SMLOUVA NA DODÁVKU A IMPLEMENTACI BEZPEČNOSTNÍCH NÁSTROJŮ I

uzavřená podle § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen „**občanský zákoník**")

Článek I.

Smluvní strany

1. Aricoma Systems a.s.

se sídlem Hornopolní 3322/34, 702 00 Ostrava – Moravská Ostrava
zastoupená: [redacted] ředitel regionálního centra
bankovní spojení: Česká spořitelna a.s.
číslo účtu: 6563752/0800
IČO: 04308697
DIČ: CZ04308697
(společnost je zapsaná v obchodním rejstříku vedeném Krajským soudem v Ostravě, sp. zn. B 11012)
(dále jen „**prodávající**")

2. Městská nemocnice Ostrava, příspěvková organizace

se sídlem Nemocniční 898/20a, 728 80 Ostrava - Moravská Ostrava
zastoupená: [redacted] ředitelem
oprávněna k zastupování po dobu nepřítomnosti ředitele:
[redacted]
na základě Pověření zastupováním statutárního orgánu
bankovní spojení: 374027793/0300
číslo účtu: Československá obchodní banka, a. s.
IČO: 00635162
DIČ: CZ00635162
(zřízená usnesením Zastupitelstva statutárního města Ostravy, zřizovací listina ve znění usnesení č. 2509/1014/32 ze dne 21. 5. 2014, příspěvková organizace nezapsaná ve obchodním rejstříku; registrace poskytovatele zdravotních služeb rozhodnutím odboru zdravotnictví Krajského úřadu Moravskoslezského kraje, č.j. MSK 80195/2025 z 26. 6. 2025 ve znění následných rozhodnutí o registraci)
ID datové schránky: r45ztzu

(dále jen „**kupující**", nebo také „**MNO**")

Článek II.

Účel smlouvy a úvodní ustanovení

1. Účelem této smlouvy je dodávka, implementace a realizace postimplementačních činností pro účely zabezpečení informačních a komunikačních systémů Městské nemocnice Ostrava podle příslušných právních předpisů v oblasti kybernetické bezpečnosti. Tato smlouva je uzavřena v návaznosti na výsledek zadávacího řízení na veřejnou zakázku s názvem *„Zajištění standardů kybernetické bezpečnosti v Městské nemocnici Ostrava*", která byla zadávána v otevřeném zadávacím řízení dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**"). Jednotlivá ujednání této smlouvy budou vykládána v souladu se zadávacími podmínkami veřejné zakázky uvedenými v zadávací dokumentaci včetně jejich příloh a v souladu s nabídkou prodávajícího podanou na veřejnou zakázku.
2. Prodávající podpisem této smlouvy garantuje kupujícímu splnění všech podmínek obsažených v zadávací dokumentaci pro plnění veřejné zakázky uvedené v odst. 1 tohoto článku.
3. Prodávající dále prohlašuje, že se detailně seznámil s rozsahem a povahou předmětu plnění této smlouvy, že jsou mu známy veškeré relevantní technické, kvalitativní a jiné podmínky nezbytné pro realizaci předmětu plnění dle této smlouvy, a že disponuje takovými kapacitami a odbornými znalostmi, které jsou nezbytné pro realizaci předmětu plnění této smlouvy za dohodnuté maximální smluvní ceny, a to rovněž ve vazbě na jím prokázanou kvalifikaci pro plnění veřejné zakázky.
4. Prodávající dále prohlašuje, že jím poskytované plnění odpovídá všem požadavkům vyplývajícím z platných právních předpisů, které se na plnění vztahují.
5. Prodávající bere na vědomí, že předmět plnění bude spolufinancován z evropských finančních zdrojů prostřednictvím Národního plánu obnovy (dále jen „**NPO**") v rámci projektu „Zajištění standardů kybernetické bezpečnosti v Městské nemocnici Ostrava", registrační číslo CZ.31.2.0/0.0/0.0/23_095/0008420.

Článek III.

Předmět plnění

1. Předmětem plnění této smlouvy je dodávka a implementace níže uvedeného zboží nebo poskytnutí souvisejících služeb včetně poskytování postimplementačních činností a požadovaných záruk v rozsahu a za podmínek dle příloh této smlouvy. Součástí plnění je dále nezbytná dokumentace, přístupová oprávnění a ostatní nezbytné náležitosti pro zajištění provozní podpory a údržby, kterou může případně poskytovat třetí strana na základě samostatné smlouvy.

   Pro vyloučení pochybnosti kupující uvádí, že následná podpora a údržba, které nejsou hrazeny s využitím NPO, nejsou předmětem této smlouvy. Kupující předpokládá, že tyto činnosti budou předmětem samostatné smlouvy na základě samostatného zadávacího řízení. Prodávající dle této smlouvy je povinen poskytnout kupujícímu nezbytnou

součinnost pro přípravu podkladů a vstupních parametrů pro účely realizace zadávacího řízení, a dále nezbytnou součinnost pro řádné plnění následné smlouvy na zajištění podpory a údržby; blíže viz příloha č. 3 této smlouvy (podklady pro zajištění podpory a údržby), kterou připravil kupující. Náklady na tuto součinnost prodávajícího jsou zahrnuty v ceně plnění dle této smlouvy.

2. Pro účely této smlouvy se zbožím rozumí technologie, řešení, služby, platformy a související SW, které představují bezpečnostní nástroje pro následující oblasti:
    - ochrana integrity komunikačních sítí (firewally, nástroj/platforma pro správu a vyhodnocování logů firewallů, EDR);
    - sběr a vyhodnocení kybernetických bezpečnostních událostí;
    - aplikační bezpečnost;
    - zajišťování úrovně dostupnosti informací (zálohovací software, zálohovací servery, pásková knihovna, diskové pole);
    - zaznamenávání činnosti IS, KS, uživatelů, administrátorů,

    a to vše v rozsahu a za podmínek dle přílohy č. 2 této smlouvy (technická specifikace) a v souladu s nabídkou prodávajícího podanou v zadávacím řízení na veřejnou zakázku.

    Pro účely této smlouvy se postimplementační činností rozumí ty implementační činnosti prodávajícího, které s ohledem na významný rozsah dodávky a služeb dle této smlouvy a paralelně realizované jiné související dodávky u kupujícího na základě samostatných smluv, mohou být v dílčích aspektech vyžadovány jako doplňkové práce po dokončení implementace z důvodů uvedených v příloze č. 2 této smlouvy, z důvodu zdržení třetích stran, potřeby koordinace s třetími stranami nebo z důvodu trvání technologických lhůt mimo kontrolu kupujícího i prodávajícího. Postimplementační činnosti zahrnují rovněž součinnost při auditu, který je povinný dle podmínek NPO, přičemž v rámci součinnosti bude prodávající povinen napravit případné nedostatky zjištěné v rámci auditu, který bude provádět třetí osoba (kupující předpokládá dokončení auditu do jednoho měsíce od převzetí implementovaného zboží).

3. Nedílnou součástí této smlouvy jsou přílohy, které detailně specifikují požadované plnění jednotlivých položek předmětu dodávky včetně požadovaných technických parametrů, licencí (vč. jejich rozsahu), doprovodných služeb a záruky o stanovených parametrech po dobu minimálně 5 let.

4. Dodávané zboží musí být nové, nepoužívané, nerepasované, výhradně od autorizovaného prodejního kanálu výrobce, přičemž musí být podporováno výrobcem v rámci jeho programu podpory a servisu. Zboží musí být dále určeno pro evropský trh a koncového odběratele MNO, což bude možné ověřit u zastoupení výrobce zboží v ČR.

5. Součástí předmětu plnění je implementace kompletní dodávky zboží u kupujícího v rozsahu dle přílohy č. 2 (technická specifikace), dodávka (poskytnutí) všech potřebných licencí pro provozování celého řešení na dobu minimálně 5 let od akceptace zboží, vč. poskytování nových verzí SW části dodávaného řešení a firmware dodávaného HW dle přílohy č. 1 (ceník).

6. Součástí předmětu plnění je rovněž poskytování záruky na celé řešení dle specifikace v článku X a přílohách této smlouvy.
7. Součástí předmětu je dále plnění povinností v oblasti kybernetické bezpečnosti dle článku VIII této smlouvy a příloh č. 4 a č. 5 této smlouvy.
8. Prodávající se zavazuje dodat kupujícímu zboží na základě této smlouvy do místa dodání, kterým je pracoviště Odboru informačních a komunikačních technologií v místě plnění (v sídle kupujícího), a implementovat celé řešení v rámci areálu kupujícího na místě určeném kupujícím.
9. Kupující se zavazuje zboží od prodávajícího převzít a zaplatit za něj dohodnutou kupní cenu.
10. Pokud pro správné a úplné fungování zboží či jeho jednotlivých položek je nezbytný operační systém či jiný software (dále též „**software**"), je součástí závazku prodávajícího též dodání takového software, v odpovídajícím počtu kusů k daným položkám zboží, včetně všech dokladů a návodů v českém jazyce, které se k software vztahují. Prodávající poskytuje kupujícímu k software licenci. Licencí se rozumí oprávnění kupujícího k výkonu práva duševního vlastnictví k software a užití software pro potřeby kupujícího a příslušných uživatelů. Licenci k software prodávající uděluje kupujícímu ve smyslu § 2358 a násl. občanského zákoníku. Kupující je oprávněn na základě udělené licence software užít:
    i. v územně neomezeném rozsahu,
    ii. v rozsahu odpovídajícímu počtu kusů položek zboží, k nimž je software dodáván a je pro fungování těchto položek zboží nezbytný a
    iii. po dobu trvání majetkových práv autora software.

    Je-li součástí dodávky tzv. proprietární SW, u kterého prodávající sám nemůže licenci poskytnout, dodá (zajistí nabytí) prodávající licenci kupujícímu ve výše uvedeném rozsahu. Odměna za poskytnutí licence je součástí kupní ceny uvedené v čl. IV této smlouvy.
11. Pokud to výrobce licence umožňuje, dodaná licence musí být trvalá a funkční i po ukončení období záruky. Pokud je licence předplacená jako služba, musí být licence zajištěna na celé období 5 let od akceptace naimplementovaného zboží.
12. Pokud to výrobce hardware umožňuje, musí být dodaná licence trvalá, která umožňuje provozování funkcionalit na neomezenou dobu. V případě, že dodávka takové licence není možná, bude dodána licence na období nejméně 5 let od akceptace zboží.
13. Pakliže po dobu trvání této smlouvy (po dobu dodávky a implementace zboží nebo po dobu trvání záruky) výrobce licence či hardware přistoupí ke změně své licenční politiky a přestane nabízet trvalou licenci (tj. prodávající objektivně nebude schopen trvalou licenci nadále zajistit ve smyslu odst. 11 a 12 tohoto článku), je prodávající oprávněn změnit nabízený typ licence (zejm. na subskripce), přičemž bude povinen zajistit licence alespoň na dobu 5 let od akceptace zboží, a to při zachování kupní ceny dle čl. IV této smlouvy.

Článek IV.

Kupní cena

1. Celková kupní cena zboží včetně licencí, implementačních prací a postimplementačních činností vč. záruky činí: **53 480 700 Kč bez DPH**.

   Rozpad ceny za jednotlivé části plnění je uveden v příloze č. 1 této smlouvy. V rámci implementačních prací jsou zahrnuty veškeré činnosti popsané v příloze č. 2 této smlouvy (technická specifikace).

2. Kupní cena obsahuje veškeré náklady prodávajícího nezbytné pro řádné a úplné poskytování předmětu plnění dle této smlouvy jako například dopravné, balné, pojištění, celní a daňové poplatky, poplatky za elektroodpad, autorské poplatky a další náklady prodávajícího, včetně nákladů na zajištění plnění záruky a postimplementačních činností. Kupní cena zahrnuje také náklady na poskytování součinnosti třetím stranám při plnění souvisejících smluv, kterými se rozumí smlouva na dodávku a implementaci bezpečnostních nástrojů II a smlouva na zajištění podpory a údržby zboží dle této smlouvy.[1]

3. Veškeré ceny uvedené v příloze č. 1 této 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 prodávající 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. Prodávající odpovídá za to, že sazba daně z přidané hodnoty je stanovena v souladu s platnými právními předpisy.

Článek V.

Doba a místo plnění

1. Prodávající se zavazuje provést dodávku zboží a implementaci na základě této smlouvy nejpozději **do 30. 4. 2026**, a to v plném rozsahu dle technické specifikace, přičemž postimplementační činnosti budou poskytovány dle požadavků kupujícího i v pozdějším termínu, který mj. závisí na plnění třetích stran dle souvisejících smluv a na provádění a výsledku nezávislého auditu. Postimplementační činnosti budou čerpány na základě požadavků kupujícího do vyčerpání maximálního objemu 100 MD, přičemž kupující se zavazuje tento objem služeb vyčerpat; součástí požadavku na čerpání postimplementační činnosti může být rovněž požadavek na zpracování harmonogramu poskytování těchto služeb v souladu s odst. 8 tohoto článku smlouvy.

[1] Smlouva na dodávku a implementaci bezpečnostních nástrojů II vzejde ze zadávacího řízení na veřejnou zakázku „Kybernetická bezpečnost v Městské nemocnici Ostrava“. Smlouva na zajištění podpory a údržby zboží vzejde ze samostatného zadávacího řízení, které bude připravováno po uzavření této smlouvy. Kupující se zavazuje prodávajícího informovat o uzavření těchto souvisejících smluv.

2. Prodávající se zavazuje poskytovat záruku na základě této smlouvy po dobu 5 let od akceptace implementovaného zboží dle předchozího odstavce. Akceptací se přitom rozumí také akceptace s výhradami.
3. Místem plnění je sídlo kupujícího dle této smlouvy. Plnění, jehož povaha to umožňuje, je možné realizovat rovněž vzdáleným přístupem při dodržení bezpečnostních a provozních pravidel kupujícího.
4. Prodávající se zavazuje předat předmět plnění kupujícímu kompletní a bez zjevných vad a včetně veškerého příslušenství (zejm. návody k použití a údržbě v českém jazyce, záruční listy apod.).
5. Prodávající nejpozději **do 10 dnů** od nabytí účinnosti této smlouvy předloží kupujícímu harmonogram plnění, přičemž:
    a. harmonogram bude zachycovat základní milníky dodávek a implementace bez postimplementačních činností;
    b. při tvorbě harmonogramu plnění musí být zachována časová proporcionalita mezi délkou plnění a délkou akceptace[2] a také rozložení doby jednotlivých dílčích plnění musí být úměrné jejich náročnosti, navrhne-li prodávající postupné předávání po dílčích plněních (dodávka, implementace, školení, dokumentace).
6. V rámci akceptace zboží provede kupující kontrolu zejm.:
    a) dodaného druhu a množství zboží vč. licencí,
    b) zjevných jakostních vlastností zboží,
    c) funkčních parametrů (výsledků akceptačního testů) a výsledků implementace,
    d) dokladů dodaných se zbožím,
    e) kvality poskytnutých doprovodných služeb.
7. O výsledku akceptace (akceptačního řízení) bude vyhotoven akceptační protokol podepsaný oprávněnými zástupci obou smluvních stran, přičemž výsledkem akceptačního řízení může být: (i) akceptováno, (ii) akceptováno s výhradami nebo (iii) neakceptováno. V případě drobných vad a nedodělků může kupující zboží akceptovat s výhradami s tím, že v akceptačním protokolu stanoví lhůtu k odstranění drobných vad a nedodělků (nebude-li dohodnuta lhůta kratší, musí být veškeré vady a nedodělky odstraněny do 100 pracovních dnů). V případě zjištění kritických vad zboží kupující odmítne jeho převzetí, tj. výsledek neakceptováno.
8. Prodávající nejpozději do 10 dnů od vznesení požadavku na konkrétní postimplementační činnost předloží kupujícímu harmonogram této služby včetně předpokládané pracnosti v počtu MD, přičemž
    a. dodání požadované postimplementační činnosti dle předloženého harmonogramu musí kupující splnit nejpozději do 43 pracovních dnů od předložení harmonogramu, nedohodnou-li se smluvní strany jinak,

[2] Nebude-li smluvními stranami dohodnuto jinak, považuje se za přiměřenou dobu pro akceptaci (vč. akceptačních testů) období 2 až 3 pracovních dní v závislosti na rozsahu dílčí části plnění. Doba akceptace se přitom počítá do celkové doby plnění.

b. pro vznesení požadavku na postimplementační činnosti slouží Help Desk nebo Hot Line prodávajícího s reakcí přijetí 1 pracovní den od nahlášení,

c. samotné vypracování harmonogramu a odhadu pracnosti není předmětem čerpání MD ze strany prodávajícího,

d. případné prodlení prodávajícího ve věci dodání harmonogramu a/nebo odhadu pracnosti postimplementačních činností, jakožto i prodlení s poskytnutím požadovaných postimplementačních činností dle harmonogramu, jsou utvrzeny smluvní pokutou dle čl. IX odst. 2 této smlouvy,

e. na výstupy vytvořené v rámci postimplementačních činností se uplatní obdobně úprava uplatňování vad a lhůt pro jejich odstranění dle čl. VII odst. 2 této smlouvy a čl. V odst. 7 této smlouvy, a to včetně související smluvní pokuty dle čl. IX odst. 2 této smlouvy.

