Instalace, konfigurace a správa zákaznických řešení telefonních služeb

REALIZOVANÉ PROJEKTY

Číslo projektu [1]

Období (od – do) 2020 – dosud

Zadavatel projektu Nemocnice Pardubického kraje, a.s.

Název projektu Dodávka nezbytné síťové infrastruktury do datového centra NPK pro běh KIS NPK a zvýšení úrovně ochrany perimetru počítačové sítě NPK

Role v projektu Projekt, realizace a následné servisní činnosti. Definování a realizace zabezpečení infrastruktury v nemocnicích Pardubického kraje a jejich vzájemného bezpečného propojení.

Dodávka a implementace síťových aktivních prvků, firewallů, sw pro správu a dohled prostředků perimetru počítačové sítě – 6,6 mil Kč bez DPH.

V rámci dodávky zakázky „Dodávka nezbytné síťové infrastruktury do datového centra NPK pro běh KIS NPK a zvýšení úrovně ochrany perimetru počítačové sítě NPK" bylo dodáno řešení včetně implementace, které zajišťovalo funkci interního firewalu i externího firewalu v objemu finančního plnění nad 1 mil. Kč

Dodávka a implementace Síťová bezpečnostní opatření – Sendbox – 6,1 mil Kč bez DPH

Hodnota zakázky více než 23 mil Kč bez DPH

Číslo projektu [2]

Období (od – do) 2019 - dosud

Zadavatel projektu Královéhradecký kraj

Název projektu Bezpečnostní infrastruktura a rozvoj TCK Královéhradeckého kraje

Role v projektu Projekt, realizace a následné servisní činnosti. Definování a realizace zabezpečení infrastruktury Královéhradeckého kraje.

V rámci dodávky projektu „Bezpečnostní infrastruktura a rozvoj TCK Královéhradeckého kraje" bylo dodáno řešení včetně implementace, které zajišťovalo funkci interního firewalu i externího firewalu v objemu finančního plnění nad 1 mil. Kč

Hodnota zakázky více než 12 mil Kč bez DPH

Číslo projektu [3]

Období (od – do) 2019 - dosud

Zadavatel projektu Zlínský kraj

Název projektu Zvýšení kybernetické bezpečnosti Zlínského kraje

Role v projektu Projekt, realizace a následné servisní činnosti. Definování a realizace zabezpečení infrastruktury Zlínského kraje.

V rámci dodávky projetu „Zvýšení kybernetické bezpečnosti

Zlínského kraje" bylo dodáno řešení včetně implementace,

které zajišťovalo funkci interního firewalu i externího firewalu

v objemu finančního plnění nad 1 mil. Kč

Hodnota zakázky více než 32 mil Kč bez DPH

Číslo projektu [4]

Období (od – do) 2011 - dosud

Zadavatel projektu Oblastní nemocnice Náchod, a.s.

Název projektu Obměna firewallů a VPN propojení nemocnic, servisní činnosti

Role v projektu Projekt, realizace a následné servisní činnosti obměny firewallů v nemocnicích Královéhradeckého kraje a jejich vzájemného bezpečného propojení.

Číslo projektu [5]

Období (od – do) 2009 – dosud

Zadavatel projektu Statutární město Hradec Králové

Název projektu Outsourcing IT infrastruktury Magistrátu města HK

Role v projektu Projekt optimalizace, realizace a následné servisní činnosti pro aktivní prvky v síti zákazníka. Definování a realizace zabezpečení perimetru sítě.

Číslo projektu [6]

Období (od – do) 2004 - dosud

Zadavatel projektu Povodí Labe, státní podnik

Název projektu Vybudování a servis rozsáhlé WAN sítě

Role v projektu Projekt, realizace a následné servisní činnosti pro aktivní prvky v síti zákazníka.

Definování a realizace zabezpečení perimetru a WAN sítě.

CERTIFIKACE 2021 – Fortinet NSE8 Network Security Expert

2017 – Fortinet NSE8 Network Security Expert

2016 – Fortinet NSE7 Security Troubleshooter

2016 – Fortinet NSE5 Security Expert

2012 - Fortinet Certified Network Security Professional

2011 - HP Accredited System Engineer – Network security

2011 - HP Accredited Integration Specialist – Network Infrastructure

2011 - Cisco Certified Network Professional Security

2006 - Cisco Wireless LAN Support Specialist

2005 - Cisco Certified Network Associate

2002 - Nortel Networks Certified Support Specialist

2002 - Nortel Networks Accelerated Router Configuration, Maidenhead, GB

1998 - Správa síťových služeb HP-UX, Hewlett-Packard, ČR

1998 - HP OpenView Network Node Manager, Hewlett-Packard, ČR

JAZYKOVÉ ZNALOSTI

MATEŘSKÝ JAZYKčeština

OSTATNÍ JAZYKY anglický jazky - středně pokročilá znalost slovem i písmem

PROFIL

Narozen v roce 1968. Od roku 1987 začal profesně působit ve společnosti Československé spoje, s.p. Zpočátku se věnoval problematice analogových a elektronických telefonů a pobočkových ústředen. Od roku 1997 se zaměřuje na problematiku informačních technologií se zaměřením na infrastrukturu LAN/WAN sítí. Od roku 2010 se specializuje na zabezpečení LAN/WAN sítí. Během své odborné kariéry získal zkušenosti se základy telefonie a principy její funkčnosti, jako základ pro fungování datové komunikace. Své vědomosti a zkušenosti dále prohluboval v oblasti přepínačů, směrovačů, bezdrátových sítí a firewallů až po nejnovější a nejmodernější technologie jako jsou IP telefonie, virtualizace, zabezpečení sítí pomocí IPS, UTM apod.

