Evidenční číslo smlouvy: 0625/2025/OIKT/1100

SMLOUVA NA ZAJIŠTĚNÍ DODÁVEK SW A HW V RÁMCI POSÍLENÍ KYBERNETICKÉ BEZPEČNOSTI

Smluvní strany:

Městská část Praha 14

se sídlem: Bratří Venclíků 1073, Černý Most, 198 00 Praha

IČO: 00231312, DIČ: CZ00231312

bank. spojení: PPF banka a.s.

č. účtu: 27-9800050998/6000

zastoupená: Jiřím Zajacem, starostou městské části

(dále jen „**Objednatel**“)

a

Next Generation Security Solutions s.r.o.

se sídlem: U Uranie 954/18, Holešovice, 170 00 Praha 7

IČO: 06291031, DIČ: CZ06291031

společnost zapsaná v obchodním rejstříku vedeném Městským soudem v Praze,

oddíl C, vložka 279627

bank. spojení: ČSOB a.s.

č. účtu: 301607295/0300

zastoupená: Mgr. Ondřejem Dedekem, jednatelem společnosti

(dále jen „**Dodavatel**“)

(Objednatel a Dodavatel dále společně jen „**Smluvní strany**“ anebo samostatně „**Smluvní strana**“)

dnešního dne uzavřely tuto Smlouvu v souladu s ustanovením § 1746 odst. 2
zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
(dále jen „**OZ**“ a „**Smlouva**“)

Smluvní strany, vědomy si svých závazků obsažených v této Smlouvě a s úmyslem být touto Smlouvou vázány, se dohodly na následujícím znění Smlouvy:

1. PREAMBULE

1.1 Objednatel prohlašuje, že:

1.1.1 je veřejnoprávní korporací;

1.1.2 splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené;

1.1.3 má zájem na uzavření této Smlouvy s odborníkem v oboru informačních technologií s dostatečnými zkušenostmi a know-how v oblasti Dodávky a zajištění Podpory výrobce a Provozní podpory (jak jsou tyto pojmy definovány níže) za podmínek dále stanovených v této Smlouvě.

1.2 Dodavatel prohlašuje, že:

1.2.1 je podnikatelem dle ustanovení § 420 a násl. OZ;

1.2.2 splňuje veškeré podmínky a požadavky ve Smlouvě stanovené a je oprávněn Smlouvu uzavřít a řádně plnit závazky v ní obsažené;

1.2.3 ke dni uzavření Smlouvy vůči němu není vedeno řízení dle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení, ve znění pozdějších předpisů, a zároveň se zavazuje Objednatele o všech skutečnostech o hrozícím úpadku bezodkladně informovat;

1.2.4 se náležitě seznámil se všemi podklady, které byly součástí zadávací dokumentace veřejné zakázky s názvem *„Posílení kybernetické bezpečnosti“* včetně všech jejich příloh (dále jen „**Veřejná zakázka**“) a které stanovují požadavky na plnění dle Veřejné zakázky; zadávací dokumentace je ke dni uzavření Smlouvy dostupná na profilu Objednatele jako zadavatele;

1.2.5 je odborně způsobilý ke splnění všech svých závazků podle Smlouvy, zejména je odborníkem v oboru informačních technologií se specializací na dodávky, zajištění jeho podpory a poskytování doprovodných služeb dle této Smlouvy a je plně seznámen s charakteristikami, funkčnostmi, technologiemi poptávanými Objednatelem. Dodavatel je proto připraven plnit své povinnosti vyplývající ze Smlouvy a dodat Objednateli HW a SW dle této Smlouvy v souladu s principy Best Industry Practice dle svého nejlepšího vědomí, ve prospěch Objednatele a s ohledem na šetření nákladů Objednatele;

1.2.6 se detailně seznámil s rozsahem a povahou plnění dle Veřejné zakázky, a to tak, že jsou mu známy veškeré relevantní technické, kvalitativní a jiné podmínky nezbytné k realizaci této Smlouvy a že disponuje takovými kapacitami a odbornými znalostmi, které jsou nezbytné pro realizaci této

Smlouvy za dohodnuté smluvní ceny uvedené ve Smlouvě, a to rovněž ve vazbě na jím prokázanou kvalifikaci pro plnění Veřejné zakázky;

1.2.7 jím poskytované plnění dle této Smlouvy odpovídá všem požadavkům vyplývajícím z platných právních předpisů, které se na plnění vztahují.

1.3 Pojmy s velkými počátečními písmeny definované ve Smlouvě budou mít význam, jenž je jim ve Smlouvě, včetně jejích příloh a dodatků, připisován.

1.4 Objednatel oznámil dne 21. 9. 2025 oznámením otevřeného řízení svůj záměr zadat Veřejnou zakázku dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**"), kdy Objednatel v zadávacím řízení vyhodnotil nabídku Dodavatele jako nejvhodnější ze všech hodnocených nabídek podaných v rámci Veřejné zakázky. Objednatel se rozhodl realizovat Veřejnou zakázku prostřednictvím Dodavatele a Dodavatel je ochoten se na realizaci podílet v souladu s podmínkami stanovenými v této Smlouvě a zadávacími podmínkami Veřejné zakázky.

2. ÚČEL SMLOUVY

2.1 Účelem této Smlouvy je realizace Veřejné zakázky dle zadávacích podmínek Veřejné zakázky, tedy zejména zajištění podmínek pro dodávku a implementaci (nasazení, nastavení) SW a HW nástrojů systému zabezpečení IT infrastruktury posilující celkovou kybernetickou bezpečnost Objednatele, zajištění/poskytnutí dalších souvisejících služeb včetně dopravy, instalace, úvodní inicializace SW a HW v prostorách Objednatele, dodání veškeré související dokumentace k HW a SW, zaškolení ICT administrátorů Objednatele, zajištění provozní podpory a podpory výrobce uvedených částí HW a SW nástrojů systému, to vše v souladu s požadavky Objednatele definovanými touto Smlouvou a zadávacími podmínkami Veřejné zakázky.

2.2 Účelem Smlouvy je dále naplnění cílů a realizace části projektu Národního plánu obnovy „Posílení kybernetické bezpečnosti Úřadu městské části Praha 14", registrační číslo projektu: CZ.31.2.0/0.0/0.0/24_145/0011561 (dále jen „**Projekt**").

2.3 Dodavatel touto Smlouvou garantuje Objednateli splnění zadání Veřejné zakázky a všech z toho vyplývajících podmínek a povinností podle zadávací dokumentace Veřejné zakázky. Tato garance je nadřazena ostatním podmínkám a garancím uvedeným v této Smlouvě. Pro vyloučení jakýchkoliv pochybností to znamená, že:

2.3.1 v případě jakékoliv nejistoty ohledně výkladu ustanovení této Smlouvy budou tato ustanovení vykládána tak, aby v co nejširší míře zohledňovala účel Veřejné zakázky vyjádřený zadávací dokumentací Veřejné zakázky;

2.3.2 v případě chybějících ustanovení této Smlouvy budou použita dostatečně konkrétní ustanovení zadávací dokumentace Veřejné zakázky;

2.3.3 v případě rozporu ustanovení libovolné Přílohy této Smlouvy s textem uvedeným ve Smlouvě, bude použito ustanovení této Smlouvy;

2.3.4 Dodavatel je vázán svou nabídkou předloženou Objednateli v rámci zadávacího řízení na zadání Veřejné zakázky, která se pro úpravu vzájemných vztahů vyplývajících z této Smlouvy použije subsidiárně.

3. PŘEDMĚT SMLOUVY

3.1 Předmětem této Smlouvy je poskytnutí plnění spočívající v komplexní dodávce a službách implementace a uvedení do provozu hardwarových a softwarových technologií včetně poskytnutí souvisejících služeb, zejména instalace, konfigurace, migrace a integrace, implementační podpory, školení administrátorů, zpracování provozní a bezpečnostní dokumentace a zajištění technické podpory výrobce/dodavatele dle odst. 3.2 této Smlouvy (dále jen „**Plnění**"), přičemž detailní specifikace Plnění je blíže určena v **Příloze č. 1** této Smlouvy, tj. v Technické specifikaci a v dalších přílohách této Smlouvy.

3.2 Předmět Plnění Dodavatele se skládá především z:

3.2.1 **dodání hardware (HW)** – zařízení a vybavení vymezených v **Příloze č. 1** této Smlouvy, a to včetně tam samostatně uvedených jednotlivých zařízení, přičemž toto plnění zahrnuje dopravu, instalaci, úvodní inicializaci v místě vymezeném v čl. 4 této Smlouvy a dodání veškeré související dokumentace (dále vše souhrnně jen „**hardware**" nebo „**dodávka hardware**");

3.2.2 **poskytnutí software (SW)** – programové vybavení, sady počítačových programů, systémový software, aplikační software, spadající svojí povahou a vlastnostmi mezi software, a včetně zajištění požadované licence k příslušnému software (dále vše souhrnně jen „**software**" nebo „**dodávka software**") za podmínek stanovených v této Smlouvě a **Příloze č. 1** této Smlouvy;

(dodávka hardware a dodávka software dále společně jako „**Dodávka**")

3.2.3 **poskytnutí služeb** – implementace a instalace software a hardware v rozsahu uvedeném v **Příloze č. 1** této Smlouvy, zaškolení zaměstnanců Objednatele či jím pověřených osob, minimálně v rozsahu nezbytném pro převzetí a správu předmětné Dodávky, uplatňování nároků na poskytování Podpory výrobce a Provozní podpory vymezené níže v odst. 3.2.4 a 3.2.5 této Smlouvy a možnosti zadávat požadavky přes webové rozhraní, telefonicky nebo e-mailem (dále jen „**Služby**");

3.2.4 **zajišťování podpory výrobce** po dobu stanovenou v **Příloze č. 2**, blíže specifikované v této Smlouvě a **Příloze č. 1 a Příloze č. 8** této Smlouvy, a to pro veškerý hardware dle odst. 3.2.1 a software dle odst. 3.2.2 této Smlouvy dodaný Dodavatelem Objednateli na základě této Smlouvy (dále jen „**Podpora výrobce**");

3.2.5 **zajišťování provozní podpory** v rozsahu činností dle čl. 5.23 po dobu stanovenou v **Příloze č. 2** této Smlouvy (dále jen „**Provozní podpora**");

(Podpora výrobce a Provozní podpora dále společně jako „**Podpora**")

3.3 Objednatel se zavazuje zaplatit Dodavateli dohodnutou cenu za řádně a včas poskytnuté Plnění a za řádně a včas poskytnutou Podporu výrobce a Provozní podporu, to vše za podmínek dále stanovených touto Smlouvou.

3.4 Dodavatel se zavazuje alokovat na poskytování Plnění dle této Smlouvy kapacity členů realizačního týmu Dodavatele a poskytovat Plnění dle Smlouvy za účasti členů realizačního týmu uvedeného v **Příloze č. 6** této Smlouvy, jimiž Dodavatel prokázal svou kvalifikaci v zadávacím řízení Veřejné zakázky. Alokací kapacity se rozumí dostupnost kteréhokoliv člena realizačního týmu nebo jeho odpovídajícího náhradníka, jenž má minimálně stejnou kvalifikaci jako nahrazovaný člen. Jakákoliv dodatečná změna členů realizačního týmu musí být předem projednána a písemně schválena Objednatelem, přičemž změna bude Objednatelem schválena v případě, že Dodavatel nahradí osobu realizačního týmu takovou osobou, která prokazatelně disponuje znalostmi a odbornou kvalifikací alespoň na úrovni, která byla u nahrazované osoby hodnocena v rámci zadávacího řízení Veřejné zakázky.

3.5 Dodavatel se zavazuje poskytovat Plnění či poskytovat Podporu výrobce či Provozní podporu sám, nebo s využitím poddodavatelů uvedených v **Příloze č. 4** této Smlouvy. Jakákoliv dodatečná změna osoby poddodavatele nebo rozsahu Plnění svěřeného poddodavateli musí být předem písemně schválena Objednatelem, ledaže by plnění původně svěřené poddodavateli realizoval Dodavatel sám. Smluvní strany výslovně uvádějí, že při poskytování Plnění prostřednictvím jakékoliv třetí osoby dle tohoto odstavce má Dodavatel odpovědnost, jako by poskytování Plnění realizoval sám.

4. DOBA A MÍSTO PLNĚNÍ

4.1 Dodavatel se touto Smlouvou zavazuje provést Plnění dle harmonogramu uvedeném v **Příloze č. 2** této Smlouvy (dále jen „**Harmonogram**“).

4.2 Místem plnění jsou prostory Objednatele na následujících adresách:

4.2.1 Bratří Venclíků 1073/8, 198 00 Praha 14 – Černý Most;

4.2.2 Bratří Venclíků 1072/6, 198 00 Praha 14 – Černý Most;

4.2.3 Bratří Venclíků 1070/2, 198 00 Praha 14 – Černý Most;

případně též jiné prostory dle **Přílohy č. 1** a dle potřeby a výslovného pokynu Objednatele.

4.3 Pokud to povaha Plnění této Smlouvy umožňuje a Objednatel vůči tomu nemá výhrady, je Dodavatel oprávněn provádět relevantní části Plnění vzdáleným přístupem.

5. ZPŮSOB PLNĚNÍ

Obecné požadavky na Plnění

5.1 Dodavatel se touto Smlouvou zavazuje provést pro Objednatele Plnění, a to v rozsahu a za podmínek dle této Smlouvy a jejích příloh.

5.2 Dodavatel prohlašuje, že veškeré dodávané Plnění je získáno legálně a umožňuje využití těchto hardware a software Objednatelem, jakožto koncovým zákazníkem, v souladu s distribučními a licenčními podmínkami výrobce zařízení. Dodavatel dále prohlašuje, že Plnění pochází z autorizovaného prodejního kanálu výrobce.

5.3 Dodavatel prohlašuje, že pro dodávané Plnění Objednateli, jakožto koncovému zákazníkovi, platí, že Objednatel není nijak omezen ve svých nárocích vyplývajících ze záruky výrobce dodávaného zařízení (má prokazatelnou záruku výrobce) a z Podpory výrobce (splňuje podmínky pro poskytování Podpory výrobce), kterou tento výrobce k dodávaným hardware a software produktům poskytuje. Dodavatel dále prohlašuje, že u Plnění je zajištěna evidence prodaného zařízení u výrobce pro poskytnutí budoucí podpory či záruky výrobcem.

5.4 Dodavatel prohlašuje, že Plnění obsahuje kompatibilní software výrobce s platnou licencí a servisní podporou výrobce a splňuje podmínky předpisů EU ohledně paralelního importu.

5.5 Dodavatel doloží Objednateli (současně s dodávkou hardware a dodávkou software dle Smlouvy) potvrzení výrobce, že dodávané Plnění (seznam sériových čísel) je určeno pro koncového zákazníka pro využití na území České republiky a že má Objednatel k tomuto Plnění zajištěnou Podporu výrobce. Pokud v databázi výrobce bude uveden jiný koncový uživatel než Objednatel, bude se jednat o porušení podmínky originálního a nového zařízení (viz níže odst. 5.6 této Smlouvy).

Dodávka hardware ve smyslu odst. 3.2.1 Smlouvy

5.6 Dodavatel se zavazuje dodat Objednateli v rámci Plnění takový hardware, který bude:

5.6.1 nový, nepoužitý a nereparovaný;

5.6.2 plně funkční;

5.6.3 použitelný Objednatelem v České republice. Zejména v této souvislosti Dodavatel zaručuje Objednateli, že hardware získal veškerá nezbytná osvědčení pro užití v České republice, a to jak z pohledu obecně závazných právních předpisů, tak podmínek výrobce pro poskytování navazujících služeb maintenance. Dodavatel předá kopie těchto osvědčení při předání dodávky;

5.6.4 určený pro evropský trh, přičemž je Dodavatel povinen do sedmi (7) pracovních dnů od doručení žádosti Objednatele o předložení potvrzení výrobce o určení dodaného zboží pro evropský trh Objednateli předložit takové potvrzení nebo případně jiný doklad výrobce prokazující pro dodaný hardware provozovaný na území České republiky poskytnutí plné Podpory a záruky výrobce při řešení technických problémů;

5.6.5 mít jakost a provedení stanovené v této Smlouvě, zejména v **Příloze č. 1** této Smlouvy, přičemž změna v parametrech dodávky hardware je možná pouze v případě, že Dodavatel prohlásí, že určitý hardware či jeho součást se již nevyrábí, toto své tvrzení doloží Dodavatel potvrzením od výrobce. V takovém případě je Dodavatel povinen dodat hardware či jeho část (i) stejné modelové řady, (ii) od stejného výrobce a (iii) který původní hardware či jeho součást nahrazuje, je plně kompatibilní s původním hardwarem či jeho částí a IT prostředím Objednatele a má obdobnou funkčnost a výkon, minimálně v úrovni specifikace pro danou komponentu požadovanou Objednatelem v **Příloze č. 1** této Smlouvy;

5.6.6 v takové jakosti a kvalitě odpovídající účelu, k němuž se hardware obvykle užívá;

5.6.7 bez materiálových, konstrukčních, výrobních a vzhledových či jiných vad;

5.6.8 splňovat veškeré nároky a požadavky českého právního řádu, zejména zákona č. 541/2020 Sb., o odpadech, ve znění pozdějších předpisů (dále jen „**zákon o odpadech**“) a zákona č. 477/2001 Sb., o obalech, ve znění pozdějších předpisů;

5.6.9 dodán včetně všech souvisejících systémových licencí specifikovaných v **Příloze č. 1** této Smlouvy či jiných systémových licencí nezbytných k řádnému využívání hardware v rozsahu a za podmínek této Smlouvy vč. jejich příloh;

5.6.10 bezpečný, zejména že dodávky neobsahují radioaktivní materiály a jiné nebezpečné látky a věci, které se mohou stát nebezpečným odpadem ve smyslu zákona o odpadech;

5.6.11 ve vlastnictví Dodavatele a které je bez dalšího oprávněn na Objednatele převést;

5.6.12 není zatížen zástavními, předkupními, nájemními či jinými právy třetích osob.

5.7 Dodavatel se zavazuje provést dopravu hardware do místa plnění dle čl. 4 této Smlouvy Objednateli a provést v místě plnění dle čl. 4 této Smlouvy implementaci, instalaci a úvodní inicializaci hardware. Dodavatel je dále povinen:

5.7.1 provést instalaci, implementaci a úvodní inicializaci hardware způsobem umožňujícím jeho spuštění, dlouhodobé provozování a zapojení do IT prostředí Objednatele, včetně případné likvidace odpadů vzniklých při instalaci;

provést instalaci, implementaci a úvodní inicializaci hardware do doby stanovené v **Příloze č. 2** této Smlouvy.

Poskytování software k Dodavatelem dodanému hardware ve smyslu odst. 3.2.2 Smlouvy

5.8 Dodavatel zaručuje Objednateli, že dodaný software bude plně funkční a způsobilý pro použití k určenému účelu a pro užití v České republice, odpovídat **Příloze č. 1** této Smlouvy, bez faktických vad, a bude splňovat veškeré nároky a požadavky českého právního řádu.

5.9 Dodavatel prohlašuje, že software nemá žádné právní vady, zejména ohledně něj není veden žádný soudní spor, jsou uhrazeny všechny daně a poplatky týkající se software.

5.10 Dodavatel se zavazuje provést implementaci, instalaci software, a to v souladu s podmínkami Podpory výrobce dle **Přílohy č. 8** této Smlouvy, a to vše do doby dle **Přílohy č. 2** této Smlouvy.

Poskytování Služeb ve smyslu odst. 3.2.3 Smlouvy

5.11 Dodavatel provede implementaci a instalaci software a hardware v rozsahu uvedeném v **Příloze č. 1** této Smlouvy a v termínu dle **Přílohy č. 2** této Smlouvy.

5.12 Dodavatel provede prezenční zaškolení příslušných ICT administrátorů Objednatele pro dodaný hardware a software v rozsahu uvedeném v **Příloze č. 1** této Smlouvy a v termínu dle **Přílohy č. 2** této Smlouvy.

5.13 Součástí školení je i poskytnutí dokumentace pro provedení školení a komplexní administraci dodaného hardware a software Dodavatelem Objednateli a ICT administrátorům tak, aby na základě takové dokumentace byli ICT administrátoři absolvující školení schopni samostatně, bez zásahů Dodavatele, ovládat a administrovat hardware a software. Nebyla-li některá z částí dokumentace vytvořena/předána pro účely ostatních částí plnění, je Dodavatel povinen ji vytvořit tak, aby byl naplněn účel Školení.

5.14 Účelem provedení školení je seznámení ICT administrátorů s dodaným hardwarem a softwarem do té míry, aby jej byli schopni samostatně užívat v souladu se svým pracovním zařazením u Objednatele.

5.15 školení se bude konat v místě plnění dle čl. 4 této Smlouvy a v den zvolený Objednatelem, přičemž termín školení může být změněn dohodou Smluvních stran. školení se bude konat v pracovní den v běžné pracovní době ICT administrátorů mezi 8:00 a 16:00 v rozsahu dle **Přílohy č. 1** této Smlouvy. Nezúčastní-li se školení všichni určení ICT administrátoři, provede Dodavatel školení zbývajících ICT administrátorů v náhradním termínu. Počet administrátorů, kteří mají absolvovat školení, je čtyři, nestanoví-li **Příloha č. 1** této Smlouvy jinak.

5.16 Školení probíhá v českém nebo slovenském jazyce, přičemž dokumentace ke školení musí být rovněž v českém nebo slovenském jazyce.

Poskytování Podpory výrobce ve smyslu odst. 3.2.4 Smlouvy

5.17 Dodavatel je současně s dodávkou hardware dle Smlouvy a po dobu poskytování Podpory výrobce dle této Smlouvy povinen:

5.17.1 mít uzavřenou dohodu o podpoře s výrobcem hardware na všechen dodaný hardware tak, aby v případě závady na dodaném hardware, kterou není Dodavatel schopen sám odstranit, bylo možné eskalovat závadu přímo k výrobci hardware nebo jím pověřeného servisního partnera;

5.17.2 zajistit Objednateli přístup k dokumentaci výrobce hardware a znalostní bázi, kterou výrobce hardware v rámci své Podpory výrobce poskytuje;

5.17.3 zajistit přímý přístup k Podpoře výrobce, včetně možnosti si sám a přímo otevřít požadavek na Podporu výrobce, provádět změny priority požadavků a případné eskalace pracovníky Objednatele, a to po celou dobu, po kterou výrobce poskytuje na dané zařízení podporu;

5.17.4 pokrytí a garanci plné funkčnosti hardware a software, včetně jejich aktualizace a předplatného.

5.18 Po dobu poskytování Podpory výrobce je Dodavatel dále povinen:

5.18.1 poskytnout Objednateli všechny relevantní software releases a verze software nabízené výrobcem software tak, aby dodané řešení vyhovovalo zadání Objednatele a fungovalo bez závad;

5.18.2 informovat Objednatele o nových verzích a funkčnostech software, které mohou rozšiřovat dodané řešení způsobem, který Objednatel shledá ve shodě s potřebami dalšího rozvoje dodaného řešení (software);

5.18.3 zajistit službu hlášení softwarových chyb, které jsou oznámeny výrobcem; a

5.18.4 umožnit eskalaci vad k výrobci software.

5.19 Dodavatel je povinen zajistit dostupnost náhradních dílů od výrobce a dostupnost Provozní podpory pro dodané řešení.

5.20 Dodavatel je povinen zajistit Podporu výrobce v příslušném režimu dle **Přilohy č.1** této Smlouvy.

5.21 Dodavatel je povinen zajistit výměnu vadného hardware za nový s garantovanou dobou opravy v příslušném režimu dle **Přilohy č.1** této Smlouvy.

5.22 Smluvní strany se dohodly, že poskytování Podpory výrobce je rozděleno do jednotlivých období stanovených v **Příloze č. 2** této Smlouvy. V období, které je v **Příloze č. 2** určeno do 31. 5. 2026, je Podpora výrobce poskytována v rámci poskytování Služeb. V následujícím obdobím od 1. 6. 2026 vymezeném v **Příloze č. 2** je Podpora výrobce poskytována za účelem zajištění udržitelnosti celého řešení, a to v rozsahu a parametrech stanovených v **Příloze č. 1 a Příloze č. 8** této Smlouvy.

Poskytování Provozní podpory ve smyslu odst. 3.2.5 Smlouvy

5.23 Dodavatel se zavazuje po dobu sjednanou v této Smlouvě poskytovat Objednateli Provozní podporu dodaného Plnění, jejímž účelem je zajistit jeho dlouhodobou provozuschopnost a udržitelnost. Provozní podpora zahrnuje zejména poskytování aktualizací, přechodů na vyšší verze, nových verzí a bezpečnostních aktualizací, jakož i diagnostiku incidentů a provádění nápravných zásahů, a to v rozsahu specifikovaném v **Příloze č. 1** této Smlouvy. Dodavatel je povinen zajistit, aby aktualizace a upgrade nenarušily integritu a funkčnost řešení, a aby byla vždy zachována technologická návaznost a související dokumentace.

5.24 Smluvní strany se dohodly, že poskytování Provozní podpory je rozděleno do jednotlivých období stanovených v **Příloze č. 2** této Smlouvy. V období, které je v **Příloze č. 2** určeno do 31. 5. 2026, je Provozní podpora poskytována v rámci

poskytování Služeb. V následujícím obdobím od 1. 6. 2026 vymezeném v **Příloze č. 2** je Provozní podpora poskytována za účelem zajištění udržitelnosti celého řešení, a to v rozsahu a parametrech stanovených v **Příloze č. 1** této Smlouvy.

5.25 Úspěšné nasazení, předání nebo akceptace jednotlivých částí řešení ani samotné poskytování Provozní podpory nijak neomezují povinnost Dodavatele zajistit nápravu v případě, že budou zjištěny vady nebo nedostatky při výstupním auditu nebo v rámci doby udržitelnosti. Náprava se provede bez zbytečného odkladu a na náklady Dodavatele, pokud není ve Smlouvě výslovně sjednáno jinak.

6. SOUČINNOST OBJEDNATELE

6.1 Objednatel se zavazuje poskytnout Dodavateli ke splnění závazků dle této Smlouvy nezbytně nutnou součinnost, zejména se zavazuje oprávněné osoby Dodavatele včas informovat o organizačních změnách, poznatcích z kontrolní činnosti a dalších skutečnostech významných pro plnění předmětu Smlouvy.

6.2 V rámci součinnosti se Objednatel zavazuje umožnit Dodavateli užití vybraných hardware a software prostředků Objednatele, a to výhradně za účelem plnění předmětu této Smlouvy a pouze po dobu účinnosti této Smlouvy. Dodavatel se zavazuje užívat tyto prostředky řádně a v souladu s provozními a bezpečnostními postupy či pokyny Objednatele. Dodavatel se dále zavazuje, že nebude s těmito prostředky Objednatele nakládat nebo je používat v rozporu s touto Smlouvou.

6.3 Objednatel je povinen zajistit Dodavateli veškerou potřebnou součinnost zaměstnanců Objednatele nebo třetích stran zajišťujících pro Objednatele služby v oblasti ICT v rozsahu potřebném pro řádné plnění dle této Smlouvy. Nesplnění pokynů při plnění pouze v důsledku nezajištění výše uvedené součinnosti nebude považováno za porušení nebo nedodržení požadované kvality Plnění a nemůže být důvodem pro neakceptování výkazu plnění Objednatelem.

7. AKCEPTACE

7.1 Plnění dle této Smlouvy, tvořící logický a funkční celek, stejně jako každá část Plnění, které představuje samostatný předmět způsobilý přejímky (dále jen „**dílčí plnění**“), bude Objednatelem akceptováno na základě akceptační procedury. Akceptační procedura zahrnuje ověření, zda Dodavatelem poskytnuté Plnění je výsledkem, ke kterému se Dodavatel zavázal, a to porovnáním skutečných vlastností jednotlivých dílčích plnění Dodavatele s jejich závaznou specifikací uvedenou ve Smlouvě vč. jejich příloh za využití akceptačních kritérií zde stanovených nebo později pro tento účel dohodnutých Smluvními stranami.