Článek VI.

Platební podmínky

1. Prodávající vystaví kupujícímu daňový doklad (fakturu) za poskytnuté plnění, který zašle elektronicky ve formátu PDF na e-mail: faktury.oikt@mnof.cz, a to nejpozději do 7. kalendářního dne ode dne uskutečnění zdanitelného plnění. Úhrada ceny za plnění (tj. cena za pořízení zboží, vč. licencí a implementačních prací, dále postimplementační činnosti a záruky) bude provedena jednorázově po předání a akceptaci kompletního/poslední plnění, přičemž přílohou faktury musí být akceptační protokol podepsaný kupujícím s výsledkem akceptováno, nebo akceptováno s výhradami. V případě, že prodávající navrhne postupné předávání po dílčích částech plnění, budou podkladem pro fakturaci akceptační protokoly za všechny dílčí části plnění. Je-li prodávající dle čl. V odst. 1 této smlouvy povinen dokončit realizaci do 30. 4. 2026, je zároveň povinen vystavit fakturu nejpozději do 4. 5. 2026.
2. Splatnost faktury je stanovena na 30 dní od data jejího vystavení.
3. Úhradu za dodané zboží provede kupující v české měně.
4. Kupující neposkytne prodávajícímu žádné zálohové platby.
5. Prodávající se zavazuje, že jím vystavená faktura bude obsahovat všechny náležitosti, které jsou stanoveny touto smlouvou a obecně závaznými právními předpisy, zejména zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „**zákon o DPH**"), a ust. § 435 občanského zákoníku. Na faktuře bude uvedeno také číslo této smlouvy a název a registrační číslo projektu dle čl. II odst. 5 této smlouvy.
6. V případě, že vystavená faktura obsahuje nesprávné cenové údaje, nesprávné náležitosti nebo chybí na faktuře některé z náležitostí uvedené v předchozích odstavcích, je kupující oprávněn fakturu vrátit prodávajícímu do doby její splatnosti. V takovém případě je prodávající povinen vystavit fakturu novou. Doba splatnosti opravené nebo doplněné faktury počne běžet dnem jejího doručení kupujícímu.

7. Za zaplacení kupní ceny se považuje předání neodvolatelného platebního příkazu ze strany kupujícího bance.

Článek VII.

Dodací a servisní podmínky

1. Na dodávku zboží je prodávajícím poskytována záruka za jakost za podmínek dle přílohy č. 1 a 2 této smlouvy, a to v délce 5 let ode dne protokolárního předání (akceptace) naimplementovaného řešení dle čl. V odst. 1 této smlouvy. Implementovaným řešením se rozumí kompletní zboží, tj. v případě postupného předávání dílčích částí musí záruka na veškeré zboží trvat alespoň 5 let od akceptace poslední dílčí části. Záruka začíná běžet dnem předání (akceptace) příslušné části plnění.
2. Veškeré vady budou kupujícím nahlašovány prostřednictvím Help Desk v souladu s přílohami č. 1 a 2 této smlouvy. Není-li mezi smluvními stranami sjednáno jinak, je prodávající povinen jakékoliv vady plnění či jeho části, které vzniknou v době trvání záruky, odstraňovat na své náklady, a to v souladu s podmínkami záruky dle příloh této smlouvy. Kategorii vady určuje kupující, přitom plnění dle této smlouvy může vykazovat dva typy – běžnou a kritickou vadu. Kritickou vadou se rozumí stav dodaného řešení, který je zásadní pro činnosti a navazující procesy kupujícího, kdy nelze v nich pokračovat z důvodu nemožnosti pokračovat v činnosti dodaného řešení nebo jeho části a koncový uživatel kupujícího nemá bez zásahu prodávajícího k dispozici žádné dočasné řešení problematického stavu.
3. Záruka je poskytována partnerem výrobce v českém jazyce dle specifikací v příloze č. 2 této smlouvy.
4. Záruka rovněž zahrnuje možnost stahování ovladačů, nových verzí firmware a manuálů pro všechna dodávaná zařízení přímo z webu výrobce.
5. Záruka na dodané zboží dále zahrnuje:
    a. výměnu vadného dílu nebo zařízení v místě plnění dle podmínek záruky v příloze č. 1;
    b. nárok na bezplatnou instalaci nových verzí firmware a software v případě, kdy aktuální verze firmware nebo software obsahuje vady, které mají vliv na kvalitu poskytované služby zařízením nebo v případě, kdy v instalovaném firmware nebo software byla odhalena bezpečnostní zranitelnost, a to v rozsahu dodané licence;
    c. nárok na podporu výrobce nebo distributora v případě softwarových nebo hardwarových závad, jejichž řešení nebude v kompetenci prodávajícího.
6. Prodávající prohlašuje, že jím nabízené a dodávané výrobky splňují veškeré požadavky na zdravotní nezávadnost a bezpečnost dle zák. č. 102/2001 Sb., o obecné bezpečnosti výrobků a o změně některých zákonů (zákon o obecné bezpečnosti výrobků), ve znění pozdějších předpisů, event. dalších platných zákonů a předpisů, a že byla přezkoumána jejich shoda podle zák. č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů. Prodávající si je plně vědom

své právní i věcné odpovědnosti za újmu vzniklou kupujícímu v případě, že uvedl nepravdivé údaje.

Článek VIII.

Kybernetická bezpečnost

1. Prodávající bere na vědomí, že kupující byl v souladu s §22a zákona č.181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících předpisů, ve znění pozdějších předpisů (dále jen „**ZKB**"), určen jako správce a provozovatel informačního systému základní služby a bude registrován jako poskytovatel regulované služby v režimu vyšších povinností ve smyslu zákona č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „**NZKB**"), a příslušných prováděcích předpisů. Kupující tedy je povinnou osobou dle ZKB/NZKB a bude povinen provádět pravidelnou analýzu rizik, identifikovat rizika a identifikovaná rizika řídit.
2. Plněním této smlouvy se stane prodávající významným dodavatelem kupujícího, a to v režimu dle NZKB a jeho prováděcích právních předpisů.
3. Bezpečnostní požadavky kladené na prodávajícího vyplývají z výše citovaných právních předpisů v oblasti kybernetické bezpečnosti v kontextu této smlouvy. Prodávající je povinen dodržovat a řídit se Pravidly chování dodavatelů v oblasti bezpečnosti informací. Pravidla chování dodavatelů v oblasti bezpečnosti jsou v aktuální verzi k dispozici na oficiálních webových stránkách zadavatele www.mnof.cz/pravidla-dodavatele.
4. Plnění předmětu smlouvy, a to ve všech jeho fázích a ve všech jeho částech, musí splňovat veškeré podmínky dle ZKB/NZKB a příslušných prováděcích právních předpisů. Prodávající se zavazuje informovat o těchto skutečnostech všechny své poddodavatele a další osoby, s jejichž pomocí či jejichž prostřednictvím bude prodávající plnit předmět této smlouvy.
5. Povinnosti a postupy v oblasti kybernetické bezpečnosti jsou uvedeny v Příloze č. 4 (Kybernetická bezpečnost) a v Příloze č. 5 (Vzdálený přístup) této smlouvy. V přílohách č. 4 a 5 je prodávající označen jako „Poskytovatel" a kupující jako „Objednatel".

Článek IX.

Sankce

1. V případě, že prodávající nepředá kompletní naimplementované zboží v termínu dle čl. V odst. 1 této smlouvy, uhradí kupujícímu smluvní pokutu ve výši 25.000 Kč za každý započatý den prodlení.
2. V případě, že prodávající nepředá harmonogram ve lhůtě dle čl. V odst. 5 a/nebo nepředá harmonogram vč. odhadu pracnosti, či samotné požadované postimplementační činnosti dle čl. V odst. 8 této smlouvy a/nebo neodstraní vady či nedodělky předaného zboží nebo služeb ve lhůtě dle čl. V odst. 7 této smlouvy, uhradí kupujícímu smluvní pokutu ve výši 3.000 Kč za každý započatý den prodlení.

3. V případě, že prodávající nedodrží lhůtu **pro zahájení prací ON-LINE odborníka od nahlášení vady** nebo **pro zahájení prací ON SITE odborníka od nahlášení vady** dle podmínek záruky v příloze č. 1 této smlouvy, uhradí kupujícímu smluvní pokutu ve výši 1.000 Kč za každý i započatý den prodlení.
4. V případě, že prodávající nedodrží lhůtu **pro odstranění kritické vady** dle podmínek záruky v příloze č. 1 této smlouvy, uhradí kupujícímu smluvní pokutu ve výši 3.000 Kč za každý i započaty den prodlení.
5. V případě, že prodávající nezajistí **Dostupnost Help Desku / Hot Line prodávajícího pro hlášení vady (24 x 7) s reakcí přijetí (2 hod. od nahlášení)** dle podmínek záruky v příloze č. 1 této smlouvy, uhradí kupujícímu smluvní pokutu ve výši 1.000 Kč za každou i započatou hodinu nefunkčnosti **Help Desku / Hot Line.**
6. V případě, že prodávající nepotvrdí přijetí hlášení v režimu plnění záruky dle přílohy č. 1 této smlouvy (lhůty běží ve sjednaném režimu, tj. např. u režimu 8x5 jen v pracovní době), uhradí kupujícímu smluvní pokutu ve výši 500 Kč za každou i započatou hodinu.
7. V případě, že prodávající poruší svou povinnost poskytovat součinnost při auditu dle čl. III odst. 2 této smlouvy nebo poruší jakoukoliv povinnost dle čl. XI odst. 4 písm. f) a/nebo h) a/nebo i) této smlouvy, uhradí kupujícímu smluvní pokutu ve výši 25.000 Kč, a to za každé jednotlivé porušení.
8. Sankce, sjednané touto smlouvou, hradí povinná strana nezávisle na tom, zda a v jaké výši vznikne druhé straně v této souvislosti újma, kterou lze vymáhat samostatně v plné výši vedle smluvní pokuty.
9. Neodstraní-li prodávající vady předmětu plnění v souladu s touto smlouvou řádně a včas, a to ani v dodatečné přiměřené lhůtě poskytnuté mu k tomu kupujícím, je kupující oprávněn nechat odstranit vady předmětu třetí osobou. Prodávající se pak zavazuje nahradit kupujícímu veškeré účelné vynaložené a prokázané náklady na odstranění vad předmětu plnění třetí osobou. Tímto není dotčen nárok kupujícího na náhradu škody, jakož ani nárok na zaplacení smluvní pokuty dle čl. IX teto smlouvy.
10. V případě prodlení kupujícího s úhradou faktury za dodané zboží uhradí kupující prodávajícímu úrok z prodlení v zákonné výši.
11. V případě, že prodávající nezajistí dostupnost Help Desku / Hot Line prodávajícího pro hlášení požadavku na postimplementační činnosti v režimu 5 x 8 s reakcí přijetí 1 pracovní den od nahlášení dle čl. V odst. 8 této smlouvy, uhradí kupujícímu smluvní pokutu ve výši 1.000 Kč za každý i započatý den Help Desku / Hot Line**.**

Článek X.

Doba trvání smlouvy

1. Smlouva se uzavírá na dobu určitou, a to do konce trvání záruky, tj. na dobu 5 let od předání a akceptace implementovaného zboží (kompletního zboží, nebo poslední dílčí části zboží, bude-li plněno po částech). Smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem uveřejnění v registru smluv. Smlouvu lze ukončit dohodou smluvních stran.

2. Kupující je oprávněn odstoupit od smlouvy v případě, že prodávající je v prodlení s plněním o více než 30 dnů.
3. Prodávající je oprávněn odstoupit od smlouvy v případě, že kupující je v prodlení se zaplacením kupní ceny déle než 30 dnů po splatnosti.
4. Účinky odstoupení nastávají dnem doručení písemného oznámení o odstoupení.

Článek XI.

Ostatní ujednání

1. Kupující nabývá vlastnického práva ke zboží (hmotným částem plnění) dnem předání v místě plnění dle článku V. této smlouvy. Tímto dnem přechází na kupujícího nebezpečí škody na věcném plnění.
2. Prodávající prohlašuje, že věcné plnění smlouvy nemá právní vady a není zatíženo právy třetích osob.
3. Prodávající odpovídá za to, že v databázi výrobce musí být kupující uveden jako první uživatel zboží, a to originálního nového zboží.
4. Prodávající je při plnění této smlouvy povinen:
   a. provádět plnění řádně a včas za použití postupů odpovídajících platným právním předpisům, technickým normám ČR a umožňovat užívání, k němuž bylo určeno;
   b. řídit se při provádění plnění pokyny kupujícího a poskytnout mu požadované informace;
   c. umožnit kupujícímu kontrolu provádění plnění, a to kdykoliv po dobu jeho realizace;
   d. odstranit zjištěné vady a nedodělky plnění na své náklady;
   e. dbát při realizaci plnění dle této smlouvy na ochranu životního prostředí a dodržovat platné technické, bezpečnostní, zdravotní, hygienické a jiné předpisy, včetně předpisů týkajících se ochrany životního prostředí; prodávající je dále povinen preferovat použití obalů z recyklovaných materiálů, je-li to možné;
   f. alokovat na realizaci této smlouvy pracovní kapacitu osob realizačního týmu uvedeného v nabídce prodávajícího podané ve veřejné zakázce (viz příloha č. 6 této smlouvy) a k plnění této smlouvy využít osob, kterými byla prokazována kvalifikace v zadávacím řízení na veřejnou zakázku. Jakákoliv dodatečná změna osoby realizačního týmu musí být předem písemně schválena kupujícím. Prodávající se v takovém případě zavazuje nahradit osobu realizačního týmu takovou osobou, která disponuje alespoň požadovanými minimálními znalostmi a odbornou kvalifikací dle požadavků kupujícího uvedených v zadávací dokumentaci veřejné zakázky. Prodávající i osoby podílející se na realizaci této smlouvy musí po celou dobu trvání této smlouvy splňovat kvalifikační kritéria stanovená v zadávací dokumentaci veřejné zakázky. Při porušení této podmínky má kupující právo odstoupit od smlouvy;
   g. prodávající před uzavřením této smlouvy poskytl seznam poddodavatelů (viz příloha č. 5 této smlouvy) a je povinen tyto smluvně zavázat tak, aby plnili veškeré povinnosti prodávajícího uvedené v této smlouvě, ve stejném rozsahu jako je zavázán sám prodávající.

h. písemně informovat kupujícího o všech případných dalších (nových) poddodavatelích a o jejich změně, a to nejpozději do 5 pracovních dnů ode dne, kdy Prodávající vstoupil s poddodavatelem ve smluvní vztah či ode dne, kdy nastala změna. Prodávající je oprávněn změnit poddodavatele, prostřednictvím kterého prokázal část splnění kvalifikace v rámci zadávacího řízení, na jehož základě byla uzavřena tato smlouva, jen z vážných objektivních důvodů a s předchozím písemným souhlasem kupujícího, přičemž nový poddodavatel musí disponovat kvalifikací v minimálně stejném či větším rozsahu, v jakém původní poddodavatel prokázal za prodávajícího. Prodávající je povinen k žádosti o udělení souhlasu s případnou změnou poddodavatele přiložit nezbytné doklady;

i. po celou dobu plnění svého závazku z této smlouvy mít na vlastní náklady sjednáno pojištění odpovědnosti za škodu způsobenou třetím osobám vyplývající z dodávaného předmětu plnění s limitem **min. 10 mil. Kč**. Pojištění musí obsahovat krytí škod způsobené na majetku, zdraví třetích osob včetně krytí odpovědnosti za finanční škody. Prodávající je povinen mít pojištění dle tohoto odstavce po celou dobu plnění této smlouvy, přičemž lze v tomto období provést změnu pojišťovatele, či jinak pojištění přepojistit;

j. předat kupujícímu kdykoliv na vyžádání kopii pojistné smlouvy či smluv na požadované pojištění dle předchozího písmene tohoto odstavce smlouvy (včetně všech dodatků) nebo certifikát příslušné pojišťovny ne starší jednoho měsíce prokazující existenci pojištění dle předchozího písmene tohoto odstavce (dobu trvání pojištění, jeho rozsah, pojištěná rizika, pojistné částky, roční limity a sublimity plnění a výši spoluúčasti), a to nejpozději do 10 dnů od obdržení příslušné žádosti.