- Orientace v síťových produktech výrobců CISCO, HP, FORTINET
- Certifikovaná znalost funkcionalit a síťových řešení uvedených výrobců
- Znalost operačních systémů, databází a obecná znalost hardware
- Podpora prodeje a předprodejních aktivit

1.2.4.1 Referenční zakázky – síťový specialista [redacted]

Číslo projektu [1]

Období (od – do) 2020 – dosud

Zadavatel projektu Nemocnice Pardubického kraje, a.s.

Název projektu Dodávka nezbytné síťové infrastruktury do datového centra NPK pro běh KIS NPK a zvýšení úrovně ochrany perimetru počítačové sítě NPK

Role v projektu Projekt, realizace a následné servisní činnosti. Definování a realizace zabezpečení infrastruktury v nemocnicích Pardubického kraje a jejich vzájemného bezpečného propojení.
Dodávka a implementace síťových aktivních prvků, firewallů, sw pro správu a dohled prostředků perimetru počítačové sítě – 6,6 mil Kč bez DPH.

V rámci dodávky zakázky „Dodávka nezbytné síťové infrastruktury do datového centra NPK pro běh KIS NPK a zvýšení úrovně ochrany perimetru počítačové sítě NPK" bylo dodáno řešení včetně implementace, které zajišťovalo funkci **interního** firewalu i externího firewalu v objemu finančního plnění nad 1 mil. Kč

Dodávka a implementace Síťová bezpečnostní opatření – Sendbox – 6,1 mil Kč bez DPH

Hodnota zakázky více než 23 mil Kč bez DPH

Číslo projektu [2]

Období (od – do) 2019 - dosud

Zadavatel projektu Královéhradecký kraj

Název projektu Bezpečnostní infrastruktura a rozvoj TCK Královéhradeckého kraje

Role v projektu Projekt, realizace a následné servisní činnosti. Definování a realizace zabezpečení infrastruktury Královéhradeckého kraje.

V rámci dodávky projektu „Bezpečnostní infrastruktura a rozvoj TCK Královéhradeckého kraje" bylo dodáno řešení včetně implementace, které zajišťovalo funkci **interního** firewalu i externího firewalu v objemu finančního plnění nad 1 mil. Kč

Hodnota zakázky více než 12 mil Kč bez DPH

Číslo projektu [3]

Období (od – do) 2019 - dosud

Zadavatel projektu Zlínský kraj

Název projektu Zvýšení kybernetické bezpečnosti Zlínského kraje

Role v projektu Projekt, realizace a následné servisní činnosti. Definování a realizace zabezpečení infrastruktury Zlínského kraje.

V rámci dodávky projetu „Zvýšení kybernetické bezpečnosti Zlínského kraje" bylo dodáno řešení včetně implementace, které zajišťovalo funkci **interního** firewalu i externího firewalu v objemu finančního plnění nad 1 mil. Kč

Hodnota zakázky více než 32 mil Kč bez DPH

FORTINET
Training Institute

FORTINET
CERTIFIED
PROFESSIONAL
Network
Security

Potvrzení, že

[redacted]

dosáhl

Fortinet certifikovaný profesionál síťové bezpečnosti

Datum dosažení:	**3. června 2021**
Datum platnosti:	**29. března 2027**
Ověřovací číslo certifikace:	**3383908345RV**

[redacted]

[redacted]

Ověřte pravost tohoto certifikátu na:
https://training.fortinet.com/admin/tool/certificate/index.ph

FORTINET
Training Institute

FORTINET
CERTIFIED
EXPERT
Cybersecurity

Potvrzení, že

[redacted]

dosáhl

Fortinet certifikovaný expert kybernetické bezpečnosti

Datum dosažení: 30. března 2017
Datum platnosti: 29. března 2027
Ověřovací číslo certifikace: NSE8-003124

[redacted]

[redacted]

Ověřte pravost této certifikace pomocí kódu: 1013292758RV
https://training.fortinet.com/admin/tool/certificate/index.php

Příloha č. 4 – Specifikace Proprietárního software

Proprietární sw není součástí dodávky

Příloha č. 5 - Cenová kalkulace

Instrukce: Účastník vyplňuje jen růžová pole a není oprávněn jinak upravovat obsah souboru s výjimkou vzorce ve sloupci E první tabulky, který účastník naváže na konkrétní řádky tabulky na listu "Položky".