7.2 Prostřednictvím akceptační procedury je prověřováno především:

7.2.1 řádné a úplné poskytnutí předmětného Plnění; a

7.2.2 plná funkčnost a úplnost požadovaných vlastností poskytnutého Plnění.

7.3 Předání a převzetí Objednatelem objednaného a Dodavatelem řádně provedeného dílčího plnění bude probíhat postupně akceptací jednotlivých dílčích

plnění, a to v termínech uvedených v této Smlouvě, resp. dle **Přílohy č. 2** této Smlouvy nebo po předchozí dohodě Smluvních stran a dle dále konkretizovaných kritérií specifikovaných dle **Přílohy č.1** této Smlouvy.

7.4 Akceptační procedura zahrnuje ověření řádného provedení jednotlivých dílčích plnění porovnáním jejich skutečných vlastností s jejich specifikací stanovenou Smlouvou; specifikací se rozumí i akceptační kritéria, jsou-li stanovena. Akceptační procedura zahrnuje také ověření, že dílčí plnění k danému dni plně odpovídá platné legislativě a že nevyžaduje provedení jeho údržby.

7.5 Akceptační procedura bude zahrnovat akceptační testy, které budou probíhat na základě specifikace akceptačních testů připravené Dodavatelem. Nedohodnou-li se Smluvní strany jinak, přípravu scénářů, příkladů a dat na akceptační test zajistí Dodavatel za přiměřené součinnosti Objednatele, a to s ohledem na účel akceptační procedury dle odst. 7.1 Smlouvy. Objednatel má právo vyjadřovat se a požadovat zapracování svých odůvodněných připomínek ke specifikaci akceptačních testů a dalším parametrům testování.

7.6 Dodavatel písemně (vč. e-mailu) vyzve Objednatele k účasti na akceptační proceduře nejméně tři (3) pracovní dny před jejím zahájením. Pokud se Objednatel nedostaví v termínu určeném pro provedení akceptačních testů, přestože byl Dodavatelem k účasti řádně vyzván, je Dodavatel oprávněn provést příslušné akceptační testy bez jeho přítomnosti. O průběhu akceptačních testů vyhotoví Dodavatel písemný záznam, v němž zejména uvede, zda testy prokázaly chyby. Objednateli budou poskytnuty originály veškerých dokumentů vypracovaných v souvislosti s provedením akceptačních testů.

7.7 Nestanoví-li specifikace akceptačních testů jinak, má se za to, že dílčí plnění splňuje stanovená akceptační kritéria za předpokladu, že toto dílčí plnění nemá žádnou vadu ve smyslu čl. 10 této Smlouvy. Objednatel je oprávněn dílčí plnění převzít i v případech, kdy počet a/nebo druh vad překračuje maximální počet stanovený pro splnění akceptačních kritérií.

7.8 Jestliže jednotlivé dílčí plnění splní akceptační kritéria akceptačních testů, Dodavatel se zavazuje nejpozději v pracovní den následující po ukončení akceptačních testů umožnit Objednateli toto dílčí plnění převzít a Objednatel se zavazuje k jeho převzetí nejpozději do tří (3) pracovních dnů. Smluvní strany se zavazují o tomto převzetí sepsat akceptační protokol.

7.9 Pokud kterékoliv z jednotlivých dílčích plnění nesplňuje stanovená akceptační kritéria nebo je splňuje s vadami, které jsou přípustné, sdělí Objednatel své připomínky písemně Dodavateli; pokud Objednatel takové dílčí plnění současně akceptuje, uvede své připomínky v akceptačním protokolu. Nesdělení připomínek nebo neoznámení některé vady při akceptaci nemá vliv na povinnost Dodavatele tuto vadu odstranit, pokud o ní ví, dodatečně ji zjistí či mu bude dodatečně oznámena.

7.10 Dodavatel je povinen vypořádat připomínky Objednatele bez zbytečného odkladu a neprodleně předložit příslušné dílčí plnění k opakované akceptaci dle této Smlouvy, za přiměřeného použití ostatních ustanovení tohoto čl. 7 Smlouvy. Akceptační procedura, včetně procesu testování a případných následných oprav,

se bude opakovat, dokud příslušné dílčí plnění nesplní akceptační kritéria pro příslušný akceptační test. V případě, že se jedná o vypořádání připomínek k dílčímu plnění, které již bylo akceptováno, namísto akceptačního protokolu Smluvní strany potvrdí písemně, že připomínky byly vypořádány.

7.11 Dohodnuté termíny pro akceptaci dílčího plnění nejsou dotčeny trváním akceptační procedury ani jakýmkoli jejím prodloužením z důvodu vad bránících akceptaci.

7.12 Nejpozději v den podpisu akceptačního protokolu jednotlivého dílčího plnění je Dodavatel povinen předat Objednateli veškerou dokumentaci k dodávanému dílčímu plnění.

8. CENA

Společná cenová ujednání:

8.1 Položkový rozpis ceny za Plnění je uveden v **Příloze č. 5** této Smlouvy.

8.2 Ceny poskytnutého Plnění jsou pro Smluvní strany závazné (nejvýše přípustné) po celou dobu účinnosti této Smlouvy. Tyto ceny bude možné překročit pouze v souvislosti se změnou daňových předpisů týkajících se DPH, a to nejvýše o částku odpovídající této legislativní změně.

8.3 Dodavatel výslovně prohlašuje, že cena za předmět Plnění poskytovaný Dodavatelem dle Smlouvy již v sobě bude zahrnovat veškeré náklady Dodavatele spojené s plněním dle této Smlouvy vč. nákladů na dopravu do místa plnění, nákladů na balení, cla, celních poplatků, licenčních a jiných poplatků. Ceny uvedené v **Příloze č. 5** této Smlouvy jsou cenami konečnými, nejvýše přípustnými a nemohou být změněny.

8.4 Cena za Plnění bude Objednatelem Dodavateli hrazena na základě daňového dokladu – faktury (dále jen „**faktura**"). Dodavatel předloží Objednateli fakturu až po řádné akceptaci příslušného Plnění Objednatelem. Objednatelem potvrzený akceptační protokol bude nedílnou přílohou každé faktury.

8.5 ***K ceně za Dodávek:***

8.5.1 Smluvní strany prohlašují, že celková cena za Dodávku dle Smlouvy uvedená v **Příloze č. 5** Smlouvy bude uhrazena na základě dílčích faktur po akceptaci příslušné dílčí Dodávky, tedy v dílčích splátkách.

8.5.2 Smluvní strany prohlašují, že cena za dodávku software je součástí ceny dodávky hardware dle této Smlouvy. Pokud je to možné je Dodavatel povinen uvést ve vystavené faktuře rozpis ceny na jednotlivé položky Dodávky, a to včetně vyčíslení ceny za dodávku software jakožto části ceny dodávky hardware.

8.6 ***K ceně Služeb:***

8.6.1 Smluvní strany prohlašují, že celková cena za Služby dle této Smlouvy uvedená v **Příloze č. 5** této Smlouvy, bude uhrazena na základě dílčích

faktur po akceptaci příslušné dílčí Dodávky a příslušné Služby k příslušné Dodávce dle **Přílohy č. 2** této Smlouvy, tedy v dílčích splátkách.

8.7 ***K ceně Podpory:***

8.7.1 Smluvní strany se dohodly, že poskytování Podpory je rozděleno do jednotlivých období stanovených v **Příloze č. 2** této Smlouvy. V období do 31. 5. 2026 je Podpora poskytována v rámci provádění jednotlivých opatření podle této Smlouvy a je zahrnuta v ceně Dodávek a Služeb; za toto období Dodavateli nenáleží samostatná úplata.

8.7.2 V následujícím období od 1. 6. 2026 vymezeném v **Příloze č. 2** této Smlouvy je Podpora poskytována jako samostatně hrazená služba. Cena za tato období je uvedena v **Příloze č. 5** této Smlouvy.

8.7.3 Cena Podpory podle odst. 8.7.2 je hrazena v dílčích splátkách, a to vždy jednou ročně (pro příslušné 12měsíční období poskytování Podpory), a to na základě faktury vystavené Dodavatelem vždy pro nadcházející období poskytování Podpory.

8.7.4 Faktura dle čl. 8.7.3 této Smlouvy může být vystavena Dodavatelem nejdříve dva (2) měsíce před počátkem výročí příslušného období poskytování Podpory.

Platební podmínky

8.8 Splatnost jednotlivých daňových dokladů – faktur se sjednává na třicet (30) dnů ode dne jejich doručení povinné Smluvní straně. Toto ustanovení se uplatní i v případě hrazení smluvních pokut. Cena bude považována za uhrazenou dnem odeslání příslušné částky z účtu Objednatele na účet Dodavatele.

8.9 Všechny faktury musí splňovat náležitosti řádného daňového dokladu požadované § 435 OZ a zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a vždy musí výslovně obsahovat následující údaje: označení Smluvních stran a jejich adresy, IČO, DIČ (je-li přiděleno), název Projektu, údaj o tom, že vystavovatel faktury je zapsán v obchodním rejstříku včetně spisové značky, označení této Smlouvy, označení poskytnutého Plnění, označení registračního čísla dotačního Projektu, jeho rozsah, jednotkovou a celkovou cenu, číslo faktury, den vystavení a lhůtu splatnosti faktury, označení peněžního ústavu a číslo účtu, na který se má platit, fakturovanou částku, razítko a podpis oprávněné osoby. Faktura bude vždy obsahovat příslušné dodací listy, akceptační protokoly vztahující se k jednotlivým částem Plnění a jiné přílohy požadované Objednatelem. Faktury budou znít na částku v české měně (Kč).

8.10 Nebude-li faktura obsahovat stanovené náležitosti a přílohy, nebo v ní nebudou správně uvedené údaje dle této Smlouvy, je Objednatel oprávněn vrátit ji ve lhůtě její splatnosti Dodavateli. V takovém případě se přeruší běh lhůty splatnosti a nová lhůta splatnosti počne běžet doručením opravené faktury.

8.11 Platby peněžitých částek se provádí bankovním převodem na účet druhé Smluvní strany uvedený ve faktuře. Peněžitá částka se považuje za zaplacenou okamžikem jejího odepsání z účtu odesílatele ve prospěch účtu příjemce.

8.12 Objednatel neposkytuje Dodavateli na předmět Plnění této Smlouvy jakékoliv zálohy.

8.13 V případě prodlení kterékoliv Smluvní strany se zaplacením peněžité částky vzniká oprávněné Smluvní straně nárok na úrok z prodlení v zákonné výši dlužné částky za každý i započatý den prodlení. Tím není dotčen ani omezen nárok na náhradu vzniklé újmy.

8.14 Objednatel bude hradit přijaté faktury pouze na bankovní účty Dodavatele zveřejněné správcem daně způsobem umožňujícím dálkový přístup ve smyslu § 96 odst. 2 zákona o DPH. V případě, že Dodavatel nebude mít svůj bankovní účet tímto způsobem zveřejněn, uhradí Objednatel Dodavateli pouze základ daně, přičemž DPH uhradí Dodavateli až po zveřejnění příslušného účtu Dodavatele v registru plátců a identifikovaných osob Dodavatelem.

8.15 Dodavatel prohlašuje, že správce daně před uzavřením této Smlouvy nerozhodl, že Dodavatel je nespolehlivým plátcem ve smyslu § 106a zákona o DPH (dále jen „**nespolehlivý plátce**"). V případě, že správce daně rozhodne o tom, že Dodavatel je nespolehlivým plátcem, zavazuje se Dodavatel o tomto informovat Objednatele do dvou (2) pracovních dní. Stane-li se Dodavatel nespolehlivým plátcem, uhradí Objednatel Dodavateli pouze základ daně, přičemž DPH bude Objednatelem uhrazena Dodavateli až po písemném doložení Dodavatele o jeho úhradě této DPH příslušnému správci daně.

9. PRÁVA A POVINNOSTI DODAVATELE

9.1 Dodavatel se zavazuje:

9.1.1 poskytovat Plnění podle této Smlouvy vlastním jménem, na vlastní odpovědnost a v souladu s pokyny Objednatele řádně a včas a s péčí řádného hospodáře odpovídající podmínkám sjednaným v této Smlouvě a s procesy *„best practice"*;

9.1.2 zabalit zboží či jinak opatřit pro přepravu způsobem zabraňujícím poškození zboží nebo znehodnocení;

9.1.3 dostane-li se Dodavatel do prodlení se svým plněním bez toho, aby to způsobil Objednatel či nastaly překážky vylučující povinnost k náhradě újmy po dobu delší než třicet (30) dnů, je Objednatel oprávněn zajistit náhradní plnění po dobu prodlení Dodavatele jinou osobou; v takovém případě se Dodavatel zavazuje nahradit v plném rozsahu náklady spojené s náhradním plněním;

9.1.4 předložit Objednateli na jeho žádost nejpozději do pěti (5) pracovních dnů ode dne jejího obdržení písemné potvrzení zastoupení výrobce o určení Plnění pro trh v České republice a pro Objednatele jako koncového zákazníka, je-li registrace koncového zákazníka nezbytná k řádnému užívání Plnění (včetně seznamu sériových čísel dodávaných zařízení);

9.1.5 poskytovat Plnění dle této Smlouvy spočívající v dopravě, instalaci, implementaci a veškeré konzultační, servisní či obdobné činnosti

vztahující se k Plnění certifikovaným pracovníkem, který je oprávněn k provádění servisních zásahů na území České republiky;

9.1.6 upozorňovat Objednatele na všechny hrozící vady svého Plnění či potenciální výpadky Plnění, jakož i poskytovat Objednateli veškeré informace, které jsou pro plnění předmětu Smlouvy nezbytné;

9.1.7 neprodleně oznámit Objednateli jakékoli překážky, které mu brání v plnění předmětu Smlouvy a výkonu dalších činností souvisejících s plněním předmětu Smlouvy;

9.1.8 upozornit Objednatele na potenciální rizika vzniku škod a provést včas a řádně na své náklady taková opatření, které riziko sníží nebo zcela vyloučí;

9.1.9 upozorňovat Objednatele v odůvodněných případech na případnou nevhodnost pokynů Objednatele;

9.1.10 i bez pokynů Objednatele provést nutné úkony, které, ač nejsou předmětem této Smlouvy, budou s ohledem na nepředvídatelné okolnosti pro plnění Smlouvy nezbytné nebo jsou nezbytné pro zamezení vzniku škody;

9.1.11 dodržovat bezpečnostní, hygienické, požární, organizační a ekologické předpisy Objednatele, se kterými byl prokazatelně seznámen nebo které jsou všeobecně známé;

9.1.12 řešit písemné požadavky či dotazy Objednatele vztahující se k předmětu Plnění dle této Smlouvy, a to nejpozději ve lhůtě pěti (5) pracovních dnů ode dne jejich doručení Dodavateli.

9.2 Dodavatel se dále zavazuje udržovat v platnosti a účinnosti po celou dobu účinnosti Smlouvy pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za škodu způsobenou Dodavatelem třetí osobě (zejména Objednateli), a to tak, že limit pojistného plnění vyplývající z pojistné smlouvy, nesmí být nižší než 30.000.000 Kč za rok, a to se spoluúčastí max. deset (10) %. Pojistnou smlouvu dle tohoto odstavce, pojistku potvrzující uzavření takové smlouvy nebo pojistný certifikát potvrzující uzavření takové smlouvy je Dodavatel povinen předložit Objednateli nejpozději do sedmi (7) pracovních dnů po uzavření této Smlouvy a dále kdykoliv po písemném vyžádání Objednatele, a to do pěti (5) pracovních dnů od doručení písemného vyžádání. Nepředložením pojistné smlouvy, pojistky nebo pojistného certifikátu ve výše uvedených lhůtách vzniká právo Objednatele na odstoupení od Smlouvy.

9.3 Dodavatel se zavazuje po celou dobu trvání smluvního vztahu založeného Smlouvou zajistit dodržování veškerých právních předpisů, zejména pak pracovněprávních (odměňování, pracovní doba, doba odpočinku mezi směnami, placené přesčasy), dále předpisů týkajících se oblasti zaměstnanosti a bezpečnosti a ochrany zdraví při práci, tj. zejména zákona č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, a zákona č. 262/2006 Sb., zákoníku práce, ve znění pozdějších předpisů, a to vůči všem osobám, které se na plnění Smlouvy podílejí (a bez ohledu na to, zda budou činnosti prováděny Dodavatelem

či jeho poddodavateli). Dodavatel se také zavazuje zajistit, že všechny osoby, které se na plnění Smlouvy podílejí (bez ohledu na to, zda budou činnosti prováděny Dodavatelem či jeho poddodavateli), jsou vedeny v příslušných registrech, jako například v registru pojištěnců ČSSZ, a mají příslušná povolení k pobytu v ČR.

9.4 Dodavatel je dále povinen zajistit, že všechny osoby, které se na plnění Smlouvy podílejí (bez ohledu na to, zda budou činnosti prováděny Dodavatelem či jeho poddodavateli) budou proškoleny z problematiky BOZP, a že jsou vybaveny osobními ochrannými pracovními prostředky dle účinné legislativy, je-li používání osobních ochranných pracovních prostředků s ohledem na předmět plnění Smlouvy vyžadováno. V případě, že Dodavatel (či jeho poddodavatel) bude v rámci řízení zahájeného dle tohoto odstavce Smlouvy orgánem veřejné moci pravomocně uznán vinným ze spáchání přestupku, správního deliktu či jiného obdobného protiprávního jednání, je Dodavatel povinen přijmout nápravná opatření a o těchto, včetně jejich realizace, písemně informovat Objednatele, a to v přiměřené lhůtě stanovené po dohodě s Objednatelem. Objednatel je oprávněn odstoupit od této Smlouvy, pokud Dodavatel nebo jeho poddodavatel bude orgánem veřejné moci uznán pravomocně vinným ze spáchání přestupku či správního deliktu, popř. jiného obdobného protiprávního jednání, v řízení dle tohoto odstavce Smlouvy.

9.5 Dodavatel musí po celou dobu trvání Smlouvy sjednat a dodržovat obdobné smluvní podmínky v oblasti rozdělení rizika a smluvních pokut se svými poddodavateli s ohledem na charakter, rozsah a cenu plnění poddodavatele, jako jsou sjednané v této Smlouvě.

9.6 Dodavatel se zavazuje po celou dobu trvání Smlouvy zajistit dodržování právních předpisů z oblasti práva životního prostředí, jež naplňuje cíle environmentální politiky související se změnou klimatu, využíváním zdrojů a udržitelnou spotřebou a výrobou, především zákona č. 114/1992 Sb., o ochraně přírody a krajiny, ve znění pozdějších předpisů a zákona č. 17/1992 Sb., o životním prostředí, ve znění pozdějších předpisů. Dodavatel se zejména zavazuje dodržovat zásadu „významného nepoškození“ životního prostředí v kontextu základních principů Projektu.

9.7 V případě, že Dodavatel (či jeho poddodavatel) bude v rámci řízení zahájeného orgánem veřejné moci pravomocně uznán vinným ze spáchání přestupku či jiného závažného protiprávního jednání v oblasti práva životního prostředí, je Dodavatel povinen:

9.7.1 o této skutečnosti nejpozději do 7 pracovních dnů písemně informovat Objednatele,

9.7.2 přijmout nápravná opatření k odstranění trvání protiprávního stavu a tento v přiměřené lhůtě odstranit a/nebo učinit prevenční nápravná opatření za účelem zamezení opakování předmětného protiprávního jednání,

9.7.3 písemně informovat Objednatele o opatřeních dle odst. 9.7.2 této Smlouvy, včetně jejich realizace, a to bezodkladně nebo v Objednatelem stanovené lhůtě (bude-li ze strany Objednatele stanovena).

9.8 Dodavatel se v rámci svých vnitřních procesů zavazuje k podpoře firemní kultury založené na motivaci pracovníků k zavádění inovativních prvků, procesů či technologií v rámci tzv. Best Practices.

9.9 Dodavatel se zavazuje uchovávat veškerou dokumentaci související s realizací Projektu včetně účetních dokladů minimálně na dobu 10 let ode ukončení doby trvání této Smlouvy.

9.10 Dodavatel se zavazuje minimálně po dobu 10 let ode dne akceptace poslední Dodávky a příslušné Služby poskytovat požadované informace a dokumentaci související s realizací Projektu zaměstnancům nebo zmocněncům pověřených orgánů (CRR, MMR, MF, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu či příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout jim při provádění kontroly součinnost.

10. ODPOVĚDNOST ZA VADY, ZÁRUKA

10.1 Dodavatel poskytuje záruku, že každá část Plnění má ke dni její akceptace funkční vlastnosti stanovené touto Smlouvou a je způsobilá k použití pro účely stanovené v této Smlouvě nebo v souladu s touto Smlouvou.

10.2 Dodavatel před dodáním Plnění dle Smlouvy předloží na vyžádání prohlášení výrobce dodávaného zařízení či jeho oficiálního zastoupení o tom, že na dodávané Plnění (seznam sériových čísel) Objednateli jako koncovému zákazníkovi bude poskytnuta k dodávanému Plnění záruka výrobce v plném výrobcem poskytovaném rozsahu.

10.3 Dodavatel poskytuje záruku za jakost každé jednotlivé části Plnění minimálně po dobu a v rozsahu stanoveném v **Příloze č.1** této Smlouvy.

10.4 Objednatel je oprávněn vady Plnění nahlásit Dodavateli kdykoli v průběhu záruční doby bez ohledu na to, kdy je zjistil, aniž by tím byla jeho práva ze záruky či práva z vad jakkoli dotčena.

10.5 Doba od zjištění vady do jejího odstranění se do trvání záruční doby nezapočítává.

10.6 Plnění má vady, zejména pokud nebylo poskytnuto ve sjednaném druhu, množství a jakosti. Za vady Plnění se považují i vady v návodech (manuálech) k použití, dokladech a dokumentech.

10.7 V případě, že je dodáno Plnění s vadami, či se na Plnění vady v záruční době vyskytnou, je Dodavatel povinen vady odstranit opravou, dodáním náhradního Plnění, či pokud Objednatel takový požadavek uvede v oznámení vad, přiměřenou slevou z ceny Plnění.

10.8 Nároky z vad Plnění se nedotýkají nároku Objednatele na náhradu újmy nebo na smluvní pokutu.

11. VLASTNICKÉ PRÁVO A UŽÍVACÍ PRÁVA

Vlastnické právo

11.1 V případě, že součástí Plnění Dodavatele podle této Smlouvy jsou věci, které se mají stát vlastnictvím Objednatele, nabývá Objednatel vlastnické právo k těmto věcem dnem předání takového plnění Objednateli na základě akceptačního protokolu podepsaného oprávněnými osobami obou Smluvních stran. Nebezpečí škody na předaných věcech přechází na Objednatele okamžikem jejich faktického předání do dispozice Objednatele, pokud o takovém předání byl sepsán písemný záznam podepsaný oprávněnými osobami Smluvních stran.

11.2 Do okamžiku nabytí vlastnického práva uděluje Dodavatel Objednateli právo dodané zboží užívat v rozsahu a způsobem, jenž vyplývá z účelu této Smlouvy, a to bez vzniku jakýchkoliv dodatečných finančních nároků nad rámec ceny sjednané v této Smlouvě. Užití zboží nezpůsobuje fikci převzetí zboží ani podpisu akceptace.

Základní rozsah licence

11.3 Vzhledem k tomu, že součástí Plnění dle této Smlouvy je i plnění, které ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „**autorský zákon**"), může naplňovat znaky autorského díla či být považováno za autorské dílo ve smyslu autorského zákona (dále společně jen „**autorská díla**"), je k tomuto plnění poskytována, postupována či zprostředkovávána (dále také společně jen „**poskytování**") licence či podlicence (dále společně jen „**licence**") za podmínek sjednaných dále v tomto článku Smlouvy.

11.3.1 Objednatel je oprávněn od okamžiku účinnosti poskytnutí licence k autorskému dílu dle odst. 11.3.3 této Smlouvy užívat toto autorské dílo k jakémukoliv účelu a v rozsahu, v jakém uzná za nezbytné, vhodné či přiměřené. Pro vyloučení pochybností to znamená, že Objednatel je oprávněn užívat autorské dílo v neomezeném množstevním a územním rozsahu, a to všemi v úvahu přicházejícími způsoby a s časovým rozsahem omezeným pouze dobou trvání majetkových autorských práv k takovémuto autorskému dílu.

11.3.2 Licence k autorskému dílu je poskytována jako nevýhradní. Objednatel není povinen licenci využít.

11.3.3 Účinnost licence nastává okamžikem akceptace dílčího plnění, které příslušné autorské dílo obsahuje; do té doby je Objednatel oprávněn autorské dílo užít v rozsahu a způsobem nezbytným k provedení akceptace příslušného dílčího plnění.

11.3.4 Udělení licence nelze ze strany Dodavatele do doby trvání této Smlouvy vypovědět a její účinnost trvá minimálně po dobu trvání této Smlouvy, nedohodnou-li se Smluvní strany výslovně jinak.

11.3.5 Pro vyloučení veškerých pochybností Smluvní strany výslovně prohlašují, že pokud při poskytování Plnění dle této Smlouvy vznikne činností Dodavatele a Objednatele dílo spoluautorů a nedohodnou-li se Smluvní strany výslovně jinak, platí, že k okamžiku vzniku takového díla spoluautorů postoupil Dodavatel Objednateli právo vykonávat majetková

autorská práva k dílu spoluautorů a udělil Objednateli souhlas k jakékoliv změně nebo jinému zásahu do díla spoluautorů. Cena za dodání Plnění dle odst. 8.1 Smlouvy je stanovena se zohledněním tohoto ustanovení a Dodavateli nevzniknou v případě vytvoření díla spoluautorů žádné nové nároky na odměnu.

11.3.6 Dodavatel je povinen postupovat tak, aby udělení licence k autorskému dílu dle této Smlouvy včetně oprávnění udělit podlicenci a souvisejících oprávnění zabezpečil, a to bez újmy na právech třetích osob.

Možnost užití standardního software

11.4 Součástí plnění může být tzv. proprietární (standardní) software anebo tzv. open source software Dodavatele nebo třetích stran (dále společně jen „**standardní software**“) u kterých Dodavatel nemůže udělit Objednateli licenci v rozsahu dle odst. 11.3 Smlouvy nebo to po něm nelze spravedlivě požadovat, pouze při splnění některé z následujících podmínek (pro vyloučení veškerých pochybností Smluvní strany uvádí, že v případě, kdy je vývoj počítačového programu hrazen Objednatelem na základě této Smlouvy, může Objednatel vždy požadovat udělení oprávnění dle odst. 11.3 Smlouvy):

11.4.1 Jedná se o software, který je v době uzavření Smlouvy prokazatelně užíván v produktivním prostředí nejméně u pěti (5) na sobě nezávislých a vzájemně nepropojených subjektů a jenž je na trhu běžně dostupný, tj. nabízený na území České republiky alespoň třemi (3) na sobě nezávislými a vzájemně nepropojenými subjekty:

a) pokud jsou tyto subjekty oprávněny takovýto software implementovat, přizpůsobovat požadavkům Objednatele a udržovat; nebo

b) pokud k takovému software není poskytnutí licence v rozsahu dle odst. 11.3 Smlouvy účelné (zejména vývojový software, databázový software, kancelářský software, operační systém aj.).

Dodavatel je povinen poskytnout Objednateli o této skutečnosti písemné prohlášení a na výzvu Objednatele tuto skutečnost prokázat.

11.4.2 Jedná se o software, který je veřejnosti poskytován zdarma, včetně detailně komentovaných zdrojových kódů, úplné uživatelské, provozní a administrátorské dokumentace a práva software měnit. Dodavatel je povinen poskytnout Objednateli o této skutečnosti písemné prohlášení a na výzvu Objednatele tuto skutečnost prokázat.