5. Všechny vztahy touto smlouvou neupravené se řídí českým právním řádem, zejména ustanoveními občanského zákoníku. Prodávající se nemůže dovolávat svých obecných dodacích, servisních či jiných obchodních podmínek nebo obdobných podmínek poddodavatelů, které by byly s touto smlouvou v rozporu.

6. Pozbude-li některé z ustanovení této smlouvy platnosti, zůstávají ostatní tímto nedotčena. Neúčinné ustanovení se nahradí takovým, které odpovídá nebo bude co nejblíže původnímu záměru ve věcném i ekonomickém smyslu.

7. Obě strany se dohodly, že veškeré případné spory, vzniklé v souvislosti s touto smlouvou, budou řešeny jednáním na úrovni statutárních zástupců smluvních stran. Nedojde-li k dohodě, k projednávání sporů mezi smluvními stranami jsou místně příslušné soudy dle sídla kupujícího.

8. Pohledávky vyplývající z této smlouvy může prodávající převést na jinou osobu jen s předchozím písemným souhlasem kupujícího.

9. Smluvní strany se zavazují, že zachovají mlčenlivost o veškerých informacích, které o sobě navzájem získaly v průběhu plnění předmětu této smlouvy a které nejsou veřejně přístupné nebo je pokládají za důvěrné. Za důvěrné a utajované informace ve smyslu tohoto článku se považují veškeré informace, které jsou jako důvěrné označeny nebo jsou takového charakteru, že mohou v případě zveřejnění přivodit kterékoliv smluvní straně újmu, bez ohledu na to, zda mají povahu osobních, obchodních či jiných

informací. Toto ujednání zaniká v případě, že se tyto informace stanou všeobecně známými.

10. Pokud je součástí předmětu smlouvy dodávka softwarových produktů, pak se kupujícímu vyhrazuje časově neomezené, nikoliv však výhradní a přenosné, právo užívat tyto softwarové produkty na výrobku, se kterým byly dodány, v nezměněné formě a pro účely uvedené v popisu produktu. Softwarové produkty a k tomu patřící dokumentace nesmí být postoupeny třetím osobám. Kupující nesmí programy kopírovat, zpětně vyvíjet nebo zpětně překládat ani vyjímat jednotlivé části programu.
11. Úplata za užívání softwaru poskytnutého s hardwarovou částí předmětu plnění je obsažena v kupní ceně předmětu plnění.
12. Smluvní strany souhlasí se zveřejněním všech náležitostí tohoto smluvního vztahu.
13. Smluvní strany shodně a svobodně prohlašují, že se bez výhrad shodly na tom, že kupující zveřejní tuto smlouvu a související přílohy v Registru smluv, ve lhůtě a za podmínek stanovených dle 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.

Sankce vůči Rusku a Bělorusku

14. Prodávající odpovídá za to, že platby poskytované kupujícím dle této smlouvy nebudou přímo nebo nepřímo ani jen zčásti zpřístupněny 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).
15. Bude-li kterékoliv z nařízení v budoucnu doplněno či nahrazeno jinou legislativou obdobného významu, uvedená povinnost se uplatní obdobně.
16. Prodávající odpovídá za to, že po dobu trvání smlouvy nejsou naplněny podmínky uvedené v nařízení Rady (EU) 2022/576 ze dne 8. dubna 2022, kterým se mění nařízení (EU) č. 833/2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, tedy zejména, že prodávající není:
    a. ruským státním příslušníkem, fyzickou nebo právnickou osobou se sídlem v Rusku,
    b. právnickou osobou, která je z více než 50 % přímo či nepřímo vlastněna některou z osob dle předešlé odrážky, nebo
    c. fyzickou nebo právnickou osobou, která jedná jménem nebo na pokyn některé z osob uvedených v předešlých odrážkách.
17. Prodávající odpovídá za to, že po dobu trvání smlouvy žádná z výše uvedených podmínek není naplněna ani u jeho poddodavatele (nebo jiné osoby prokazující za Prodávajícího kvalifikaci), který se bude na plnění této smlouvy podílet z více jak 10 % hodnoty plnění.

18. Prodávající je povinen kupujícího bezodkladně informovat o jakýchkoliv skutečnostech, které mohou mít vliv na odpovědnost prodávajícího dle odst. 14 nebo 16 tohoto článku smlouvy. Prodávající je současně povinen kdykoliv poskytnout kupujícímu bezodkladnou součinnost pro případné ověření pravdivosti těchto informací.
19. Dojde-li k porušení pravidel dle odst. 14 nebo 16 tohoto článku smlouvy, je kupující oprávněn odstoupit od této smlouvy; odstoupení se však nedotýká povinností prodávajícího 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.
20. Dojde-li k porušení pravidel dle odst. 14 nebo 16 tohoto článku smlouvy, je prodávající povinen zaplatit kupujícímu smluvní pokutu ve výši 200.000 Kč, a to za každý jednotlivý případ porušení. Smluvní pokuty se nezapočítávají na náhradu případně vzniklé škody, kterou lze vymáhat samostatně vedle smluvní pokuty, a to v plné výši.

Dotační podmínky

21. Prodávající je dále povinen postupovat při plnění smlouvy tak, aby nebylo ohroženo financování z dotace dle čl. II odst. 5 této smlouvy; zejména je prodávající povinen:
    a. Vytvořit zaměstnancům nebo zmocněncům poskytovatele dotace, tj. Ministerstvu vnitra, Ministerstvu pro místní rozvoj, Ministerstvu financí, orgánům finanční správy, auditnímu orgánu či pověřenému auditnímu subjektu, Evropské komisi, Evropskému účetnímu dvoru, Nejvyššímu kontrolnímu úřadu a dalším oprávněným orgánům státní správy, podmínky k provedení kontroly vztahující se k realizaci projektu, poskytnout minimálně do konce roku 2036 veškeré doklady vážící se k realizaci projektu, umožnit průběžné ověřování souladu údajů o realizaci projektu uváděných ve zprávách o realizaci projektu se skutečným stavem v místě jeho realizace a poskytnout součinnost všem osobám oprávněným k provádění kontroly, umožnit vstup na pozemky dotčené projektem a jeho realizací.
    b. Uchovávat odpovídajícím způsobem veškerou dokumentaci související s realizací projektu včetně účetních dokladů minimálně do 31. 12. 2036. Pokud je v českých právních předpisech stanovena lhůta delší, musí ji zhotovitel použít.

Článek XII.

Závěrečná ujednání

1. Tato smlouva je vyhotovena v jednom vyhotovení v elektronické podobě, přičemž každá ze smluvních stran obdrží elektronicky podepsaný originál této smlouvy.
2. Jakékoli změny a dodatky této smlouvy musí být učiněny písemně a schváleny podpisem obou smluvních stran. Tyto dodatky se stanou nedílnou součástí této smlouvy.
3. Smluvní strany se podpisem smlouvy dohodly, že vylučují aplikaci ustanovení § 557 občanského zákoníku.

4. Pro vyloučení pochybností prodávající výslovně potvrzuje, že je podnikatelem, uzavírá smlouvu při svém podnikání, a na smlouvu se tudíž neuplatní ustanovení § 1793 občanského zákoníku.
5. Prodávající na sebe v souladu s ustanovením § 1765 odst. 2 občanského zákoníku přebírá nebezpečí změny okolností. Tímto však nejsou nikterak dotčena práva smluvních stran upravená v této smlouvě.
6. Obě smluvní strany prohlašují, že tato smlouva vyjadřuje jejich vůli a nepodepisují ji v tísni za nápadně nevýhodných podmínek. Smluvní strany souhlasí bez výhrad s jejím obsahem a na důkaz toho připojují své podpisy.
7. Nedílnou součástí této smlouvy jsou následující přílohy:
   1) Ceník vč. podmínek záruky
   2) Technická specifikace
   3) Podklady pro zajištění podpory a údržby
   4) Kybernetická bezpečnost
   5) Vzdálený přístup
   6) Seznam poddodavatelů
   7) Realizační tým

V Ostravě dne dle data elektronického podpisu	V Ostravě dne dle data elektronického podpisu
Prodávající: Aricoma Systems a.s.	Kupující: Městská nemocnice Ostrava,

[redacted]

Legenda:
24x7 = nepřetržitě; 12x7 = nepřetržitě mimo noční dobu od 21:00 hod (v ČR);
8x5 = v běžné pracovní době;
NBD / 2BD / 3BD = další / druhý / třetí pracovní den (v ČR);
MD = pracovní den (8 pracovních hodin) jednoho lidského zdroje
P1, P3 - přílsušné přílohy smlouvy č. 1 a č. 3

Záruka v trvání 60 měsíců od akceptace plnení smlouvy a související podmínky Záruky s možností hlášení vad 24x7 s potvrzením přijetí hlášení do 2 hodin od nahlášení v režimu plnění Záruky

Vyplní dodavatel (žlutá pole níže kromě tohoto)

Technická specifikace - odstavec	Upřesnění položky	Počet [ks]	Licence upřesnění	Režim plnění Záruky (doba pro potvrzení běží jen v tomto režimu)	Upřesnění obsahu Záruky	Lhůta pro zahájení prací odborníka ON LINE / ON SITE od nahlášení	Lhůta pro odstra-nění kritické vady od nahlá-šení	Doprovodné služby implementace: Minimální (P1+P3) požadované kapacity [MD]	Nabídka kapacity [MD]	Nabídková cena jednoho MD bez DPH [Kč]	Nabídková cena jednoho MD s DPH [Kč]	Dodávky zboží: konkrétní zařízení, řešení nebo typ (zkráceně)	počet (u-veďte, je-li relevantní) [ks]	jednotková cena bez DPH [Kč]	jednotková cena s DPH [Kč]	CENA CELKEM: Souhrnná celková cena bez DPH [Kč]	Souhrnná celková cena s DPH [Kč]
Přípravné práce, řízení projektu	**služby**							20	20	18 585	22 488					371 700	449 757
1.1.1. Firewall pro interní segmenty	**HW + systémový SW + služby**	2		8x5	vč. signatur	NBD / 2BD	3BD	32	36	18 585	22 488	[redacted]	2	4 344 249	5 256 541	9 357 558	11 322 645
1.1.2. Pobočkový firewall	**HW + systémový SW + služby**	3		8x5	vč. signatur	NBD / 2BD	3BD	21	27		22 488		3	1 128 908	1 365 979	3 888 519	4 705 108
1.1.3 Nástroj/platforma pro správu a vyhodnocování logů firewallů	**systémový SW + služby**	3		8x5	vč. signatur	NBD / -	3BD	21	25		22 488		1	671 645	812 690	1 136 270	1 374 887
1.1.4 EDR systém pro ochranu operačních systémů	**systémový SW + testovací prostředí OS + služby**	1	EDR pro 1300 OS testovací prosředí pro Apple, Linux a Windows	8x5	vč. signatur, SW	NBD / -	3BD	57	57	18 585	22 488		1	8 138 849	9 848 007	9 198 194	11 129 815
1.2 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí	**SW + služby**	1	8000 EPS nebo 20 aktivních uživatelů nebo 150 GB/den	8x5	vč. signatur, SW	2BD / -	3BD	34	34	18 585	22 488		1	8 590 108	10 394 031	9 221 998	11 158 618
1.3 Řešení pro zajištění aplikační bezpečnosti	**SW + služby**	1	1000 aktiv/assetů	8x5	vč. signatur, SW	2BD / -	3BD	18	21	18 585	22 488		1	1 848 395	2 236 558	2 238 680	2 708 803
1.4.1 Zálohovací software	**SW + služby**	1	100 VM	8x5	SW	NBD	3BD	17	20	18 585	22 488		1	1 638 327	1 982 376	2 010 027	2 432 133
1.4.2 Zálohovací servery	**HW + systémový SW + služby**	2		24x7	SW, firmware	NBD / NBD	3BD	9	12				2	1 893 434	2 291 055	4 009 888	4 851 964
1.4.3 Pásková knihovna	**HW + systémový SW + služby**	1		24x7	SW, firmware	NBD / NBD	3BD	5	6	18 585			1	873 138	1 056 497	984 648	1 191 424
1.4.4. Diskové pole pro nestrukturovaná data v roli primárního úložiště záloh	**HW + systémový SW + služby**	1		24x7	SW, firmware	NBD / NBD	3BD	25	26				1	7 258 076	8 782 272	7 741 286	9 366 956
1.5 Nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů	**SW + služby**	1		8x5	SW	2BD / -	3BD	49	61	18 585	22 488		1	329 747	398 994	1 463 432	1 770 753
Post implementační činnosti	**služby**							100	100	18 585	22 488					1 858 500	2 248 785
												CENA CELKEM JAKO KRITÉRIUM ZAKÁZKY:				**53 480 700**	**64 711 647**

Technická specifikace

Městská nemocnice Ostrava (dále jen MNO) plánuje provést zvýšení kybernetické bezpečnosti. Cílem tohoto projektu je implementace technických opatření definovaných potřebou shody s Vyhláškou o kybernetické bezpečnosti MNO, resp. příslušnými právní předpisy v oblasti kybernetické bezpečnosti.

Tento dokument popisuje minimální technické požadavky, jejichž nesplnění vede k vyloučení účastníka ze zadávacího řízení na veřejnou zakázku. Posouzení splnění těchto požadavků bude mít tyto fáze:

i. Kontrola vyplněných dokumentů a posouzení shody s minimálními technickými požadavky.
ii. V případě nejasností o splnění minimálních technických parametrů zašle zadavatel žádost o objasnění nabídky na účastníka, a to případně i opakovaně. Zejména pak pokud nejsou poskytnuty úplné požadované informace o předmětu plnění.

Technické řešení je požadováno pro zvýšení úrovně bezpečnosti. Všechny požadavky jsou stanoveny, tak aby nabízené prvky prováděly úplnou kontrolu analyzovaného provozu. Za žádných okolností není možné, aby jakákoliv nabízená komponenta prováděla pouze dílčí inspekci obsahu. Jakýkoliv packet, rámec či soubor musí být v každém kroku průchodu bezpečnostní platformou prohlédnut.

Selektivní inspekce provozu není možná na základě žádného kritéria. Pakliže má bezpečnostní platforma možnost konfigurace množiny signatur, kterou bude provoz kontrolován, bude vždy použit takové nastavení, aby bylo dosaženo maximální úrovně kybernetické bezpečnosti. Minimální technické požadavky na výkonnost jsou stanoveny s ohledem na tuto skutečnost.

Pakliže dodávané řešení provádí selektivní inspekci (nebo inspekci s neúplným setem signatur), dodá účastník **čestné prohlášení výrobce** (potvrzeno výrobcem), že dodávané komponenty plní výkonnostní parametry s úplnou inspekcí a úplným setem signatur.

Účastník dodává řešení formou celku a nese veškeré náklady na integraci a nasazení všech požadovaných funkcí. Účastník prohlašuje, že se před podáním nabídky důkladně seznámil s požadavky dle této technické specifikace (vč. požadavků na konfigurační práce).

Pokud bude součástí jakéhokoliv řešení server, pak musí být zajištěna jeho správa. Zadavatel aktuálně využívá nástroj HPE OneView + iLo Advanced. Zadavatel požaduje licenční pokrytí případných nových serverů těmito nástroji, nebo kompletní náhradu nástroje HPE OneView + iLo Advanced pro všechny stávající servery, přičemž náklady na tuto náhradu budou promítnuty v nabídkové ceně. Případný nový nástroj musí pokrýt 30

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

ks serverů z generací HPE Proliant Gen 10, Gen 11 a Gen12. Případný nový nástroj musí podporovat nejméně funkce pokryté nástrojem HPE OneView.

Minimální technické parametry byly upraveny na základě odpovědí z předběžné tržní konzultace, které se účastnily tyto společnosti:

Aricoma Systems a.s.

DATASYS s.r.o.

V odpovědi v tabulce níže vyplní účastník souhlasné nebo nesouhlasné stanovisko ke splnění, technický popis, jak požadavek plní a odkaz na dokumentaci výrobce. Dokumentace výrobce může být v české nebo anglickém jazyce, odkaz může být pomoc funkčního URL, pomocí citace veřejně dostupného a vyhledatelného textu nebo pomocí symbolického vyznačení v dokumentu přiloženého v nabídce.

Ukázka vyplnění VZOR (nejedná se o požadavek):

ID	Minimální technický požadavek	Odpověď účastníka
0	Řešení musí obsahovat nejméně 24 GbE portů vybavených PoE	[redacted]

Akceptovatelné vyplnění, kde má zadavatel možnost si ověřit deklarované skutečnosti.