Implementace/cena za člověkoden (MD) [redacted]

	Kategorie	Implementace MD	Cena bez implementace včetně záruky na 5 let *	Cena full maintenance na 4 roky	Cena celkem bez DPH	Cena celkem s DPH
1	Vsetínská nemocnice a.s. Antivirová ochrana + EDR	[redacted]				
2	Vsetínská nemocnice a.s. Web aplikacni firewall (AWAF)					
3	Vsetínská nemocnice a.s. Wi-fi AP					
4	Vsetínská nemocnice a.s. Dodávka a implementace systému PIM/PAM					
5	Vsetínská nemocnice a.s. Interní Firewall					
6	Vsetínská nemocnice a.s. MFA / ochrana přístupu uživatelů					
7	Vsetínská nemocnice a.s. Single Sign-On (SSO)					
8	Vsetínská nemocnice a.s. System řízení přístupu do sítě 802.1x					
9	Systém pro analýzu síťového provozu a bezpečnostní monitoring					
10	Vsetínská nemocnice a.s. Hardening					
11	Back Up Trezor - diskový úložný systém - dodávka a implementace					
12	Vsetínská nemocnice a.s. Servery, Switche, Záložní zdroje					
13	Vsetínská nemocnice a.s. Backup Server					
14	Vsetínská nemocnice a.s. Zálohovací SW					
	SUMA					

Kategorie	Cena za rok	Cena za 4 roky bez DPH	Cena za 4 roky s DPH
SLA podpora dodavatele v režimu 24-7 bez full maintenance	[redacted]		
Full maintenance (včetně maintenance licencí)			
SUMA			

Kategorie	Cena za hodinu	Cena za rok (24hod)	Cena za 4 roky bez DPH (96 hod)	Cena za 4 roky s DPH
Služby rozvoje	[redacted]			

	Cena celkem bez DPH	Cena celkem s DPH
SUMA celkem = Cena celkem	41 881 100,00 Kč	50 676 131,00 Kč

* účastník naváže vzorec na konkrétní řádky z listu "Položky", které se vztahují k předmětnému bodu technické specifikace

Instrukce: sloupec F- Typ vybíráme zda se jedná o dodávku SW, HW, HW+SW nebo maintenance
sloupec G - Kategorie(záložka "Přehled" sloupec C) vybíráme oblast které se daná položka týká

#	PartNumber	Výrobce	Popis	Typ	Kategorie	Jednotková nabídková cena za jeden kus v Kč bez DPH	Nabízený počet kusů celkem	Celková výše nabídkové ceny za všechny kusy v Kč bez DPH
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
Celkem								

SLA (HW)

Dohoda o úrovni Služeb podpory a Služeb rozvoje

(Service Level Agreement)

Příloha č. 6 Smlouvy

1 Účel a pojmy

1.1 Účel

Účelem tohoto dokumentu je vymezit Služby podpory a Služby rozvoje, které jsou poskytovány na základě Smlouvy a definovat jejich požadovanou úroveň.

1.2 Slovník pojmů

Systém	Souhrnné označení všech položek HW a/nebo SW, dodaných na základě Smlouvy.
Akceptační řízení	Postup sjednaný smluvními stranami a popsaný ve smlouvě, jehož účelem je ověřit, že Plnění ve smyslu Smlouvy bylo řádně dokončeno. v rámci řešení Požadavků Objednatele při akceptačním řízení Poskytovatel prokazuje, že je realizace Požadavku dokončena a splňuje Akceptační kritéria. Akceptační řízení je ukončeno a dokumentováno podpisem „Akceptačního protokolu“.
Dostupnost	Parametr, který vyjadřuje provozní spolehlivost procentem celkového provozního času, ve kterém není užívání Systému omezováno výskytem Vad kategorie A. Závazný způsob výpočtu je uveden dále v textu.
Helpdesk	Webová aplikace provozovaná Poskytovatelem, určená jako jednotné místo pro hlášení Vad, Chyb a Incidentů, a také pro zadávání Požadavků na Služby rozvoje a Vyžádaných konzultací a služeb.
Hotline	Telefonická služba, poskytovaná Objednateli Poskytovatelem nepřetržitě k rychlému hlášení Vad, Chyb a Incidentů kategorie A a B.
Chyba	Zvláštní typ vady, která byla způsobena vlivem neodborné manipulace či svévolného poškození ze strany Objednatele či osoby pověřené Objednatelem a k jejímuž odstranění je třeba součinnosti Poskytovatele. Účelně vynaložené náklady Poskytovatele spojené s odstraněním Chyb budou Objednateli účtovány sazbou Služeb rozvoje; odstranění chyb se však nepočítá do předpokládaného objemu Služeb rozvoje. Kategorizace Chyb, stejně jako sjednané doby pro jejich odstranění, je stejná jako u Vad.