11.4.3 Jedná se o software, (i) který je integrální součástí hardware dodávaného jako část plnění Smlouvy, nebo (ii) který nad takovým hardware poskytuje pouze abstrakční vrstvu pro správu, konfiguraci, informační bezpečnost, programování aplikací nebo jiné obdobné účely, vše za podmínky, že spouštění takového software je od výrobce příslušného hardware předepsáno pro jeho korektní fungování a zároveň se jedná o software, k němuž není poskytnutí licence v rozsahu dle odst. 11.3 Smlouvy účelné.

Dodavatel je povinen poskytnout Objednateli o této skutečnosti písemné prohlášení a na výzvu Objednatele tuto skutečnost prokázat.

Dodavatel je povinen udržovat prohlášení dle tohoto odst. 11.4 Smlouvy v platnosti. V případě že Dodavatel poruší tuto povinnost, nepředloží Objednateli příslušné prohlášení či nejpozději do jednoho (1) měsíce na výzvu Objednatele relevantní skutečnosti neprokáže, je Objednatel oprávněn požadovat úhradu smluvní pokuty ve výši 100.000 Kč za každý jednotlivý případ a bezodkladné zajištění nápravy, a to včetně náhrady příslušného software.

11.4.4 Součástí licence je též právo k provedeným změnám konfigurace či nastavením počítačových programů.

Minimální rozsah licence

11.5 Pokud se bude jednat o standardní software dle odst. 11.4 Smlouvy, tak na rozdíl od licence ke zbývajícím částem plnění udělované dle odst. 11.3 Smlouvy postačí, aby udělená licence k takovému software zahrnovala nevýhradní oprávnění užít jej jakýmkoli způsobem nejméně po dobu dvou (2) let ode dne akceptace poslední dílčí Dodávky, na území České republiky a v množstevním rozsahu, který je objektivně nezbytný pro pokrytí potřeb Objednatele ke dni uzavření této Smlouvy, a to včetně práva Objednatele do standardního software zasahovat, pokud tak stanoví příslušné ustanovení odst. 11.4 této Smlouvy.

11.6 Nelze-li to na Dodavateli spravedlivě požadovat a není-li to v rozporu s ustanoveními čl. 11.4 Smlouvy, **nemusí** být Objednateli ke standardnímu softwaru **předány zdrojové kódy** a stejně tak nemusí být Objednateli poskytnuto právo do standardního softwaru zasahovat, vždy však musí být předána kompletní uživatelská, administrátorská a provozní dokumentace. Součástí licence je též právo k provedeným změnám konfigurace či nastavením počítačových programů.

11.7 Dodavatel se zavazuje samostatně zdokumentovat veškeré využití standardního software v rámci plnění a předložit Objednateli ucelený přehled využitého standardního software, jehož součástí budou licenční podmínky takového standardního software a seznam jeho alternativních dodavatelů. Tento přehled je Dodavatel povinen předložit Objednateli vždy do tří (3) pracovních dnů po akceptaci plnění, v jehož rámci Dodavatel využil standardní software a dále vždy do jednoho (1) měsíce od doručení výzvy Objednatele, kterou může Objednatel učinit kdykoli, nejpozději však do dvou (2) let od skončení platnosti Smlouvy z jakéhokoli důvodu.

11.8 Jestliže jsou s užitím standardního software spojeny jednorázové či pravidelné poplatky, je Dodavatel povinen v rámci ceny Plnění řádně uhradit všechny tyto poplatky nejméně po dobu dvou (2) let ode dne akceptace poslední dílčí Dodávky. Nad rámec ceny Dodávky nebudou Dodavateli hrazeny žádné další poplatky či odměny.

Přechod práv, licenční odměna a garance rozsahu licence

11.9 Práva získaná v rámci plnění této Smlouvy přechází i na případného právního nástupce Objednatele. Případná změna v osobě Dodavatele (např. právní

nástupnictví) nebude mít vliv na oprávnění udělená v rámci této Smlouvy Dodavatelem Objednateli.

11.10 Bez ohledu na formu uzavření licenční smlouvy platí, že Dodavatel je vždy povinen zajistit poskytnutí licence dle podmínek stanovených Smlouvou, a to bez ohledu na případný rozdílný obsah standardních licenčních podmínek vykonavatele majetkových práv k takovým autorským dílům.

12. OPRÁVNĚNÉ OSOBY

12.1 Každá ze Smluvních stran jmenuje oprávněnou osobu, popř. zástupce oprávněné osoby. Oprávněné osoby budou zastupovat Smluvní stranu ve smluvních, obchodních a technických záležitostech souvisejících s plněním této Smlouvy.

12.2 Oprávněné osoby jsou oprávněny jménem Smluvních stran provádět zejména veškeré úkony v rámci realizace Smlouvy, zastupovat Smluvní strany ve změnovém řízení a připravovat dodatky ke Smlouvě pro jejich písemné schválení osobám oprávněným zavazovat Smluvní strany (statutárním orgánům), nebo jejich zplnomocněným zástupcům.

12.3 Oprávněné osoby nejsou zmocněny k jednání, jež by mělo za přímý následek změnu této Smlouvy nebo jejího předmětu.

12.4 Jména oprávněných osob jsou uvedena v **Příloze č. 3** této Smlouvy a jejich role stanoví tato Smlouva.

12.5 Smluvní strany jsou oprávněny změnit oprávněné osoby, jsou však povinny na takovou změnu druhou Smluvní stranu písemně upozornit ve lhůtě tří (3) dnů. Zmocnění zástupce oprávněné osoby musí být písemné s uvedením rozsahu zmocnění. Změna oprávněných osob dle tohoto článku může být provedena jednostranným písemným oznámením vůči druhé Smluvní straně, a to bez nutnosti uzavírání dodatku ke Smlouvě.

12.6 Smluvní strany tímto prohlašují, že budou jako samostatní správci zpracovávat osobní údaje fyzických osob jednajících na straně druhé Smluvní strany (zejména pokud se jedná o identifikační a kontaktní údaje oprávněných osob) a případně dalších osob podílejících se na plnění Smlouvy (jako subjekty údajů) pro účely plnění Smlouvy, interní evidence správce a ochranu jeho práv, dodržování zákonných povinností vztahujících se ke správci.

12.7 Právní základ pro takové zpracování osobních údajů je oprávněný zájem správce na řádném plnění uzavřené Smlouvy, oprávněný zájem správce na evidenci smluv, ve kterých je správce smluvní stranou, a na ochraně jeho práv, nutnost plnění zákonných povinností, kterým správce podléhá, zejména v oblasti daňových a účetních zákonů.

12.8 Osobní údaje musí být uchovávány po dobu trvání této Smlouvy a plnění povinností z ní vyplývajících a po dobu nezbytnou k plnění právních povinností Smluvních stran.

12.9 Subjekt osobních údajů má právo na:

12.9.1 přístup k jeho osobním údajům;

12.9.2 opravu, doplnění nebo vymazání osobních údajů správcem;

12.9.3 omezení zpracování osobních údajů správcem;

12.9.4 vysvětlení zpracování osobních údajů správcem;

12.9.5 námitku proti zpracování osobních údajů;

12.9.6 získání osobních údajů od správce v rámci práva na přenositelnost údajů;

12.9.7 podání stížnosti k dozorovému úřadu.

12.10 Obě Smluvní strany se zavazují informovat své zaměstnance a dodavatele o zpracování jejich osobních údajů jinou Smluvní stranou na základě této Smlouvy bez zbytečného odkladu.

13. OCHRANA INFORMACÍ

13.1 Smluvní strany jsou si vědomy toho, že v rámci plnění závazků z této Smlouvy:

13.1.1 si mohou vzájemně vědomě nebo opominutím poskytnout informace, které budou považovány za důvěrné (dále jen „**Důvěrné informace**“),

13.1.2 mohou jejich zaměstnanci a osoby v obdobném postavení získat vědomou činností druhé Smluvní strany nebo i jejím opominutím přístup k Důvěrným informacím druhé Smluvní strany.

13.2 Smluvní strany se zavazují, že žádná z nich nezpřístupní třetí osobě Důvěrné informace, které při plnění této Smlouvy získala od druhé Smluvní strany.

13.3 Za třetí osoby podle odst. 13.2 Smlouvy se nepovažují:

13.3.1 zaměstnanci Smluvních stran a osoby v obdobném postavení,

13.3.2 orgány Smluvních stran a jejich členové,

13.3.3 ve vztahu k Důvěrným informacím Objednatele poddodavatelé Dodavatele,

13.3.4 ve vztahu k Důvěrným informacím Dodavatele externí Dodavatelé Objednatele, a to i potenciální,

za předpokladu, že se podílejí na plnění této Smlouvy nebo na plnění spojeném s Plněním dle této Smlouvy, Důvěrné informace jsou jim zpřístupněny výhradně za tímto účelem a zpřístupnění Důvěrných informací je v rozsahu nezbytně nutném pro naplnění jeho účelu a za stejných podmínek, jaké jsou stanoveny Smluvním stranám v této Smlouvě.

13.4 Smluvní strany se zavazují v plném rozsahu zachovávat povinnost mlčenlivosti a povinnost chránit Důvěrné informace vyplývající z této Smlouvy a též z příslušných právních předpisů, zejména povinnosti vyplývající z nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), CELEX: 32016R0679 (dále jen „**Nařízení**").

13.5 Smluvní strany pro vyloučení pochybností prohlašují, že při zpracování osobních údajů dle této Smlouvy vystupují jako samostatní správci dle Nařízení. V případě potřeb Smluvní strany uzavřou samostatnou Smlouvu o zpracování osobních údajů.

13.6 Smluvní strany se v této souvislosti zavazují poučit veškeré osoby, které se na jejich straně budou podílet na plnění této Smlouvy, o výše uvedených povinnostech mlčenlivosti a ochrany Důvěrných informací a dále se zavazují vhodným způsobem zajistit dodržování těchto povinností všemi osobami podílejícími se na plnění této Smlouvy.

13.7 Budou-li údaje, ke kterým Dodavatel získá přístup v souvislosti s plněním dle této Smlouvy mít povahu osobních údajů dle Nařízení, je Dodavatel povinen přijmout veškerá opatření k tomu, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k těmto osobním údajům, jejich změně, zničení či ztrátě, neoprávněným přenosům či jinému zneužití, a zajistit nakládání s osobními údaji v souladu s Nařízením a příslušnými právními předpisy na ochranu osobních údajů.

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

13.9 Nedohodnou-li se Smluvní strany výslovně písemnou formou jinak, považují se za Důvěrné implicitně všechny informace, které jsou anebo by mohly být součástí obchodního tajemství, tj. například, ale nejenom, popisy nebo části popisů technologických procesů a vzorců, technických vzorců a technického know-how, informace o provozních metodách, procedurách a pracovních postupech, obchodní nebo marketingové plány, koncepce a strategie nebo jejich části, nabídky, kontrakty, smlouvy, dohody nebo jiná ujednání s třetími stranami, informace o výsledcích hospodaření, o vztazích s obchodními partnery, o pracovněprávních otázkách a všechny další informace, jejichž zveřejnění přijímající Smluvní stranou by předávající straně mohlo způsobit újmu.

13.10 Bez ohledu na výše uvedená ustanovení se veškeré informace vztahující se k předmětu této Smlouvy a příslušné dokumentaci považují výlučně za Důvěrné informace Objednatele a Dodavatel je povinen tyto informace chránit v souladu s touto Smlouvou. Dodavatel při tom bere na vědomí, že povinnost ochrany těchto informací podle tohoto článku 13 Smlouvy se vztahuje pouze na Dodavatele.

13.11 Pokud jsou Důvěrné informace poskytovány v písemné podobě anebo ve formě textových souborů na elektronických nosičích dat (médiích), je předávající strana povinna upozornit přijímající stranu na důvěrnost takového materiálu jejím

vyznačením alespoň na titulní stránce nebo přední straně média. Absence takovéhoto upozornění však nezpůsobuje zánik povinnosti ochrany takto poskytnutých informací.

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

13.12.1 se staly veřejně známými, aniž by jejich zveřejněním došlo k porušení závazků přijímající Smluvní strany či právních předpisů,

13.12.2 mají být zpřístupněny Objednatelem na základě zákona, například zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, či jiného právního předpisu včetně práva EU nebo závazného rozhodnutí oprávněného orgánu veřejné moci, a Smluvní strany si v takovém případě poskytnou nezbytnou součinnost ke splnění takové zákonné povinnosti,

13.12.3 měla přijímající Smluvní strana prokazatelně legálně k dispozici před uzavřením této Smlouvy, pokud takové informace nebyly předmětem jiné, dříve mezi Smluvními stranami uzavřené Smlouvy o ochraně informací,

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

13.12.5 po podpisu této Smlouvy poskytne přijímající straně třetí osoba, jež není omezena v takovém nakládání s informacemi,

13.12.6 jsou obsažené ve Smlouvě a jsou uveřejněné dle zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů (dále jen „**Zákon o registru smluv**“) a v souladu se ZZVZ.

13.13 Za porušení povinnosti mlčenlivosti Smluvní stranou se považují též případy, kdy tuto povinnost poruší kterákoliv z osob uvedených v odst. 13.3 Smlouvy, které daná Smluvní strana poskytla Důvěrné informace druhé Smluvní strany.

13.14 Poruší-li Dodavatel povinnosti vyplývající z této Smlouvy ohledně ochrany Důvěrných informací, je povinen zaplatit Objednateli smluvní pokutu ve výši 1.000.000 Kč za každé nikoliv nepodstatné porušení takové povinnosti.

13.15 Ukončení platnosti této Smlouvy z jakéhokoliv důvodu se nedotkne ustanovení tohoto článku 13 Smlouvy a jejich účinnost přetrvá i po ukončení účinnosti této Smlouvy.

13.16 Dodavatel dále výslovně prohlašuje a bere na vědomí, že tato Smlouva nepředstavuje jeho obchodní tajemství ani neobsahuje jeho Důvěrné informace a souhlasí s tím, aby tato Smlouva byla v plném rozsahu zveřejněna v souladu se zákonnými povinnostmi Objednatele.

14. SOUČINNOST A VZÁJEMNÁ KOMUNIKACE

14.1 Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých závazků. Smluvní strany jsou povinny

informovat druhou Smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění této Smlouvy.

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

14.3 Veškerá komunikace mezi Smluvními stranami bude probíhat prostřednictvím oprávněných osob vymezených v **Příloze č. 3** této Smlouvy, statutárních orgánů Smluvních stran, popř. jimi písemně pověřených pracovníků.

14.4 Všechna oznámení mezi Smluvními stranami, která se vztahují k této Smlouvě, nebo která mají být učiněna na základě této Smlouvy, musí být učiněna v písemné podobě a druhé Smluvní straně doručena buď osobně nebo prostřednictvím datové schránky příslušné Smluvní strany, není-li stanoveno nebo mezi Smluvními stranami dohodnuto jinak. Nemá-li komunikace dle předchozí věty mít vliv na platnost a účinnost Smlouvy, připouští se též doručení prostřednictvím e-mailu na adresy uvedené v **Příloze č. 3** této Smlouvy. Dodavatel je oprávněn komunikovat s Objednatelem prostřednictvím datové schránky.

14.5 Ukládá-li Smlouva doručit některý dokument v písemné podobě, může být doručen buď v tištěné podobě nebo v elektronické (digitální) podobě jako dokument aplikace MS Word verze 2003 nebo vyšší, MS Excel 2003 nebo vyšší či PDF (verze založena na specifikaci ISO 32000-1:2008) na dohodnutém médiu.

14.6 Smluvní strany se zavazují, že v případě změny své poštovní adresy, nebo e-mailové adresy budou o této změně druhou Smluvní stranu informovat nejpozději do tří (3) dnů.

14.7 Dodavatel se zavazuje ve lhůtě pěti (5) pracovních dnů ode dne doručení odůvodněné písemné žádosti Objednatele o výměnu oprávněné osoby Dodavatele podílející se na plnění této Smlouvy, s níž Objednatel nebyl z jakéhokoliv důvodu spokojen, nahradit jinou vhodnou osobou s odpovídající kvalifikací.

14.8 Dodavatel se zavazuje poskytnout Objednateli potřebnou součinnost při výkonu finanční kontroly dle zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů.

15. NÁHRADA ÚJMY

15.1 Každá ze Smluvních stran nese odpovědnost za způsobenou újmu v rámci platných právních předpisů a této Smlouvy. Obě Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod.

15.2 Žádná ze Smluvních stran neodpovídá za újmu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé Smluvní strany. V případě, že Objednatel poskytl Dodavateli chybné zadání a Dodavatel s ohledem na svou povinnost poskytovat Plnění s odbornou péčí mohl a měl chybnost takového zadání zjistit, smí se ustanovení předchozí věty dovolávat pouze v případě, že na chybné zadání Objednatele písemně upozornil a Objednatel trval na původním zadání.

15.3 Žádná ze Smluvních stran není odpovědná za újmu a není ani v prodlení, pokud k tomuto došlo výlučně v důsledku prodlení s plněním závazků druhé Smluvní strany nebo v důsledku překážek vylučujících povinnost k náhradě újmy ve smyslu § 2913 odst. 2 OZ (dále jen „**vyšší moc**“).

15.4 Za vyšší moc se podle této Smlouvy považují mimořádné nepředvídatelné a nepřekonatelné překážky bránící dočasně nebo trvale plnění povinností stanovených v této Smlouvě, pokud nastaly po jejím uzavření nezávisle na vůli povinné Smluvní strany a jestliže tyto překážky nemohly být povinnou Smluvní stranou odvráceny ani při vynaložení veškerého úsilí, které lze rozumně v dané situaci požadovat.

15.5 Za vyšší moc se však nepokládají okolnosti, jež vyplývají z osobních nebo hospodářských poměrů povinné Smluvní strany a dále překážky plnění, které byla příslušná Smluvní strana povinna překonat nebo odstranit podle této Smlouvy, obchodních zvyklostí nebo obecně závazných právních předpisů nebo jestliže může důsledky své odpovědnosti smluvně převést na třetí osobu, jakož i okolnosti, které se projevily až v době, kdy povinná Smluvní strana již byla v prodlení.

15.6 Smluvní strany se zavazují upozornit druhou Smluvní stranu bez zbytečného odkladu na vzniklé překážky vylučující povinnost k náhradě újmy. Smluvní strany se zavazují k vyvinutí maximálního úsilí k odvrácení a překonání překážek vylučujících povinnost k náhradě újmy. Každá ze Smluvních stran je oprávněna požadovat náhradu újmy v plném rozsahu i v případě, že se jedná o porušení povinnosti, na kterou se dle této Smlouvy vztahuje smluvní pokuta nebo sleva z ceny.

15.7 Případná náhrada újmy bude zaplacena v měně platné na území České republiky, přičemž pro propočet na tuto měnu je rozhodný kurs České národní banky ke dni vzniku újmy.

15.8 Každá ze Smluvních stran je oprávněna požadovat náhradu újmy i v případě, že se jedná o porušení povinnosti, na kterou se vztahuje smluvní pokuta nebo sleva z ceny, a to v celém rozsahu nebo slevy z ceny dle této Smlouvy.

16. SANKCE

16.1 Smluvní strany se dohodly, že:

16.1.1 V případě, že Dodavatel je v prodlení s provedením Dodávky dle Harmonogramu, je Dodavatel povinen uhradit a Objednatel je oprávněn po prodávajícím požadovat uhrazení smluvní pokuty ve výši 0,1 % z celkové nabídkové ceny za Dodávku uvedenou v nabídce Dodavatele, a to za každý i započatý den prodlení.

16.1.2 V případě, že dojde k porušení povinnosti dle odst. 5.3 nebo 5.5 této Smlouvy, může Objednatel požadovat po Dodavateli jednorázovou smluvní pokutu ve výši 500.000 Kč. Současně bude mít Objednatel právo odstoupit od této Smlouvy z důvodu podstatného porušení Smlouvy.

16.1.3 V případě, že Dodavatel nesplní povinnost dle odst. 5.6.4 Smlouvy do sedmi (7) pracovních dnů od doručení žádosti Objednatele o předložení

potvrzení výrobce o určení dodaného zboží pro evropský trh případně jiného dokladu výrobce prokazující pro dodaná zařízení provozovaná na území ČR poskytnutí plné podpory a záruky výrobce při řešení technických problémů, může Objednatel požadovat po Dodavateli jednorázovou smluvní pokutu ve výši 500.000 Kč. Současně bude mít Objednatel právo odstoupit od této Smlouvy z důvodu podstatného porušení Smlouvy.

16.1.4 V případě, že porušení povinnosti dle odst. 5.21 Smlouvy, může Objednatel požadovat po Dodavateli smluvní pokutu ve výši 10.000 Kč za každý jednotlivý případ porušení povinnosti.

16.1.5 V případě, že v průběhu záruční doby Objednatel zjistí, že vlastnosti (zejm. technické parametry) zboží jsou prokazatelně v rozporu s touto Smlouvou (nesplňují minimální požadované parametry uvedené v zadávací dokumentaci), může Objednatel požadovat po Dodavateli jednorázovou smluvní pokutu ve výši 500.000 Kč. Současně bude mít Objednatel právo odstoupit od této Smlouvy z důvodu podstatného porušení Smlouvy.

16.1.6 Pro případ prokazatelného porušení povinnosti Dodavatele dle čl. 9 (s výjimkou odst. 9.2) Smlouvy vzniká Objednateli, nárok na smluvní pokutu ve výši 5.000 Kč za každé jednotlivé porušení;

16.1.7 Za porušení povinnosti uvedené v odst. 9.2 této Smlouvy, tj. porušení povinnosti Dodavatele mít po celou dobu platnosti Smlouvy sjednáno pojištění odpovědnosti za škodu způsobenou v souvislosti s výkonem podnikatelské činnosti v rozsahu stanoveném v odst. 9.2 této Smlouvy, uhradí Dodavatel smluvní pokutu ve výši 5.000 Kč za každý den porušení povinnosti stanovené v odst. 9.2 této Smlouvy.

16.2 Smluvní strany se dále dohodly, že:

16.2.1 V případě, že Dodavatel bude k poskytování Plnění využívat poddodavatele nebo členy realizačního týmu v rozporu s ustanoveními odst. 3.4 nebo odst. 3.5 této Smlouvy, vzniká Objednateli nárok na zaplacení smluvní pokuty ve výši 50.000 Kč za každý jednotlivý případ takového porušení Smlouvy.

16.2.2 V případě porušení jakékoliv povinnosti Dodavatele dle článku čl. 19 Smlouvy vzniká Objednateli nárok na zaplacení smluvní pokuty ve výši 100.000 Kč za každý jednotlivý případ porušení. V případě porušení jakékoliv povinnosti Dodavatele dle článku čl. 20 Smlouvy vzniká Objednateli nárok na zaplacení smluvní pokuty ve výši 100.000 Kč za každý jednotlivý případ porušení.

16.2.3 Za porušení povinnosti mlčenlivosti specifikované v článku 13 této Smlouvy uhradí Dodavatel Objednateli částku 50.000 Kč za každý jednotlivý případ porušení této povinnosti.

16.3 Smluvní strany se dohodly na tom, že další sankce jsou dále stanoveny v **Přílohy č. 1** této Smlouvy.

16.4 Smluvní pokuty a/nebo úroky z prodlení jsou splatné třicátý (30.) den ode dne doručení písemné výzvy oprávněné Smluvní strany k jejich úhradě povinnou Smluvní stranou, není-li ve výzvě uvedena lhůta delší. Oprávněná Smluvní strana je současně oprávněna jednostranně započíst svou pohledávku na smluvní pokutu a/nebo úroky z prodlení proti jakékoli splatné či budoucí pohledávce povinné Smluvní strany.

16.5 Není-li dále stanoveno jinak, zaplacení jakékoliv sjednané smluvní pokuty nezbavuje povinnou Smluvní stranu povinnosti splnit své závazky.

16.6 Zaplacením smluvní pokuty není dotčeno právo Objednatele na náhradu újmy v celém rozsahu. Výše smluvních pokut se do výše náhrady újmy nezapočítává.

17. ZMĚNOVÉ ŘÍZENÍ, VYHRAZENÁ ZMĚNA ZÁVAZKU

17.1 Kterákoliv ze Smluvních stran je v průběhu trvání této Smlouvy oprávněna písemně navrhnout změny specifikace Plnění. V případě, že změnu specifikace navrhne Objednatel, je Dodavatel povinen vynaložit veškeré úsilí k tomu, aby změnu specifikace přijal. Objednatel není povinen přijmout změnu specifikace navrhovanou Dodavatelem.

17.2 Objednatel však bez přiměřeného důvodu neodepře změnu specifikace spočívající v nahrazení zařízení nebo komponentu jeho produktovým nástupcem, pokud bude splňovat minimální technické požadavky stanovené Objednatelem na původní zařízení nebo komponentu uvedené v zadávací dokumentaci a bude nabízen za shodnou nebo nižší cenu. Případnou změnu specifikace dle předchozí věty si Smluvní strany vyhrazují ve smyslu § 100 odst. 1 ZZVZ.

17.3 Dodavatel se na písemnou výzvu Objednatele zavazuje do deseti (10) pracovních dnů vyhodnotit důsledky navržených změn specifikace Plnění, které budou zahrnovat hodnocení dopadů těchto změn na cenu a rozsah Plnění, dohodnuté termíny plnění, rozsah potřebné součinnosti a jakékoliv další relevantní aspekty smluvního vztahu (dále jen „**Hodnocení důsledků**“). Pokud si vypracování Hodnocení důsledků vyžádá dodatečné náklady nebo pokud by jeho vypracování mohlo mít negativní dopad na plnění závazků Dodavatele dle této Smlouvy, vypracuje Dodavatel Hodnocení důsledků na základě písemné dohody s Objednatelem o úhradě nákladů na vypracování Hodnocení důsledků a o úpravě dalších smluvních podmínek, kterých se vypracování Hodnocení důsledků může dotknout.

17.4 Jakékoliv změny specifikace Plnění či poskytování služeb dle Smlouvy musí být dohodnuty formou písemného dodatku k této Smlouvě podle odst. 22.1 Smlouvy, kterým dojde k úpravě smluvních podmínek v souladu s Hodnocením důsledků, není-li touto Smlouvou stanoveno jinak.

17.5 Jakékoliv změny technické specifikace Plnění uvedené v **Příloze č. 1** Smlouvy musí být sjednány v souladu s příslušnými právními předpisy včetně ZZVZ.

18. PLATNOST A ÚČINNOST SMLOUVY

18.1 Tato Smlouva nabývá platnosti dnem jejího podpisu oběma Smluvními stranami a účinnosti dnem uveřejnění v registru smluv dle Zákona o registru smluv a uzavírá se na dobu určitou v délce dle **Přílohy č. 2** této Smlouvy.

18.2 Každá Smluvní strana je oprávněna odstoupit od této Smlouvy z důvodů stanovených touto Smlouvou.

18.3 Objednatel je oprávněn odstoupit od této Smlouvy v případě, že:

18.3.1 Dodavatel opakovaně (nejméně dvakrát) v průběhu jednoho kalendářního měsíce poskytne vadné Plnění, které způsobí nebo může reálně způsobit výpadek IT infrastruktury Objednatele či jeho podstatné části; nebo

18.3.2 Dodavatel nedodá Dodávky a Služby v souladu s harmonogramem uvedeným v **Příloze č. 2** a nezjedná nápravu ani do pěti (5) kalendářních dnů ode dne doručení písemného oznámení Objednatele o takovém prodlení.