ID	Minimální technický požadavek	Odpověď účastníka
0	Řešení musí obsahovat nejméně 24 GbE portů vybavených PoE	[redacted]

Nedůsledné vyplnění, kde zadavatel neumí ověřit, zda-li je minimální technická specifikace splněna. Vyplnění odpovědi účastníka tímto způsobem výrazně komplikuje ověření splnění minimální technické specifikace. V případě vyplnění nabídky tímto způsobem je nucen zadavatel využít další prostředky (ověřování, doplňující dotazy apod.) pro zjištění, zda-li nabízený předmět plnění splňuje minimální technickou specifikaci.

Zde končí VZOR a začíná minimální technická specifikace.

Nabídka musí obsahovat:

a) **Popis řešení**
b) **BOM, seznam všech part numbers, popisů výrobce a počtu jednotlivých kusů**
c) **Datové listy výrobce formou funkčního odkazu nebo souboru**
d) **Harmonogram implementace**

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

Zadavatel v technické specifikaci **zvýraznil** požadavky na dokumenty, které mají být součástí nabídky.

V případě, že je požadováno potvrzení výrobce, je tím myšleno čestné prohlášení v českém jazyce potvrzené zástupcem výrobce vztaženo k předmětu plnění této veřejné zakázky.

Veškerý hardware dodaný zadavateli musí být nový a určený přímo pro zadavatele. Účastník dodá **čestné prohlášení výrobce**. Prohlášení bude obsahovat odkaz na toto výběrové řízení.

Součástí dodávky musí být veškeré kabely/transceivery potřebné ke zprovoznění řešení. Zadavatel pro transceivery a DAC kabely připouští použití OEM komponent. Ke každé OEM komponentě musí být dodáno 2% spare dílů (zaokrouhleno vždy celé ks nahoru). Nejméně však tolik, aby dokázaly vytvořit jeden ucelený spoj.

Pokud technická specifikace připouští alternativní řešení, pak to neznamená povolení variantní nabídky. Ale použití jiného technologického postupu a podmínek stanovených k jeho naplnění.

Pokud je požadované řešení/funkce dosaženo/a pomocí integrace, pak je účastník povinen doložit **popis integrace** v rámci nabídky. Nativní integrace mohou být doloženy pomocí dokumentu výrobce. Integrace vyžadující vývoj jsou vždy popsány účastníkem do úrovně detailního návrhu.

Definice pojmů

AAA protokol (Authentication, Authorization, and Accounting) - je soubor protokolů a služeb pro správu přístupu k IT systémům a jejich používání. Authentication (Autentizace): Ověření identity uživatele (např. pomocí hesla, certifikátu). Authorization (Autorizace): Určení, jaké služby nebo zdroje může ověřený uživatel využívat. Accounting (Účtování): Sledování a záznam využívání síťových služeb (např. pro účely správy, plánování nebo fakturace).

Comware - operační systém sítových prvků využívaných zadavatelem.

Control plane – řídící vrstva sítových technologií, která je zodpovědná za rozhodování, správu a konfiguraci.

Data plane – komunikační vrstva, která je zodpovědná za přenos uživatelských dat (paketů) ze zdroje do cíle.

Erasure coding - je metoda ochrany a ukládání dat v distribuovaných systémech (např. PACS úložiště), která zajišťuje vysokou odolnost proti ztrátě dat s nižšími nároky na úložný prostor ve srovnání s tradičním zrcadlením (replikací).

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

Gartner – nezávislá komerční společnost provádějící testy a srovnání komponent.

HPE iLO Advanced a HPE OneView– Aktuálně využívaný nástroj pro správu serverů zadavatelem.

Incident – technický problém způsobený účastníkem.

IOPS – počet vstupně výstupních operací za vteřinu.

Low-code – je přístup k vývoji softwaru, který umožňuje rychle navrhovat, vytvářet a nasazovat aplikace s minimálním množstvím ručně psaného kódu. Místo psaní tisíců řádků kódu od nuly využívá vizuální vývojové prostředí s předpřipravenými komponentami, šablonami a funkcemi typu drag-and-drop (přetáhni a pusť).

MD – člověkoden, 8 hodin práce vykonané při realizaci projektu.

Multitenantní/tenant – je prostředí ve kterém se vyskytuje více zákazníků/tenantů. Tenant představuje instanci prostředí zákazníka.

No-code - je přístup k vývoji softwaru, který umožňuje úplné vytvoření aplikací a digitálních produktů (webové stránky, mobilní aplikace, automatizace procesů) bez psaní jediného řádku kódu. Cílem je zpřístupnit vývoj softwaru netechnickým uživatelům, aby mohli rychle digitalizovat a automatizovat své obchodní procesy.

OEM - znamená z angličtiny Original Equipment Manufacturer, což se do češtiny volně překládá jako výrobce náhradních dílů odlišný od původního výrobce hardware.

Vada – také technický problém způsobený chybou dodávaného produktu. Zadavatel předpokládá, že se jedná o výrobek třetí strany.

VTEP - je zkratka pro VXLAN Tunnel Endpoint (Koncový bod tunelu VXLAN). Jde o klíčovou součást architektury VXLAN, která se používá pro další rozšíření síťových segmentů VXLAN o další sítě Layer 2 (VLAN) a Layer 3 (IP síť).

x86_64 – procesorová architektura x86_64 je označení pro 64bitovou verzi sady instrukcí procesorové architektury x86, která je dominantní ve většině osobních počítačů a serverů. Jde o zpětně kompatibilní rozšíření původní 32bitové (IA-32) a 16bitové architektury x86.

1.1. Nástroj pro ochranu integrity komunikačních sítí

Položky dle požadavku 1.1.1-1.1.3 musí tvořit jeden logický celek. Nejméně software komponenty zajišťující kybernetickou bezpečnost musí pocházet od jednoho výrobce. Dle zjištění z PTK požaduje zadavatel, aby tento výrobce byl uveden v Magic Quadrantu společnosti Gartner pro síťové firewally (Network Firewalls/Hybrid Mesh Firewall) jako

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

vedoucí technologie (Leaders) v posledních třech letech před zahájením zadávacího řízení (2025, 2024, 2023).

1.1.1. Firewall pro interní segmenty (2 ks)

ID	Minimální technický požadavek	Odpověď účastníka
1	1 nebo 2 RU pro montáž do standardního 19“ racku včetně ližin a ramene pro organizaci napájecích kabelů.	[redacted]
2	Nejméně 10 x 25 GbE porty pro připojení s rozhraním SFP28, nejméně 1 port pro out of band management s rozhraním RJ-45 (1Gbps).	
3	Možnost rozšíření nebo přímé osazení o/s nejméně 4 x 100GbE porty s rozhraním QSFP28.	
4	Nejméně 32 CPU jader o frekvenci nejméně 2.5Ghz při zpracování instrukcí x86_64. Součin jader [počet] a frekvence na všech jádrech [Ghz] musí být roven anebo větší než 80.	
5	Nejméně 2 interní za chodu vyměnitelné AC napájecí zdroje.	
6	Nejméně 2 x 480 GB SSD v zrcadleném Raid poli.	
7	Nejméně 128 GB RAM s podporou funkce ECC.	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

8	Výčet požadovaných funkcí: SPI Firewall, IPS, Antivirus, Antibot, Detekce aplikací na bráně, Emulace neznámých hrozeb, Extrakce neznámých hrozeb, Filtrování URL a webového obsahu.	[redacted]
9	Výkon při nasazení všech funkcí a úplné inspekci každého packetu procházejícího firewallem všemi bezpečnostními moduly nejméně: 20 Gbps.	
10	Schopnost a licenční výbava pro nasazení nejméně 15 virtuálních firewallů s podporou VXLAN s možností definice VNI. Řešení musí fungovat i jako VTEP.	
11	Výkon firewallu SPI nejméně 100 Gbps	
12	Nejméně 60 milionů současných síťových spojení za vteřinu.	
13	Nejméně 1 milion nových spojení za vteřinu.	
14	Firewall funguje jako proxy pro emailový provoz (SMTP). Přijímá emaily, předává je dál k inspekci a po dokončení inspekce je posílá na další hop (např. interní mailový server).	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

15	Firewall musí obsahovat filtrování emailové komunikace na základě textu, obsahu a zdrojové adresy odesílatele. Firewall musí vkládat do textu emailu varování upozorňující na původ emailu (nejméně pro kategorie: externí a interní).	[redacted]
16	Firewall rozpoznává provoz sociálních sítí a umí zakázat komunikaci na sociální sítě na základě typu sociální sítě, uživatele, který požaduje přístup k sociální síti a na základě obsahu na sociální síti.	
17	VPN koncentrátor pro SSL a IPSec za použití AES-256.	
18	Clusterování v režimu active-active, kdy provoz prochází oběma firewally současně. V případě výpadku jednoho přebírá funkci druhý firewall. Platí i pro případ údržby. Rozhraní pro active-active synchronizaci nejsou zahrnuta v portové výbavě výše a musí být dodána navíc k portům výše. Rozhraní musí být redundantní o nejmenší	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

	prostupnosti 100Gbps (duplex).	
19	Požadavek na řešení ochrany proti zero day útokům a pishingu včetně ochrany na úrovni protokolu DNS a SSL inspekcí. Tyto funkce musí být licenčně pokryty a zařízení musí mít dostatečný výkon k jejich naplnění dle požadavku 9.	[redacted]
20	Možnost rozšířit o licenci pro řešení ochrany IoT zdravotnických zařízení. Tyto funkce musí mít dostatečný výkon k jejich naplnění dle požadavku 9.	
21	Možnost rozšířit o licenci pro SD-WAN obsahující identifikaci a aplikací. Schopnost využití více WAN linek najednou a směrování aplikací do různých WAN linek podle typu aplikace stavu linky.	
22	Rozpoznání nejméně 7000 kategorií aplikací či konkrétních aplikací. Rozpoznání musí být použitelné v bezpečnostních politikách/pravidlech.	
23	Předdefinované dynamické objekty pro nejčastější	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

	cloudové služby nejméně MS Azure, AWS, GCP, Office365, Zoom, Dropbox a případně další.	[redacted]
24	Předdefinované dynamické objekty pro geografické lokality do úrovně států.	
25	Integrace se zdroji identit MS AD, LDAP, MS EntraID.	
26	Integrace s 802.1X platformou Aruba Networks ClearPass v majtku zadavatele. **Nutno předložit jako součást nabídky integrační dokument výrobce popisující jednotlivé atributy.**	
27	Nabízený produkt nesmí mít více než 15 CVE za poslední tři roky (2025, 2024, 2023) před zahájením zadávacího řízení na webu cve.org. Řešení musí být nástrojem pro zvýšení úrovně kybernetické bezpečnosti, a nikoliv zdrojem dalších zranitelností.	
28	Záruka 8x5 NBD na 5 let včetně signatur na popsané funkce.	

1.1.2. Pobočkový firewall (3 ks)

ID	Minimální technický požadavek	Odpověď účastníka
1	1 nebo 2 RU pro montáž do	[redacted]

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

	standardního 19“ racku včetně ližin a ramene pro organizaci napájecích kabelů.	[redacted]
2	Nejméně 4 x 10 GbE porty pro připojení s rozhraním SFP+, nejméně 15 portů s rozhraním 1GbE, nejméně 1 port pro out of band management s rozhraním RJ-45 (1Gbps).	
3	Zařízení je od stejného výrobce jako firewall pro interní segmenty. V případě nejasnosti rozhoduje, že je pod správou stejného management nástroje.	
4	Nejméně 2 za chodu vyměnitelné AC napájecí zdroje.	
5	Výčet požadovaných funkcí: SPI Firewall, IPS, Antivirus, Antibot, Detekce aplikací na bráně, Emulace neznámých hrozeb, Extrakce neznámých hrozeb, Filtrování URL a webového obsahu.	
6	Výkon při nasazení všech funkcí a úplné inspekci každého packetu procházejícího firewallem všemi bezpečnostními moduly nejméně: 4 Gbps.	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

7	Výkon firewallu SPI nejméně 12 Gbps	[redacted]
8	Firewall rozpoznává provoz sociálních sítí a umí zakázat komunikaci na sociální sítě na základě typu sociální sítě, uživatele, který požaduje přístup k sociální síti a na základě obsahu na sociální síti.	
9	VPN koncentrátor pro SSL a IPSec za použití AES-256.	
10	Požadavek na řešení ochrany proti zero day útokům a pishingu včetně ochrany na úrovni protokolu DNS a SSL inspekcí. Tyto funkce musí být licenčně pokryty a zařízení musí mít dostatečný výkon k jejich naplnění dle požadavku 9.	
11	Možnost rozšířit o licenci pro řešení ochrany IoT zdravotnických zařízení. Tyto funkce musí mít dostatečný výkon k jejich naplnění dle požadavku 9.	
12	Možnost rozšířit o licenci pro SD-WAN obsahující identifikaci a aplikací. Schopnost využití více WAN linek najednou a směrování aplikací do	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

	různých WAN linek podle typu aplikace stavu linky.	[redacted]
13	Rozpoznání nejméně 7000 kategorií aplikací či konkrétních aplikací. Rozpoznání musí být použitelné v bezpečnostních politikách/pravidlech.	
14	Předdefinované dynamické objekty pro nejčastější cloudové služby nejméně MS Azure, AWS, GCP, Office365, Zoom, Dropbox a případně další.	
15	Předdefinované dynamické objekty pro geografické lokality do úrovně států.	
16	Integrace se zdroji identit MS AD, LDAP, MS EntraID.	
17	Integrace s 802.1X platformou Aruba Networks ClearPass v majektu zadavatele. **Nutno předložit součástí nabídky integrační dokument výrobce popisující jednotlivé atributy.**	
18	Nabízený produkt nesmí mít více než 15 CVE za poslední tři roky (2025, 2024, 2023) před zahájením zadávacího řízení na webu cve.org. Řešení musí být nástrojem	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

	pro zvýšení úrovně kybernetické bezpečnosti, a nikoliv zdrojem dalších zranitelností.	[redacted]
19	Záruka 8x5 NBD na 5 let včetně signatur na popsané funkce.	

1.1.3. Nástroj/platforma pro správu a vyhodnocování logů firewallů (1 ks)

ID	Minimální technický požadavek	Odpověď účastníka
1	Platforma může běžet na dedikované appliance nebo ve VMware virtualizaci zadavatele, platforma nesmí běžet na žádném z firewallů výše. Pokud se jedná o HW appliance, nebo není možné z nějakého důvodu využít HA virtualizace VMware, pak je nutné dodat 2ks řešení platformy pro správu a vyhodnocování logů. V případě dodání 2ks řešení je nutné zajistit, aby platforma podporovala vlastní automatické řešení vysoké dostupnosti. Alternativně je možné postavit virtualizaci vlastní s dvěma servery a dvěma diskovými poli se synchronní replikací.	[redacted]
2	Nejméně 2 x 25 GbE porty pro připojení s rozhraním SFP28, nejméně 1 port pro out of band management s rozhraním RJ-45 (1Gbps). Požadavek není relevantní pro virtuální variantu.	
3	Zařízení, respektive jeho software část, pochází od stejného výrobce jako firewall pro interní segmenty.	
4	Nejméně 2 interní za chodu vyměnitelné AC napájecí zdroje. Požadavek není relevantní pro virtuální variantu.	
5	Platforma musí umožnit licenčně spravovat všechny funkce všech firewallů.	
6	Platforma udržuje konfigurace všech firewallů a provádí jejich správu.	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

7	Platforma sbírá logy ze všech firewall a vyhodnocuje je. Je možné se prokliknout z libovolného logu k události, či pravidlu které jej vygenerovalo. Musí platit i v obou opačných směrech. Vyhodnocené logy nabízí v přehledném dashboardu k zobrazení.	[redacted]
8	Integrace s platformou SIEM/SOAR bez nutnosti dalších komponent, respektive případné komponenty musí být v ceně.	
9	Platforma generuje reporty a umožňuje automatickou notifikaci.	
10	Platforma dokáže udržet na externím úložišti mapovaném přes NFS protokol nejméně 40 TB logů. V případě, že se jedná o HW appliance musí obsahovat 10% kapacity jako zápisovou a čtecí cache a zbytek kapacity nejméně na 24 médiích. Řešení musí zvládat nejméně 175GB logů denně.	
11	Výkon platformy musí být takový, že dokáže zpracovat nejméně v peaku 10 000 logů za vteřinu a v průměru bude zpracovávat zhruba 1000 logů za vteřinu. V případě virtuální varianty zajišťuje hardware zadavatel. Zadavatel počítá v průměru na log 2000 bytů.	
12	Podpora API rozhraní pro zajištění kompletní a plnohodnotné správy paralelně k lokální/GUI/CLI administrací. API musí mít nastavení oprávnění pro zabezpečení.	
13	Licenčně musí být pokryto nejméně 5ks dodávaných firewallů s možností pouze licenčního rozšíření nejméně na 10ks firewallů.	
14	Řešení by mělo poskytovat přehled o bezpečnostních hrozbách, umožňovat forenzní analýzu událostí, generovat reporty a umožňovat rychlou reakci na bezpečnostní incidenty.	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

15	Řešení musí být schopno vytvářet vlastní korelační pravidla událostí, ještě před odesláním do platformy SIEM/SOAR.	[redacted]
16	Řešení musí analyzovat události v reálném čase. Součástí akceptace bude penetrační test/inteligentní port scan na aplikační úrovni a proběhne porovnání událostí proti skriptu.	
17	Lze nakonfigurovat automatickou reakci na události nejméně: poslání emailové notifikace, spuštění skriptu a vytvoření pravidla na spravovaných firewallech.	
18	Záruka 8x5 NBD na 5 let včetně signatur na popsané funkce.	