Incident	Nefunkčnost nebo nesprávná funkčnost Systému nebo jeho části, která není způsobena Poskytovatelem ani Objednatelem, není Vadou ani Chybou ve smyslu této přílohy a vzniká z důvodů na straně třetí osoby či v důsledku jiné okolnosti (např. vyšší moc). Řešení incidentů je stejně jako odstraňování vad zahrnuto v ceně Služeb podpory. Kategorizace Incidentů, stejně jako sjednané doby pro jejich odstranění, je stejná jako u Vad.
Koncový uživatel	Jakýkoli pracovník Objednatele, užívající v rámci plnění svých pracovních povinností Systém nebo jeho část.
Nouzový režim	Dočasné řešení Vad, Chyb nebo Incidentů kategorie A, které zajistí Objednateli alespoň takový režim užívání Systému, kdy je Objednatel schopen plnit své závazky vůči třetím osobám a státu a Systém nevykazuje nadále charakteristiky vady kategorie A.
Požadavek	Pojem používán výhradně jako požadavek na Služby rozvoje, tedy jde o požadavky na změnu nebo přidání funkcionality Systému, případně změny v nastavení Systému; jde typicky, ale nikoliv výlučně, o Požadavky, týkající se aplikační/softwarové části Systému.
Repair Time	Doba vyřešení Vady, Chyby a Incidentu a znamená dobu mezi časem od prokazatelného oznámení (přijetí) Vady, Chyby a Incidentu ze strany Objednatele Poskytovateli, a časem prokazatelného vyřešení Vady, Chyby a Incidentu Poskytovatelem.
Response Time	Doba reakce na Vadu, Chybu, Incident nebo Požadavek a znamená dobu mezi časem prokazatelného nahlášení Vady, Chyby, Incidentu nebo Požadavku ze strany Objednatele Poskytovateli, a časem prokazatelné reakce Poskytovatele na jejich oznámení. Reakcí Poskytovatele se rozumí kvalifikovaná reakce pracovníkem, který je kompetentní oznámenou událost řešit, ne administrativní reakce (např. automatizované nebo jiné potvrzení přijetí oznámení).
Rollback	Postup, při kterém je nově nainstalovaná aktualizace (verze) Systému odinstalována a je znovu uvedena do provozu verze původní.
SLA	Service Level Agreement – tato dohoda o rozsah a úrovni Služeb podpory a Služeb rozvoje.
Vada	Nefunkčnost nebo nesprávná funkčnost Systému nebo jeho části, rozpor mezi vlastnostmi Systému (nebo jeho samostatné dílčí části) a vlastnostmi popsanými v Technické specifikaci, Cílovém konceptu nebo

	Dokumentaci Systému se zohledněním případných změn v Akceptačním protokolu**,** nebo rozpor s vlastnostmi Systému, popsanými v objednané úpravě Systému. Odstraňování vad je zahrnuto v ceně Služeb podpory
Vyžádané konzultace a služby	Odborné telefonické, písemné nebo osobní konzultace nebo jiné služby, týkající se předmětu smlouvy, které jsou poskytnuty Poskytovatelem na vyžádání Objednatele a nejsou součástí jiných poskytovaných Služeb podpory. V SLA je definován rozsah Vyžádaných konzultací a služeb, které jsou zahrnuty do paušální úhrady Služeb podpory. Vyžádané konzultace a služby ke Službám rozvoje budou hrazeny dle hodinové sazby za Služby rozvoje.

2 Obecná ustanovení

2.1 Poskytovatel je certifikovaným partnerem nebo má souhlas od výrobce k poskytování Služeb podpory(servisu) nebo Služeb rozvoje Systému.

2.2 Poskytovatel bere na vědomí, že vlastníkem dat vložených Objednatelem do Systému je Objednatel, že data uložená v Systému jsou pro Objednatele nepostradatelná a ztrátou přístupu k nim nebo nemožností jejich zpracování by Objednateli vznikla škoda.

2.3 Odpovědnými osobami pro potřeby poskytování Služeb podpory a Služeb rozvoje jsou:

a) za Objednatele: [redacted]
    a. Kontaktní údaje dispečinku Objednatele:
        i. tel.: [redacted]
        ii. email: [redacted]
b) za Poskytovatele: [redacted]
    a. Kontaktní údaje dispečinku Poskytovatele:
        i. Hotline v pracovní době: [redacted]
        ii. Hotline mimo pracovní dobu: [redacted]
        iii. e-mail: [redacted]

2.4 Komunikace týkající se běžných technických anebo organizačních konzultací mohou být mezi odpovědnými osobami prováděny i telefonicky. Tyto konzultace budou zahrnuty do rozsahu poskytování Služeb podpory anebo Služeb rozvoje pouze po písemné dohodě Poskytovatele a Objednatele. Písemná dohoda může proběhnout i e-mailem, nebo prostřednictvím systému Helpdesk.

3 Služby podpory a jejich parametry

3.1 Služby podpory jsou

3.1.1 Zajištění správného, stabilního a plného fungování Systému po celou dobu trvání Smlouvy zejména v souvislosti s úpravami a rozvojem programového vybavení Systému prováděného jeho výrobcem nebo Poskytovatelem v případě SW a plnou funkčnost Systému bez snížení výkonu, spolehlivosti a bezpečnosti v případě HW.

3.1.2 Garance průběžné podpory a údržby programových úprav (zejména převod programových úprav do nových verzí systému, komplexní testování definovaných programových úprav) v případě SW.