18.3.3 Dodavatel je v prodlení s plněním svých ostatních povinností déle než deset (10) kalendářních dní a nezjedná nápravu ani do pěti (5) kalendářních dnů ode dne doručení písemného oznámení Objednatele o takovém prodlení; nebo

18.3.4 dojde k porušení povinnosti ochrany Důvěrných informací dle této Smlouvy ze strany Dodavatele; nebo

18.3.5 na majetek Dodavatele je prohlášen úpadek, Dodavatel sám podá dlužnický návrh na zahájení insolvenčního řízení nebo insolvenční návrh je zamítnut proto, že majetek nepostačuje k úhradě nákladů insolvenčního řízení (ve znění insolvenčního zákona); nebo

18.3.6 Dodavatel vstoupí do likvidace; nebo

18.3.7 Dodavatel předem neoznámí Objednateli jakoukoliv změnu osoby poddodavatele nebo zvětšení rozsahu plnění svěřeného poddodavateli ve smyslu odst. 3.5 této Smlouvy, nebo k takovéto změně Objednatel nedá předem souhlas dle téhož článku.

18.4 Dodavatel je oprávněn odstoupit od této Smlouvy v případě prodlení Objednatele se zaplacením jakékoliv splatné částky dle této Smlouvy po dobu delší než šedesát (60) kalendářních dnů, pokud Objednatel nezjedná nápravu ani v dodatečné přiměřené lhůtě, kterou mu k tomu Dodavatel poskytne v písemné výzvě ke splnění povinnosti, přičemž tato lhůta nesmí být kratší než patnáct (15) kalendářních dnů od doručení takovéto výzvy.

18.5 Účinky odstoupení od Smlouvy nastávají dnem doručení písemného oznámení o odstoupení druhé Smluvní straně.

18.6 Objednatel je oprávněn tuto Smlouvu písemně vypovědět (a to i částečně) bez udání důvodů, a to s jedno (1) měsíční výpovědní dobou, která uplyne ke konci měsíce následujícího po měsíci doručení písemné výpovědi Dodavateli. Tuto výpověď nebo částečnou výpověď je Objednatel oprávněn učinit kdykoliv po dobu trvání této Smlouvy.

18.7 Ukončením platnosti této Smlouvy nejsou dotčena ustanovení Smlouvy týkající se licencí, záruk, práv z vady, povinnosti nahradit újmu a povinnosti hradit smluvní pokuty, ustanovení o ochraně informací, ani další ustanovení a nároky, z jejichž povahy vyplývá, že mají trvat i po zániku platnosti této Smlouvy.

18.8 Zánikem platnosti této Smlouvy není dotčeno vzájemné plnění, pokud bylo řádně poskytnuto ani práva a nároky z takových plnění vyplývající. V případě, kdy by však Objednatel odstoupil od Smlouvy z důvodu takového porušení smluvní povinnosti Dodavatele, že se plnění Dodavatele stalo pro Objednatele nepotřebným, bude toto plnění Dodavateli vráceno a ten bude povinen vrátit Objednateli zaplacenou cenu.

19. KYBERNETICKÁ BEZPEČNOST

19.1 Dodavatel prohlašuje, že je poskytovatelem regulované služby ve smyslu zákona č. 264/2025 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů.

19.2 Dodavatel se zavazuje plnit a dodržovat veškeré povinnosti, které se na Dodavatele v této souvislosti vztahují.

19.3 Dodavatel prohlašuje, že má implementována veškerá bezpečnostní opatření k zajištění důvěrnosti, integrity a dostupnosti regulované služby v souladu se zákonem o kybernetické bezpečnosti a příslušnými prováděcími předpisy, a to minimálně v rozsahu požadavků uvedených v **Příloze č. 7** této Smlouvy (dále jen „**Kybernetické požadavky**").

19.4 Dodavatel umožní Objednateli v roční periodě po dobu trvání této Smlouvy a jeden (1) rok po ukončení trvání této Smlouvy provedení zákaznického auditu v souladu s požadavky **Přílohy č. 7**:

19.4.1 jehož rozsah bude ohraničen využíváním ICT prostředků Dodavatele pro potřeby plnění této Smlouvy a uloženými či zpracovávanými daty a informacemi Objednatele v ICT prostředí Dodavatele; a

19.4.2 jehož předmětem bude naplnění Kybernetických požadavků a hodnocení rizik dle **Přílohy č. 7** této Smlouvy.

19.5 Objednatel je oprávněn při kontrole Kybernetických požadavků využít třetí stranu. V případě využití třetí strany bude Objednatel odpovídat za třetí stranu, jako by kontrolu prováděl sám, včetně odpovědnosti za způsobenou újmu.

19.6 Dodavatel umožní Objednateli kontrolu Kybernetických požadavků provedenou prostředky Objednatele nebo třetí strany, a to v lokalitě Dodavatele i vzdáleně, pokud to technické prostředky Dodavatele umožňují.

19.7 Dodavatel se zavazuje poskytnout Objednateli součinnost minimálně v rozsahu deset (10) ČD při provádění každého zákaznického auditu ze strany Objednatele a pro tuto činnost zajistit účast kvalifikovaných pracovníků.

19.8 Dále se Dodavatel zavazuje nedostatky zjištěné na základě provedeného hodnocení rizik dle **Přílohy č. 7** této Smlouvy nebo v rámci provedeného auditu dle této Smlouvy a **Přílohy č. 7** této Smlouvy odstranit ve lhůtě určené v písemném oznámení Objednatele. Nestanoví-li Objednatel lhůtu v písemném oznámení,

zavazují se Smluvní strany dohodnout na lhůtě pro odstranění nedostatku, která nepřevýší devadesát (90) dnů.

19.9 Dodavatel se dále dle této Smlouvy zavazuje:

19.9.1 poskytnout na vyžádání Objednateli dokumenty a obdobné vstupy, které budou prokazovat naplnění Kybernetických požadavků;

19.9.2 na požádání s Objednatelem konzultovat kdykoli v průběhu poskytování Služeb dle této Smlouvy detailní nastavení bezpečnostních opatření k naplnění Kybernetických požadavků a pro takovéto konzultace zajistit účast kvalifikovaných pracovníků;

19.9.3 neprodleně informovat Objednatele o všech významných změnách v naplnění Kybernetických požadavků, které nastanou kdykoli v průběhu trvání této Smlouvy;

19.9.4 informovat Objednatele o významné změně ovládání Dodavatele. Ovládáním se rozumí vliv, ovládání či řízení dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích);

19.9.5 bezodkladně a s vyvinutím nejlepšího úsilí zajistit náhradní způsob naplnění Kybernetických požadavků, pokud stávající řešení přestalo být funkční a efektivní;

19.9.6 bezodkladně informovat Objednatele o bezpečnostních incidentech, které mohou ovlivnit poskytování Služeb dle této Smlouvy; a

19.9.7 při výkonu své činnosti včas a prokazatelně upozornit Objednatele na zřejmou nevhodnost jeho příkazů či doporučení vztahující se ke Kybernetickým požadavkům a jejichž následkem může vzniknout újma nebo nesoulad se ZKB nebo jinými obecně závaznými právními předpisy.

19.10 Dodavatel se zavazuje dodávat pouze hardware, které splňuje požadavky právních předpisů na kybernetickou bezpečnost a digitální odolnost hardware jakožto věci s digitálním obsahem a digitálními prvky tak, aby je Dodavatel mohl bez omezení provozovat na území EHP.

20. INFORMAČNÍ POVINNOST DODAVATELE

20.1 Dodavatel je povinen Objednatele bez zbytečného odkladu informovat o identifikovaných kybernetických bezpečnostních incidentech a hrozbách souvisejících s plněním Smlouvy a/nebo s daty, nejpozději však do dvanácti (12) hodin od jejich výskytu.

20.2 Dodavatel je povinen poskytnout Objednateli veškerou součinnost nutnou ke splnění povinností Objednatele v oblasti řízení rizik, zejména při:

20.2.1 identifikaci aktiv v rámci předmětu plnění Smlouvy a jejich kategorizaci, hodnocení a zařazení do bezpečnostních úrovní,

20.2.2 identifikaci, analýze a hodnocení rizik pro aktiva,

20.2.3 ošetření rizik včetně zpracování prohlášení o aplikovatelnosti a plánu zvládání rizik pro aktiva;

20.3 Dodavatel je povinen Objednatele informovat o:

20.3.1 významné změně ovládání Dodavatele, přičemž ovládáním se rozumí vliv, ovládání či řízení dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů; či ekvivalentní postavení, a to do 20 pracovních dnů od uskutečnění této změny,

20.3.2 změně vlastnictví či oprávnění nakládat se zásadními aktivy využívanými Dodavatelem k plnění Smlouvy, a to do 20 pracovních dnů od uskutečnění této změny, a

20.3.3 fyzických osobách přicházejících do kontaktu s důvěrnými informacemi Objednatele,

přičemž k informování využije Dodavatel definovaný postup skrze kontaktní osobu.

20.4 Dodavatel je povinen poskytnout Objednateli a příslušným dozorovým orgánům veškerou nutnou součinnost v případě dozorového auditu za účelem ověření řízení kybernetické bezpečnosti.

20.5 Učiní-li orgány činné v trestním řízení nebo jiné orgány státní správy jakoukoli právně závaznou žádost o poskytnutí dat Objednatele směrem k Dodavateli, je Dodavatel povinen tuto skutečnost oznámit Objednateli s předstihem před poskytnutím takových informací, pokud mu to právní předpisy nezakazují.

20.6 Dodavatel je povinen Objednatele informovat o žádosti cizozemského orgánu o zpřístupnění nebo předání dat zpracovávaných na území cizího státu, vyjma situace, kdy by takové informování bylo v rozporu s právním řádem, v jehož působnosti dochází ke zpracování dat nebo podle kterého byla žádost podána.

21. ŘEŠENÍ SPORŮ

21.1 Práva a povinnosti Smluvních stran touto Smlouvou výslovně neupravené se řídí OZ a příslušnými právními předpisy souvisejícími.

21.2 Smluvní strany se zavazují vyvinout maximální úsilí k odstranění vzájemných sporů vzniklých na základě této Smlouvy nebo v souvislosti s touto Smlouvou, včetně sporů o její výklad či platnost a usilovat o jejich vyřešení nejprve smírně prostřednictvím jednání oprávněných osob nebo pověřených zástupců, a to do šedesáti (60) kalendářních dnů ode dne doručení výzvy ke smírnému vyřešení sporu zaslané kteroukoliv Smluvní stranou druhé Smluvní straně.

21.3 Nebude-li sporná záležitost vyřešena dle odst. 21.2 této Smlouvy do šedesáti (60) kalendářních dnů ode dne doručení výzvy ke smírnému vyřešení sporu zaslané kteroukoliv Smluvní stranou druhé Smluvní straně, bude tento spor rozhodován s konečnou platností u příslušného obecného soudu České republiky. Smluvní strany se dohodly, že místně příslušným soudem pro řešení případných sporů bude soud příslušný dle místa sídla Objednatele.

22. ZÁVĚREČNÁ USTANOVENÍ

22.1 Tato Smlouva představuje úplnou dohodu Smluvních stran o předmětu této Smlouvy. Tuto Smlouvu je možné měnit pouze písemnou dohodou Smluvních stran ve formě číslovaných dodatků této Smlouvy, podepsaných osobami oprávněnými jednat jménem Smluvních stran, přičemž jakákoliv změna Smlouvy bude provedena v souladu se ZZVZ.

22.2 Pokud by se kterékoliv ustanovení této Smlouvy ukázalo být neplatným nebo nevynutitelným nebo se jím stalo po uzavření této Smlouvy, pak tato skutečnost nepůsobí neplatnost ani nevynutitelnost ostatních ustanovení této Smlouvy, nevyplývá-li z donucujících ustanovení právních předpisů jinak. Smluvní strany se zavazují takové neplatné či nevynutitelné ustanovení nahradit v souladu se ZZVZ platným a vynutitelným ustanovením, které je svým obsahem nejbližší účelu neplatného či nevynutitelného ustanovení.

22.3 Smluvní strany ujednávají, že v případě jakéhokoli rozporu, nesouladu nebo odlišné úpravy mezi textem této Smlouvy a ustanoveními **Přílohy č. 1** této Smlouvě se použijí a mají přednost ustanovení obsažená v uvedené **Příloze č. 1** této Smlouvy. Tímto ujednáním nejsou dotčena ostatní ustanovení Smlouvy, která zůstávají v platnosti a účinnosti.

22.4 Uzavření smlouvy bylo odsouhlaseno usnesením Rady městské části č. 735/RMČ/2025 ze dne 19. 11. 2025.

22.5 Smluvní strany souhlasí s uveřejněním plného znění této Smlouvy v registru smluv podle Zákona o registru smluv, a rovněž na profilu Objednatele, případně i na dalších místech, kde tak stanoví právní předpis. Uveřejnění Smlouvy prostřednictvím registru smluv zajistí Objednatel.

22.6 Právní vztahy v této Smlouvě neupravené nebo upravené jen částečně se řídí právním řádem České republiky, zejména příslušnými ustanoveními OZ.

22.7 Veškerá práva a povinnosti vyplývající z této Smlouvy přecházejí, pokud to povaha těchto práv a povinností nevylučuje, na právní nástupce Smluvních stran.

22.8 Dodavatel není oprávněn postoupit peněžité nároky vůči Objednateli na třetí osobu bez předchozího písemného souhlasu Objednatele.

22.9 Nedílnou součást Smlouvy tvoří tyto přílohy:

1. **Příloha č. 1**: Detailní technická specifikace Plnění
2. **Příloha č. 2:** Harmonogram
3. **Příloha č. 3**: Oprávněné osoby
4. **Příloha č. 4**: Seznam poddodavatelů
5. **Příloha č. 5**: Specifikace ceny
6. **Příloha č. 6**: Seznam členů realizačního týmu
7. **Příloha č. 7:** Kybernetické požadavky
8. **Příloha č. 8:** Specifikace Podpory výrobce

Smluvní strany prohlašují, že si tuto Smlouvu přečetly, že s jejím obsahem souhlasí a na důkaz toho k ní připojují svoje podpisy.

Objednatel	**Dodavatel**
V Praze dne (dle el. podpisu)	V Praze dne (dle el. podpisu)
[redacted]	[redacted]
Městská část Praha **14**	Next Generation Security Solutions s.r.o.
Jiří Zajac,	Mgr. Ondrej Dedek,
starosta	jednatel

Příloha č. 1

Technická specifikace Plnění

V této příloze Objednatel vymezuje minimální požadavky na Plnění v podobě specifikace minimálních technických a funkčních parametrů uvedených na listu *tech. spec. checklist* v **Příloze č. 1** této Smlouvy. Dodavatel může nabídnout dodávky s lepšími parametry (v případě, že lze objektivně stanovit, že se jedná o parametry lepší), nikoli s parametry horšími, než požaduje Objednatel.

Pro usnadnění orientace je u jednotlivých typů buněk označení: **ID číslo.**

Technická specifikace je rozdělena do následujících opatření:

ID01 – Pokročilý síťový monitoring
ID02 – Posílení primárního datového centra
ID03 – Výměna a implementace aktivních síťových prvků
ID04 – Výměna a implementace WiFi infrastruktury
ID05 – Výměna a implementace zálohovací infrastruktury
ID06 – Zavedení systému řízení kybernetické bezpečnosti a výkon role manažera KB
ID07 – Firewally pro detašovaná pracoviště
ID08 – Kompletní správa životního cyklu logů
ID09 – Automatická, periodická kontrola stavu bezpečnosti IT systémů a aplikací

Příloha č. 2

Harmonogram

Název opatření	Termín realizace opatření, tj. realizace Dodávek a Služeb dle Opatření	Nejzazší doba pro realizaci
ID01 – Pokročilý síťový monitoring	T1	T0 + max. 75 kalendářních dní
ID02 – Posílení primárního datového centra	T2	T0 + max. 75 kalendářních dní
ID03 – Výměna a implementace aktivních síťových prvků	T3	T0 + max. 75 kalendářních dní
ID04 – Výměna a implementace WiFi infrastruktury	T4	T0 + max. 75 kalendářních dní
ID05 – Výměna a implementace zálohovací infrastruktury	T5	T0 + max. 75 kalendářních dní
ID06 – Zavedení systému řízení kybernetické bezpečnosti a výkon role manažera KB	T6	T0 + max. 75 kalendářních dní
ID07 – Firewally pro detašovaná pracoviště	T7	T0 + max. 75 kalendářních dní
ID08 – Kompletní správa životního cyklu logů	T8	T0 + max. 75 kalendářních dní
ID09 – Automatická, periodická kontrola stavu bezpečnosti IT systémů a aplikací	T9	T0 + max. 75 kalendářních dní

Detailní harmonogram pro jednotlivá Opatření ID01 až ID09 bude předložen Dodavatelem jako součást jeho podané nabídky

Dodavatel respektuje výše uvedenou nejzazší dobu pro realizaci opatření.

Poskytování Podpory **(platí souhrnně pro všechna opatření ID01 až ID09)**	Termín zahájení Podpory	Délka poskytování Podpory
Podpora výrobce – do 31. 5. 2026	TX	od TX do 31. 5. 2026
Podpora výrobce – po 1. 6. 2026	1. 6. 2026	od 1. 6. 2026 + 60 měsíců
Provozní podpora – do 31. 5. 2026	TX	od TX do 31. 5. 2026
Provozní podpora – po 1. 6. 2026	1. 6. 2026	od 1. 6. 2026 + 60 měsíců

T0 = den účinnosti Smlouvy.

TX = termín akceptace příslušného Dodávky a Služby dle Technické specifikace.

Harmonogram Smlouvy plyne z technických důvodů na straně Objednatele a Objednatel považuje porušení Harmonogramu za podstatné porušení Smlouvy.

Příloha č. 3

Oprávněné osoby

Za Objednatele:

ve věcech smluvních:

Jméno a příjmení	[redacted]
Adresa	
E-mail	
Telefon	

ve věcech obchodních:

Jméno a příjmení	[redacted]
Adresa	
E-mail	
Telefon	

ve věcech technických:

Jméno a příjmení	[redacted]
Adresa	
E-mail	
Telefon	

ve věcech kybernetické bezpečnosti:

Jméno a příjmení	[redacted]
Adresa	
E-mail	
Telefon	

Za Dodavatele:
ve věcech smluvních:

Jméno a příjmení	[redacted]
Adresa	
E-mail	
Telefon	

ve věcech obchodních:

Jméno a příjmení	[redacted]
Adresa	
E-mail	
Telefon	

ve věcech technických:

Jméno a příjmení	[redacted]
Adresa	
E-mail	
Telefon	

ve věcech kybernetické bezpečnosti:

Jméno a příjmení	[redacted]
Adresa	
E-mail	
Telefon	

Příloha č. 4

Seznam poddodavatelů

1)

Název:	TOTAL SERVICE a.s.
Sídlo:	U Uranie 954/18, Holešovice, 170 00 Praha 7
Právní forma:	Akciová společnost
Identifikační číslo:	25618067
Rozsah a identifikace plnění Smlouvy:	40 % - Dodávka, implementace a zprovoznění storage, serverové, firewallové a Wi-Fi infrastruktury datového centra, včetně instalace, konfigurace a správy operačních systémů Linux a Windows, zajištění provozuschopnosti serverového a síťového prostředí, spolupráce při testování, uvedení do provozu a zpracování provozní dokumentace, zajištění dvou členů týmu a služby spojené s jejich pozicí.

Příloha č. 5
Specifikace ceny

ID opatření	Název opatření	Dodávka HW, SW (licencí)	Služby (instalace, implementace, školení, ad.)	Technická podpora na 60 měsíců (od 1.6.2026)
01	Pokročilý síťový monitoring	**Cena v Kč bez DPH**		
		2 344 100,00 Kč	406 000,00 Kč	1 672 500,00 Kč
		Cena v Kč vč. DPH		
		2 836 361,00 Kč	491 260,00 Kč	2 023 725,00 Kč

ID opatření	Název opatření	Dodávka HW, SW (licencí)	Služby (instalace, implementace, školení, ad.)	Technická podpora na 60 měsíců (od 1.6.2026)
02	Posílení primárního datového centra - redundance	**Cena v Kč bez DPH**		
		6 014 800,00 Kč	620 000,00 Kč	4 344 200,00 Kč
		Cena v Kč vč. DPH		
		7 277 908,00 Kč	750 200,00 Kč	5 256 482,00 Kč

ID opatření	Název opatření	Dodávka HW, SW (licencí)	Služby (instalace, implementace, školení, ad.)	Technická podpora na 60 měsíců (od 1.6.2026)
03	Výměna a implementace aktivních síťových prvků	**Cena v Kč bez DPH**		
		1 210 000,00 Kč	120 000,00 Kč	800 000,00 Kč
		Cena v Kč vč. DPH		
		1 464 100,00 Kč	145 200,00 Kč	968 000,00 Kč

ID opatření	Název opatření	Dodávka HW, SW (licencí)	Služby (instalace, implementace, školení, ad.)	Technická podpora na 60 měsíců (od 1.6.2026)
04	Výměna a implementace WiFi infrastruktury	**Cena v Kč bez DPH**		
		630 000,00 Kč	340 000,00 Kč	460 000,00 Kč
		Cena v Kč vč. DPH		
		762 300,00 Kč	411 400,00 Kč	556 600,00 Kč

ID opatření	Název opatření	Dodávka HW, SW (licencí)	Služby (instalace, implementace, školení, ad.)	Technická podpora na 60 měsíců (od 1.6.2026)
05	Výměna a implementace zálohovací infrastruktury	**Cena v Kč bez DPH**		
		5 141 200,00 Kč	720 000,00 Kč	4 039 200,00 Kč
		Cena v Kč vč. DPH		
		6 220 852,00 Kč	871 200,00 Kč	4 887 432,00 Kč

ID opatření	Název opatření	Dodávka HW, SW (licencí)	Služby (instalace, implementace, školení, ad.)	Technická podpora na 60 měsíců (od 1.6.2026)
06	Zavedení systému řízení kybernetické bezpečnosti včetně sledování a vyhodnocování rizik a atributů na úrovni podpůrných aktiv a výkon role manažera KB	**Cena v Kč bez DPH**		
		1 180 000,00 Kč	623 000,00 Kč	1 420 000,00 Kč
		Cena v Kč vč. DPH		
		1 427 800,00 Kč	753 830,00 Kč	1 718 200,00 Kč

ID opatření	Název opatření	Dodávka HW, SW (licencí)	Služby (instalace, implementace, školení, ad.)	Technická podpora na 60 měsíců (od 1.6.2026)
07	Firewally pro detašovaná pracoviště	**Cena v Kč bez DPH**		
		375 900,00 Kč	140 000,00 Kč	430 600,00 Kč
		Cena v Kč vč. DPH		
		454 839,00 Kč	169 400,00 Kč	521 026,00 Kč

ID opatření	Název opatření	Dodávka HW, SW (licencí)	Služby (instalace, implementace, školení, ad.)	Technická podpora na 60 měsíců (od 1.6.2026)
08	Kompletní správa životního cyklu logů	**Cena v Kč bez DPH**		
		1 919 300,00 Kč	388 000,00 Kč	1 597 400,00 Kč
		Cena v Kč vč. DPH		
		2 322 353,00 Kč	469 480,00 Kč	1 932 854,00 Kč

ID opatření	Název opatření	Dodávka HW, SW (licencí)	Služby (instalace, implementace, školení, ad.)	Technická podpora na 60 měsíců (od 1.6.2026)
09	Automatická, periodická kontrola stavu bezpečnosti IT systémů a aplikací	**Cena v Kč bez DPH**		
		443 000,00 Kč	134 000,00 Kč	470 800,00 Kč
		Cena v Kč vč. DPH		
		536 030,00 Kč	162 140,00 Kč	569 668,00 Kč

Celková cena

Položka	Cena v Kč bez DPH	Cena v Kč vč. DPH	
Celkem Dodávka HW, SW (licencí) = ID01+ID02+ID03+ID04+ID05+ID06+ID07+ID08+ID09	19 258 300,00 Kč	23 302 543,00 Kč	
Celkem Služby (instalace, implementace, školení, ad.) = ID01+ID02+ID03+ID04+ID05+ID06+ID07+ID08+ID09	3 491 000,00 Kč	4 224 110,00 Kč	
Celkem Dodávka HW, SW a Služeb	22 749 300,00 Kč	27 526 653,00 Kč	
Celkem Technická podpora na 60 měsíců (od 1.6.2026) = ID01+ID02+ID03+ID04+ID05+ID06+ID07+ID08+ID09	15 234 700,00 Kč	18 433 987,00 Kč	

Příloha č. 6

Seznam členů realizačního týmu

Pozice (role)	Identifikační údaje osoby	Dodavatel/ člen společnosti dodavatelů / poddodavatel, k němuž osoba patří
1. Projektový manažer	[redacted]	dodavatel
2. Specialista architekt řešení		dodavatel
3. Specialista systémů řízení bezpečnosti informací (SŘBI)		dodavatel
4. IT specialista OS Linux		poddodavatel TOTAL SERVICE a.s.
5. IT specialista OS Windows		poddodavatel TOTAL SERVICE a.s.

Příloha č. 7

Kybernetická bezpečnost

Za účelem povinností stanovených Objednateli jakožto poskytovali regulované služby v oblasti řízení bezpečnosti dodavatelského řetězce, je Dodavatel povinen nad rámec povinností stanovených Smlouvou plnit níže uvedené povinnosti zejm. součinnostního a bezpečnostního charakteru dle této **Přílohy č. 7** této Smlouvy.

Dodavatel je povinen plnit relevantní povinnosti v rozsahu a způsobem, aby byl naplněn účel právní úpravy bezpečnostních opatření, kybernetických bezpečnostních incidentů, protiopatření, náležitostí podání v oblasti kybernetické bezpečnosti a likvidaci dat ve vztahu k povinnostem, které tato právní úprava stanovuje Objednateli, jakožto povinné osobě dle předpisů z oblasti kybernetické bezpečnosti, a to i v případě změny příslušné právní úpravy. V takovém případě je Objednatel oprávněn požadovat od Dodavatele přiměřenou součinnost i nad rámec povinností stanovených v této **Příloze č. 7** této Smlouvy, avšak vždy pouze za účelem zajištění plnění povinnosti Dodavatele z oblasti kybernetické bezpečnosti ve smyslu shora uvedeného.

1. OBECNÁ USTANOVENÍ

1.1 Tato příloha (dále jen „**Příloha**“) tvoří nedílnou součást Smlouvy. Povinnosti Dodavatele uvedené v této příloze se vztahují výhradně ke Službám, které jsou předmětem Smlouvy.

1.2 Není-li dále stanoveno jinak nebo nevyplývá-li jinak z kontextu, mají pojmy počínající velkým písmenem v této Příloze shodný význam, jaký mají ve Smlouvě. Smluvní strany nad rámec Smlouvy vymezují následující pojmy:

1.2.1 **Data** znamenají data, záznamy, soubory, obsah, osobní údaje a další informace Objednatele, (a) shromážděné, přijaté nebo uchovávané Dodavatelem v souvislosti s plněním Smlouvy; (b) poskytnuté Objednatelem; nebo (c) odvozené z (a) a (b). Data podle této Smlouvy jsou klasifikována jako důvěrné informace, nebo se z jiných důvodů jedná o údaje vyžadující ochranu před neoprávněným přístupem, únikem, porušením nebo jiným odhalením;

1.2.2 **ZKB** znamená zákon č. 264/2025 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů.

1.3 Rozsah zapojení Dodavatele na rozvoji a provozu primárních a podpůrných aktiv Objednatele je určen předmětem Smlouvy a jejími přílohami včetně této Přílohy. Rozsah zapojení Dodavatele na zajištění bezpečnosti těchto aktiv je určen zejména touto Přílohou.

2. BEZPEČNOST INFORMACÍ

2.1 Dodavatel se zavazuje při nakládání s Daty chránit jejich důvěrnost, dostupnost a integritu s ohledem na jejich povahu a klasifikaci v souladu s touto Přílohou a dále v souladu se standardním bezpečnostním rámcem ISO 27001, případně dalším bezpečnostním rámcem jako např. NIST Cyber Security Framework nebo SSAE 18 SOC 2, a to do té míry, do jaké to není v rozporu s touto Přílohou.