1.1.4. EDR systém pro ochranu operačních systémů (1300 ks operačních systémů)

Po analýze technického řešení se na rozdíl od PTK zadavatel rozhodl, že bude požadovat EDR/XDR platformu s použitím odlišného AV engine a dalších ochran od platformy nabízené jako technické řešení pro kapitoly 1.1.1-1.1.3. Důvodem pro toto rozhodnutí je zajištění analýzy obsahu pomocí dvou odlišných technologií. Zejména pak antivirová ochrana a žádná další komponenta použitá v prvcích kapitol 1.1.1-1.1.3 nesmí být shodná s platformou nabízenou v kapitole 1.1.4. V tomto postupu se zadavatel rozhodl pro dual-vendor strategii. Účastník předloží součástí nabídky **čestné prohlášení výrobce v české jazyce, prokazující splnění tohoto požadavku**.

Dle zjištění z PTK požaduje zadavatel, aby tento výrobce byl uveden v Magic Quadrantu společnosti Gartner pro ochranu koncových stanic (Endpoint Protection Platform) jako vedoucí technologie (Leaders) v posledních třech letech (2025, 2024, 2023).

ID	Minimální technický požadavek	Odpověď účastníka
1	Obsahuje mechanismy ochrany proti malware a ransomware, ochrany proti pishingovým útokům, klasický antivirus a IPS, EDR modul s vizualizací vektoru útoku, systém pro emulaci a extrakci hrozeb.	[redacted]

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

2	Podporuje ochranu operačních systémů a je na nich přímo provozována: Microsoft Windows 10 a 11, Windows server 2022, 2019, 2016 a 2012 R2.	
3	Podporuje ochranu operačních systémů a je na nich přímo provozována: Ubuntu 20 a výše, RHEL/Oracle Linux 7, 8, 9 a výše, CentOS 7,8 a výše, SUSE Linux Enteprise Server 12 SP1 a vyšší, Mac OS 12 a výše.	
4	Součástí řešení musí být nejméně jeden testovací fyzický notebook určený pro testování MacOS a procesory M4 určený pro český trh.	
5	Součástí řešení musí být nejméně tři testovací fyzické notebooky určené pro testování OS Linux určené pro český trh.	
6	Součástí řešení musí být nejméně šest testovacích fyzických notebooků určených pro testování OS Windows určených pro český trh.	
7	Musí mít schopnost identifikovat a reportovat zranitelnosti v softwaru na koncových bodech, které by mohly být zneužity.	
8	Řešení musí využívat pokročilou behaviorální analýzu k identifikaci podezřelých aktivit, které by mohly naznačovat probíhající útok, i když	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

	se jedná o neznámou hrozbu (zero-day).	[redacted]
9	Řešení umožňuje šifrování disků a omezování použití fyzických portů chráněných koncových stanic.	
10	Řešení obsahuje detekci chování uživatelů ve spojení s analýzou chování pomocí umělé inteligence.	
11	Záruka 8x5 NBD na 5 let včetně signatur na popsané funkce.	

1.2. Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí (8000 EPS nebo 20 aktivních uživatelů nebo 150GB/denně)

Nástroj musí nabízet úzkou integraci s řešením pro ochranu koncových bodů dle bodu 1.1.4. Zadavatel nepožaduje řešení od jednoho výrobce, ale požaduje, aby nástroj bodu 1.2 používal pro své potřeby operací, kde je vyžadován agent na koncové stanici software dodaný v bodě 1.1.4. Instalaci dalšího software agenta čistě pro potřeby bodu 1.2 zadavatel nepřipouští. Tato úprava byla provedena jako reakce na odpovědi z PTK.

ID	Minimální technický požadavek	Odpověď účastníka
1	Zadavatel požaduje platformu určená k zefektivnění a automatizaci bezpečnostních operací. Jejím cílem je snížit čas potřebný k detekci a reakci na bezpečnostní incidenty a zvýšit	[redacted]

	produktivitu bezpečnostního týmu.	
2	Nástroj se musí integrovat s dalšími bezpečnostními i IT nástroji (SIEM, EDR, NDR, sandboxy, firewally, nástroje pro správu zranitelností, nástroje pro správu identit a přístupu, cloudové služby, a mnoho dalších). To umožňuje centralizovat akce napříč celým bezpečnostním stackem.	[redacted]
3	Nástroj musí obsahovat digitální tržiště, kde jsou dostupné různé automatizační skripty od různých výrobců. O tyto skripty je následně možné rozšířit naši knihovnu automatizací.	
4	Zadavatel požaduje vizuálně editovatelné playbooky (automatizované pracovní postupy). Tyto playbooky umožňují automatizovat repetitivní, časově náročné úkoly, jako je sběr informací o hrozbách, obohacení alertů, izolace kompromitovaných endpointů, blokování	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

	škodlivých IP adres a domén.	[redacted]
5	Nástroj obsahuje centralizovanou správu incidentů. Poskytuje centrální repozitář pro všechny incidenty, které jsou vygenerovány na základě logů přijatých do systému z různých zdrojů, min. však koncových stanic a firewallů. Umožňuje sledovat jejich stav, prioritu a přiřazení k řešiteli.	
6	Nástroj obsahuje funkce automatizace od reakce na phishingové útoky, detekci malwaru, správu zranitelností, až po reakci na incidenty v cloudu a forenzní analýzu.	
7	Nástroj obsahuje virtuální pracovní prostor podporující spolupráci řešitelů v reálném čase. Umožňuje sdílení informací, provádění příkazů a skriptů, zaznamenávání poznámek a komentářů a dokumentování průběhu vyšetřování.	
8	Nástroj obsahuje přehled událostí/důkazů, který slouží k rekonstrukci řetězců útoku a ukládání	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

	všech relevantních důkazů a informací souvisejících s incidentem.	[redacted]
9	Nástroj automaticky dokumentuje všechny provedené akce a kroky vyšetřování, což je klíčové pro audit, reporting a sdílení znalostí.	
10	Nástroj shromažďuje a agreguje informace o hrozbách a o indikátorech kompromitace vyskytujících se v incidentech (např. Unit 42, AutoFocus či jiné rovnocenné, ale i komerční a open-source TI feedy, ISAC/ISAO).	
11	Nástroj koreluje a skóruje indikátory kompromitace (IOCs) a hrozeb proti specifickému prostředí zákazníka.	
12	Nástroj umožňuje automaticky tlačit aktualizované IOCs do bezpečnostních kontrol (např. firewallů, EDR) pro okamžitou detekci a prevenci.	
13	Nástroj umožňuje vytvářet plně přizpůsobitelné dashboardy a reporty pro vizualizaci klíčových	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

	metrik SOC a stavu incidentů.	[redacted]
14	Nástroj umožňuje vytvářet metriky SOC: Poskytuje přehled o počtu incidentů a dalších důležitých provozních metrikách.	
15	Nástroj obsahuje předpřipravené integrace a playbooky. Rozsáhlé tržiště, kde mohou uživatelé stahovat předpřipravené integrace, playbooky, balíčky obsahu (content packs) a nástroje pro různé bezpečnostní nástroje a případy použití.	
16	Řešení pro správu incidentů musí mít schopnost integrace s firewall technologiemi třetích stran, a to minimálně Fortinet, Check Point Software Technologies a Palo Alto Networks.	
17	Řešení musí mít schopnost automaticky hodnotit incidenty pomocí strojového učení, statistické analýzy a atributů	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

	incidentů a následně identifikovat vysoce rizikové incidenty.	[redacted]
18	Řešení musí umožnit zobrazení informací o hrozbách přicházejících z různých IP adres a geolokací.	
19	Řešení musí uchovávat data minimálně po dobu 31 dní od zachycení logu. Toto období musí být rozšířitelné minimálně formou dodatečné licence, která může být vztažena ke kapacitě či přímo časovému údaji. Řešení musí uchovávat forenzní data po dobu minimálně 365 dní.	
20	Musí obsahovat úzkou integraci s dodávaným EDR/XDR agentem/modulem (dále jen agent). Řešení musí poskytovat podporu pro řízení přístupu, a to minimálně na úrovni pozic řešitelů (RBAC) jakož i možnost přiřadit určité agenty (SW) umístěné na koncových operačních systémech určitému řešiteli/analytikovi.	
21	Řešení musí podporovat správu a sběr telemetrie	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

	agentů, kteří se nemohou připojit na internet (tzv. air-gapped sítě) prostřednictvím jednoho nebo více virtuálních strojů, které mohou fungovat jako broker/proxy server s podporou klastrování.	[redacted]
22	Řešení musí nabízet předdefinované šablony zpráv, což umožní rychlý a komplexní přehled o prostředí s možností uložení a exportu.	
23	Řešení musí obsahovat nástroj pro zjednodušení procesu forenzní analýzy. Minimálně musí umožnit přístup k artefaktům jako historie prohlížeče, záznamy událostí a klíče registrů.	
24	Řešení musí obsahovat správu zranitelností pro koncové stanice, kde je aktivní agent.	
25	Řešení musí umožnit řešiteli vyhledat a zneškodnit škodlivý soubor pro všechny chráněné koncové stanice.	
26	Záruka 8x5 2BD na 5 let včetně signatur na popsané funkce.	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

[redacted]

1.3. Řešení pro zajištění aplikační bezpečnosti (pro 1000 aktiv/asetů)

Nástroj bude nasazen hlavně pro skenování aktiv centrální lokality. Nástroj bude nasazován v rámci jednotlivých segmentů, podle potřeb zadavatele. Nejedná se o distribuované řešení.

Agentní skenování bude použito pro okamžité ověření stavu sledovaného aktiva. Bez agentní skenování pro pravidelnou kontrolu stavu informačních aktiv. Pro aktiva chráněná nástrojem PAM počítá zadavatel s použitím agendového přístupu. Zejména pak pro kontrolu konfigurací.

Požadavky byly upraveny na základě zjištění z PTK.

ID	Minimální technický požadavek	Odpověď účastníka
1	Agentní a bez agentní skenování aktiv/asetů, včetně lehkého endpoint agenta pro nepřetržitou sběr dat i z obtížně dostupných aktiv, a také tradiční bez agentní skenování sítě.	[redacted]
2	Nástroj automaticky	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

	objevuje a inventarizuje všechna připojená zařízení v síti, včetně serverů, pracovních stanic, IoT zařízení a cloudových aktiv. Integruje se s DHCP, poskytovateli cloudových služeb (AWS, Azure) a dalšími zdroji.	[redacted]
3	Nástroj využívá rozsáhlou a neustále aktualizovanou databázi známých zranitelností a chybných konfigurací, aby nic nebylo přehlédnuto.	
4	Nástroj využívá pokročilý model skórování rizik, který kombinuje kontext hrozeb z reálného světa, dopad, atraktivitu aktiv pro útočníky a chování útočníků. Tímto způsobem prioritizuje zranitelnosti na základě jejich skutečné hrozby pro vaši organizaci, nikoli pouze na	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

	základě skóre CVSS.	[redacted]
5	Nástroj používá skórování CVSSv3 se zpětnou kompatibilitou s CVSSv2. U každé zranitelnosti je uveden kontext a skóre respektive bodové riziko zranitelnosti. U zranitelností jsou uváděny odkazy na Exploit DB a CISA KEV list. Případně alternativu postavenou na otevřeném základu nejméně s obsahem požadovaných webových databází.	
6	Nástroj využívá databázi zranitelností CVE, každá odhalená zranitelnost bude pojmenována a identifikována (výjimku by tvořila prokazatelná zero day zranitelnost).	
7	Nástroj umožňuje vytvářet a spravovat projekty nápravy, sledovat pokrok a přidělovat úkoly napříč týmy.	
8	Nástroj poskytuje podrobné a přesné informace o zranitelnosti, jejím umístění, způsobu detekce, riziku a	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

	doporučeních pro nápravu.	[redacted]
9	Nástroj nabízí konfigurovatelné možnosti automatizace workflow k urychlení implementace oprav a snížení manuálního úsilí.	
10	Nástroj skenuje konfigurace zařízení, identifikuje oblasti zranitelnosti a nedodržování předpisů či dle shody z definované šablony. V rámci kontroly musí také proběhnout analýza konfigurací s cílem nalezení chyby v konfiguraci, a to i pokud by chyba byla obsažena v šabloně. Nástroj kontroluje nedostatečná bezpečností nastavení. Šablony musí podporovat nejméně CIS Security a STIG formáty. Případně alternativu postavenou na otevřeném základu nejméně s obsahem požadovaných formátů.	
11	Nástroj podporuje skenování a reporting shody s průmyslovými	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

	standardy a regulačními požadavky (např. SCAP, PCI).	[redacted]
12	Nástroj umožňuje vytvářet a vynucovat bezpečnostní zásady. Dále pak pro každou zranitelnost uvede doporučení pro nápravu. Cílem je určit následující kroky po identifikaci zranitelnosti.	
13	Nástroj poskytuje dynamické a přizpůsobitelné dashboardy pro rychlý přehled o stavu zranitelností, expozici rizik a pokroku nápravy.	
14	Nástroj generuje detailní reporty (např. pro audit, pro technické týmy, pro vedení) s informacemi o skenovaných aktivech, nalezených zranitelnostech, exploitech a trendech.	
15	Nástroj podporuje export dat do různých formátů (PDF, CSV, XML) pro další analýzu nebo integraci s jinými nástroji.	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

16	Nástroj obsahuje API integrace pro propojení s nástroji třetích stran.	[redacted]
17	Záruka 8x5 2BD na 5 let včetně signatur na popsané funkce.	

1.4. Technické řešení pro zajištění dostupnosti informací (zálohování)

1.4.1. Zálohovací software (pro 100 VM)

Zadavatel aktuálně využívá Veeam Data Platform, pro 120 VM. Nové licence/řešení musí licenčně doplnit tento zálohovací software. Zadavatel nevylučuje použití jiného zálohovacího software, než VDP. Nicméně v takovém případě je nutné splnit dvě podmínky:

a) řešení musí pokrýt 220 VM anebo 110 TB dat uložených na NAS anebo 660 osobních počítačů/koncových zařízení. Licence je možné kombinovat.
b) řešení musí mít stejné nebo lepší funkce než stávající řešení Veeam Data Platform – viz příloha č. 8 zadávací dokumentace.

Záruky SW dle Smlouvy – 8x5 NBD na 5 let.

1.4.2. Zálohovací servery (2ks)

Zadavatel aktuálně využívá servery HPE Proliant Gen10, Gen11 a Gen 12. Zálohovací servery musí využívat technické řešení, které bude kompatibilní se stávajícím nástrojem na správu HPE ilO Advanced. Zejména pak pro hromadnou správu. Je možné buď využít integraci se stávajícími nástroji pro správu, nebo je nahradit nástroji novými se stejnou funkční výbavou. Licenční podpora musí pokrýt nejméně 30 serverů. Aktuální nástroj na správu je HPE OneView.