3.1.3 Provozování Helpdesku Poskytovatelem.

3.1.4 Provozování nepřetržité telefonické služby Hotline k urgentnímu řešení Chyb, Vad a Incidentů kategorie A a B.

3.1.5 Odstraňování Vad Systému Poskytovatelem ve stanovených termínech.

3.1.6 Podpora a součinnost při řešení Chyb ve stanovených termínech.

3.1.7 Podpora a součinnost při řešení Incidentů ve stanovených termínech.

3.1.8 Provádění profylaktických prohlídek Systému v pravidelných dohodnutých intervalech: minimálně 1x měsíčně. Poskytovatel z těchto prohlídek předá dohodnutým způsobem protokol, který bude obsahovat soupis provedených prací a výsledná doporučení pro úpravy a rozvoj systému.

3.1.9 Zajištění plného souladu instalovaného SW Systému s platnou legislativou České republiky po celou dobu platnosti a účinnosti Smlouvy ve všech částech Systému, a to nejpozději dnem účinnosti legislativních změn.

3.1.10 Dodávky oprav, updatů, upgradů a nových verzí SW komponent Systému.

3.1.11 Implementace oprav, updatů, upgradů a nových verzí SW komponent Systému po předchozí domluvě a v součinnosti s Objednatelem. Pro vyloučení pochybností se uvádí, že součinnost Objednatele u této služby neruší povinnost Poskytovatele provést instalaci. Tuto povinnost má Poskytovatel vždy, není-li v konkrétním případě s Objednavatelem dohodnuto jinak.

3.1.12 Poskytování Vyžádaných konzultací k implementovanému Systému je v ceně Služeb podpory. Poskytování Vyžádaných konzultací a dalších služeb (včetně Služeb rozvoje) nad rámec výše uvedených bodů Služeb podpory **v celkovém max. rozsahu 96 hodin za každých 48 měsíců od akceptace díla/dodávky** .

3.2 Postupy Služeb podpory při aktualizacích a odstávkách jsou závazně tyto:

3.2.1 Pokud budou nutné aktualizace Systému nebo jeho částí, budou realizovány podle následujících pravidel:

3.2.1.1 Poskytovatel musí navrhnout scénář aktualizace včetně scénáře pro Rollback.

3.2.1.2 Objednatel odsouhlasí scénář aktualizace.

3.2.1.3 Pokud je pro danou část Systému k dispozici testovací prostředí:

3.2.1.3.1 Poskytovatel provede aktualizaci dle popsaného scénáře na testovacím prostředí.

3.2.1.3.2 Objednatel provede test a odsouhlasí provedení scénáře do produkce.

3.2.1.3.3 V případě zjištěné Vady provede Poskytovatel Rollback dle scénáře a následně navrhne upravený scénář.

3.2.1.3.4 Pokud Objednatel podle výsledku testu odsouhlasí aktualizaci produkčního systému

3.2.1.3.5 Poskytovatel se součinností Objednatele realizuje scénář na produkčním systému.

3.2.1.3.6 Poskytovatel provede v součinnosti s Objednatelem testy funkčnosti Systému.

3.2.1.3.7 Pokud Systém po aktualizaci vykazuje vady kategorie A nebo B, provede Poskytovatel Rollback dle scénáře a následně navrhne upravený scénář.

3.2.1.4 Pokud pro danou část Systému není k dispozici testovací prostředí:

3.2.1.4.1 Poskytovatel provede aktualizaci dle popsaného scénáře na produkčním prostředí.

3.2.1.4.2 Poskytovatel průběžně testuje úspěšnost jednotlivých kroků aktualizací, pokud je to možné.

3.2.1.4.3 Poskytovatel provede v součinnosti s Objednatelem testy funkčnosti Systému.

3.2.1.4.4 Pokud Systém po aktualizaci vykazuje vady kat. A nebo B, provede Poskytovatel Rollback dle scénáře a následně navrhne upravený scénář.

3.2.2 Odstávky Systému budou plánovány podle následujících pravidel:

3.2.2.1 Poskytovatel odhadne trvání odstávek ve scénáři dle předchozího odstavce.

3.2.2.2 Určení času realizace těchto scénářů je právem Objednatele. Objednatel je oprávněn požadovat jejich realizaci mimo hlavní provoz Objednatele. Pro účely tohoto ustanovení je doba hlavního provozu Objednatele stanovena od 05:00 do 19:00 včetně víkendů a svátků.

3.2.2.3 Pokud to realizace doporučení umožní, Poskytovatel při odstávce využije architekturu vysoké dostupnosti k tomu, aby umožnil Objednateli provoz bez ztráty dostupnosti informačního systému jako celku i v případě aktualizací systému.

3.2.3 Aktualizace firmware serverů, diskových polí (pokud jsou potřeba), firewall a prvků síťové infrastruktury provádí Poskytovatel po domluvě s Objednatelem v závislosti na charakteru aktualizací. Aktualizace vSphere provádí poskytovatel po domluvě s Objednatelem v závislosti na charakteru aktualizací. Aktualizace musí být prováděny tak, aby neovlivňovaly provoz Objednatele, zejména se musí provádět bez odstávky virtuálních serverů, které budou na dodaném Systému provozovány.