2.2 Dodavatel je povinen zavést vhodná bezpečnostní opatření pro ochranu Dat alespoň v rozsahu této Přílohy.

2.3 Dodavatel jmenuje odpovědnou kontaktní osobu ve věcech kybernetické bezpečnosti pro potřeby zajištění plnění požadavků podle této Přílohy a Smlouvy v oblasti kybernetické bezpečnosti a související komunikace s Objednatelem. Poskytovatel je povinen oznámit kontaktní údaje této osoby Objednateli v **Příloze č. 3** Smlouvy – „Oprávněné osoby".

3. UŽITÍ A ZPŘÍSTUPNĚNÍ DAT

3.1 Dodavatel je oprávněn používat nebo sdílet Data pouze pro účely a způsobem, který stanoví Smlouva a její přílohy, a v souladu s příslušnými právními předpisy, po dobu trvání Smlouvy a po jejím ukončení, dokud má Dodavatel Data nadále ve své dispozici.

3.2 Dodavatel bere na vědomí, že veškerá Data zůstávají předmětem výhradních práv Objednatele, který je jediným vlastníkem Dat a pořizovatelem databází, ve kterých jsou Data uložena.

3.3 Dodavatel se zavazuje zachovávat mlčenlivost o Datech a jejich obsahu.

3.4 Dodavatel se zavazuje šifrovat v prostředí Poskytovatele uložená Data minimálně v souladu se standardem šifrování dat AES-256.

3.5 Dodavatel je povinen omezit přístup k Datům Objednatele pouze na ty zaměstnance a třetí strany, u kterých přístup vyžaduje plnění Smlouvy nebo plnění zákonných povinností. Dodavatel nesmí umožnit přístup k Datům Objednatele jiným třetím stranám bez předchozího písemného souhlasu Objednatele. Vysloví-li Objednatel v souladu se Smlouvou nebo jinak písemně souhlas se zapojením konkrétního poddodavatele do plnění Smlouvy, uděluje tím souhlas se zpřístupněním Dat Objednatele poddodavateli v rozsahu nezbytném pro plnění Smlouvy poddodavatelem.

3.6 V případě, že Objednatel při hodnocení rizik spojených se Smlouvou identifikuje skutečnosti, jejichž existence tvoří:

3.6.1 kybernetickou hrozbu a výskyt této hrozby je velmi pravděpodobný až víceméně jistý či předpokládaná realizace hrozby je častější než jednou za měsíc, nebo

3.6.2 riziko pro předmět Smlouvy a toto riziko je na natolik závažné (kritické), že jeho existence je nepřípustná a musí být neprodleně zahájeny kroky k jeho odstranění,

může Objednatel Dodavateli uložit přijetí dalších bezpečnostních opatření ve smyslu ZKB, případně zákona, který ZKB nahradí. Objednatel při naplnění podmínek výše předá Dodavateli popis vybraných bezpečnostních opatření, která navrhuje zavést ke snížení identifikovaného rizika. Dodavatel je oprávněn bez zbytečného odkladu, nejpozději však do 15 pracovních dní, podat připomínky k formě zvolených bezpečnostních opatření (včetně přehledu očekávaných

finančních dopadů na zavedení bezpečnostních opatřeních na straně Dodavatele) a případně navrhnout jinou formu zvolených bezpečnostních opatření. Dohodnou-li se Objednatel a Dodavatel na zavedení bezpečnostních opatření, na termínu jejich zavedení a na tom, kdo ponese náklady na jejich zavedení, je Dodavatel povinen bez zbytečného odkladu zavést daná bezpečnostní opatření a jejich zavedení oznámit Objednateli.

3.7 V případě, že cizozemský orgán požádá o zpřístupnění nebo předání Dat zpracovávaných na území cizího státu, Objednatel takové žádosti vyhoví:

3.7.1 až po provedení přezkoumání zákonnosti žádosti,

3.7.2 až po vynaložení veškerého úsilí k zabránění zpřístupnění nebo předání Dat v rámci možností daných právním řádem, v jehož působnosti dochází ke zpracování Dat nebo podle kterého byla žádost podána,

3.7.3 pouze v nezbytném rozsahu.

4. AUTORSTVÍ PROGRAMOVÉHO KÓDU A LICENCE

4.1 Smluvní strany ve Smlouvě sjednaly právo Objednatele k předmětům duševního vlastnictví. Úprava práv Objednatele k předmětům duševního vlastnictví se řídí Smlouvou.

5. BEZPEČNOSTNÍ DOKUMENTACE

5.1 Dodavatel se v souvislosti s řízením kybernetické bezpečnosti zavazuje vypracovat a udržovat příslušnou bezpečnostní dokumentaci týkající se nastaveného systému řízení bezpečnosti informací a zabezpečení plnění Smlouvy, minimálně v rozsahu dle této Přílohy.

5.2 Dodavatel je povinen bezpečnostní dokumentaci podle této Přílohy pravidelně revidovat a aktualizovat, nejméně však 1× za rok, a kdykoli při významné změně a materiální změně skutečností zachycených v bezpečnostní dokumentaci.

6. ŘÍZENÍ AKTIV

6.1 Dodavatel se zavazuje minimálně:

6.1.1 identifikovat primární a podpůrná aktiva využívaná pro plnění Smlouvy;

6.1.2 určit vazby mezi primárními a podpůrnými aktivy a případně určit vazby na současná aktiva Objednatele;

6.1.3 tento seznam aktiv a jejich vazby udržovat aktuální a na vyžádání ho zpřístupnit (ve formě nahlédnutí) Objednateli.

7. ŘÍZENÍ RIZIK

7.1 Dodavatel se zavazuje minimálně:

7.1.1 řídit rizika, která mohou ovlivnit poskytování předmětu plnění Smlouvy, v souladu s následujícími minimálními požadavky na řízení rizik:

a) stanovit metodiku pro určování a hodnocení rizik, včetně kritérií pro akceptovatelnost rizik,

b) při určování rizik s ohledem na aktiva určit relevantní hrozby a zranitelnosti,

c) provádět hodnocení rizik v pravidelných intervalech alespoň jednou ročně a při významných změnách, přičemž budou zohledněny relevantní hrozby a zranitelnosti a posouzeny možné dopady na aktiva využívaná pro plnění Smlouvy,

d) zpracovat přehled všech bezpečnostních opatření, která byla aplikována, včetně způsobu plnění,

e) zpracovat plán zvládání rizik, který obsahuje minimálně popis bezpečnostních opatření a konkrétní způsob jejich realizace, cíle a přínosy bezpečnostních opatření a určení odpovědností,

f) zavádět bezpečnostní opatření v souladu s plánem zvládání rizik;

7.1.2 informovat Objednatele o způsobu řízení rizik, zbytkových rizicích souvisejících s plněním Smlouvy a předložit Objednateli zprávu o hodnocení aktiv a rizik, která jsou využívána pro plnění Smlouvy a o zbytkových rizicích souvisejících s aktivy využívanými pro plnění Smlouvy do 30 dnů od data účinnosti Smlouvy a následně v intervalu jednou za dva roky nebo v případě významné změny ovlivňující bezpečnost těchto aktiv;

7.1.3 reagovat na změny a upravit na své straně bezpečnostní opatření tak, aby odpovídala novému stavu po provedení změny;

7.1.4 pravidelně (minimálně 1× ročně) testovat zranitelnosti poskytovaných Služeb, a to prostřednictvím pravidelného penetračního testování a kontroly nasazených aktualizací, aby bylo zajištěno, že jsou bezpečnostní opatření aktuální vůči novým hrozbám. Poskytovatel je povinen o výsledcích testování dle tohoto odstavce Objednatele písemně informovat neprodleně po vyhotovení závěrečné zprávy z takového testování.

8. BEZPEČNOST LIDSKÝCH ZDROJŮ

8.1 Poskytovatel se zavazuje minimálně:

8.1.1 prověřit každého pracovníka před umožněním přístupu k aktivům Objednatele nebo před jeho zapojením do činností, které by mohly ovlivnit předmět plnění Smlouvy, a to alespoň z hlediska:

a) kontroly dosaženého vzdělání a odborné kvalifikace,

b) profesních zkušeností, jde-li o pracovníky, kteří mají zastávat bezpečnostní nebo administrátorské role;

8.1.2 zavést pravidelné školení svých pracovníků v oblasti kybernetické bezpečnosti a základní kybernetické hygieny a vést o tomto školení spolehlivou evidenci;

8.1.3 poučit své pracovníky o požadavcích dle této Přílohy před umožněním jejich přístupu k Datům nebo před jejich zapojením do činností, které by mohly ovlivnit bezpečnost v souvislosti s předmětem plnění Smlouvy;

8.1.4 zajistit, aby pracovníci před umožněním jejich přístupu k Datům nebo před zapojením do činností, které by mohly ovlivnit bezpečnost předmětu plnění Smlouvy, měli uzavřenou dohodu o zachování mlčenlivosti (důvěrnosti) Dat s adekvátní dobou trvání povinnosti mlčenlivosti;

8.1.5 zajistit procesy a pravidla vedení disciplinárního řízení (zejména odstupňované reakce) a v případě potřeby provádět disciplinární řízení k přijetí opatření vůči pracovníkům, kteří porušili povinnosti v oblasti kybernetické bezpečnosti;

8.1.6 zajistit dostatečnou míru zastupitelnosti pro technické bezpečnostní aspekty plnění Smlouvy.

8.2 Poddodavatel Dodavatele, který přistupuje k Datům, je povinen dodržovat veškeré povinnosti uvedené v odst. 8.1 této Přílohy ve vztahu ke svým zaměstnancům, případně dalším osobám, které se podílejí na realizaci předmětu plnění Smlouvy dle pokynů poddodavatele Dodavatele. Dodavatel je povinen poddodavatele o povinnostech plynoucích z odst. 8.1 této Přílohy řádně poučit a uzavřít s poddodavatelem písemnou smlouvu v souladu s čl. 23 této Přílohy.

9. ŘÍZENÍ PROVOZU

9.1 Dodavatel se zavazuje minimálně:

9.1.1 stanovit práva a povinnosti administrátorů, uživatelů a osob zastávajících bezpečnostní role;

9.1.2 stanovit pravidla a postupy pro ochranu před škodlivým kódem;

9.1.3 stanovit pravidla a postupy pro řízení technických zranitelností;

9.1.4 stanovit pravidla a postupy k provádění pravidelného zálohování a kontroly použitelnosti prováděných záloh;

9.1.5 stanovit pravidla pro zajištění oddělení vývojového, testovacího a provozního prostředí.

10. ŘÍZENÍ ZMĚN

10.1 Dodavatel se zavazuje minimálně:

10.1.1 sledovat a identifikovat změny, které mají nebo mohou mít vliv na zajištění kybernetické bezpečnosti Dat a informovat Objednatele o této skutečnosti;

10.1.2 poskytnout Objednateli veškeré potřebné informace a součinnost v procesu řízení a evidence změn. Informace musí být poskytnuty v rozsahu, který Objednateli umožní:

a) posoudit, zda změna ve vztahu k plnění dle Smlouvy je významnou změnou,

b) posoudit rizika související s významnou změnou ve vztahu k plnění dle Smlouvy, testovat změnu před nasazením do provozu a posoudit možnost případného navrácení do původního stavu,

c) přijmout přiměřená opatření ke zvládání rizik souvisejících s touto změnou, nebo změnu vůbec neprovést, pokud nelze přijmout opatření snižující tato rizika na akceptovatelnou úroveň,

d) dokumentovat posouzení rizik souvisejících s významnou změnou ve vztahu k plnění dle Smlouvy a přijatá opatření, a

e) provést další činnosti u významných změn dle potřeb Objednatele;

10.1.3 reagovat na významné změny, zejména aktualizovat hodnocení rizik, bezpečnostní a provozní dokumentaci a upravit na své straně bezpečnostní opatření tak, aby odpovídala novému stavu po provedení změny.

11. ŘÍZENÍ KONTINUITY ČINNOSTÍ

11.1 Dodavatel se v rozsahu předmětu plnění dle Smlouvy zavazuje zavést a udržovat vhodná opatření pro zajištění kontinuity činností. Zejména se Dodavatel zavazuje:

11.1.1 zajistit adekvátní kontinuitu aktiv, která jsou potřebná k poskytování plnění dle Smlouvy; a

11.1.2 pravidelně kontrolovat a testovat, že je schopen zajistit kontinuitu aktiv při dodržení sjednané úrovně plnění dle Smlouvy.

11.2 Dodavatel se zavazuje poskytnout nezbytnou součinnost při zpracování a testování plánů kontinuity, plánů obnovy a havarijních plánů a plnění dalších povinností Objednatele a následně v případě aktivace plánů kontinuity, plánů obnovy nebo havarijních plánů, poskytnout nezbytnou součinnost při jejich plnění. Objednatel se zavazuje uhradit Dodavateli účelně vynaložené náklady na poskytnutí této součinnosti.

12. AKVIZICE, VÝVOJ A ÚDRŽBA

12.1 Dodavatel se zavazuje minimálně:

12.1.1 zajistit, aby zajištění bezpečnosti informací bylo zahrnuto do všech vývojových, implementačních či akvizičních projektů, kde je reálné narušení informační bezpečnosti Dat a ochrany soukromí, a vyčlenit pro tento účel potřebné zdroje;

12.1.2 zajistit oddělení vývojového, testovacího a provozního prostředí;

12.1.3 dodržovat nejlepší praxi v oblasti bezpečného vývoje a postupovat při vývoji v souladu s dalšími pokyny Objednatele.

13. ŘÍZENÍ PŘÍSTUPU

13.1 Dodavatel se zavazuje minimálně:

13.1.1 provozovat ke zpracování Dat pouze taková aktiva, která umožňují správu rolí a uživatelů a která neumožní činnost uživatelů bez autentizace a zároveň umožňují ochranu autentizačního mechanismu před neoprávněným přístupem a prolomením autentizačních parametrů;

13.1.2 zajistit, aby uživatelské účty byly adekvátně chráněny prostřednictvím autentizačních mechanismů;

13.1.3 zajistit, aby uživatelé chránili své uživatelské účty, zejména své autentizační údaje a nástroje a aby neposkytli tyto údaje třetí straně;

13.1.4 udělovat přístup pracovníkům podle zásady „need-to-know“ a průběžně kontrolovat a vyhodnocovat oprávněnost a potřebu přístupu;

13.1.5 zajistit kontrolu podezřelých přístupů a aktivit;

13.1.6 v případě potřeby bezodkladně odebrat přístupová oprávnění, zejména pokud

a) zaměstnanec již nepotřebuje přístup k plnění svých pracovních povinností (např. pokud došlo ke změně pozice zaměstnance/odchod z projektu apod.),

b) zaměstnanec se dopustil závažného porušení povinností v oblasti kybernetické bezpečnosti nebo existují důvodné obavy, že se takového porušení dopustí,

c) zaměstnanec nesplňuje požadavky na přístup k Datům nebo požadavky na zapojení do činností, které by mohly ovlivnit bezpečnost předmětu plnění Smlouvy,

d) se ukáže potřeba přijmout mimořádné bezpečností opatření spočívající v odebrání přístupu (zejména pokud Poskytovatel dal zaměstnanci výpověď z výpovědního důvodu podle § 52 písm. f), g) a h) zákoníku práce),

e) byl ukončen pracovní poměr (nebyl-li přístup odebrán dříve),

f) došlo k úniku autentizačních údajů (hesla);

13.1.7 vést evidenci o udělených a odebraných přístupových oprávněních;

13.1.8 vést evidenci o všech přístupech k Datům Objednatele, kdy je Dodavatel povinen archivovat záznamy o všech přístupech po dobu 1 roku;

13.1.9 zajistit zabezpečení a správu koncových zařízení (pracovní stanice typu osobní počítač nebo notebook, mobilní koncová zařízení – přenosná zařízení typu telefon, tablet, notebook, netbook, PDA apod.) prostřednictvím kterých lze přistupovat k Datům, a to minimálně v rozsahu seznámení uživatelů a zajištění souladu s politikou pro šifrování Dodavatele.

14. ZVLÁDÁNÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ A INCIDENTŮ

14.1 Dodavatel se zavazuje minimálně:

14.1.1 zajistit, aby jeho pracovníci a poddodavatelé oznamovali neobvyklé chování technických aktiv a podezření na jakékoliv zranitelnosti a hrozby;

14.1.2 po dobu 6 měsíců vést a uchovávat záznamy o kybernetických bezpečnostních incidentech a o jejich zvládání;

14.1.3 prošetřit a určit příčiny kybernetického bezpečnostního incidentu;

14.1.4 poskytnout Objednateli aktivní součinnost a relevantní informace o příčinách, podezřelém zařízení či osobě na straně Dodavatele v případě kybernetického bezpečnostního incidentu souvisejícího s Daty;

14.1.5 navrhnout a realizovat Dodavatelem odsouhlasená bezpečnostní opatření dle požadavků Objednatele v dohodnutých termínech pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu nebo hrozby;

14.1.6 vypracovat plán reakce na incidenty, který bude obsahovat konkrétní plán kroků, které musí Dodavatel případně i Objednatel, dodržet v případě bezpečnostního incidentu, a to ve vztahu k jednotlivým potenciálním druhům incidentů, a postupovat v souladu s tímto plánem.

15. FYZICKÁ BEZPEČNOST

15.1 Dodavatel se zavazuje minimálně:

15.1.1 zajistit dodržování politiky čistého stolu;

15.1.2 zajistit kanceláře, pracovní místnosti a prostory v případě jejich opuštění tak, aby nemohlo dojít k nedovolenému vstupu neoprávněných osob;

15.1.3 zajistit uzamykání pracovních stolů, skříní, kontrolovat uzavření oken;

15.1.4 zajistit dodržování režimových opatřeních v případě režimových pracovišť (perimetr s řízeným vstupem).

16. BEZPEČNOST KOMUNIKAČNÍCH SÍTÍ

16.1 Dodavatel se zavazuje minimálně:

16.1.1 zajistit vhodnou segmentaci komunikační sítě;

16.1.2 zajistit, aby komunikační síť byla chráněna bezpečným rozhraním, přičemž bude povolena pouze nutná komunikace;

16.1.3 zajistit, aby na síťových zařízeních byly spuštěny pouze nutné služby;

16.1.4 zajistit, aby byly sledovány zranitelnosti nasazených síťových zařízení a aby zjištěné zranitelnosti byly odstraňovány v dostatečných intervalech;

16.1.5 zajistit, aby přenos informací a dat v rámci komunikační sítě byl šifrován.

17. SPRÁVA A OVĚŘOVÁNÍ IDENTIT

17.1 Dodavatel se zavazuje minimálně:

17.1.1 používat nástroj pro správu a ověření identity (autentizační mechanismus), který přenáší a ukládá autentizační parametry v šifrované podobě;

17.1.2 používat autentizační mechanismus, který je založený na více faktorové autentizaci s nejméně dvěma různými typy faktorů, pokud je to možné;

17.1.3 v případě ztráty, vyzrazení nebo podezření na kompromitaci autentizačních nástrojů nebo parametrů okamžitě změnit parametry autentizace;

17.1.4 aktiva, která nepodporují více faktorovou autentizaci, dočasně zajistit autentizací pomocí podobně silných kryptografických klíčů nebo hesel;

17.1.5 v rámci systému vynucovat hesla s vlastnostmi podle aktuální nejlepší praxe, pokud je autentizace založena na heslech a nevyužívá se více faktorové autentizace.

18. OCHRANA PŘED ŠKODLIVÝM KÓDEM

18.1 Dodavatel se zavazuje minimálně:

18.1.1 zajistit použití nástroje pro nepřetržitou automatickou ochranu koncových zařízení;

18.1.2 monitorovat a řídit používání výměnných zařízení a datových nosičů a řídit jejich automatické spouštění;

18.1.3 provádět pravidelnou a účinnou aktualizaci nástroje pro ochranu před škodlivým kódem.

19. DETEKCE, ZAZNAMENÁVÁNÍ A VYHODNOCOVÁNÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ

19.1 Dodavatel se zavazuje minimálně:

19.1.1 zajistit, aby všechny klíčové prvky propojující významné uzly interních komunikačních sítí, bezpečnostní síťové prvky a všechny prvky na vnějším perimetru měly aktivní monitorování kybernetických bezpečnostních událostí;

19.1.2 zajistit, aby monitorování sítě zajišťovalo ověření a kontrolu přenášených dat v rámci komunikační sítě a mezi komunikačními sítěmi, ověření a kontrolu přenášených dat na perimetru komunikační sítě;

19.1.3 zajistit, aby detekovaná nežádoucí komunikace byla automaticky blokována;

19.1.4 zajistit, aby po dobu 6 měsíců byly zaznamenávány kybernetické bezpečnostní události narušující integritu síťových prvků nebo síťové komunikace, aby tyto záznamy byly uchovány a poskytnuty Objednateli na vyžádání;

19.1.5 zajistit, aby primární reakcí byla eskalace bezpečnostní události nebo incidentu do příslušných hlášení, případně přímá eskalace na příslušné odpovědné pracovníky.

20. APLIKAČNÍ BEZPEČNOST

20.1 Dodavatel se zavazuje minimálně:

20.1.1 užívat technická aktiva, která jsou podporována;

20.1.2 sledovat dostupnost opravných balíčků nebo záplat a zajistit bezodkladnou bezpečnostní aktualizaci;

20.1.3 pokud není bezpečnostní aktualizace dostupná, zajistit jiné kompenzační řešení, případně zranitelnost může být akceptována.

21. KRYPTOGRAFICKÉ ALGORITMY

21.1 Dodavatel se zavazuje minimálně:

21.1.1 používat pouze aktuálně doporučované a odolné kryptografické algoritmy a kryptografické klíče podle nejlepší praxe.

22. KONTROLA A AUDIT

22.1 Objednatel je oprávněn, na základě předchozí výzvy ze strany Objednatele doručené v přiměřeném časovém předstihu (nejméně však 30 dní předem), provést kontrolu a audit údajů, účtů, záznamů, pracovních postupů, dokumentace, aktiv, prostor (včetně kontroly fyzického perimetru) a technických prostředků vztahujících se k plnění Smlouvy a této Přílohy, a to za účelem ověření plnění povinností vyplývajících ze Smlouvy, jejích příloh a této Přílohy (dále jen „**Audit**“).

22.2 Audit bude prováděn dle potřeb Objednatele a pak mimořádně v případech bezpečnostních událostí, důvodného podezření na nedostatečnou úroveň ochrany aktiv Objednatele, důvodného podezření na nakládání s aktivy v rozporu s relevantními ustanoveními Smlouvy a důvodného podezření na nedodržení bezpečnostních opatření, podle této Přílohy.

22.3 Audit bude prováděn Objednatelem nebo jím pověřenou třetí stranou smluvně zavázanou k mlčenlivosti minimálně v rozsahu odpovídajícím povinnostem mlčenlivosti Objednatele dle Smlouvy, a která není k Dodavateli v soutěžním nebo jiném konkurenčním postavení.

22.4 Dodavatel poskytne veškerou nezbytnou součinnost k řádnému provedení a dokončení Auditu, zejména umožní přístup k údajům, účtům, záznamům, pracovním postupům, dokumentaci, jiným dokladům či podkladům, k aktivům, do prostor (včetně kontroly fyzického perimetru) a k technickým prostředkům vztahujícím se k plnění Smlouvy a této Přílohy za účelem uskutečnění Auditu. Dodavatel zajistí součinnost kvalifikovaných pracovníků.

22.5 Jakákoliv data, informace nebo jiná aktiva získaná při Auditu mohou být použita výhradně pro účely Auditu, vyhodnocení jeho výsledků a přijetí navazujících opatření, a další potřeby Objednatele při řízení vztahu s Dodavatelem.

22.6 Dodavatel je povinen bez zbytečného odkladu, nejpozději však do 1 měsíce od ukončení auditu, předložit Objednateli návrhy opatření napravujících nedostatky zjištěné při Auditu. Jednotlivá opatření navržená v návaznosti na výsledky Auditu podléhají před jejich přijetím Dodavatelem předchozímu schválení ze strany Objednatele. Návrhy zřejmě nevhodných

či neúčinných opatření Objednatel odmítne a Dodavatel je povinen v přiměřené lhůtě stanovené Objednatelem navrhnout jiná vhodná opatření. Dodavatel je taktéž povinen se na výzvu Objednatele podrobit dodatečné kontrole ze strany Objednatele nebo osoby, která Audit provedla, za účelem ověření nápravy nedostatků zjištěných při Auditu a kontroly přijatých opatření.

23. PODDODAVATELÉ A JEJICH ŘETĚZENÍ

23.1 Dodavatel se zavazuje, že pravidla dle této Přílohy budou dodržovat i poddodavatelé Dodavatele a jejich pracovníci podílející se na plnění Smlouvy. Dodavatel Objednateli na písemné vyžádání doloží, že u poddodavatelů smluvně vyžaduje dodržování pravidel dle této Přílohy, a to poskytnutím příslušné smlouvy s konkrétním poddodavatelem do 10 dnů ode dne jejího vyžádání Objednatelem (Dodavatel může anonymizovat části smlouvy, které považuje za obchodní tajemství do té míry, aby anonymizace nebránila Objednateli v kontrole plnění povinnosti dle tohoto článku).

23.2 Dodavatel se zavazuje soustavně (případně pravidelně dle povahy) dohlížet na plnění této Přílohy ze strany jeho poddodavatelů a jejich pracovníků, vyžadovat a vymáhat její plnění.

23.3 Za porušení pravidel dle této Přílohy poddodavatelem odpovídá Dodavatel Objednateli jako by je porušil sám. Dodavatel odpovídá za zajištění dostatečné znalosti pravidel dle této Přílohy ze strany poddodavatelů a jejich pracovníků.

23.4 Dodavatel je oprávněn využít k plnění dle Smlouvy poddodavatele za podmínek stanovených Smlouvou.

24. PŘEDÁNÍ A LIKVIDACE DAT

24.1 Dodavatel se zavazuje na základě výzvy Objednatele bez zbytečného odkladu předat Objednateli bezpečným způsobem, ve strojově čitelné podobě a ve formátu zaručujícím kompatibilitu v procesu migrace jakákoli Data v dispoziční sféře Dodavatele (pokud jde o data v databázích pak ve standardním exportním formátu dané databáze, aby bylo možné předaný soubor co nejjednodušším způsobem bez nutnosti dalších nedůvodných úprav nasadit do databáze na produkčním prostředí). Dodavatel se k výzvě Objednatele zavazuje poskytnout nezbytnou součinnost, přičemž si Smluvní strany mohou písemně dohodnout jiný způsob předání Dat. Dodavatel je povinen, i bez výzvy Objednatele, předat Objednateli Data do sedmi (7) dnů po skončení účinnosti Smlouvy.

24.2 Smluvní strany při ukončení Smlouvy z jakéhokoli důvodu vyvinou veškeré úsilí k tomu, aby do doby dokončení migrace Dat či převodu plnění dle Smlouvy k Objednateli nebo jinému dodavateli, nedošlo k narušení parametrů plnění ve Smlouvě do té doby definovaných, a aby případný nový dodavatel dostal veškeré informace o plnění Smlouvy potřebné pro pokračování nebo nahrazení takového plnění.

24.3 Dodavatel se zavazuje do 30 dnů od obdržení výzvy Objednatele předat Objednateli:

24.3.1 aktualizovanou dokumentaci, kterou vytvořil nebo spravuje,

24.3.2 úplný a aktuální zdrojový kód v případech, kde se Smlouvou zavázal k jeho předání,

24.3.3 seznam platných administrátorských účtů využívaných v prostředí Objednatele,

24.3.4 úplnou „knowledge base“ týkající se poskytování Služeb, vč. popisu a seznamu uzavřených a neuzavřených servisních požadavků,

24.3.5 aktuální seznam standardních provozních úkonů pro údržbu aktiv Objednatele, kterých se Smlouva týká.