ID	Minimální technický požadavek	Odpověď účastníka
1	Montáž do standardního 19“ racku o maximální výšce 4 RU. 24 diskových LFF pozic a nejméně 12 EDSFF	[redacted]

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

	diskových pozic pro NVMe disky.	[redacted]
2	Nejméně 2 za chodu vyměnitelné napájecí zdroje s platinovou účinností. Server musí být v dodávané konfiguraci schopen fungovat na jeden napájecí zdroj s tím, že jeho zátěž nesmí překročit 75%.	
3	Nejméně 2 CPU, každé o nejméně 16 jádrech zpracovávající X86_64 instrukce s výkonem SPEC CPU® 2017 Floating Point Speed 265 Base bodů.	
4	Nejméně 16 ks 32GB DDR4 nebo DDR5 RAM modulů o frekvenci nejméně 5600Mhz s podporou ECC. Každý jeden paměťový kanál CPU musí být osazen alespoň jedním modulem.	
5	Nejméně dvě dvouportové síťové karty o rychlosti 10/25 Gbps nebo 100 Gbps.	
6	Nejméně jedna FC karta o rychlosti	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

	32Gbps pro připojení páskové mechaniky.	[redacted]
7	Nejméně 12 SSD disků EDSFF o velikosti 3.2TB s DWPD4 a vyšším.	
8	Nejméně 2 SSD pro boot hypervisoru vSphere o velikosti min. 480GB v RAID 1 poli.	
9	Nejméně jeden diskový řadič pro připojení 24 LFF disků včetně příslušné kabeláže. Řadič bude mít nejméně 8GB cache chráněné baterií nebo kondenzátorem. Včetně 24 x min. 20 TB HDD min. 7200 rpm.	
10	Licence na MS Windows Server 2022 nebo 2025 Standard	
11	Licence VMware vSphere Enterprise Plus na všechna CPU jádra.	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

12	TPM čip, standardní ližiny do racku a rameno pro organizaci kabeláže.	[redacted]
13	Záruka výrobce 24x7 se zásahem následujícího pracovního dne v místě instalace na 5 let.	

1.4.3. Pásková knihovna (1ks)

ID	Minimální technický požadavek	Odpověď účastníka
1	Knihovna bude osazena nejméně dvěma mechanikami LTO-9 s použitím protokolu FC. Je požadována technologie právě LTO-9, kvůli zajištění zpětné kompatibility s páskami LTO-8.	[redacted]
2	Montáž do standardního 19“ racku o maximální výšce 4 RU.	
3	Redundantní napájecí zdroje.	
4	Podpora šifrování páskových médií.	
5	Nejméně 24 pozic pro pásková média. součástí dodávky bude 20 LTO-9 médií a jedno čistící médium.	
6	Záruka výrobce 24x7 se zásahem následujícího	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

	pracovního dne v místě instalace na 5 let.	[redacted]

1.4.4. Diskové pole pro nestrukturovaná data v roli primárního úložiště záloh (1ks)

Zadavatel požaduje univerzální scale out diskové pole typu NAS/S3 pro nestrukturovaná data. Zadavatel nepožaduje diskové pole s blokovými funkcemi s NAS hlavou. Diskové pole bude sloužit k ukládání nesourodých dat. Budou se zde potkávat velmi malé soubory (logy, 200B) a velké soubory (zálohy, >20TB). Požadavky na výkon jsou stanoveny interním výpočtem a je velmi pravděpodobné, že na pole budou v jeden čas tisíce přístupů. Zadavatel požaduje, aby si diskové pole zachovalo své vlastnosti s požadovanou kapacitou. Účastník může počítat s úplným zaplněním diskového pole na 100% požadované kapacity výše uvedenými daty. Pakliže dochází k degradaci výkonu či jiných vlastností zaplněním diskového pole, musí účastník dodat více než 100% požadované kapacity a to tak, aby k degradaci nedocházelo.

ID	Minimální technický požadavek	Odpověď účastníka
1	Scale out architektura s nejméně **čtyřmi** identickými uzly (fyzická oddělitelná zařízení umístitelná do jiného racku) postavená na principu redundance médií pomocí technologie erasure coding. Řešení musí být odolné na výpadek jednoho celého uzlu a nejméně 2 médií-disků z každého uzlu.	[redacted]
2	Montáž do standardního 19“ racku o maximální výšce 12 RU.	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

3	Diskové pole bude využívat protokol NFS v4.1 a v menší míře protokol SMB v3.	[redacted]
4	Řešení musí podporovat protokol S3 pro přesouvání záloh a musí disponovat vlastním REST API pro kompletní správu pole a diskového prostoru z aplikace.	
5	Kontinuální asynchronní replikace mezi dvěma scale-out clustery dostupnými přes směrovanou síť o prostupnosti 50Gbps (duplex). Druhé pole bude nakoupeno později a není předmětem nabídky. Replikace musí probíhat na úrovni souborové vrstvy, nikoliv na úrovni blokové vrstvy.	
6	Řešení musí být schopno získat identitu a strom přístupových oprávnění na základě čtení uživatelského stromu z Microsoft Active Directory a Linux LDAP. Řešení musí používat obě funkce, nikoliv však zároveň.	
7	Řešení musí být vybaveno přístupovými seznamy a to	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

	zejména pro protokol NFS. Bezpečnost musí být vázána k souboru a k uživatelské identitě přistupujícího uživatele. Nejméně musí být rozpoznány příznaky čtení, zápis a řízení oprávnění k souboru.	[redacted]
8	Řešení musí být prezentováno uživatelům jako jeden name space. Řešení musí mít integrovaný load balancer, tak aby zátěž byla mezi uzly rozkládána rovnoměrně.	
9	Řešení musí podporovat snapshoty a to tak, že snapshot vytvoří zámek na dané souborové struktuře a následně nebude možné se soubory manipulovat. V kombinaci se zálohovacím software musí tato funkce vytvářet nepozměnitelný repositář záloh.	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

10	Řešení musí podporovat šifrování dat (data at rest encryption). Požadavek je alespoň na šifrování pomocí AES-256. Šifrování nesmí být založeno na hardware, pro případ potřeby migrace mezi jednotlivými hardwarovými platformami. Řešení musí chránit média i poté co byla vyřazena z provozu a nedopatřením se vyřazené médium dostane do nesprávných rukou. Řešení musí obsahovat interní transparentní správu klíčů. Řešení musí obsahovat mechanismus pro efektivní rotaci šifrovacích klíčů.	[redacted]
11	Uložená data budou komprimována a potenciálně i šifrována. Funkce deduplikace a komprese není požadována. Deduplikační a kompresní poměr nelze započíst do výpočtu celkové kapacity. Požadovaná čistá kapacita je nejméně 600 TB. Kapacita musí být rozšiřitelná nejméně na	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

	desetinásobek, pouze přidáváním hardware/software v rámci jednoho clusteru. Zadavatel předpokládá, že řešení bude větší než-li 12 RU.	[redacted]
12	Diskové pole bude sloužit pro paralelní přístup systému i uživatelů. Diskové pole musí být schopno zároveň komunikovat s nejméně 2000 uživateli a 200 systémy (NFSv4.1). Diskové pole musí disponovat nejméně 40ti CPU jádry o základní frekvenci nejméně 2.2 GHz.	
13	Diskové pole musí disponovat nejméně 4 x 25 GbE front and porty a 4 x 25GbE backend porty. Porty lze v případě sdílení libovolně kombinovat. Celkový nejmenší počet portů je 8 ks. Každý uzel musí disponovat nejméně dvěma porty.	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

14	Diskové pole musí disponovat nejméně 65 000 IOPS (NFSv4.1). Celkový výkon pro čtení musí být nejméně 6 GB za vteřinu a celkový výkon pro zápis nejméně 4 GB za vteřinu. Jedno spojení musí být schopno zapisovat rychlostí nejméně 1 GB za vteřinu a číst rychlostí 2 GB za vteřinu.	[redacted]
15	V případě rozšíření kapacity na trojnásobek musí dojít k zvýšení výkonu diskového pole nejméně na dvojnásobek. Stejná logika musí být aplikovatelná pro všechna rozšíření.	
16	Řešení musí být vybaveno analytickým dashboardem, který v reálném čase zobrazí IOPS a prostupnost (čtení a zápis zobrazeno separátně) pro jednotlivé části souborového stromu. Dashboard musí zobrazit zaplnění jednotlivých větví, respektive	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

	složek souborového stromu. Dashboard musí zobrazit počet připojených klientů. Data musí být dostupná nejméně pro 24 hodin.	[redacted]
17	Schopnost vytvoření globálního name space mezi více scale-out clustery diskového pole. Globální namespace umožňuje jak čtení, tak i zápis.	
18	Záruka výrobce 24x7 se zásahem následujícího pracovního dne v místě instalace na 5 let.	

1.5. Nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů

Zadavatel nepožaduje dodání hardware. Zadavatel předpokládá dodávku formou SW VM pro prostředí VMware vSphere. Pakliže to technické řešení vyžaduje, pak je možné dodat jako vlastní virtualizaci. Řešení vlastní virtualizace musí obsahovat nejméně dvě disková pole a dva servery. Alternativně je možné řešit režim vysoké dostupnosti pomocí all in one appliance (HCI). V takovém případě je nutné zajistit, aby měla appliance či disková pole stejnou kapacitu jako požadované řešení diskového pole pro nestrukturovaná data.

ID	Minimální technický požadavek	Odpověď účastník
1	Zadavatel požaduje	[redacted]

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

	schopnost provádět výkonné fulltextové vyhledávání na strukturovaných i nestrukturovaných datech, včetně řazení relevance (relevance scoring), zvýrazňování (highlighting) a návrhů (suggestions).	[redacted]
2	Zadavatel požaduje schopnost seskupovat data, tak aby bylo možné provádět komplexní analýzu dat, ať už jde o filtrování, souhrnné statistiky nebo složité výpočty (např. terms aggregations, date histograms, metrics aggregations, agregace na základě topologických dat).	
3	Nástroj musí mít distribuovanou architekturu, která umožňuje horizontální škálování přidáváním dalších uzlů pro zvládnutí velkých objemů dat a vysokého počtu	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

	dotazů. To zahrnuje: - Vytváření clusterů uzlů s primárními a replikovými shardy pro redundanci dat a automatické převzetí služeb při selhání. - Cluster automaticky zpracovává selhání uzlů a vyvažuje data mezi dostupnými uzly. - Snadné rozšíření kapacity clusteru přidáním dalších uzlů (scale-out). - Cluster může být umístěn na virtulizaci VMware vSphere (dodávka pouze software) nebo bude dodán jako hardware appliance. V případě hardware appliance, se bude jednat nejméně o dva servery a dvě disková pole vytvářející synchronně	[redacted]

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

	replikovaný vMSC cluster.	[redacted]
4	Komplexní RESTful API pro interakci s nástrojem (indexování, vyhledávání, správa dat).	
5	Oficiální klientské knihovny pro různé programovací jazyky (Java, Python, .NET, PHP, Ruby, JavaScript atd.).	
6	Zabezpečená komunikace mezi uzly v clusteru a mezi klienty a clusterem dle doporučení NÚKIB na kryptografické prostředky.	
7	Definování rolí s konkrétními oprávněními (např. pouze pro čtení k určitým indexům, pro zápis k jiným) a přiřazování těchto rolí uživatelům nebo skupinám. To umožňuje řídit, kdo může provádět úkony na definovaných oblastech funkcí či datech.	
8	Vestavěná správa uživatelů a rolí (nativní realm) a možnost spravovat uživatele ze	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

	souboru (file realm).	[redacted]
9	Kontrola přístupu k nástroji na základě IP adres.	
10	Úložiště klíčů pro bezpečné ukládání citlivých nastavení, jako jsou hesla.	
11	Zaznamenávání událostí souvisejících se zabezpečením pro monitorování a dodržování předpisů.	
12	Vytváření záloh indexů a jejich obnova.	
13	Automatizace uchovávání dat a přesouvání mezi datovými úrovněmi (např. z horkého do teplého do studeného úložiště).	
14	Pohodlný způsob správy časových řad dat (data streams).	
15	Nástroje pro pomoc s	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

	upgradem nabízeného clusteru.	[redacted]
16	Záruky SW dle Smlouvy – 8x5 2BD na 5 let.	

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

2. Požadavky na implementaci

Zadavatel předpokládá následující minimální požadavky na implementaci řešení. 1 MD = uváděno jako 1 člověkoden, tj. 8 hodin práce specialisty. Předpoklady pracnosti byly upraveny na základě odpovědí z PTK, přičemž účastník nabídne vlastní pracnost v rámci své nabídky (může nabídnout stejnou nebo vyšší).

Produkt	Činnost	Min. pracnost
Přípravné práce	Aktualizace katalogu služeb	5 MD
	Aktualizace katalogu rizik	5 MD
	Tvorba dokumentu SoW/detailní návrh	10 MD
Interní firewall	Nasazení SPI, NAT, VPN a L3 vlastností	10 MD
	Nasazení IPS a aplikační kontroly	15 MD
	Penetrační test dodaného řešení	2 MD
Pobočkový firewall	Nasazení SPI, NAT, VPN a L3 vlastností	10 MD
	Nasazení IPS a aplikační kontroly	5 MD
	Penetrační test dodaného řešení	2 MD
Nástroj pro správu	Nasazení nástroje a registrace FW	5 MD
	Nasazení vnitřní korelace	5 MD
	Nasazení reportingu dle předpisů zadavatele	7 MD
EDR	Vyladění profilů EDR pro jednotlivé role a způsoby užití	20 MD
	Nasazení na koncové stanice pomocí politik	10 MD
	Řešení potíží s platformou EDR	10 MD
	Konfigurace dashboardů pro řešení kybernetických incidentů	10 MD
Sběr vyhodnocování kybernetických incidentů	Instalace a integrace s platformou pro zaznamenávání událostí a činností	5 MD
	Nastavení dashboardů pro jednotlivé pohledy	10 MD
	Příprava automatizace pro prostředí zadavatele	10 MD
	Nastavení reportingu	5 MD
Aplikační bezpečnost	Nasazení platformy	2 MD
	Volba testů pro jednotlivé assety/informační aktiva	10 MD
	Vytvoření periodické metodiky testování	3 MD
Zálohovací software	Instalace nových instancí management konzole zálohovacího serveru	2 MD
	Přidání nových backup proxy, klientů a přidání další zařízení pro zálohování	13 MD
Zálohovací servery	Instalace	7 MD

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

Pásková knihovna	Instalace a přidání do zálohovacího software	3 MD
Diskové pole pro nestrukturovaná data	Sestavení scale-out clusteru a ověření funkcí	5 MD
	Konfigurace front end protokolů a přidávání klientů, konfigurace API, přidání identity apod.	15 MD
Nástroj pro zaznamenávaní událostí a činností	Konfigurace platformy a zprovoznění požadovaných funkcí	5 MD
	Přidává datových zdrojů a konfigurace parserů	20 MD
	Konfigurace dashboardů, přehledů a reportingu	20 MD
Post implementační práce	Ladění technologií po nasazení	50 MD
	Nasazení funkcí, které byly požadovány, ale nebyly implementovány při úvodní implementaci	50 MD

Zadavatel požaduje provedení všech prací v rámci implementace, a to i za situace, že se účastník domnívá, že činnosti nebudou potřeba. Zadavatel uvádí, že odhady pracnosti jsou minimální. Účastník uvede pracnost potřebnou pro nasazení všech požadovaných funkcí, která bude stejná nebo vyšší než-li odhad zadavatele. Uvedení nižší hodnoty odhadu pracnosti, než-li je odhad zadavatele, představuje nesplnění minimální technické specifikace, a je důvodem pro vyloučení nabídky.

Zadavatel požaduje činnosti, které nebude z technických a organizačních důvodů provést při úvodní implementaci. Tyto činnosti jsou popsány jako post implementační práce. Post implementační práce budou vyžádány v průběhu 60 měsíců. Zadavatel nespecifikuje, na jakou technologii budou tyto práce použity. Zadavatel tuto informaci nemá a není schopen poskytnout.

Post implementační činnosti budou obsahovat takové technické zásahy, které dále upraví nastavení dodávaných systému/technologií, tak aby lépe odpovídalo potřebám zadavatele. Například ladění konfigurace modulu IPS či citlivosti antiviru, úprava parametrů zálohování, přidávání pravidel pro platformu 802.1X a podobně. Zadavatel záměrně neuvádí úplný výčet činností, pouze činnosti omezuje na dodávané technologie. Post implementační činnosti představují vyladění konfigurací k naplnění technologických představ zadavatele. Post implementační činnosti není možné vykonat jednorázově během implementace hlavně z důvodu omezených lidských zdrojů na straně zadavatele a také proto, aby implementační doba odstávky netrvala nepřiměřeně dlouho. Post implementační činnosti nebrání předání systémů/technologií do provozu, ale představují optimalizaci jejich fungování, a to i ve vazbě na potřebu koordinace s dodavateli dle souvisejících smluv.

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

Každá část musí obsahovat náklad na projektové řízení, dokumentaci a zaškolení obsluhy. Tyto činnosti jsou automaticky zahrnuty do předpokládané pracnosti. Pracnost je uvedena pro všechny nabízené kusy.