3.3 Jestliže ve vztahu k plnění podle Smlouvy vznikne v souvislosti se zaváděním nebo aktualizaci sytému řízení bezpečnosti informací nebo v souvislosti se zaváděním, prováděním nebo aktualizací bezpečnostních opatření podle zákona o kybernetické bezpečnosti a jeho prováděcích předpisů potřeba uzavřít dodatek k této smlouvě nebo zvláštní smlouvu, zavazuje se Poskytovatel poskytnout Objednateli veškerou součinnost nezbytnou k formulaci obsahu takového dodatku, resp. smlouvy. Poskytovatel se pro tento případ rovněž zavazuje poskytnout součinnost směřující k uzavření takového dodatku, resp. smlouvy v souladu se ZZVZ.

3.4 Školení, dokumentace a služby informovanosti při poskytování Služeb podpory

3.4.1 Poskytovatel zaškolí správce Systému nebo jiné osoby, určené Objednatelem, při implementaci nových verzí a/nebo úprav, buď vzdáleně formou videokonference nebo na místě u Objednatele.

3.4.2 K dodaným úpravám a aktualizacím Systému musí být dodána vždy s předstihem změnová dokumentace a změny se musí promítnout do uživatelské a správcovské dokumentace nejpozději ke dni instalace změny.

3.4.3 Pokud je součástí Systému aplikační software, zavazuje se Poskytovatel bez prodlení informovat Objednatele o veškerých softwarových produktech, nebo jejich částech, uvolňovaných v rámci této podpory a rovněž o všech nově samostatně dodávaných funkcích a modulech tohoto aplikačního SW.

3.5 Parametry řešení Vad, Chyb a Incidentů

3.5.1 Kategorie Vad, Chyb a Incidentů jsou definovány takto:

KATEGORIE VADY CHYBY INCIDENTU	POPIS KATEGORIE
A (kritická)	Událost v Systému, která je zásadní pro činnost Objednatele; nelze pokračovat v činnosti Systému nebo jeho části a není k dispozici žádné dočasné řešení problému.
B (závažná)	Událost v Systému, kdy je důležitá funkcionalita nebo důležitá část Systému nefunkční nebo v podstatných rysech vykazuje nesprávnou funkčnost a toto není možné nahradit jinou funkcionalitou nebo částí Systému.
C (běžná)	Událost, která není kritická nebo závažná, ale při níž je některá z funkcionalit nebo částí Systému nedostupná nebo pracuje chybně, je však možné ji dočasně nahradit jiným doporučeným způsobem nebo přerušit použití funkce nebo dané části Systému až do zajištění nápravy bez významného dopadu na činnost Objednatele.

3.5.2 Parametry Response Time a Repair Time jsou definovány takto (není-li v technické specifikaci zvláštní úprava u konkrétního HW/SW)

KATEGORIE VADY CHYBY INCIDENTU	RESPONSE TIME (běží od prokazatelného nahlášení)	REPAIR TIME (běží od prokazatelného oznámení, tj. přijetí)
A (kritická)	2 h	2 h
B (závažná)	2 h	36 h
C (běžná)	5 prac. dnů	bude dohodnutý ad hoc u každého incidentu

3.5.3 Parametr Dostupnost je definován jako poměr součtu času, kdy je informační systém v provozu bez výskytu Vad kategorie A oproti celkovému očekávanému provoznímu času za vyhodnocované období (tedy bez časů profylaktických prohlídek a dohodnutých plánovaných odstávek a Objednatelem nahlášených odstávek z důvodu Vad či Incidentů). Počítá se s provozem 24x7, včetně sobot, nedělí a svátků. Vyhodnocuje se obvykle měsíčně za uplynulé období trvání SLA, nejméně však jedenkrát za rok. Vyjadřuje se v procentech se dvěma desetinnými místy. Dostupnost Systému je požadovaná **nejméně na úrovni 99,95 %** za hodnocené období.

3.6 Postupy služeb Helpdesku a Hotline a řešení Vad, Chyb a Incidentů

3.6.1 Oznamovat Vady, Chyby, Incidenty i Požadavky jsou oprávněny určené osoby za Objednatele. Seznam těchto osob a případné změny uvede v Helpdesku osoba oprávněná ve věcech smluvních dle Smlouvy.

3.6.2 Pro hlášení Vad, Chyb a Incidentů kategorie A a B je k dispozici telefonická Hotline dostupná nepřetržitě (24x7). Běh lhůt, ve kterých je Poskytovatel povinen reagovat (Response Time) na Vady, Chyby, a Incidenty, popřípadě je odstranit (Repair Time), počíná běžet okamžikem nahlášení/oznámení. Po nahlášení na Hotline je Poskytovatel povinen vytvořit nebo doplnit záznam do Helpdesku.