24.4 Dodavatel se zavazuje při ukončení účinnosti Smlouvy, případně na písemnou žádost Objednatele, bez zbytečného odkladu po předání Dat, nejpozději však do 14 dnů, zlikvidovat Data v souladu s touto Přílohou za podpůrného užití pravidel v následující tabulce, to vše za možného dozoru zástupce Objednatele. Tato povinnost se nevztahuje na Data, která Dodavatel potřebuje za účelem plnění zákonné povinnosti či povinnosti stanovené mu rozhodnutím správního orgánu či za účelem hájení oprávněných zájmu Dodavatele (například v případě probíhajícího či hrozícího sporu).

24.5 Tabulka č. 1: Pravidla pro likvidaci dat

Přípustný způsob likvidace podle úrovně důležitosti aktiva		
Způsob likvidace	**Popis způsobu likvidace**	**Přípustnost využití způsobu likvidace dle úrovně důležitosti aktiva**
Odstranění	Způsob likvidace nosičů informací a Dat tak, aby byla nedostupná (například odstranění datového souboru, vyhození nosiče do odpadu). V případě získání nosiče informací a Dat je možné s vynaložením určitého úsilí informace a Data obnovit. Tato metoda není vhodná pro nosiče informací a Dat neumožňující opětovný zápis.	Nízká (Neveřejné)
Přepsání	Způsob likvidace spočívá v opakovaném přepsání informací a Dat náhodnými hodnotami. Volně dostupné nástroje neumožňují obnovení po násobném přepsání informací a Dat. Přepsání může být nahrazeno nebo kombinováno s bezpečnou likvidací kryptografických klíčů k zašifrovaným informacím a Datům. Tato metoda není vhodná pro poškozené nosiče, nosiče neumožňující opětovný zápis, případně pro nosiče s velkou paměťovou kapacitou.	Nízká (Neveřejné) Střední (Pro vnitřní potřebu)
Fyzická likvidace	Způsob likvidace spočívající ve zničení nosiče informací a Dat, popřípadě v rozebrání nosiče a následného zničení (například mechanickým, či chemickým působením vč. tepelného). Nosič informací a Dat po fyzické likvidaci nelze znovu použít. Informace a Data není možné z tohoto nosiče obnovit ani při vynaložení značného množství prostředků a úsilí.	Nízká (Neveřejné) Střední (Pro vnitřní potřebu) Vysoká a kritická (Chráněné)

25. ZÁVĚREČNÁ UJEDNÁNÍ

25.1 Smluvní strany se zavazují postupovat v souladu s relevantními obecně závaznými právními předpisy.

25.2 Dodavatel se zavazuje postupovat v souladu s bezpečnostními politikami, které mu budou Objednatelem zpřístupněny.

25.3 Dodavatel se zavazuje přenést na jakéhokoli poddodavatele, který bude schválen Objednatelem, ujednání k zajištění kybernetické bezpečnosti uvedené ve Smlouvě a v této Příloze v rozsahu, který je relevantní pro plnění poskytovaná daným poddodavatelem a tato ujednání nesmí být v rozporu s požadavky uvedenými ve Smlouvě a v této Příloze.

25.4 Dodavatel se zavazuje při výkonu své činnosti včas a prokazatelně upozornit Objednatele na zřejmou nevhodnost jeho příkazů či doporučení vztahujících se k pravidlům bezpečnosti, jejichž následkem může vzniknout újma nebo nesoulad s právními předpisy a zajistit ve spolupráci s Objednatelem náhradní způsob naplnění pravidel bezpečnosti, pokud stávající řešení přestalo být funkční nebo efektivní.

25.5 Pokud není ve Smlouvě nebo v této Příloze uvedeno jinak, odměna za provádění povinností a opatření dle této Přílohy je součástí odměny dle Smlouvy.

25.6 Čl. 24 této Přílohy se uplatní podpůrně s ohledem na čl. 13 Smlouvy.

Příloha č. 8

Specifikace Podpory výrobce

Výrobce musí garantovat Podporu pro každou nabízenou položku Plnění po dobu dle **Přílohy č. 2** této Smlouvy. To zahrnuje plné pokrytí a garanci plné funkčnosti systémů, jejich aktualizace a předplatné.

V případě aktualizace podmínek Podpory výrobce je Dodavatel povinen poskytnout Objednateli tyto aktualizované obchodní podmínky podpory výrobce a nemusí být uzavřen dodatek.

Podmínky podpory výrobce se uplatní pouze v části týkající se Podpory výrobce, přičemž k ustanovením limitujícím náhradu škody či obdobným ustanovením limitujícím odpovědnost výrobce, uplatnění sankcí či dalším ustanovením, které jsou v rozporu s textem Smlouvy se nepřihlíží.

Název opatření	Odkaz na konkrétní podmínky Podpory výrobce na dodaný HW a SW v rámci opatření	Splněny podmínky Podpory výrobce dle Přílohy č. 1 Smlouvy a dle dalších požadavků Objednatele ve Smlouvě
ID01 – Pokročilý síťový monitoring	https://docs.teskalabs.com/	ANO
ID02 – Posílení primárního datového centra	https://www.ibm.com/mysupport/s/?language=en_US&lnk=flathl#support-basics https://support.hpe.com/connect/s/	ANO
ID03 – Výměna a implementace aktivních síťových prvků	https://support.hpe.com/connect/s/	ANO
ID04 – Výměna a implementace WiFi infrastruktury	https://help.ui.com/hc/en-us	ANO
ID05 – Výměna a implementace zálohovací infrastruktury	https://www.ibm.com/mysupport/s/?language=en_US&lnk=flathl#support-basics https://support.hpe.com/connect/s/	ANO

ID06 – Zavedení systému řízení kybernetické bezpečnosti a výkon role manažera KB	Podmínky podpory výrobce jsou přiloženy na konci dokumentu.	ANO
ID07 – Firewally pro detašovaná pracoviště	https://support.fortinet.com/	ANO
ID08 – Kompletní správa životního cyklu logů	https://www.greycortex.com/cs	ANO
ID09 – Automatická, periodická kontrola stavu bezpečnosti IT systémů a aplikací	https://www.tenable.com/services	ANO

8. Další požadavky zadavatele

8.1. Návrh dodavatele dle odst. 12.1 ZD

TECHNICKÁ SPECIFIKACE

8.1.1. ID01 – Pokročilý síťový monitoring

1. Úvod a metodika

Tento dokument definuje předmět a závaznou technickou specifikaci pro implementaci nástroje pro sběr, analýzu a ukládání síťových toků (NetFlow/IPFIX) s napojením na zrcadlené porty (SPAN) síťových přepínačů a/nebo na dedikované sondy. Veškeré toky budou předávány do centralizovaného kolektoru, který bude zabezpečovat jejich příjem, normalizaci, dlouhodobé uložení a analytické zpracování včetně detekce nestandardních a podezřelých síťových aktivit. Detekované události musí být v reálném čase předávány do centrálního nástroje správy logů (SIEM/Log Management) a současně musí být k dispozici mechanismus notifikací správci kritických systémů a případně obsluze externího SOC.

Součástí plnění bude konfigurace zdrojů toků, nastavení retenčních politik, indexace a vyhledávání v historii síťového provozu tak, aby nástroj podporoval forenzní analýzy kybernetických i provozních incidentů. Dodavatel předá dokumentaci architektury, konfiguračního nastavení a provozních postupů; akceptace proběhne doložením funkčního příjmu toků z definovaných segmentů, demonstrací vyhledávání a korelací v historických datech a prokazatelným předáním událostí do centrální správy logů.

2. Specifikace dodávaného hardware, software a služeb instalace, implementace a školení

Specifikace nástroje pro analýzu a ukládání síťových toků

Systém pro analýzu síťového provozu a bezpečnostní monitoring, který okamžitě identifikuje bezpečnostní rizika a události a který splňuje klíčové požadavky uvedené níže.

Podpora na licence ve všech úrovních musí být zajištěna přímo jejich výrobcem, kterého může zadavatel přímo kontaktovat.

Součástí nabídky dodavatele bude vyjma zajištění instalace a zprovoznění nabízeného řešení včetně zaškolení uživatelů zadavatele rovněž 10 MD, které budou složit pro rozvoj a profylaxi řešení systému pro bezpečnostní analýzu síťového provozu interní sítě

Dodavatel vyplní následující tabulku specifikace nabízeného plnění. Ve sloupci „Splnění parametrů dodavatele – DOPLNÍ DODAVATEL“ dodavatel doplní:

- ANO/NE v závislosti na tom, zda nabízené plnění či jeho část požadavek zadavatele splňuje/nesplňuje,
- specifikaci konkrétního parametru či popis naplnění požadavku zadavatele,
- číselnou hodnotu v případě požadavku zadavatele, který obsahuje číselně vyjádřitelný parametr
- přesnou specifikaci HW, SW nebo služby
- volitelně odkaz na dodavatelem přiložený dokument ve formátu PDF

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

P. č.	Požadavek zadavatele – minimální dodávaný parametr	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
Systém pro analýzu síťového provozu – obecné požadavky		
1.	Systém složený z hardwarových zařízení musí monitorovat síťovou aktivitu v reálném čase a identifikovat potenciální kybernetické hrozby, bezpečnostní rizika a anomální chování a musí o nich v reálném čase vytvářet upozornění.	ANO Nabízené řešení je kombinace HW a SW s vlastním operačním systémem; monitoruje síťovou aktivitu v reálném čase, identifikuje a vytváří upozornění o událostech – kybernetické hrozby, bezpečnostní rizika a anomálie v síti.
2.	Dodaný systém musí analyzovat síť na základě zrcadleného síťového provozu ze SPAN portů nebo TAPů (nikoliv jen na základě statistických protokolů typu NetFlow) a zároveň bez potřeby nasazovat agenty na koncové stanice nebo další zařízení v síti.	ANO Nabízené řešení analyzuje síť na základě zrcadla provozu ze SPAN portů nebo TAPů a současně nevyžaduje instalaci agentů na koncových bodech a dalších zařízeních.
3.	Systém musí analyzovat obsah datových paketů v reálném čase a detekovat protokol nebo aplikaci na základě obsahu provozu prostřednictvím DPI (Deep Packet Inspection), nikoli pouze čísla portu.	ANO Nabízené řešení analyzuje obsah datových paketů v reálném čase, detekuje protokol a/nebo aplikaci na základě provozu prostřednictvím DPI.
4.	Dodaný systém musí být schopen analyzovat síť také na základě zpracování statistických protokolů typu NetFlow, IPFIX, NetStream, Cisco NSEL a případně dalších obdobných.	ANO Nabízené řešení umožňuje analyzovat síť také na základě zpracování statistických protokolů typu NetFlow, IPFIX, NetStream, Cisco NSEL a dalších.
5.	Systém musí být plně funkční v offline prostředí objednatele bez využití cloudového prostředí pro sběr, ukládání a zpracování dat a veškeré konfigurace a reporting jsou k dispozici přímo v systému.	ANO Nabízené řešení umožňuje plnou funkcionalitu v offline prostředí uživatele bez využití cloudu pro sběr, ukládání a zpracování dat, konfiguraci a reporting přímo ze systému.
6.	Aktualizace systému musí být možné provádět uživatelsky v offline režimu.	ANO Nabízené řešení umožňuje aktualizaci a upgrade systému uživatelsky v offline režimu.
Systém pro analýzu síťového provozu – zpracování a ukládání síťových toků		
7.	Systém ukládá síťové toky ve formátu, který umožní analýzu síťové komunikace na úrovni jednotlivých toků, včetně dohledání informací o aplikačních transakcích a jejich metadatech z L2 až L7, obsažených v daném síťovém toku.	ANO Nabízené řešení umožňuje ukládat síťové toky ve formátu, který umožňuje analýzu síťové komunikace na úrovni jednotlivých toků včetně informací o aplikačních transakcích a jejich metadatech (L2 – L7) v síťovém toku.

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

P. č.	Požadavek zadavatele – minimální dodávaný parametr		Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
8.	Požadované protokoly pro ukládání aplikačních metadat z jednotlivých transakcí jsou: DHCP, DNS, SMB, HTTP, HTTPS, SMTP, SMTPS, POP3, IMAP, SSH, LDAP, LDAPS, KERBEROS, SNMP, CIFS, MSSQL, RDP, SIP, TELNET, FTP, FTP-DATA, TFTP, TFTP-DATA, NFS, ARP, SSL/TLS zapouzdření.		ANO Nabízené řešení umožňuje ukládat aplikační metadata ve všech uvedených / požadovaných formátech.
9.	Je požadováno vysokorychlostní úložiště pro uchování historie datových toků minimálně 1,5 TB v technologii SSD.		ANO Nabízené řešení je navrženo s využitím HW složeného z vysokorychlostního úložiště s kapacitou více než 22 TB pro uchování historie datových toků.
10.	Analýza aplikačních a systémových logů Systém musí být schopen sbírat a analyzovat aplikační a systémové logy ve formátu syslog z dohledovaných zařízení a identifikovat nebezpečné nebo potenciálně škodlivé aktivity, jakož i obohatit data v systému o informace z nástrojů třetích stran (zejména identita uživatelů z logů v SIEMu nebo firewallu).		ANO Nabízené řešení umožňuje sbírat a analyzovat aplikační a systémové logy ve formátu syslog z monitorovaných zařízení a identifikovat potenciálně škodlivé aktivity.
11.	Všechna data jsou uložena v relační databázi (nikoli souborovém systému), všechna pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem a výsledky hledání jsou k dispozici okamžitě, i když se vyhledává v časovém intervalu několika týdnů.		ANO Nabízené řešení umožňuje automatickou indexaci všech polí a položek přijatých systémem; nad všemi položkami je možné ihned provádět vyhledávání bez potřeby dodatečného ručního indexování.
Systém pro analýzu síťového provozu – uživatelské rozhraní			
12.	Systém musí poskytovat jednotné grafické uživatelské rozhraní pro veškerou práci uživatelů, včetně všech detekcí, analýzy síťových statistik, nastavení systému, konfiguraci alertů, reportů a dashboardů.		ANO Nabízené řešení poskytuje jednotné uživatelské rozhraní pro práci uživatelů včetně detekcí a analýzy síťových statistik, nastavení a konfigurace alertů, reportů a dashboardů.
13.1.	Systém musí být schopen vytváření profilů a skupin uživatelů pro omezení funkcionality produktu a viditelnosti uložených dat s podporou minimálně:	Granulárního nastavení přístupu k analytickým i konfiguračním/administrativním komponentám systému s definovanými úrovněmi přístupu (alespoň read, write, execute)	ANO Nabízené řešení umožňuje vytvářet profily a skupiny uživatelů s podporou granulárního nastavení přístupu ke komponentám systému s úrovní přístupu read, write, execute.

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

P. č.	Požadavek zadavatele – minimální dodávaný parametr		Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
13.2.		Granulárního nastavení přístupu k datům z různých segmentů sítě organizace s definovanými úrovněmi přístupu (alespoň read, write, execute)	ANO Nabízené řešení umožňuje vytvářet profily a skupiny uživatelů s podporou granulárního nastavení přístupu k datům z různých segmentů sítě s úrovní přístupu read, write, execute.
13.3.		Vytváření vlastních filtrů veškerých dat a jejich sdílení mezi uživateli a skupinami uživatelů	ANO Nabízené řešení umožňuje vytvářet profily a skupiny uživatelů s podporou vytváření vlastních filtrů dat a jejich sdílení mezi uživateli a skupinami.
13.4.		Vytváření vlastních uživatelských pohledů, reportů, dashboardů apod.	ANO Nabízené řešení umožňuje vytvářet profily a skupiny uživatelů s podporou vytváření vlastních uživatelských pohledů, reportů, dashboardů a dalších typů výstupů.
Systém pro analýzu síťového provozu – automatické hlášení (alerty) a reporting			
14.	Systém musí být schopen upozorňovat uživatele prostřednictvím minimálně emailu a logu o všech identifikovaných událostech a dále o událostech filtrovaných minimálně dle IP a MAC adresy, podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu.		ANO Nabízené řešení umožňuje notifikaci uživatelů prostřednictvím emailu, logu o detekovaných událostech, o událostech dle IP a MAC adresy, podsítě, závažnosti, kategorie, země, uživatele, síťové služby, portu, typu provozu z/do internetu atd.
15.	Tyto alerty musí být systém schopen dodávat i ve strojově čitelném formátu pro vyžití v nástrojích typu SIEM a musí obsahovat minimálně kompletní informace o detekované události včetně URL odkazu na danou událost v reportovaném období do grafického rozhraní systému.		ANO Nabízené řešení umožňuje dodávat alerty také ve strojově čitelném formátu pro využití v nástrojích typu SIEM, s obsahem kompletních informací o detekované události včetně URL v reportovaném období do GUI.
16.	Systém musí mít možnost vytváření automatizovaných manažerských reportů o stavu kybernetické bezpečnosti z pohledu zprávy kybernetických incidentů ideálně dle oblastí jejich vzniků (např.: doména, web, email apod.).		ANO Nabízené řešení umožňuje vytvářet automatizované manažerské reporty o stavu kybernetické bezpečnosti z hlediska kybernetických incidentů dle oblasti jejich vzniku – doména, web, email atd.
17.	Je požadováno vytváření automatizovaných reportů v českém jazyce.		ANO Nabízené řešení umožňuje vytvářet reporty v českém jazyce.
Systém pro analýzu síťového provozu – integrace systému			

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

P. č.	Požadavek zadavatele – minimální dodávaný parametr		Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
18.1.	Systém musí poskytovat hotové nástroje umožňující integraci se softwarem třetích stran bez použití API systému, a to minimálně:	Syslog, CEF a LEEF pro export událostí včetně plné podpory filtrů (exportování pouze požadovaných dat)	ANO Nabízené řešení poskytuje hotové nástroje pro integraci se SW třetích stran bez API: Syslog, CEF, LEEF pro export událostí včetně podpory filtrů.
18.2.		Přímé URL odkazy na libovolnou obrazovku grafického uživatelského rozhraní a filtrovaná zobrazení v grafickém uživatelském rozhraní	ANO Nabízené řešení poskytuje hotové nástroje pro integraci se SW třetích stran bez API: přímé URL odkazy na obrazovky GUI a filtrovaná zobrazení v GUI.
18.3.		Export informací o toku ve formátu IPFIX nebo podobném formátu včetně plné podpory filtrů (exportovat lze pouze požadovaná data)	ANO Nabízené řešení poskytuje hotové nástroje pro integraci se SW třetích stran bez API: export informací o toku ve formátu IPFIX apod. včetně podpory filtrů.
18.4.		Integrace se službami identity uživatelů bez nutnosti konfigurace zasílání logů do systému Microsoft Active Directory	ANO Nabízené řešení poskytuje hotové nástroje pro integraci se SW třetích stran bez API: integrace se službami identit uživatelů bez potřeby konfigurace logů do MS AD.
18.5.		Integrace s firewally pro automatické a manuální reakce vyvolané systémem	ANO Nabízené řešení poskytuje hotové nástroje pro integraci s firewally pro automatické a manuální reakce.
18.6.		Integrace s nástroji pro řízení přístupu k síti, pro automatickou a manuální reakci systému	ANO Nabízené řešení poskytuje hotové nástroje pro integraci s nástroji pro řízení přístupu k síti pro automatickou a manuální reakci.
Systém pro analýzu síťového provozu – podpora EDR			
19.	Systém musí poskytovat nástroje umožňující přímou integraci se softwarem EDR třetích stran pro získání informací a zkvalitnění detekce.		ANO Nabízené řešení poskytuje nástroje pro integraci se SW EDR třetích stran pro získání informací a zkvalitnění detekce.
Architektura nasazení – obecné požadavky			

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

P. č.	Požadavek zadavatele – minimální dodávaný parametr		Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
20.	Pro všechny HW komponenty senzor a kolektor je požadován formát 1U nebo 2U server o velikosti 19“.		ANO Nabízené řešení je All-in-One – kolektor a sensor na jednom HW ve formátu 1U nebo 2U server o velikosti 19 ´´.
21.	Pro všechny HW komponenty senzor a kolektor je požadován duální zdroj napájení se schopností hot-swap.		ANO HW komponenty - senzor a kolektor v jednom zahrnují duální zdroj napájení se schopností hot-swap.
22.	Pro všechny HW komponenty senzor a kolektor je požadováno samostatné síťové rozhraní pro vzdálenou správu serveru v případě výpadku systému typu IPMI, IDRAC, ILO apod.		ANO Nabízený HW - kolektor a senzor zahrnuje samostatné síťové rozhraní pro vzdálenou správu serveru v případě výpadku systému typu IPMI, IDRAC, ILO apod.
Architektura nasazení –požadavky pro pokrytí IT prostředí			
23.	Je požadován 1x HW jedno zařízení, které kombinuje datový kolektor a sensor o minimální celkové schopnosti zpracovat 1Gbps průměrného provozu pro alespoň 3000 monitorovaných IP adres. Monitorovací rozhraní jsou požadována minimálně 4x1GbE a 2x10/25GbE optická, vč. kompatibilních SFP modulů. Na zařízení je požadována dostupná historie dat uložená na rychlém úložišti o čisté velikosti alespoň 1,5 TB s technologií SSD a RAID1.		ANO, Nabízené řešení AllinOne plní uvedené požadavky
Schopnost detekce bezpečnostních událostí – monitorování zařízení, segmentů sítě a využívaných síťových služeb			
24.1.	Dodaný systém musí identifikovat všechna zařízení připojená do sítě včetně koncových zařízení, serverů, IoT zařízení apod. Zároveň musí být systém schopen identifikovat změny v síti – minimálně:	Změna IP/MAC adresy hosta	ANO Nabízené řešení identifikuje všechna zařízení připojená do sítě včetně koncových zařízení, serverů a IoT. Rovněž identifikuje změny v síti – IP/MAC adresy hosta.
24.2.		Duplicitní IP/MAC adresa	ANO Dtto – duplicitní IP/MAC adresa
24.3.		Změna VLAN	ANO Dtto – změna VLAN
24.4.		Vytvoření nové podsítě	ANO Dtto – vytvoření nové podsítě
24.5.		Připojení nového zařízení	ANO Dtto – připojení nového zařízení
24.6.		Použití nebo vznik nové služby	ANO Dtto – použití / vznik nové služby

P. č.	Požadavek zadavatele – minimální dodávaný parametr		Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
24.7.		Nedostupnost dříve dostupné a komunikující služby nebo dříve dostupného a komunikujícího zařízení	ANO Dtto – nedostupnost dříve dostupné a komunikující služby nebo zařízení
24.8.		Přístup nového zařízení ke službě či zařízení	ANO Dtto – přístup nového zařízení ke službě či zařízení
24.9.		Ověřování platnosti interních certifikátu pro validní TLS šifrování u HTTPS a upozornění před datem jejich vypršení	ANO Dtto – ověřování platnosti interních certifikátů pro validní TLS šifrování u HTTPS a upozornění před jejich datem expirace
25.	Systém musí uživateli umožnit pomocí těchto detekčních metod nastavovat bezpečnostní politiky pro různé segmenty sítě a pro různá zařízení a na porušení těchto politik reagovat upozorněním.		ANO Nabízené řešení umožňuje pomocí detekčních metod nastavovat bezpečnostní politiky pro různé segmenty sítě a pro různá zařízení a reagovat na porušení politik.
Schopnost detekce bezpečnostních událostí – samostatné učení behaviorálních aktivit a detekce anomálií			
26.	Systém musí používat matematické metody samostatného učení pro analýzu síťové aktivity, vytvářet a v čase automaticky modifikovat modely chování na základě běžného chování jednotlivých zařízení a na nich provozovaných služeb v rámci celé organizace.		ANO Nabízené řešení používá matematické metody samostatného učení pro analýzu síťové aktivity, vytváří a modifikuje modely chování na základě běžného chování zařízení a provozovaných služeb v rámci organizace.
27.1.	Systém musí mít schopnost na základě matematického modelu daného zařízení a jeho služeb identifikovat nestandardní síťové chování, a to zejména odchylky od modelu normálního chování pro:	Odchylku od modelu pro přenos dat, toků a paketů	ANO Nabízené řešení umožňuje na základě matematického modelu zařízení a jeho služeb identifikovat nestandardní chování, zejména odchylky od modelu chování pro přenos dat, toků a paketů.
27.2.		Odchylku od modelu pro počet komunikačních partnerů	ANO Dtto odchylky od modelu pro počet komunikačních partnerů.
27.3.		Odchylku od modelu entropie na komunikačních portech	ANO Dtto odchylky od modelu entropie na komunikačních portech.

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

P. č.	Požadavek zadavatele – minimální dodávaný parametr		Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
27.4.		Odchylku od modelu pro počet síťových toků a využitých síťových služeb	ANO Dtto odchylky od modelu pro počet síťových toků a využitých síťových služeb.
27.5.		Odchylku od modelu výkonnosti sítě (rychlost přenosu) a aplikací (doba odezvy)	ANO Dtto odchylky od modelu výkonnosti sítě a aplikací – rychlost přenosu a doba odezvy.
28.	Samostatné učení je požadováno na všech síťových zařízeních a na nich provozovaných službách (port číslo 0 až 65535 u TCP i UDP) na IPv4 a IPv6 a dalších protokolech L3 a L4 síťové vrstvy.		ANO Nabízené řešení uplatňuje samostatné učení na všech síťových zařízeních a na nich běžících službách (porty 0 – 65535 u TCP a UDP) na IPv4/ IPv6 a dalších protokolech L3 a L4.
Schopnost detekce bezpečnostních událostí – identifikace neznámých hrozeb a podezřelých chování			
29.1.	Systém musí být schopen detekovat neznámé hrozby, které nelze identifikovat prostřednictvím detekčních signatur, jako jsou trojské koně, botnety apod. Zejména musí být identifikovány tyto příznaky potenciálně škodlivého chování:	Průzkumné aktivity v síti	ANO Nabízené řešení detekuje neznámé hrozby, které nelze identifikovat na základě signatur: např. trojské koně a botnety, na základě průzkumných aktivit v síti.
29.2.		Detekce podezřelého strojového chování, které nevytvářejí lidští uživatelé sítě	ANO Nabízené řešení detekuje neznámé hrozby na základě detekce podezřelého strojového chování.
29.3.		Detekce repetitivních vzorců chování na síti	ANO Nabízené řešení detekuje neznámé hrozby na základě detekce repetitivních vzorců chování v síti.
29.4.		Detekce botnetů a ovládání kompromitované stanice	ANO Nabízené řešení detekuje neznámé hrozby na základě detekce botnetů a ovládání kompromitované stanice.
29.5.		Detekce příznaků těžení kryptoměn	ANO Nabízené řešení detekuje neznámé hrozby na základě detekce příznaků těžení kryptoměn.
29.6.		Útoky hrubou silou a enumerace dat	ANO Nabízené řešení detekuje neznámé hrozby na základě detekce útoků hrubou silou a enumerace dat.
29.7.		Rozpoznání tunelovaného síťového provozu – alespoň IPv4 prostřednictvím IPv6 a DNS tunely	ANO Nabízené řešení detekuje neznámé hrozby na základě rozpoznání tunelovaného síťového provozu – Ipv4 prostřednictvím IPv6 a DNS tunely.