Všechny technologie musí plnit požadavek na výkonnost a dostupnost. Tyto hodnoty budou ověřeny v rámci akceptace řešení, pracnost na akceptaci je zahrnuta také v rámci odhadu.

Nemocniční 898/20a, 728 80 Ostrava – Moravská Ostrava
T 596 191 111 F 596 618 781
www.mnof.cz

Příloha 3

Zajištění podpory a údržby

Technická specifikace - odstavec	Upřesnění položky	Požadovaná dokumentace a školení v [MD] jako součást plnění PRODÁVAJÍCÍHO	Upřesnění podmínek a požadavků pro umožnění zajištění následné podpory a údržby případnou TŘETÍ STRANOU (přístupová práva ad.)
1.1.1. Firewall pro interní segmenty	HW + systémový SW + služby	**5 MD** (2 MD – administrační školení (policy, clusterování, IPS, SSL inspekce), 3 MD – provozní dokumentace (postupy, recovery, zálohy konfigurace))	Poskytnutí administrátorského účtu s RBAC, přístup k GUI + CLI, export konfiguračních šablon, API přístup, přístup k HA clusteru; dokumentace architektury a síťových vazeb.
1.1.2. Pobočkový firewall	HW + systémový SW + služby	**4 MD** (2 MD – školení pro lokální administraci a policy management, 2 MD – provozní dokumentace)	RBAC přístup k centrálnímu managementu, VPN připojení, export konfiguračních šablon, přístup k centrálnímu logovacímu systému a API.
1.1.3 Nástroj/platforma pro správu a vyhodnocování logů firewallů	systémový SW + služby	**4 MD** (3 MD – školení na management konzoli, reporting a analýzu logů, 1 MD – dokumentace integračních bodů a procesů)	Přístup přes GUI a API rozhraní, oprávnění k read-only i read-write operacím dle RBAC, export konfigurační databáze, export logů pro potřeby log managementu a následné analýzy SIEM/SOAR. Generování reportů.
1.1.4 EDR systém pro ochranu operačních systémů	systémový SW + testovací prostředí OS + služby	**7 MD** (5 MD – školení bezpečnostního týmu (dashboard, detekce, reakce), 2 MD – dokumentace nasazení agentů a politiky nasazení)	API přístup k EDR konzoli, read access k telemetrickým údajům, export konfiguračních profilů, přístup k repozitáři agentů a testovacím stanicím.
1.2 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí	SW + služby	**4 MD** (3 MD – školení SOC týmu (tvorba playbooků, reporting), 1 MD – dokumentace integrací (EDR, firewally))	Přístup přes API, integrační účty s omezeným rozsahem, export playbooků a dashboardů, přístup k instalovaným agentům v testovacím prostředí. Řešení incidentů v rámci war roomů.

1.3 Řešení pro zajištění aplikační bezpečnosti	SW + služby	**3 MD** (2 MD – školení bezpečnostního analytika a admina (analýza zranitelností, reporting), 1 MD – dokumentace konfigurace a testovacích postupů)	Přístup k portálovému rozhraní a API, read-only k databázi zranitelností, export výsledků skenů pro potřeby dalšího zpracování a ukládání logů, možnost importu externích šablon.
1.4.1 Zálohovací software	SW + služby	**2 MD** (1 MD – školení provozních techniků (Veeam/alternativa), 1 MD – dokumentace konfigurace záloh, postupy obnovy)	Admin přístup do management konzole, export jobů a konfigurací, přístup k API, přístup k repozitářům a logům. Zálohování a obnova koncových stanic a sítových úložišť.
1.4.2 Zálohovací servery	HW + systémový SW + služby	**2 MD** (1 MD – školení na správu hardware a monitoring, 1 MD – dokumentace konfigurace a připojení do zálohovací platformy)	IPMI/iLo přístup, root/administrátorská práva v hypervisoru, přístup k síťovým rozhraním, dokumentace topologie a úložišť.
1.4.3 Pásková knihovna	HW + systémový SW + služby	**2 MD** (1 MD – školení na obsluhu a rotaci médií, 1 MD – dokumentace konfigurace a postupy obnovy)	Admin přístup přes management rozhraní knihovny, CLI/API přístup k páskovému robotu, přístup ke konfiguračním souborům.
1.4.4. Diskové pole pro nestrukturovaná data v roli primárního úložiště záloh	HW + systémový SW + služby	**5 MD** (4 MD – školení na správu clusteru a rozhraní, 1 MD – dokumentace konfigurace a replikace)	Administrátorský přístup přes GUI a CLI, přístup k REST API, export konfigurace a topologie, dokumentace uživatelských oprávnění a ACL. Vytváření snapshotů, nepozměnitelnost dat a export dat.
1.5 Nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů	SW + služby	**4 MD** (3 MD – školení na fulltext vyhledávání a analýzu událostí, 1 MD – dokumentace indexačních struktur a zálohování dat)	Přístup přes API a GUI, read-only přístup do úložiště indexů a konfigurací, export nastavení clusteru a datových politik.

Příloha 4

Kybernetická bezpečnost

1. Úvodní informace

1. Poskytovatel je povinen dodržovat a řídit se Pravidly chování dodavatelů v oblasti bezpečnosti informací. Pravidla chování dodavatelů v oblasti bezpečnosti jsou v aktuální verzi k dispozici na webových stránkách Objednatele: www.mnof.cz/pravidla-dodavatele. S těmito Pravidly je povinen obeznámit i své poddodavatelé a vyžadovat od nich jejich dodržování.
2. Poskytovatel prohlašuje, že má zavedena všechna bezpečnostní opatření, procesy a technologie, které prohlásil za zavedené v Příloze Zadávací dokumentace „Hodnocení úrovně kybernetické bezpečnosti účastníka", která byla součástí nabídky Poskytovatele a bere na vědomí, že Hodnocení bude požadováno i od jeho případných poddodavatelů.
3. Poskytovatel bere na vědomí, že veškeré aktivity Poskytovatele a jeho plnění realizované v prostředí Objednatele mohou být monitorovány a vyhodnocovány v rozsahu předmětu plnění.

2. Vzdálený přístup

1. Objednatel upozorňuje, že v případě potřeby vzdáleného přístupu k informačním a komunikačním systémům a informacím Objednatele, bude toto možné pouze na základě Přílohy 5 Vzdálený přístup u této smlouvy.

3. Kontaktní údaje

1. Pro účely komunikace ve věci kybernetické bezpečnosti (opatření, události a incidenty) Objednatel stanovuje 2 režimy z hlediska naléhavosti:
   a) běžný, kdy kontaktní osobou je [redacted]0, e-mail: kb@mnof.cz,
   b) a naléhavý, kdy Objednatel požaduje navíc komunikaci pomocí mob.: [redacted] a dvojice e-mailů: it@mnof.cz a kb@mnof.cz (Objednatel výslovně vyžaduje triplicitní směrování komunikace, tedy telefonem a dvojicí e-mailů do doby dohodnutí dalšího postupu oprávněnými osobami dle Smlouvy).

4. Zákaznický Audit

1. Poskytovatel je povinen umožnit pracovníkům Objednatele provedení auditu kybernetické bezpečnosti a poskytnout jim při provádění tohoto auditu nezbytnou součinnost minimálně v rozsahu dvou (2) člověkodní na každou jednu organizaci (tj. v případě poddodavatelů 2 člověkodny pro každého poddodavatele) při provádění každého auditu (kontroly) ze strany Objednatele a pro tuto činnost zajistit účast kvalifikovaných pracovníků.
2. Poskytovatel umožní Objednateli tuto kontrolu provedenou prostředky Objednatele nebo třetí stranou, a to v lokalitě Poskytovatele i vzdáleně, pokud to technické prostředky Poskytovatele umožňují.

3. Objednatel se zavazuje vyrozumět Poskytovatele o termínu a případně o osobě pověřené provedením auditu, alespoň 3 pracovní dny předem.
4. Poskytovatel se zavazuje nedostatky zjištěné na základě provedeného auditu (kontroly) odstranit ve lhůtě určené v písemném oznámení Objednatele. Nestanoví-li Objednatel lhůtu v písemném oznámení, zavazuji se Smluvní strany dohodnout na lhůtě pro odstranění nedostatků, která nepřevýší 90 kalendářních dnů.
5. Náklady na uskutečnění auditu ponese každá smluvní strana zvlášť. Poskytovatel nemá právo na poskytnutí úhrady nákladů či jakéhokoliv jiného plnění v souvislosti s auditem (kontrolou).

5. Povinnosti Poskytovatele

1. Poskytovatel se dále zavazuje:
   a) poskytnout na vyžádání Objednateli dokumenty, zprávy a obdobné informace, které budou prokazovat naplnění bezpečnostních požadavků, plynoucích ze Smlouvy a jejich Příloh a z Pravidel chování dodavatelů;
   b) na vyžádání s Objednatelem konzultovat kdykoli v průběhu účinnosti této Smlouvy detailní nastavení bezpečnostních opatření k naplnění bezpečnostních požadavků a pro takovéto konzultace zajistit účast kvalifikovaných pracovníků;
   c) neprodleně informovat Objednatele o všech významných změnách v plnění bezpečnostních požadavků, které nastanou kdykoli v průběhu účinnosti této Smlouvy;
   d) bezodkladně a s vyvinutím nejlepšího úsilí zajistit náhradní způsob naplnění bezpečnostních požadavků, pokud stávající řešení přestalo být funkční a efektivní;
   e) bezodkladně a prokazatelně (písemně) informovat Objednatele o kybernetických bezpečnostních událostech a incidentech, které mohou ovlivnit poskytování služeb dle této Smlouvy. Poskytovatel je zároveň povinen ve lhůtě do 48 hodin od zjištění kybernetického bezpečnostního incidentu písemně (např. e-mailem) informovat o způsobu nápravy takovéto incidentu, a není-li možné v dané lhůtě nápravu zajistit, informovat rovněž o nejbližším možném termínu nápravy, který musí být Objednatelem odsouhlasen. Stejnou informační povinnost dle tohoto odstavce má Poskytovatel v případě, kdy dojde při plnění této smlouvy k situaci, která může mít pro Objednatele významné dopady, které by mohly být srovnatelné s kybernetickým bezpečnostním incidentem;
   f) při výkonu své činnosti včas a prokazatelně (písemně) upozornit Objednatele na zřejmou nevhodnost jeho příkazů či doporučení vztahujících se k bezpečnostním opatřením a jejichž následkem může vzniknout újma nebo nesoulad s platnými a účinnými právními předpisy či jinými předpisy vztahujícími se k poskytování služeb dle této Smlouvy.
2. Poskytovatel je povinen v rámci Plnění nebo Služby podpory zajistit:
   a) logování technických dat Informačního systému na navržené infrastruktuře, která jsou nutná mj. pro dohled a servis, ale také na základě plnění ZKB
   b) zajistit zaznamenávání událostí Informačního systému a jeho uživatelů a administrátorů dle ustanovení §22 VKB, přístupů do Informačního systému.

   Poskytovatel je povinen návrhem infrastruktury zajistit možnost logy uchovávat po dobu 18 měsíců a/nebo je poskytnout Objednateli ve strojově zpracovatelné formě k dalšímu zpracování a/nebo uchování. Logy musí být přístupné určeným osobám Objednatele. Technické logy nesmí obsahovat osobní údaje.

3. Poskytovatel se zavazuje, že data objednatele, která jsou svým obsahem citlivá, nebudou prodávajícím při poskytovaní plnění mimo technické a programové prostředky Objednatele. Za citlivá data se považují všechny osobní údaje dle specifikace zák. č. 110/2019, o zpracování osobních údajů, ve znění pozdějších předpisů, a ta data, která Objednatel označil jako citlivá formou písemného sdělení Poskytovateli. Objednatel se zavazuje, že data označena jako citlivá, nebude Poskytovateli jakoukoliv formou zasílat (případně zaslané osobní údaje vždy anonymizuje). Pokud k tomu přesto dojde, provede Poskytovatel na vlastní náklady neprodleně výmaz (skartaci) těchto dat (u osobních údajů v nezbytných případech z důvodu plnění požadovaných služeb provede Poskytovatel jejich anonymizaci) a informuje o tom neprodleně písemné odpovědnou osobu Objednatele.

6. Sankce

1. Za prokázané porušení povinností Poskytovatele v oblasti kybernetické bezpečnosti zde uvedených nebo bezpečnostních pravidel uvedených v čl. 1, odst. 1 této Přílohy, uhradí Poskytovatel Objednateli smluvní pokutu ve výši 10.000,- Kč (slovy: deset tisíc korun českých) za každý jednotlivý případ porušení výše uvedených povinností Poskytovatele.

Příloha 5

Vzdálený přístup

I. Předmět přílohy o vzdáleném přístupu

1. Pro zajištění řádného plnění Poskytovatele a současně za účelem zajištění bezpečnosti vnitřní sítě Objednatele, jeho informačních systémů a komunikačních systémů (dále jen „informační systém“) sjednávají Objednatel s Poskytovatelem touto Přílohou podmínky pro přístup Poskytovatele do vnitřní sítě Objednatele prostřednictvím VPN Objednatele (dále jen „Podmínky“). Podmínkami jsou stanoveny vzájemné povinnosti smluvních stran, které souvisejí se vzdáleným přístupem Poskytovatele do vnitřní sítě Objednatele, k informačním systémům a informacím prostřednictvím VPN Objednatele (dále jen „VPN přístup“).
2. Za tímto účelem:
    a. Objednatel zřídí Poskytovateli VPN přístup a zajistí jeho dostupnost po určenou dobu, za podmínek dále uvedených v této Příloze.
    b. VPN přístup bude Poskytovatelem využíván pouze prostřednictvím osob, které Poskytovatel předem určil a nahlásil zde popsaným způsobem straně Objednatele. Tyto osoby se podílejí nebo budou podílet na plnění závazků Poskytovatele podle Přílohy a Smlouvy (dále jen „zaměstnanec Poskytovatele“). Definice zaměstnance Poskytovatele je využívána i ve vztahu k pracovníkům, kteří jsou vůči Poskytovateli v pozici poddodavatele či obdobném.
    c. VPN přístup bude Poskytovateli zřízen a ponechán pouze v případě, bude-li to pro Poskytovatele nezbytné pro plnění Smlouvy.

II. Zřízení VPN přístupu

1. Zřízením VPN přístupu Poskytovateli se rozumí proces, kterým je zaměstnanci Poskytovatele vytvořen uživatelský účet, pomocí kterého následně může přistupovat, prostřednictvím VPN klienta, do vnitřní sítě Objednatele prostřednictvím VPN Objednatele.
2. Poskytovatel musí žádat o zřízení VPN prostřednictvím formuláře „Žádost o zřízení/pozastavení/ukončení VPN přístupu Poskytovatele do vnitřní sítě Objednatele“ (dále jen „Žádost“), viz čl. VIII této Přílohy. Tato Žádost musí splňovat následující:
    a. Každá Žádost je vyplněna pro jednu konkrétní fyzickou osobu. V případě, že Poskytovatel hromadně požaduje přístup pro více zaměstnanců, vyplní pro každého z nich zvlášť body dle čl. VIII odst. 3 a 4 v rámci jedné Žádosti.
    b. Anonymní sdílené VPN nejsou povoleny.
    c. Poskytovatel může žádat o VPN přístup maximálně po dobu účinnosti Smlouvy.
3. Vyplněnou a podepsanou Žádost zašle Poskytovatel e-mailem na 2 adresy: na oprávněnou/kontaktní osobu dle Smlouvy a rovněž na adresu it@mnof.cz. Žádost musí být podepsaná uznávaným elektronickým podpisem oprávněné osoby uvedené ve

Smlouvě za Poskytovatele. E-mailovou zprávu zasílá Poskytovatel nejpozději 5 pracovních dnů před datem, od kterého Poskytovatel požaduje zřídit zaměstnanci Poskytovatele VPN přístup.

4. Poskytovatel odpovídá za to, že všechny údaje uvedené v Žádosti jsou správné a platné. V případě, že dojde ke změně některého údaje uvedeného v Žádosti, je Poskytovatel povinen nejpozději do 7 kalendářních dnů od změny předložit novou Žádost s vyznačením požadovaných změn.
5. Objednatel doručenou Žádost posoudí z hlediska potřebnosti VPN přístupu pro předmětné plnění Poskytovatele, formálních a věcných náležitostí, případně požádá Poskytovatele o doplnění (opravu) Žádosti.
6. Objednatel zašle Poskytovateli a zaměstnanci Poskytovatele prostřednictvím e-mailu informaci o schválení/neschválení Žádosti.
    a. V případě neschválení Žádosti Objednatel poskytne zdůvodnění.
    b. V případě schválení Žádosti zasílá Objednatel následně na e-mailovou adresu zaměstnance Poskytovatele též informace potřebné pro nastavení VPN přístupu, tj. postup, jakým způsobem se zaměstnanec Poskytovatele připojí přes VPN do prostředí Objednatele.
7. Objednatel zasílá zaměstnanci Poskytovatele na jeho e-mailovou adresu uvedenou v Žádosti přidělené uživatelské jméno a zároveň na jeho mobilní telefonní číslo uvedené v Žádosti heslo.