3.6.3 Pro hlášení Vad, Chyb, Incidentů i Požadavků je dostupná Poskytovatelem provozovaná webová aplikace HelpDesk, obsluhovaná pracovníky Poskytovatele v pracovní dny mezi 8:00 a 16:00 CET/CEST. Běh lhůt, ve kterých je Poskytovatel povinen reagovat (Response Time) na Vady, Chyby, a Incidenty, popř. je odstranit (Repair Time), počíná běžet okamžikem nahlášení/oznámení v pracovní dny mezi 8:00 a 16:00, jinak v 8:00 následujícího pracovního dne, pokud nebyla událost kategorie A nebo B hlášena prostřednictvím Hotline. Pracovními dny se rozumí pondělí–pátek, kromě státních svátků v ČR.

3.6.4 Veškeré lhůty řešení Vad, Chyb a Incidentů budou měřeny v reálném čase. Do měření času se nezapočítává:

a) Prodlení v komunikaci prokazatelně zaviněné Objednatelem, evidované v systému Helpdesk nebo komunikací pomocí e-mailu v případě, že je Helpdesk nefunkční.
b) Prodlení v komunikaci se třetími stranami a v jejich součinnosti, je-li nezbytná, prokazatelně zaviněné těmito stranami (poskytovateli okolních subsystémů, HW a jiných SW), pokud jde o subsystémy, které souvisejí s provozem Systému a nejsou v odpovědnosti Poskytovatele nebo jeho poddodavatelů.
c) Posun času řešení na základě písemného rozhodnutí o tomto posunu Objednatelem a čas, potřebný na poskytnutí nezbytné součinnosti ze strany Objednatele, ke které byl Poskytovatelem Objednatel písemně (také emailem či prostřednictvím Helpdesk) vyzván.

3.6.5 Do měření času se naopak započítává doba, po kterou řeší incident poddodavatelé Poskytovatele nebo výrobci jednotlivých součástí Systému; Poskytovatel se nemůže zříct odpovědnosti za dodržení termínů poukazem na termíny svých poddodavatelů nebo výrobců dodaných částí Systému.

3.6.6 Chyby, Vady a Incidenty, jejich výskyt, způsob řešení a termíny zaznamenání a vyřešení, jak jsou uvedeny níže, jsou oběma smluvními stranami zaznamenávány v Helpdesku.

3.6.7 Kategorizaci Vady, Chyby či Incidentu provádí Objednatel. Objednatel je rovněž oprávněn stanovit priority řešení s tím, že Poskytovatel má právo odmítnout prioritní řešení, pokud řádně a ve lhůtě Repair Time odůvodní nemožnost prioritního řešení.

3.6.8 Lhůty pro řešení Požadavků si Objednatel dohodne s Poskytovatelem u každého Požadavku jednotlivě, podle charakteru daného Požadavku.

3.6.9 Poskytovatel a Objednatel se dohodnou na způsobu eskalace řešení Požadavků.

3.6.10 V případě, kdy není Helpdesk funkční, je Objednatel oprávněn Vadu, Chybu a Incident oznámit e-mailem nebo hlásit na telefonní číslo hotline Poskytovatele s tím, že Poskytovatel poté bez zbytečného odkladu zaznamená toto oznámení do Helpdesk, přičemž uvede, že se jedná o oznámení dodatečné a obě strany si v Helpdesk potvrdí původní čas (e-mailového, telefonického) přijetí oznámení.

3.6.11 Poskytovatel má právo provést verifikaci, zda jde o Vadu, Chybu nebo Incident a verifikaci kategorizace, a případně sdělit svůj nesouhlas s klasifikací Vady, Chyby nebo Incidentu stanovenou Objednatelem; uplynutím Response Time pro Vadu, Chybu nebo Incident dle klasifikace provedené Objednatelem zaniká právo Poskytovatele na sdělení nesouhlasu. V případě, kdy Poskytovatel nesouhlasí s klasifikací, je povinen odůvodnit tento nesouhlas a prokázat odůvodněnost svého návrhu překlasifikace. O případné překlasifikaci rozhoduje s konečnou platností Osoba oprávněná ve věcech smluvních na straně Objednatele. Poskytovatel má přitom povinnost i ve sporných případech a případech, kdy nesouhlasí s klasifikací Vady, Chyby nebo Incidentu, postupovat podle rozhodnutí a klasifikace Vady, Chyby nebo Incidentu provedené Objednatelem, a to až do případného pravomocného rozhodnutí soudu o klasifikaci Vady, Chyby nebo Incidentu; tím není dotčeno případné právo Poskytovatele na náhradu mu vzniklé škody v souvislosti s nesprávnou klasifikací provedenou Objednatelem.

3.6.12 Objednatel připouští postupné řešení Vad, Chyb a Incidentů, a to tak, že z kategorie A je možné pomocí Nouzového režimu navrženého Poskytovatelem ve sjednané době snížit kategorizaci na B a obdobně i z B na C, takové řešení je však podmíněno souhlasem Objednatele zaznamenaným v systému Helpdesk.

3.6.13 Poskytovatel nenese odpovědnost za věcnou a obsahovou správnost dat zadaných Koncovými uživateli. Do času dle sjednaných SLA se nezapočítává čas potřebný na nezbytnou obnovu nebo opravu chybných nebo nedostupných dat, pokud tuto chybovost dat nebo jejich nedostupnost nezpůsobil Poskytovatel nebo vada systému.