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

P. č.	Požadavek zadavatele – minimální dodávaný parametr		Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
Schopnost detekce bezpečnostních událostí – detekce na základě databáze známých hrozeb			
30.1.	Systém musí být schopen identifikovat hrozby a reportovat události na základě:	Detekční databáze známých hrozeb, tj. malware (trojské koně, viry, červy, rootkity, apod.), známých útoků (exploity) a zranitelností, porušení bezpečnostních pravidel a „best practices“ a dalších rizik	ANO Nabízené řešení identifikuje hrozby a reportuje události na základě databáze známých hrozeb – malware, známých útoků a zranitelností, porušení bezpečnostních pravidel a best practices apod.
30.2.		Reputační databáze známých škodlivých IP adres, TLS certifikátů, záznamů DNS a hostname, URL adres a hashů souborů	ANO Nabízené řešení identifikuje hrozby a reportuje události na základě reputační databáze známých škodlivých IP adres, TLS certifikátů, záznamů DNS a hostname, URL adres a hashů souborů.
31.	Tyto databáze musí být aktualizované minimálně na hodinové bázi. Nesmí se jednat pouze o volně dostupné/open-source databáze, ale musí se jednat o komerční databázi renomovaného vendora nebo poskytovatele těchto služeb.		ANO Nabízené řešení využívá komerční databáze hrozeb Proofpoint, které jsou aktualizovány na hodinové bázi.
32.	Uživatel musí být schopen importovat vlastní záznamy.		ANO Nabízené řešení umožňuje uživateli importovat vlastní záznamy.
33.	Systém musí využívat tuto detekci pro veškerý monitorovaný provoz (na perimetru i v interní síti mezi všemi segmenty), nikoliv pouze pro omezený segment nebo podmnožinu celkové komunikace.		ANO Nabízené řešení využívá výše uvedenou detekci pro veškerý monitorovaný provoz.
34.	Databáze detekčních pravidel (signatur) musí být založena na pokročilých regulárních výrazech pro zpracování řetězců, které dokáží provádět inspekci veškeré síťové komunikace od L2 (Ethernet apod.) po L7. Systém musí detekovat události na základě vysokého počtu signaturních pravidel (minimálně několik desítek tisíc). Systém musí umožňovat centrální správu detekčních pravidel z jednoho místa pro všechny senzory.		ANO Databáze detekčních pravidel nabízeného řešení je založena na pokročilých regulárních výrazech pro zpracování řetězců, které umožňují inspekci veškeré síťové komunikace od L2 po L7. Události jsou detekovány na základě desítek tisíc signaturních pravidel.

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

P. č.	Požadavek zadavatele – minimální dodávaný parametr		Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
35.	Uživatel musí být schopen přidávat vlastní detekční pravidla v praktickém a obecně využívaném formátu, prostřednictvím grafického rozhraní s průvodcem (wizard), nikoliv jen textovou řádkou. Příklad možné syntaxe detekčního pravidla: *alert tcp $HOME_NET any -> any any (msg:"Command Shell Access"; content:"C:\\Users\\Administrator\\Desktop\\hfs2.3b"; sid:1000001; rev:1;)*		ANO Uživatel nabízeného řešení může přidávat vlastní detekční pravidla v praktickém a obecně užívaném formátu.
36.	Analýza šifrované komunikace Vedle samostatného učení musí systém používat další metody pro analýzu šifrované komunikace, minimálně TLS fingerprinting a s ní spojenou detekci známých hrozeb.		ANO Nabízené řešení využívá kromě samostatného učení také další metody pro analýzu šifrované komunikace, jako např. TLS fingerprint a s ní spojenou detekci známých hrozeb.
Schopnost detekce bezpečnostních událostí – asistované učení			
37.1.	Je požadován uživatelsky přívětivý proces vytváření pravidel pro zpřesnění detekce a eliminaci falešně pozitivní detekce, a to na základě minimálně následujících parametrů:	IP adresa	ANO Nabízené řešení poskytuje uživatelsky přívětivou formu vytváření pravidel pro zpřesnění detekce na základě IP adresy.
37.2.		MAC adresa	ANO Dtto na základě MAC adresy.
37.3.		Hostname	ANO Dtto na základě hostname.
37.4.		Segment sítě / podsíť	ANO Dtto na základě segmentu sítě / podsítě.
37.5.		Lokalita – ASN, země, apod.	ANO Dtto na základě lokality.
37.6.		Směr komunikace – určení klienta, nebo serveru	ANO Dtto na základě směru komunikace – klienta / serveru.
37.7.		Detekovaná událost – kategorie, název apod.	ANO Dtto na základě sdetekované události – např. kategorie, názvu.
37.8.		Použité služby, protokolu, portu	ANO Dtto na základě služby, protokolu, portu.
37.9.		Libovolné kombinaci výše popsaných	ANO Dtto na základě kombinace výše uvedených parametrů.
38.	Systém musí být schopen eliminovat falešné alarmy i pro události detekované v historii.		ANO Nabízené řešení dokáže eliminovat falešné alarmy i pro události detekované v historii.
Požadavky na zajištění síťové viditelnosti – vyhledávání, filtrování a vizualizace dat			

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

P. č.	Požadavek zadavatele – minimální dodávaný parametr		Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
39.	Systém musí být schopen okamžitého (v řádu vteřin) vyhledávání a vizualizace pro forenzní analýzu a podporu threat hunting bez zvláštního dotazovacího jazyka.		ANO Nabízené řešení vyhledává a vizualizuje data pro forenzní analýzu a podporu threat huntingu v řádu vteřin bez použití zvláštního dotazovacího jazyka.
40.1.	Jedná se o možnost okamžitě filtrovat a vyhledávat v plné historii všech uložených dat, tj. bezpečnostních událostí, síťových toků a agregovaných síťových statistikách (tabulky a grafy), a to minimálně:	Podle parametrů IP a MAC adresa, hostname, username (identita uživatele), příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (služba z pohledu klient nebo server), číslo portu, VLAN, země, ASN	ANO Nabízené řešení filtruje a vyhledává v plné historii bezpečnostních událostí, síťových toků a síťových statistikách podle IP a MAC adresy, hostname, username, směru provozu, síťové služby, lokální / vzdálené služby, čísla portu, VLAN, země, ASN.
40.2.		Prostřednictvím full-textového vyhledávání v datech a vyhledávání na základě definice směru (zdroj, cíl) a logických výrazů and, or, not	ANO Nabízené řešení prohledává data full-textově a na základě definice směru a logických výrazů.
41.	Systém musí pro vyhledávání poskytovat již předpočítané hodnoty výkonnostních a behaviorálních charakteristik pro každé zařízení v síti a pro všechny na něm provozované služby, bez nutnosti zpracování surových dat ze síťových logů.		ANO Nabízené řešení poskytuje pro vyhledávání předpočítané hodnoty výkonnostních a behaviorálních charakteristik pro každé zařízení v síti a na něm poskytované služby bez potřeby zpracování surových dat z logů.
42.	Systém musí být schopen filtrovat a vizualizovat výsledky v grafech, výčtových tabulkách s možností řazení a TOP N statistikách.		ANO Nabízené řešení filtruje a vizualizuje výsledky v grafech, výčtových tabulkách a možností řazení a TOP N statistikách.

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

P. č.	Požadavek zadavatele – minimální dodávaný parametr		Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
43.	Systém musí být schopen ukládat a následně vyhledávat aplikační metadata (vždy dotaz i odpověď všech transakcí v toku) minimálně z následujících protokolů, které jsou nebo mohou být využívány ve vnitřní síti organizace: FTP, FTP-DATA, TFTP, TFTP-DATA, SSH, Telnet, SMTP, SMTPS, DNS, DHCP, HTTP, HTTPS, NTP, SMB, SNMP, LDAP, NFS, RDP, ARP, MS-SQL, SIP, Kerberos, SSL/TLS. Metadata jsou v tomto případě chápána jako přenášená aplikační metadata nebo vlastní data servisních protokolů. U protokolu HTTP například http hlavička s metodou, URI, host, user-agent, cookies apod. V odpovědi pak návratový kód a další http parametry.		ANO Nabízené řešení ukládá a následně vyhledává aplikační metadata (dotaz i odpověď transakcí toku) ze všech uvedených protokolů.
44.	Systém umožnuje provádět uživatelsky jednoduché a okamžité vizualizace síťových prostupů mezi zařízeními a podsítěmi. Využitím uživatelského datového filtru lze vizualizační pohledy libovolně modifikovat.		ANO Nabízené řešení umožňuje vytvářet uživatelsky jednoduché a okamžité vizualizace síťových prostupů mezi zařízeními a podsítěmi s možností modifikace.
45.	Zaznamenávání a ukládání plného provozu Je požadováno volitelné nahrávání plného síťového provozu (full packet capture) ve formátu PCAP na všech dodaných zařízeních minimálně na základě parametrů: cílová a zdrojová IP/MAC adresa, podsíť, využitý protokol, IPv4 nebo IPv6. Zaznamenávání je možno zapínat automaticky dle detekovaných událostí, nebo uživatelskou aktivací.		ANO Nabízené řešení umožňuje zvolit zaznamenávání a nahrávání plného síťového provozu (full packet capture) ve formátu PCAP na základě parametrů cílová a zdrojová IP/MAC, podsíť, protokol, IPv4/IPv6. Lze automaticky zapínat dle události nebo uživatelsky.
Monitorování politik kybernetické bezpečnosti			
48.1.	Systém musí umožňovat vytváření komplexních komunikačních a bezpečnostních politik, a to minimálně:	Monitorovat definovanou komunikační matici a detekovat, kdy jsou tyto matice porušeny – alespoň jaké zařízení smí komunikovat s jakým zařízením, přes jaký protokol, v jakém čase.	ANO Nabízené řešení umožňuje vytváření komplexních komunikačních a bezpečnostních politik, monitorovat definovanou komunikační matice a detekovat jejich porušení - která zařízení mohou navzájem komunikovat, přes jaký protokol, v jakém čase apod.
48.2.		Detekce změn v síti – přinejmenším nové komunikační vektory, nová nebo změněná zařízení a podsítě, obcházení perimetru.	ANO Nabízené řešení detekuje změny v síti – komunikační vektory, nová / změněná zařízení a podsítě, obcházení perimetru.

P. č.	Požadavek zadavatele – minimální dodávaný parametr		Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
49.1.	Pro účely monitorování politik kybernetické bezpečnosti musí systém poskytovat uživatelský rámec pro definování pravidel pomocí:	Uživatelem definované podsítě na základě rozsahů IP adres	ANO Nabízené řešení poskytuje pro účely monitorování politik KB uživatelský rámec pro definování pravidel pomocí uživatelem definované podsítě na základě rozsahů IP adres.
49.2.		Uživatelsky libovolně definovaných skupin zařízení	ANO Dtto na základě uživatelsky definovaných skupin zařízení.
49.3.		Automaticky přiřazené značky/tagu zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy	ANO Dtto na základě automaticky přiřazené značky zařízení, popisující účel a chování – pro všechny uvedené typy zařízení.
Management bezpečnostních událostí a incidentů			
50.1.	Systém musí poskytovat funkcionalitu pro reporting bezpečnostních incidentů (prohlášení identifikované události za bezpečnostní incident), včetně:	Spolupráci a sdílení informací při analýze identifikovaných bezpečnostních incidentů včetně potřebného workflow mezi jednotlivými uživateli s podporou automatizovaných oznámení o změně stavu události či přiřazení řešitele	ANO Nabízené řešení umožňuje reporting bezpečnostních incidentů – sdílení informací při analýze identifikovaných incidentů a workflow mezi uživateli s podporou automatizovaných notifikací o změně stavu / přiřazení řešitele.
50.2.		Jednoduché sdílení informací o bezpečnostních incidentech, včetně uživatelem zadaných komentářů	ANO Nabízené řešení umožňuje jednoduché sdílení informací o bezpečnostních incidentech včetně komentářů uživatele.

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

P. č.	Požadavek zadavatele – minimální dodávaný parametr		Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
50.3.		Možnost vyhledávání a filtrování nad všemi událostmi z pohledu workflow bezpečnostního incidentů (reportovaná událost, událost v řešení, vyřešená událost, události v řešení daného uživatele apod.)	ANO Nabízené řešení umožňuje vyhledávat a filtrovat nad všemi událostmi z pohledu workflow incidentů.
50.4.		Možnost exportování dat do emailu, csv, pdf, syslogu a podobně	ANO Nabízené řešení umožňuje exporty dat do emailu, csv, pdf, syslog atd.
50.5.		Možnost exportu bezpečnostních událostí a incidentů do systémů typu ticket management třetích stran	ANO Nabízené řešení umožňuje export událostí a incidentů do tiketovacích nástrojů třetích stran.
Detekce úniku dat			
51.	Systém musí být schopen detekovat přenosy citlivých souborů a dat definovaných pomocí jejich názvů, hashů, specifického binárního obsahu (vodoznaku) nebo regulárních výrazů (např. rodné číslo).		ANO Nabízené řešení detekuje přenosy citlivých souborů a dat definovaných pomocí uvedených parametrů.
52.	Systém musí být schopen detekovat přenosy citlivých souborů a dat alespoň u následujících protokolů: HTTP, FTP, SMTP, SMB, NFS.		ANO Nabízené řešení detekuje přenosy citlivých souborů a dat u uvedených protokolů.
53.1.	V rámci historických metadat u HTTP, FTP, SMTP, SMB a NFS je požadováno ukládání informací o všech po síti přenášených souborech alespoň v rozsahu:	Název souboru	ANO Nabízené řešení ukládá v rámci historických metadat informace o souborech přenášených po síti – název souboru.
53.2.		Velikost souboru	ANO Dtto velikost souboru.
53.3.		HASH souboru	ANO Dtto HASH souboru.
Monitoring výkonu aplikací a sítě			
54.1.	Systém v celé monitorované síti, mezi všemi zařízeními a na všech službách měří a vytváří automaticky (bez nutnosti nastavovat	Přenosová rychlost sítě	ANO Nabízené řešení v celé monitorované síti měří a vytváří automaticky model normálního chování pro přenosovou rychlost sítě.

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

P. č.	Požadavek zadavatele – minimální dodávaný parametr		Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
54.2.	manuálně limitní hodnoty) model normálního chování pro výkonnostní parametry minimálně:	Rychlost odezvy aplikace	ANO Dtto pro rychlost odezvy aplikace.
54.3.		Odezva systému z pohledu uživatele	ANO Dtto pro odezvu systému z pohledu uživatele.
55.1.	Výpočet uvedených výkonnostních parametrů a automatické detekce anomálií na základě odchylky od modelu normálního chování musí být prováděna pro:	Všechny porty a služby TCP	ANO Dtto pro všechny porty a služby TCP.
55.2.		Pro všechny kombinace služeb a zařízení	ANO Dtto pro všechny kombinace služeb a zařízení.
56.	Systém musí v celé monitorované síti, mezi všemi zařízeními a na všech službách měřit informace o retransmission paketech, out of order paketech, TTL, QoS a komunikaci blokované firewally.		ANO Nabízené řešení v celé monitorované síti měří informace o retransmission paketech, out of order paketech, TTL, QoS a komunikaci blokované firewally.
Monitoring cloudových služeb			
57.	Systém musí být schopen monitorovat přístupy zařízení a uživatelů ke cloudovým službám, a to minimálně Google Workspace a Microsoft Office 365, vč. monitoringu operací se soubory, změn oprávnění a nastavení a neúspěšných přístupů.		ANO Nabízené řešení monitoruje přístupy zařízení a uživatelů ke cloudovým službám, např. Google Workspace a MS Office 365 včetně monitorvoní operací se soubory, změn oprávnění a nastavení a neúspěšných přístupů.
58.	Systém musí být schopen tyto informace autonomně a průběžně získávat z aplikačních rozhraní těchto cloudových služeb bez nutnosti využití řešení třetích stran.		ANO Nabízené řešení průběžně získává výše uvedené informace z aplikačních rozhraní cloudových služeb bez potřeby využití řešení třetích stran.
Inventarizace sítě a grafická vizualizace topologie			
59.	Systém musí být schopen zobrazit celý inventář monitorované sítě s počtem zařízení v jednotlivých lokalitách, segmentech, nebo podsítích. Včetně detailního přehledu zařízení.		ANO Nabízené řešení umožňuje zobrazit inventář monitorované sítě s počty zařízení v lokalitách, segmentech, podsítích včetně detailu zařízení.
60.	Systém musí být schopen graficky vykreslit celou topologii sítě, dle zaznamenané komunikace.		ANO Nabízené řešení umožňuje graficky vykreslit topologii sítě dle zaznamenané komunikace
61.	Systém musí být schopen zobrazit inventář jednotlivých lokalit, přehledy zařízení, přehledy výrobců, tagy zřízení, uživatele.		ANO Nabízené řešení zobrazit inventář jednotlivých lokalit, přehledy zařízení, výrobců, tagů, uživatelů.

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

P. č.	Požadavek zadavatele – minimální dodávaný parametr	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
62.	Systém umožnuje všechny inventory informace řadit dle různých parametrů.	ANO Nabízené řešení umožňuje všechny inventory informace řadit dle různých parametrů.

V případě, že nabídka dodavatele nebude bezvýhradně splňovat veškeré požadované parametry, tj. v případě vyčíslitelného parametru nabídka nesplní požadovanou minimální hodnotu a v případě nevyčíslitelného parametru bude u požadavku uvedeno NE, případně ze specifikace konkrétního parametru či popisu naplnění požadavku zadavatele bude vyplývat, že parametr či požadavek zadavatele není splněn, může být nabídka vyřazena a účastník vyloučen z účasti v zadávacím řízení pro nesplnění podmínek účasti.

2.a Akceptační kritéria

Akceptace proběhne v souladu s příslušným ustanovením smlouvy a dodavatel mj. zajistí implementaci nástroje pro sběr, analýzu a ukládání síťových toků (NetFlow/IPFIX) s napojením na zrcadlené porty (SPAN) síťových přepínačů a/nebo na dedikované sondy. Veškeré toky budou předávány do centralizovaného kolektoru, který bude zabezpečovat jejich příjem, normalizaci, dlouhodobé uložení a analytické zpracování včetně detekce nestandardních a podezřelých síťových aktivit. Detekované události musí být v reálném čase předávány do centrálního nástroje správy logů (SIEM/Log Management) a současně musí být k dispozici mechanismus notifikací správci kritických systémů a případně obsluze externího SOC.

Akceptační parametry

Akceptační kritérium	Způsob ověření	Výsledek	Poznámka / Podpis
Funkční příjem toků	Kolektor přijímá síťové toky (NetFlow/IPFIX) z definovaných segmentů		
Vyhledávání v historických datech	Demonstrace vyhledávání podle IP adres, portů, protokolů a časových období		
Korelace dat	Předvedení funkční korelace událostí v historických datech		
Předání událostí do centrální správy logů	Ověření předání detekovaných událostí do SIEM/Log Management v reálném čase		

3. Specifikace služeb technické podpory dodavatele na 60 měsíců od 1. 6. 2026 do 31.5.2031.

Specifikace služeb technické podpory je uvedena v samostatném dokumentu:

- 01 – Technická specifikace – Společná definice technické podpory pro ID01 – ID09

Zadavatel tímto výslovně stanoví, že nepožaduje žádnou záruku nad rámec a mimo rozsah technické podpory vymezený v tomto dokumentu a dokumentu „01 – Technická specifikace – Společná definice technické podpory pro ID01 – ID09“ (dále jen „Společná definice“). Veškeré záruční povinnosti dodavatele, včetně úrovní služeb, reakčních dob, způsobu eskalace, podmínek dostupnosti, režimu aktualizací, EoL/EoS a výluk plnění, se řídí výlučně tímto dokumentem a Společnou definicí. Jakákoli plnění spočívající v rozvojových zásazích, změnových požadavcích, úpravách nad rámec specifikace či integracích nevyplývajících ze Společné definice nejsou součástí záruky, ledaže budou výslovně sjednána zvláštní smlouvou nebo dodatkem.

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

V případě rozporu nebo kolizního výkladu mezi touto technickou specifikací a Společnou definicí má přednost tato technická specifikace. Společná definice slouží jako doplňující a výkladový dokument a uplatní se pouze v rozsahu, v němž není v rozporu s touto Technickou specifikací.

3a Akceptační kritéria

Dodavatel se zavazuje poskytovat technickou podporu v rozsahu a za podmínek stanovených tímto dokumentem a Společnou definicí po dobu od 1. 6. 2026 do 31. 5. 2031 (60 měsíců). Dodavatel podpisem smlouvy stvrzuje, že po uvedené období bude plnit sjednané SLA a ostatní povinnosti dle tohoto dokumentu a Společné definice; nesplnění těchto povinností bude posuzováno jako porušení smlouvy se všemi z toho vyplývajícími právními následky podle smlouvy a příslušných právních předpisů.

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

8.1.2. ID02 - Posílení primárního datového centra - redundance

1. Úvod a metodika

Tento dokument definuje předmět a závaznou technickou specifikaci pro posílení stávajících virtualizačních clusterů (Hyper-V) v rozsahu 2 uzlů s cílem odstranit jednotlivé body selhání (SPOF) a zajistit vysokou dostupnost služeb. Součástí bude implementace redundantních klastrových řešení, replikace dat a připravené, zdokumentované postupy failoveru mezi clustery tak, aby byla zajištěna kontinuita poskytovaných služeb i při výpadku části infrastruktury.

Návrh a provedení musí být v návaznosti na doporučení ANSI/TIA 942 (TIER) v přiměřeném rozsahu pro prostředí zadavatele a musí zahrnovat optimalizaci konfigurace včetně bezpečnostního hardeningu. Akceptace proběhne předvedením úspěšného řízeného failoveru kritických služeb dle scénářů připravených dodavatelem a schválených zadavatelem a doložením dokumentace konfigurace, replikací, plánů obnovy a provozních postupů.

2. Specifikace dodávaného hardware, software a služeb instalace, implementace a školení

Dodavatel vyplní následující tabulku specifikace nabízeného plnění. Ve sloupci „Splnění parametrů dodavatele – DOPLNÍ DODAVATEL“ dodavatel doplní:

- ANO/NE v závislosti na tom, zda nabízené plnění či jeho část požadavek zadavatele splňuje/nesplňuje,
- specifikaci konkrétního parametru či popis naplnění požadavku zadavatele,
- číselnou hodnotu v případě požadavku zadavatele, který obsahuje číselně vyjádřitelný parametr
- přesnou specifikaci HW, SW nebo služby
- volitelně odkaz na dodavatelem přiložený dokument ve formátu PDF

Minimální technické parametry – 4 ks serverů včetně licencí a implementace

Parametr	Popis	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
1.	Server – velikost a vnitřní uspořádání: Rack provedení, 1U, min. 8 diskových slotů s možností rozšíření na 10 diskových pozic. Pro přístup ke všem komponentám serveru není nutné nářadí, barevně značené hot-plug vnitřní komponenty. Pojízdné ližiny pro osazení do rozvaděče a rameno na kabeláž.	ANO
2.	Server – procesor: 2-socketový systém osazený dvěma procesory s parametry min. 2.8 GHz, min. 16 core, min. 37.5MB L3 cache a podporou sběrnice DDR5 5200 MT/s s maximálním příkonem 195W https://www.spec.org/cpu2017/results/cpu2017.html Floating Rates Base: min. 486 bodů pro plně osazený server Integer Rates Base: min. 339 bodů pro plně osazený server	ANO - INT Xeon-G 6526Y CPU
3.	Server – rychlost RAM – min. 5600 MHz DDR5	5600 MHz

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

4.	Server – velikost RAM – min. 512 GB, osazeno 8x64 GB moduly, celkově rozšiřitelná až na 8TB typu DDR5	512 GB
5.	2x M.2 SSD disk 480 GB v RAID 1	Ano
6.	Server – síťový interface: Min. 2x 25Gbit SFP28 LAN na kartě nezabírající místo v PCIE slotu včetně 2ks SFP28 Transcieverů	Ano – 2x 25Gb
7.	Server – management konzole: Vyžadována je schopnost monitorovat a spravovat server out-of-band bez nutnosti instalace agenta do operačního systému. Možnost vzdáleného managementu skrze cloud konzoli, bez nutnosti lokálního přístupu. Pokud je k tomuto přístupu třeba licence, musí být součástí konfigurace serveru. Management serveru nezávislý na operačním systému Možnost stažení aktualizací lokálně z internetu (FTP, nebo HTTP) IPMI 2.0 Vestavěná diagnostika komponent Web GUI management vestavěný v managementu Možnost přesměrování sériové linky managementu po LAN Zabezpečená komunikace SSH/HTTPS Podpora SNMP, HTML5 Vícefaktorové ověřování přístupu k managementu serveru Záznam a přehrání záznamu situace posledního crash-screen operačního systému Integrace s Directory Services (AD, LDAP) Management nástroje musí umět poskytovat ovladače instalovaným operačním systémům bez speciální dedikované partition na interních discích serveru a nezávisle na těchto discích (úložiště nezávislé na OS) Nezávislý management musí disponovat dedikovaným ethernet portem, který není součástí požadovaných ethernet portů s možností failover konfigurace na jeden z portů na základní desce (LOM) Firmware všech součástí serveru musí být kryptograficky podepsán tak, aby v rámci distribučního řetězce nemohlo dojít k jeho narušení nebo jeho alternaci. Při zapnutí serveru musí proběhnout kontrola kryptografických podpisů a skutečného obsahu firmwarů jednotlivých komponent. V případě, že jsou některé z nich narušeny, musí server umožnit automatický návrat k posledním validním firmware, či zastavit boot a umožnit administrátorovi přes vzdálené rozhraní nápravu nahráním autentické verze firmware. Možnost integrace do prostředí VMware vCenter Lifecycle Manager (vLCM) pro zjednodušení správy	Ano

	životního cyklu serverů přímo z konzole VMware vCenter	
8.	Server – zdroje/napájení: redundantní síťové napájecí zdroje min. 1000W Titanium s možností nastavení limitů výkonu a spotřeby v BIOSu (Power Budgeting)	Ano – 1000W
9.	Server – podpora výrobce: Záruka vč. technické podpory na 5 let v režimu NBD, započetí opravy nejpozději následující pracovní den od nahlášení závady, oprava v místě instalace serveru, servis je poskytován výrobcem serveru, jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému, v případě poruchy a výměny SSD disků požadujeme ponechání vadných disků, možnost stažení ovladačů a management software na webových stránkách, doprava serveru do místa v ČR specifikovaného zadavatelem v ceně serveru	Ano
10.	Server – Interface: 5x USB + 1 volitelný, 1x VGA, 1x Display port volitelný, 1x Serial port volitelný, 1x RJ45 dedikovaný pro vzdálenou správu, 1x přední service port, systemový display volitelný	ANO
11.	Podpora všech běžných OS: Microsoft, VMware, Red Hat, SUSE, Canonical Ubuntu, Oracle Linux and Oracle VM, XenServer a další	ANO
12.	Server – licence, které budou kompatibilní nebo budou technicky i kvalitativně srovnatelné s níže uvedeným výčtem potřebných licencí pro správný chod serveru: 2 x MS Windows Server 2025 Datacenter	ANO
13.	Server – dodání a nastavení: Zboží musí být nové, nepoškozené a určené přímo pro „zákazníka“ s garancí výrobce serveru. Příprava nového serveru Instalace a konfigurace virtualizační platformy Instalace a konfigurace Serverů, které budou kompatibilní se současným využívaným systémem ve společnosti. (Windows) migrace firemního prostředí na nové servery asistence s nasazením aplikací 3. stran vytvoření a nastavení zálohovacího scénáře nové serverové infrastruktury propojení na vzdálený replikační server v jiné lokalitě s úložištěm a kopií všech dat pro obnovu v případě havárie primární lokality provedení testovací obnovy infrastruktury doložené protokolem	ANO