III. Pozastavení VPN přístupu

1. Pozastavením VPN přístupu se rozumí proces na straně Objednatele, kterým Objednatel z dále uvedených důvodů dočasně znemožní zaměstnanci Poskytovatele přístup do vnitřní sítě Objednatele.
2. Objednatel si vyhrazuje právo pozastavit zaměstnanci Poskytovatele VPN přístup v případě zjištění porušení nebo podezření na nedodržení některého ustanovení této Přílohy a také Smlouvy, příp. při nereagování na validační e-mail nebo při podezření na kybernetickou bezpečnostní událost související s osobou zaměstnance Poskytovatele/Poskytovatele, příp. VPN přístupem (dále jen „Událost“);
3. Po vyhodnocení Události informuje Objednatel Poskytovatele o opětovném umožnění VPN přístupu zaměstnanci Poskytovatele nebo o ukončení VPN přístupu zaměstnanci Poskytovatele, přičemž uvede zdůvodnění svého postupu a své zjištění.
4. Poskytovatel může požádat o pozastavení VPN přístupu zaměstnanci Poskytovatele prostřednictvím zaslání Žádosti dle čl. II. odst. 2 Přílohy.

IV. Ukončení VPN přístupu

1. Ukončením VPN přístupu se rozumí proces, při kterém je Poskytovateli/zaměstnanci Poskytovatele trvale zablokován přístupu do vnitřní sítě Objednatele prostřednictvím VPN Objednatele.
2. Objednatel ukončí Poskytovateli/ zaměstnanci Poskytovatele VPN přístup:
    a. v případě uplynutí doby, na kterou byl VPN přístup podle Žádosti schválen;

b. dnem ukončení účinnosti Smlouvy;
c. na základě žádosti Poskytovatele;
d. na základě žádosti zaměstnance Poskytovatele;
e. po příslušném vyhodnocení Události;
f. na základě žádosti Poskytovatele dle odst., písm. 3.d, 3.e, 3.f tohoto článku.

3. Poskytovatel je povinen vždy na e-mail: kb@mnof.cz a současně na it@mnof.cz a současně telefonicky na tel. [redacted] (Objednatel vyžaduje triplicitní informaci, tedy telefonem a dvojím e-mailem), bezodkladně informovat Objednatele v případech, když:
   a. došlo k podezření na kompromitaci přihlašovacího hesla k přidělenému uživatelskému jménu zaměstnance Poskytovatele sloužícímu pro VPN přístup;
   b. došlo k podezření na ztrátu/odcizení nebo ke ztrátě/ odcizení koncového zařízení zaměstnanci Poskytovatele, z něhož realizuje VPN přístup;
   c. došlo k podezření na kompromitaci nebo ke kompromitaci interních informačních systémů a/nebo komunikačních systémů Poskytovatele;

   bezodkladně žádat Objednatele o ukončení VPN přístupu v případech, když:

   d. došlo/dojde k ukončení smluvního vztahu mezi zaměstnancem Poskytovatele a Poskytovatelem;
   e. zaměstnanec Poskytovatele se přestal/přestane podílet na plnění závazků Poskytovatele v rámci podílení se na Plnění a Službách pro Objednatele sjednaných Smlouvou;
   f. došlo/dojde k ukončení smluvního vztahu mezi Poskytovatelem a jeho poddodavatelem, je-li zaměstnanec Poskytovatele ve smluvním vztahu k tomuto poddodavateli.
4. Odpovědnost za veškeré činnosti realizované pod přiděleným účtem příslušného zaměstnance Poskytovatele ve vnitřní síti Objednatele nese do splnění příslušné povinnosti dle odst. 3 tohoto článku Poskytovatel.
5. VPN přístup bude v případech uvedených:
   a. pod odst., písm. 2.a. nebo 2.b tohoto článku ukončen příslušným dnem;
   b. pod odst., písm. 2.c nebo 2.d tohoto článku do 3 pracovních dnů od doručení žádosti o ukončení VPN přístupu, pokud nebude v žádosti o ukončení VPN přístupu požadováno pozdější datum ukončení;
   c. pod odst., písm. 2.e nebo 2.f tohoto článku po vyhodnocení Události /po doručení žádosti Objednateli.
6. V případě ukončení VPN přístupu dle odst., písm. 2.d tohoto článku je zaměstnanec Poskytovatele povinen o této skutečnosti neprodleně informovat Poskytovatele; splnění této jeho povinnosti si zajistí Poskytovatel.

V. Povinnosti Poskytovatele a zaměstnance Poskytovatele

1. Poskytovatel je povinen dodržovat všechna ustanovení této Přílohy a zajistit jejich dodržování jednotlivými zaměstnanci Poskytovatele.

2. Poskytovatel je povinen:
    a. prokazatelně seznámit zaměstnance Poskytovatele s právy a povinnostmi vyplývajícími pro něj z této Přílohy a prokazatelně zaměstnance Poskytovatele poučit o jeho povinnostech uvedených v této Příloze, a to nejpozději v den podání příslušné Žádosti a na vyzvání Objednatele tuto skutečnost také Objednateli ve lhůtě uvedené v příslušné písemné výzvě, která nebude kratší než 5 pracovních dnů, doložit;
    b. zajistit, aby zaměstnanec Poskytovatele dodržoval povinnosti a postupy vyplývající pro něj z této Přílohy;
    c. zajistit, že jsou zaměstnancem Poskytovatele dodržována taková bezpečnostní opatření, která zamezí narušení nebo ohrožení bezpečnosti vnitřní sítě Objednatele, informačního systému a informací Objednatele.
3. Objednatel je oprávněn kontrolovat plnění ustanovení této Přílohy na straně Poskytovatele. Poskytovatel je povinen poskytnout Objednateli nezbytné podklady, součinnost, případně umožnit kontrolu na místě.
4. Poskytovatel je dále povinen zajistit, aby zaměstnanec Poskytovatele realizoval VPN přístup pouze z koncového zařízení, které:
    a. je chráněno antivirovou a antimalwarovou ochranou a má aktuální virovou databázi;
    b. má instalováno a má aktivní (zapnuto) firewallové řešení operačního systému a/nebo HIDS/HIPS (Host Intrusion Detection System/ Host Intrusion Prevention System jsou řešení, která umožňují ochránit uživatele, operační systém a data před útoky po síti a před škodlivým kódem);
    c. má instalovány dostupné bezpečnostní záplaty a aktualizace zveřejněné výrobcem operačního systému a aplikací a operační systém je podporovaný výrobcem;
    d. má nastaveno uzamčení koncového zařízení v případě nečinnosti zaměstnance Poskytovatele;
    e. má chráněn přístup do BIOS koncového zařízení;
    f. má šifrován pevný disk koncového zařízení minimálně v případě práce s osobními údaji Objednatele;
    g. umožňuje přístup ke koncovému zařízení pouze po zadání přihlašovacích údajů.
5. Povinnosti zaměstnance Poskytovatele:
    a. realizovat přístup do vnitřní sítě Objednatele pouze prostřednictvím VPN Objednatele;
    b. pro přístup do vnitřní sítě Objednatele používat jako přihlašovací heslo unikátní, tj. heslo, které není shodné s jinými hesly používanými zaměstnancem Poskytovatele (kdekoliv);
    c. nesmí sdílet s třetími osobami své přístupové údaje určené pro VPN přístup;
    d. nesmí sdílet VPN připojení s jiným zařízením prostřednictvím sdílení připojení na síťové úrovni;
    e. neukládat své přihlašovací údaje pro VPN přístup do koncového zařízení;

f. nezasahovat do konfiguračních souborů a nastavení VPN klienta dodaného ze strany Objednatele;
g. ukončit VPN přístup (navázané spojení) v případě, že koncové zařízení nechává bez dozoru;
h. nepokoušet se narušit bezpečnost vnitřní sítě Objednatele;
i. bezodkladně žádat Objednatele prostřednictvím tel.: [redacted] a e-mailů: it@mnof.cz a kb@mnof.cz (Objednatel výslovně vyžaduje triplicitní žádost, tedy telefonem a dvojicí e-mailů):
    i. zablokování přístupových údajů sloužících k VPN přístupu v případě podezření na kompromitaci/ ztrátu/odcizení koncového zařízení nebo přístupových údajů;
    ii. zablokování přístupových údajů k VPN přístupu v případě zjištění dalších hrozeb narušení bezpečnosti vnitřní sítě Objednatele, např. výskyt spywaru.
j. chránit informace získané při VPN přístupu, a to i tehdy, pokud přímo nesouvisejí s plněním dle Přílohy a Smlouvy;
k. zachovávat mlčenlivost o všech skutečnostech, se kterými se seznámil v rámci plnění Přílohy a Smlouvy a které nejsou veřejně známé nebo veřejně dostupné;
l. vzít na vědomí, že Objednatel je oprávněn monitorovat přístupy zaměstnance Poskytovatele do informačních systémů a vnitřní sítě Objednatele a je oprávněn pozastavit/ukončit zaměstnanci Poskytovatele VPN přístup v případě nesplnění jeho povinností a požadavků uvedených v této Příloze;
m. odpovědět na validační e-mail Objednatele nejpozději do 14 kalendářních dnů ode dne, kdy mu byl doručen. Objednatel přitom je povinen zaslat kopii validačního e-mailu souběžně i na oprávněnou/kontaktní osobu Poskytovatele.

6. Poskytovatel nese plnou odpovědnost za nedodržení povinností kterýmkoli zaměstnancem Poskytovatele daných zaměstnanci Poskytovatele touto Přílohou.

VI. Sankce

1. Pokud Poskytovatel nesplní své povinnosti stanovené v čl. V., odst. 2, písm. 2.a této Přílohy, tj. že ve lhůtě uvedené v příslušné písemné výzvě nedoloží Objednateli příslušné skutečnosti, a to ani přes dodatečnou písemnou výzvu Objednatele s poskytnutím přiměřené lhůtě k nápravě, je Poskytovatel povinen za každý den prodlení zaplatit Objednateli smluvní pokutu ve výši 500 Kč.
2. Za porušení jednotlivých povinností daných touto Přílohou Poskytovateli, které Poskytovatel neodstranil ani přes písemnou výzvu Objednatele s poskytnutím přiměřené lhůty k nápravě:
    a. v čl. IV., odst. 3, písm. 3.a až 3.f této Přílohy nebo
    b. v čl. V., odst. 1 nebo odst. 2, písm. 2.a této Přílohy (tj. že zaměstnance Poskytovatele neseznámí s jeho právy a povinnostmi nebo nepoučí zaměstnance Poskytovatele o jeho povinnostech vyplývajících pro zaměstnance Poskytovatele z této přílohy) nebo
    c. v čl. V., odst. 2, písm. 2.b nebo 2.c této Přílohy nebo

d. v čl. V odst. 5, písm. 5.a až 5.k Přílohy

je Poskytovatel povinen zaplatit Objednateli v každém jednotlivém případě porušení příslušné povinnosti smluvní pokutu ve výši 20 000,- Kč, a to i opakovaně.

3. Za porušení jednotlivých povinností stanovených touto Přílohou zaměstnanci Poskytovatele v čl. V., odst. 5, písm. 5.m této Přílohy, které Poskytovatel neodstranil ani přes písemnou výzvu Objednatele s poskytnutím přiměřené lhůty k nápravě, je Poskytovatel povinen zaplatit Objednateli v každém jednotlivém případě porušení příslušné povinnosti smluvní pokutu ve výši 5 000,- Kč, a to i opakovaně.
4. Pokud dojde současně k porušení jedné a téže povinnosti uložené touto Přílohou Poskytovateli i zaměstnanci Poskytovatele, lze příslušnou sankci uplatnit vůči Poskytovateli pouze jedenkrát; tím není vyloučena možnost opakovaného postihu Poskytovatele, pokud opětovně k porušení jedné a téže povinnosti dojde.

VII. Závěrečná ustanovení

1. Pokud není v této Příloze výslovně stanoveno jinak, komunikují Poskytovatel a Objednatel ve věci VPN přístupu prostřednictvím oprávněných/kontaktních osob uvedených ve Smlouvě.
2. V případě, že v době trvání Smlouvy bude nutné přijmout takové bezpečnostní opatření, které vyvolá potřebu upravit Podmínky, zejména bude-li se jednat o bezpečnostní opatření směřující ke zlepšení systému řízení bezpečnosti informací Objednatele, řešení kybernetického bezpečnostního incidentu a s tím spojené potřeby minimalizace vzniklého bezpečnostního rizika nebo o povinnost přijmout opatření vydané Národním úřadem pro kybernetickou a informační bezpečnosti dle zákona č. 264/2025 Sb., o kybernetické bezpečnosti, v aktuálním znění, zavazují se smluvní strany vyvinout maximální součinnost směřující k uzavření dodatku k Příloze, kterým budou tyto Podmínky odpovídajícím způsobem upraveny.

VIII Žádost o zřízení/pozastavení/ukončení VPN přístupu Poskytovatele do vnitřní sítě Objednatele

Žádost obsahuje tyto povinné položky v daném pořadí a s daným číslováním:

1. Evidenční číslo Smlouvy, na základě které je/byl/bude VPN přístup pro Poskytovatele prostřednictvím zaměstnance Poskytovatele požadován
2. Poskytovatel: Jméno a příjmení oprávněné osoby Poskytovatele dle Smlouvy
3. Fyzická osoba, pro niž je/byl/bude VPN přístup požadován (zaměstnanec Poskytovatele):
    a. Jméno, Příjmení, titul
    b. Mobilní telefon, E-mail
    c. Zdůvodnění potřebnosti zřízení/pozastavení/ukončení VPN přístupu ve vztahu k dále uvedenému vybavení
    d. Fyzická osoba je
        i. zaměstnancem Poskytovatele: Ano/Ne

ii. poddodavatele: *doplňte název poddodavatele*

4. Seznam systémů, pro které je/byl/bude zřízen/zrušen VPN přístup:
   a. Název systému
      i. Server / IP adresa systému / použitá technologie (protokol) vzdáleného přístupu
      ii. Platnost od-do
      iii. Stav: zřídit **Nové** připojení, ponechat **Stávající** připojení, **Ukončení** stávajícího připojení
   b. Případně doplňte název dalšího systému s upřesňujícím členěním bodů i, ii, a iii.
5. Datum a podpis oprávněné osoby uvedené ve Smlouvě na straně Poskytovatele.

Seznam poddodavatelů

pro veřejnou zakázku: **Zajištění standardů kybernetické bezpečnosti v Městské nemocnici Ostrava**
zadávanou zadavatelem: Městská nemocnice Ostrava, příspěvková organizace

Dodavatel:

Aricoma Systems, a. s.
IČ: 04308697
Hornopolní 3322/34 70200 Ostrava Moravská Ostrava

tímto čestně prohlašuje, že pro plnění výše uvedené veřejné zakázky jsou mu známi tito poddodavatelé:

Identifikace poddodavatele	
Název poddodavatele *(název, obchodní firma, příp. jméno a příjmení)*	IXPERTA s.r.o.
IČ	27599523
Sídlo	Lihovarská 1060/12 19000 Praha Libeň
Část veřejné zakázky, kterou bude poddodavatel plnit	Prokázání technická kvalifikace dle ust. § 79 ZZVZ

V Ostravě dne 5.1.2026

…….
[redacted]ditel regionálního centra

Příloha č. 7 Realizační tým

Jméno a příjmení člena realizačního týmu, který se bude podílet na plnění veřejné zakázky	**Uvedení pozice v realizačním týmu při plnění veřejné zakázky s uvedením jeho expertní znalosti**	**Kontaktní e-mail**
[redacted]	vedoucí realizačního týmu (projektový manažer) PRINCE2	[redacted]
	Technický konzultant – specialista na firewally (CCSM)	
	Technický konzultant – specialista na firewally (CCSM)	
	Technický konzultant – specialista na ochranu koncových stanic	
	Technický konzultant – specialista na ochranu koncových stanic (Palo Alto Networks Micro-Credential Cortex XDR Support-Engineer certificate)	
	Technický konzultant – specialista na datová centra (VCP)	om
	Technický konzultant – specialista na datová centra (VCP, Qumulo solution architekt)	

[redacted]	Bezpečnostní specialista (CompTIA Security+)	[redacted]
	Architekt infrastrukturních řešení (Archimate)	