3.6.14 Poskytovatel oznamuje vyřešení Vad, Chyb, Incidentů i Požadavků zápisem do systému Helpdesk, v případě kategorie A a B v době mimo provozní dobu Helpdesku také telefonicky oprávněné osobě, která Vadu, Chybu a Incident hlásila.

3.6.15 Objednatel má právo nesouhlasit s vyřešením Vady, Chyby a Incidentu. V případě nesouhlasu s tímto řešením předloží reklamaci vyřešení. Tato reklamace obnovuje řešení Požadavku Objednatele na odstranění Vady, Chyby či Incidentu. Do celkového času řešení se doba od předání řešení do předání reklamace nezapočítává.

3.6.16 Na způsobu řešení a eventuální změně lhůty vyřešení Vady, Chyby, Incidentu i Požadavku se Poskytovatel a Objednatel mohou v konkrétním případě dohodnout jinak, vždy však zápisem v systému Helpdesku a oprávněnými osobami obou smluvních stran.

3.6.17 Vyhodnocení měřených parametrů Response time, Repair time a Dostupnost zasílá Poskytovatel Objednateli měsíčně. Toto vyhodnocení slouží jako podklad pro vzájemnou komunikaci Objednatele s Poskytovatelem za účelem udržení požadované úrovně SLA.

3.6.18 Pokud bude Poskytovatel pro dodržení parametrů SLA vyžadovat připojení Informačního systému na vzdálený dohled, Objednatel mu toto připojení umožní za podmínek, které jsou v souladu se Zákonem o kybernetické bezpečnosti.

3.7 Sankce za nedodržení požadovaných parametrů služeb Podpory jsou definovány ve Smlouvě.

4 Služby rozvoje a jejich postupy a parametry

4.1 Vymezení Služeb rozvoje

4.1.1 V rámci této Smlouvy jsou Služby rozvoje realizovány především řešením Požadavků na změnu nebo přidání funkcionality Systému, případně na změny v nastavení Systému; jde typicky, ale nikoliv výlučně, o Požadavky, týkající se aplikační/softwarové části Systému. Součástí Služeb rozvoje jsou také Vyžádané konzultace ke Službám rozvoje.

4.2 Postup zadávání a řešení Požadavků

4.2.1 Objednatel je oprávněn zadat Poskytovateli Požadavek formou zápisu do Helpdesku oprávněnou osobou Objednatele. Seznam oprávněných osob poskytne Poskytovateli osoba oprávněná ve věcech smluvních formou zápisu do Helpdesku.

4.2.2 Poskytovatel má právo si vyžádat od Objednatele nezbytné konzultace k vysvětlení specifikace Požadavku.

4.2.3 Poskytovatel vypracuje návrh realizace, který předá Objednateli formou zápisu do Helpdesku a který bude obsahovat zejména tyto části:

a) Specifikace Požadavku
b) Popis řešení
c) Požadavky na součinnost Objednatele
d) Termín realizace
e) Způsob předání a akceptační kritéria
f) Pracnost v MD, cena návrhu řešení a cena jeho realizace
g) Doba platnosti nabídky

4.2.4 Objednatel předloženou nabídku posoudí a v případě souhlasu potvrdí objednávku vystavením objednávky na dílo Poskytovateli dle nabídky a následně zápisem oprávněnou osobou v Helpdesku.

4.2.5 Nabídka Poskytovatele musí být zpracována v souladu s Best Practice daného oboru, včetně využití dostupných kvalitních a efektivních postupů, přičemž rozsah potřebných prací nesmí být neodůvodněně nadhodnocen.

4.2.6 Poskytovatel zdokumentuje postup řešení a zápisem v Helpdesku provede oznámení o ukončení řešení a vyzve Objednatele zápisem v Helpdesku k akceptaci řešení.

4.2.7 V případě úspěšné akceptace oprávněná osoba Objednatele potvrdí akceptaci řešení formou zápisu v Helpdesku.

4.2.8 Výsledky plnění Služeb rozvoje jsou po jejich akceptaci Objednatelem předmětem Služeb podpory.

4.3 Parametry zpracování Požadavků

4.3.1 Parametry zpracování Požadavků jsou definovány takto

KROK	DOBA REAKCE

Převzetí Požadavku (Response time)	3 pracovní dny
Písemné sdělení navrhovaného termínu, ceny a návrhu řešení (u Požadavků na úpravu v rozsahu větším než 10 člověkohodin)	15 pracovních dnů od převzetí Požadavku
Odsouhlasení termínu a návrhu řešení zástupcem Objednatele (vč. zapracování připomínek Objednatele, budou-li)	15 pracovních dnů od předání návrhu
Předání otestované realizace Požadavku.	dle odsouhlaseného termínu

4.3.2 Vyhodnocení měřených reakčních dob zasílá Poskytovatel Objednateli měsíčně. Toto vyhodnocení slouží jako podklad pro vzájemnou komunikaci Objednatele s Poskytovatelem za účelem udržení požadované úrovně SLA.