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

Minimální technické parametry – 1 ks serveru včetně licencí a implementace

Parametr	Popis	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
1.	Server – velikost a vnitřní uspořádání: Rack provedení, 1U, min. 8 diskových slotů s možností rozšíření na 10 diskových pozic. Pro přístup ke všem komponentám serveru není nutné nářadí, barevně značené hot-plug vnitřní komponenty. Pojízdné ližiny pro osazení do rozvaděče a rameno na kabeláž.	ANO
2.	Server – procesor: 2-socketový systém osazený dvěma procesory s parametry min. 2.8 GHz, min. 16 core, min. 37.5MB L3 cache a podporou sběrnice DDR5 5200 MT/s s maximálním příkonem 195W https://www.spec.org/cpu2017/results/cpu2017.html Floating Rates Base: min. 486 bodů pro plně osazený server Integer Rates Base: min. 339 bodů pro plně osazený server	ANO - INT Xeon-G 6526Y CPU
3.	Server – rychlost RAM – min. 5600 MHz DDR5	ANO
4.	Server – velikost RAM – min. 1024 GB, osazeno 16x64 GB moduly, celkově rozšiřitelná až na 8TB typu DDR5	ANO
5.	2x M.2 SSD disk 480 GB v RAID 1	ANO
6.	Server – síťový interface: Min. 2x 25Gbit SFP28 LAN na kartě nezabírající místo v PCIE slotu včetně 2ks SFP28 Transcieverů	ANO – 2x25Gb
7.	Server – management konzole: Vyžadována je schopnost monitorovat a spravovat server out-of-band bez nutnosti instalace agenta do operačního systému. Možnost vzdáleného managementu skrze cloud konzoli, bez nutnosti lokálního přístupu. Pokud je k tomuto přístupu třeba licence, musí být součástí konfigurace serveru. Management serveru nezávislý na operačním systému Možnost stažení aktualizací lokálně z internetu (FTP, nebo HTTP) IPMI 2.0 Vestavěná diagnostika komponent Web GUI management vestavěný v managementu Možnost přesměrování sériové linky managementu po LAN Zabezpečená komunikace SSH/HTTPS Podpora SNMP, HTML5 Vícefaktorové ověřování přístupu k managementu serveru Záznam a přehrání záznamu situace posledního crash-screen operačního systému	ANO

	Integrace s Directory Services (AD, LDAP) Management nástroje musí umět poskytovat ovladače instalovaným operačním systémům bez speciální dedikované partition na interních discích serveru a nezávisle na těchto discích (úložiště nezávislé na OS) Nezávislý management musí disponovat dedikovaným ethernet portem, který není součástí požadovaných ethernet portů s možností failover konfigurace na jeden z portů na základní desce (LOM) Firmware všech součástí serveru musí být kryptograficky podepsán tak, aby v rámci distribučního řetězce nemohlo dojít k jeho narušení nebo jeho alternaci. Při zapnutí serveru musí proběhnout kontrola kryptografických podpisů a skutečného obsahu firmwarů jednotlivých komponent. V případě, že jsou některé z nich narušeny, musí server umožnit automatický návrat k posledním validním firmware, či zastavit boot a umožnit administrátorovi přes vzdálené rozhraní nápravu nahráním autentické verze firmware. Možnost integrace do prostředí VMware vCenter Lifecycle Manager (vLCM) pro zjednodušení správy životního cyklu serverů přímo z konzole VMware vCenter	
8.	Server – zdroje/napájení: redundantní síťové napájecí zdroje min. 1000W Titanium s možností nastavení limitů výkonu a spotřeby v BIOSu (Power Budgeting)	ANO – 1000W
9.	Server – podpora výrobce: Záruka vč. technické podpory na 5 let v režimu NBD, započetí opravy nejpozději následující pracovní den od nahlášení závady, oprava v místě instalace serveru, servis je poskytován výrobcem serveru, jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému, v případě poruchy a výměny SSD disků požadujeme ponechání vadných disků, možnost stažení ovladačů a management software na webových stránkách, doprava serveru do místa v ČR specifikovaného zadavatelem v ceně serveru	ANO
10.	Server – Interface: 5x USB + 1 volitelný, 1x VGA, 1x Display port volitelný, 1x Serial port volitelný, 1x RJ45 dedikovaný pro vzdálenou správu, 1x přední service port, systemový display volitelný	ANO
11.	Podpora všech běžných OS: Microsoft, VMware, Red Hat, SUSE, Canonical Ubuntu, Oracle Linux and Oracle VM, XenServer a další	ANO
12.	Server – licence, které budou kompatibilní nebo budou technicky i kvalitativně srovnatelné s níže uvedeným výčtem potřebných licencí pro správný	ANO

	chod serveru: 2 x MS Windows Server 2025 Standard 1 x MS SQL Server Standard v nejnovější dostupné verzi, 8 virtuálních jader	
13.	Server – dodání a nastavení: Zboží musí být nové, nepoškozené a určené přímo pro „zákazníka“ s garancí výrobce serveru. Příprava nového serveru Instalace a konfigurace virtualizační platformy Instalace a konfigurace Serverů, které budou kompatibilní se současným využívaným systémem ve společnosti. (Windows) migrace firemního prostředí na nové servery asistence s nasazením aplikací 3. stran vytvoření a nastavení zálohovacího scénáře nové serverové infrastruktury propojení na vzdálený replikační server v jiné lokalitě s úložištěm a kopií všech dat pro obnovu v případě havárie primární lokality provedení testovací obnovy infrastruktury doložené protokolem	ANO

Minimální technické parametry – 3 ks serverů včetně licencí a implementace

Parametr	Popis	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
1.	Server – velikost a vnitřní uspořádání: Rack provedení, 1U, min. 8 diskových slotů s možností rozšíření na 10 diskových pozic. Pro přístup ke všem komponentám serveru není nutné nářadí, barevně značené hot-plug vnitřní komponenty. Pojízdné ližiny pro osazení do rozvaděče a rameno na kabeláž.	ANO
2.	Server – procesor: 2-socketový systém osazený jedním procesorem s parametry min. 2.8 GHz, min. 16 core, min. 37.5MB L3 cache a podporou sběrnice DDR5 5200 MT/s s maximálním příkonem 195W https://www.spec.org/cpu2017/results/cpu2017.html Floating Rates Base: min. 486 bodů pro plně osazený server Integer Rates Base: min. 339 bodů pro plně osazený server	ANO - INT Xeon-G 6526Y CPU
3.	Server – rychlost RAM – min. 5600 MHz DDR5	ANO
4.	Server – velikost RAM – min. 64 GB, osazeno 2x32 GB moduly, celkově rozšiřitelná až na 8TB typu DDR5	ANO
5.	2x M.2 SSD disk 480 GB v RAID 1 pro instalaci	ANO
6.	Server – síťový interface: Min. 2x 25Gbit SFP28 LAN na kartě nezabírající místo v PCIE slotu včetně 2ks SFP28 Transcieverů	ANO - 2x25Gb

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

7.	Server – management konzole: Vyžadována je schopnost monitorovat a spravovat server out-of-band bez nutnosti instalace agenta do operačního systému. Možnost vzdáleného managementu skrze cloud konzoli, bez nutnosti lokálního přístupu. Pokud je k tomuto přístupu třeba licence, musí být součástí konfigurace serveru. Management serveru nezávislý na operačním systému Možnost stažení aktualizací lokálně z internetu (FTP, nebo HTTP) IPMI 2.0 Vestavěná diagnostika komponent Web GUI management vestavěný v managementu Možnost přesměrování sériové linky managementu po LAN Zabezpečená komunikace SSH/HTTPS Podpora SNMP, HTML5 Vícefaktorové ověřování přístupu k managementu serveru Záznam a přehrání záznamu situace posledního crash-screen operačního systému Integrace s Directory Services (AD, LDAP) Management nástroje musí umět poskytovat ovladače instalovaným operačním systémům bez speciální dedikované partition na interních discích serveru a nezávisle na těchto discích (úložiště nezávislé na OS) Nezávislý management musí disponovat dedikovaným ethernet portem, který není součástí požadovaných ethernet portů s možností failover konfigurace na jeden z portů na základní desce (LOM) Firmware všech součástí serveru musí být kryptograficky podepsán tak, aby v rámci distribučního řetězce nemohlo dojít k jeho narušení nebo jeho alternaci. Při zapnutí serveru musí proběhnout kontrola kryptografických podpisů a skutečného obsahu firmwarů jednotlivých komponent. V případě, že jsou některé z nich narušeny, musí server umožnit automatický návrat k posledním validním firmware, či zastavit boot a umožnit administrátorovi přes vzdálené rozhraní nápravu nahráním autentické verze firmware. Možnost integrace do prostředí VMware vCenter Lifecycle Manager (vLCM) pro zjednodušení správy životního cyklu serverů přímo z konzole VMware vCenter	ANO
8.	Server – zdroje/napájení: redundantní síťové napájecí zdroje min. 1000W Titanium s možností nastavení limitů výkonu a spotřeby v BIOSu (Power Budgeting)	ANO – 1000W
9.	Server – podpora výrobce: Záruka vč. technické podpory na 5 let v režimu	ANO

	NBD, započetí opravy nejpozději následující pracovní den od nahlášení závady, oprava v místě instalace serveru, servis je poskytován výrobcem serveru, jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému, v případě poruchy a výměny SSD disků požadujeme ponechání vadných disků, možnost stažení ovladačů a management software na webových stránkách, doprava serveru do místa v ČR specifikovaného zadavatelem v ceně serveru	
10.	Server – Interface: 5x USB + 1 volitelný, 1x VGA, 1x Display port volitelný, 1x Serial port volitelný, 1x RJ45 dedikovaný pro vzdálenou správu, 1x přední service port, systemový display volitelný	ANO
11.	Podpora všech běžných OS: Microsoft, VMware, Red Hat, SUSE, Canonical Ubuntu, Oracle Linux and Oracle VM, XenServer a další	ANO
12.	Server – licence, které budou kompatibilní nebo budou technicky i kvalitativně srovnatelné s níže uvedeným výčtem potřebných licencí pro správný chod serveru: 1 x MS Windows Server 2025 Standard	ANO
13.	Server – dodání a nastavení: Zboží musí být nové, nepoškozené a určené přímo pro „zákazníka“ s garancí výrobce serveru. Příprava nového serveru Instalace a konfigurace virtualizační platformy Instalace a konfigurace Serverů, které budou kompatibilní se současným využívaným systémem ve společnosti. (Windows) migrace firemního prostředí na nové servery asistence s nasazením aplikací 3. stran vytvoření a nastavení zálohovacího scénáře nové serverové infrastruktury propojení na vzdálený replikační server v jiné lokalitě s úložištěm a kopií všech dat pro obnovu v případě havárie primární lokality provedení testovací obnovy infrastruktury doložené protokolem	ANO

Deduplikační diskové uložiště

Minimální technické parametry – 1ks diskového uložiště včetně licencí a implementace

Položka	Parametr	Popis	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
1.	Architektura	✓ modulární, minimálně dvou řadičové all flash / hybridní diskové pole active-active designu založené na NVMe architektuře, řešení je koncipováno jako HW, SW a FW od jednoho výrobce	ANO, modulární, dvou řadičové all flash / hybridní diskové pole active-active designu založené na NVMe architektuře, řešení je

			koncipováno jako HW, SW a FW od IBM
2.	Výkonnost	✓ škálování výkonnosti je možné nativním přidáváním dalších řadičů minimálně do osmi řadičové konfigurace a škálování kapacit pomocí expanzních jednotek. Škálování řadičů ani expanzních jednotek není povoleno řešit pomocí externí virtualizace nebo podvěšením dalšího pole a řadičů	ANO, škálování výkonnosti je možné přidáváním dalších řadičů minimálně do 32 řadičové konfigurace a škálování kapacit pomocí expanzních jednotek
3.	Rozšiřitelnost, podporované disky a moduly	✓ celková velikost cache/RAM v jednom řadiči je minimálně 128GB ✓ celková nativní rozšiřitelnost je minimálně 400 disků, v případě nasazení více řadičů minimálně dvojnásobek disků. Jak je popsáno výše na řádku výkonnost, nelze toto řešit pomocí externí virtualizace nebo podvěšením dalšího pole a řadičů ✓ podpora 2,5" nebo 3,5" disků technologie SSD/flash včetně rotačních disků a to současně: - podpora SCM (Storage Class Memory) - enterprise úrovně tzn. minimálně eMLC, 3D TLC, SLC nebo eSLC nebo enterprise flash modulů s hodnotou DWPD 1 a vyšší - všechny požadované typy SSD musí být NVMe architektury - rotační disky minimálně na SAS 3.0 architektuře - řešení musí umožňovat nasazení redukce dat tak v reálném čase tak, aby nedošlo k žádnému ovlivnění výkonu jednotlivých řadičů, tzn. je požadována separátní HW technologie, která je nezávislá na výpočetním výkonu jednotlivých řadičů a zajišťuje maximálně efektivní redukci dat nezávisle na typu ukládaných dat	ANO, celková velikost cache/RAM v jednom řadiči je 128 GB ANO, celková rozšiřitelnost je minimálně 440 disků, v případě nasazení více řadičů, více než 30x tolik disků. ANO, podporuje 2,5" nebo 3,5" disků technologie SSD/flash včetně rotačních disků a to současně ANO, podporuje SCM (Storage Class Memory) ANO, podporuje SSD enterprise úrovně 3D TLC, SLC a enterprise flash modulů s hodnotou DWPD minimálně 1 a vyšší ANO, všechny požadované typy SSD jsou NVMe standardu a je možné je současně osadit (mixovat) v rámci jedné diskové police ANO, řešení umožňuje nasazení redukce dat v reálném čase tak, že nedochází k žádnému ovlivnění výkonu jednotlivých řadičů, tzn. je obsažena separátní HW technologie, která je nezávislá na výpočetním výkonu jednotlivých řadičů a zajišťuje maximálně efektivní redukci dat nezávisle na typu ukládaných dat

		✓ podpora minimálně následujících režimů RAID - 1, 5, 6, 10 nebo minimálně DRAID 1 a 6	ANO, podporuje DRAID 1, 5 a 6
4.	Minimální požadovaná hrubá kapacita a ochrana dat	✓ Tier 0: minimálně 14 TB na SSD / Flash ve variantě enterprise (DWPD 2 a vyšší, maximální velikost jednoho SSD nebo flash modulu je 2TB)	Tier 0: 15,32 TB na SSD variantě enterprise, velikost jednoho SSD nebo flash modulu je 1,92 TB)
5.	Konektivita k hostitelským serverům (front-end)	✓ diskové pole obsahuje připojení diskového pole blokovým přístupem pomocí 32Gbit FC. Jsou požadovány min. 4 porty 32Gb FC na řadič, tzn. minimálně 8x 32Gbit FC portů včetně osazených SW SFP převodníky s možností rozšíření 32Gbit FC portů na dvojnásobek a dále možnost osazení minimálně 12 Gbit ethernet portů do nabízených řadičů	ANO, diskové pole obsahuje připojení diskového pole blokovým přístupem pomocí 32Gbit FC. Jsou osazeny 4 porty 32Gb FC na řadič, tzn. 8x 32Gbit FC portů včetně osazených SW SFP převodníky s možností rozšíření 32Gbit FC portů na dvojnásobek a dále možnost osazení minimálně 12 Gbit ethernet portů do nabízených řadičů
6.	Funkcionality pro efektivní ukládání a správu dat	✓ vytváření virtuálních logických disků ✓ thin provisioning (včetně detekce a reklamace prázdného prostoru) ✓ komprese dat v reálném čase bez nutnosti dedikování dodatečného diskového prostoru pro post-processing pro celou nabízenou kapacitu včetně patřičného HW akcelerátoru nebo na jednotlivých modulech ✓ deduplikace dat v reálném čase bez nutnosti dedikování dodatečného diskového prostoru pro post-processing pro celou požadovanou kapacitu včetně SW licence ✓ šifrování dat minimálně pro flash kapacitu ve standardu minimálně FIPS 140-2 nebo 3 bez nutnosti přítomnosti speciálních pevných disků včetně příslušné licence. Pokud nabízené řešení neumožňuje šifrování dat nad úrovní disků, jsou požadovány SED disky pro celou	ANO, nabízené doskové pole plně podporuje: - vytváření virtuálních logických disků - Thin provisioning (včetně detekce a reklamace prázdného prostoru) ANO, komprese dat je možná v reálném čase a je bez nutnosti dedikování dodatečného diskového prostoru pro post-processing na jednotlivých FCM modulech ANO, deduplikace dat je v reálném čase bez nutnosti dedikování dodatečného diskového prostoru pro post-processing pro celou požadovanou kapacitu včetně SW licence ANO, šifrování dat pro flash kapacitu je ve standardu FIPS 140-3 Level 1

		nabízenou flash kapacitu, opět minimálně ve standardu FIPS 140-2 nebo 3 ✓ inteligentní správa výkonnostních charakteristik (pro minimálně 3 tiery a to včetně SCM) virtualizovaných diskových prostorů (automatická migrace více utilizovaných dat na rychlejší disky nebo SSD/SCM) ✓ podpora externí storage virtualizace pro stávající disková pole a možnost dalšího připojení externích diskových polí od různých výrobců min. pro účely migrace. Seznam podporovaných diskových systému je veřejně dostupný. ✓ Podpora nástrojů pro sledování historických dat o vytížení datového úložiště (minimálně počet IOps, latence, propustnost, alokovaná kapacita, využití keší) s granularitou na hosta či LUN s historií minimálně 1 rok (možnost řešit externích SW nástrojem v rámci dodávky) ✓ Microsoft VSS podpora ✓ VMware VAAI, VVOL podpora, dále je požadován VASA provider přímo ve FW nabízeného diskového pole	ANO, v ceně řešení je inteligentní správa výkonnostních charakteristik (pro 3 tiery včetně SCM) virtualizovaných diskových prostorů (automatická migrace více utilizovaných dat na rychlejší disky nebo SSD/SCM) ANO, podporuje externí storage virtualizace pro stávající disková pole a možnost dalšího připojení externích diskových polí od různých výrobců min. pro účely migrace. Seznam podporovaných diskových systému je veřejně dostupný. ANO, obsahuje nástroj pro sledování historických dat o vytížení datového úložiště (minimálně počet IOps, latence, propustnost, alokovaná kapacita, využití keší) s granularitou na hosta či LUN s historií minimálně 1 rok pomocí obsažené licence pro Spectrum Control Select Edition / Storage Insights PRO ANO, podporuje Microsoft VSS a VMware VAAI, VASA a VVOL, VASA provider je přímo ve FW nabízeného diskového pole
7.	Podpora operačních systémů a hypervizorů	✓ IBM AIX 7.1, 7.2 a vyšší ✓ IBM VIOS 2.2 a vyšší ✓ Oracle Enterprise Linux 8.x a vyšší ✓ Oracle DB 11.x a 12.x a vyšší ✓ RHEL 6.x a vyšší ✓ VMware 7 a vyšší včetně VAAI a VASA integrací ✓ Windows server 2016 a vyšší	ANO, podporuje, viz. ZDE
8.	Typ přístupu k datům	✓ blokový, standard FCP a iSCSI	ANO, podporuje

9.	Bezpečnost	✓ ochrana proti ransomware útokům nativní funkcionalitou nabízeného pole v rámci jeho funkcionalit – řešení z aplikační vrstvy pomocí aplikací třetích stran nebo za asistence zálohovacího SW není přípustné. Řešení musí být pro tento účel jasně popsané a určené, např. ochrana LUNu pouze nastavením do read-only modu není dostatečná pro splnění tohoto požadavku	ANO, ochrana proti ransomware útokům je nativní funkcionalitou nabízeného pole v rámci jeho funkcionalit a je obsažena v nabízeném řešení – Inline Data Corruption Detection a IBM Safeguarded Copy
10.	Bezpečnost	✓ řešení musí umožňovat detekci ransomware v reálném čase na blokové úrovni před uložením na disky / flash moduly	ANO, pomocí integrované funkcionality Inline Data Corruption Detection
11.	Bezpečnost	✓ řešení musí umožňovat kontrolu zapsaných dat (bloků) přímo na jednotlivých SSD / flash modulech	ANO, řešení umožňuje kontrolu zapsaných dat (bloků) přímo na jednotlivých SSD / flash modulech
12.	Kopírovací funkce - licence musí být součástí nabídky a musí být na neomezeno u kapacitu, počet disků, expanzích jednotek atd.	✓ zrcadlení virtuálního disku tzn. ochrana virtualizovaných dat v režimu RAID1 (s možností zdvojení dat virtuálního disku i na dvě pole) ✓ možnost vytváření snapshotů (CoW a RoW) a klonů v následujících režimech: - snapshot se po určité době může automaticky stát klonem - inkrementální snapshoty, tzn. kopírují se jen rozdílová data mezi dvěma okamžiky iniciace klonu - reverzní snapshoty, tzn. lze provést zpětné přesunutí dat z klonu do původního originálního Volume - lze udržovat až 4 inkrementálně pořizované klony z jednoho originálu (s možností reverzních snapshotů) ✓ interní/externí zrcadlení logického (virtuálního) disku z jednoho zdroje do dvou cílů pro zvýšení dostupnosti v případě výpadku jednoho cíle	ANO, plně podporuje, licence resp. funkce jsou součástí nabízeného řešení

13.	Zajištění kontinuální dostupnosti dat (DR a HA řešení) - licence musí být součástí nabídky a musí být na neomezeno u kapacitu, počet disků, expanzích jednotek atd.	✓ upgrade software a hardware u řadičů je proveditelné za chodu a bez ztráty přístupu hostitelských serverů k datum ✓ diskové musí být možné spojit do clusteru, který umožňuje vytvoření jednoho funkčního celku, zrcadlení dat mezi jednotlivými poli apod. ✓ vytvoření HA řešení s automatickým failover bez dalších vícenákladů, které je navíc nezávislé na běžných OS nebo virtualizační platformě včetně příslušných licencí ✓ podpora replikace do třetí lokality ✓ SW pro redundantní datové cesty v ceně řešení ✓ Nabízené řešení musí být plně kompatibilní s VMware Metro Storage Cluster funkcionalitou, tzn. musí být dohledatelné v matici kompatibility na stránkách VMware	ANO, upgrade software a hardware u řadičů je proveditelné za chodu a bez ztráty přístupu hostitelských serverů k datům. ANO, jednotlivá disková pole je možné spojit do clusteru, který umožňuje vytvoření jednoho funkčního celku, zrcadlení dat mezi jednotlivými poli apod. ANO, vytvoření HA řešení s automatickým failover bez dalších vícenákladů, které je navíc nezávislé na OS nebo virtualizační platformě včetně příslušných licencí pro Policy Based HA ANO, podporuje replikace do třetí lokality. ANO, obsahuje SW pro redundantní datové cesty v ceně řešení. ANO, nabízené řešení je plně kompatibilní s VMware Metro Storage Cluster funkcionalitou, tzn. dohledatelná v matici kompatibility na stránkách VMware.
14.	Migrace dat	✓ transparentní migrace (tzn. možnost zdarma migrovat data ze stávajících diskových polí na nová disková úložiště) s možnosti rozšíření o synchronní a asynchronní zrcadlení logických (virtuálních) disků v případě více lokalit	ANO, obsahuje transparentní migrace (tzn. možnost zdarma migrovat data ze stávajících diskových polí na nová disková úložiště) s možností rozšíření o synchronní a asynchronní zrcadlení logických (virtuálních) disků v případě více lokalit.
15.	Počet hostitelských serverů připojovaných k diskovému poli	✓ řešení obsahuje licence na neomezený počet připojení hostitelských serverů	ANO, obsahuje
16.	Správa diskového	✓ SW pro plnohodnotnou správu diskového pole a diskových	ANO, je obsažen SW pro plnohodnotnou správu

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

	pole a další dostupné funkcionality	subsystémů, možnost ovládání přes CLI, GUI (ze std. web browseru) ✓ Remote Service (call home) v ceně řešení ✓ Příkazy prováděné v GUI jsou uchovávány v tzv. "AuditLogu" v podobě standardních CLI příkazů, které lze později snadno zkopírovat a aplikovat při programování uživatelských skriptů např. pro podporu automatizace zálohování atd. ✓ Je požadováno potvrzení od lokálního zastoupení výrobce, že nabízené řešení je určeno pro český (EU) trh a bude servisním střediskem výrobce plně podporováno. Servisní podpora výrobce bude v českém jazyce	diskového pole a diskových subsystémů, možnost ovládání přes CLI, GUI (ze std. web browseru) ANO, Remote Service (call home) je v ceně nabízeného řešení ANO, příkazy prováděné v GUI jsou uchovávány v tzv. "AuditLogu" v podobě standardních CLI příkazů, které lze později snadno zkopírovat a aplikovat při programování uživatelských skriptů např. pro podporu automatizace zálohování atd. ANO, je přiloženo potvrzení od lokálního zastoupení výrobce, nabízené řešení je určeno pro český (EU) trh a bude servisním střediskem výrobce plně podporováno. Servisní podpora výrobce bude v českém jazyce
17.	Příslušenství	✓ Součástí dodávky je veškerá potřebná kabeláž pro plné zapojení všech portů do instalovaného prostředí a potřebná napájecí kabeláž kompatibilní s napájecími lištami v RACK skříních.	ANO, součástí dodávky je veškerá potřebná kabeláž pro plné zapojení všech portů do instalovaného prostředí a potřebná napájecí kabeláž kompatibilní s napájecími lištami v RACK skříních.
18.	Servisní podpora	✓ Minimálně 5 let; v režimu 24x7 s odstraněním závady do 24h od nahlášení.	ANO, obsahuje podporu na 5 let v režimu 24x7 s garantovanou dobou opravy do 24h od nahlášení.

Ostatní podmínky:

- Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství)
- Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů.
- Je požadována záruka na hardware s výměnou NBD v délce 60 měsíců. Tato záruka musí být garantovaná výrobcem zařízení.
- Je přípustné, aby servis poskytovaný výrobcem byl realizován pověřeným certifikovaným (autorizovaným) dodavatelem, přičemž takto zajišťovaný servis musí být co do rozsahu, SLA, reakčních lhůt, použitých náhradních dílů a odborné kvalifikace personálu identický se servisem poskytovaným přímo výrobcem, bez jakéhokoli zhoršení kvality či dostupnosti. Dodavatel nese i v takovém případě plnou odpovědnost za splnění

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

smluvních povinností a zachování jediného kontaktního místa, přičemž je povinen na žádost zadavatele doložit platnou certifikaci/autorizační vztah takového subjektu.
- Uchazeč je povinen s dodávkou doložit oficiální potvrzení lokálního zastoupení výrobce o všech dodávaných zařízeních (seznam sériových čísel dodávaných zařízení) pro český trh.

2.a. Akceptační kritéria

Akceptace proběhne v souladu s příslušným ustanovením smlouvy a dodavatel mj. zajistí, že dodané řešení zajišťuje vysokou dostupnost služeb a splňuje požadavky uvedené níže.

Specifikace pro naplnění parametrů

Akceptační kritérium	Způsob ověření	Výsledek	Poznámka / Podpis
Úspěšný řízený failover kritických služeb	Předvedení řízeného failoveru kritických služeb dle schválených scénářů zadavatelem		
Dokumentace konfigurace	Doložení dokumentace konfigurace prostředí		
Dokumentace replikací	Doložení dokumentace replikací		
Dokumentace plánů obnovy	Doložení dokumentace plánů obnovy		
Dokumentace provozních postupů	Doložení provozních postupů k zajištění kontinuity služeb		

3. Specifikace služeb technické podpory dodavatele na 60 měsíců od 1. 6. 2026 do 31.5.2031.

Specifikace služeb technické podpory je uvedena v samostatném dokumentu:

- 01 – Technická specifikace – Společná definice technické podpory pro ID01 – ID09

Zadavatel tímto výslovně stanoví, že nepožaduje žádnou záruku nad rámec a mimo rozsah technické podpory vymezený v tomto dokumentu a dokumentu „01 – Technická specifikace – Společná definice technické podpory pro ID01 – ID09“ (dále jen „Společná definice“). Veškeré záruční povinnosti dodavatele, včetně úrovní služeb, reakčních dob, způsobu eskalace, podmínek dostupnosti, režimu aktualizací, EoL/EoS a výluk plnění, se řídí výlučně tímto dokumentem a Společnou definicí. Jakákoli plnění spočívající v rozvojových zásazích, změnových požadavcích, úpravách nad rámec specifikace či integracích nevyplývajících ze Společné definice nejsou součástí záruky, ledaže budou výslovně sjednána zvláštní smlouvou nebo dodatkem.

V případě rozporu nebo kolizního výkladu mezi touto technickou specifikací a Společnou definicí má přednost tato technická specifikace. Společná definice slouží jako doplňující a výkladový dokument a uplatní se pouze v rozsahu, v němž není v rozporu s touto Technickou specifikací.

3.a. Akceptační kritéria

Dodavatel se zavazuje poskytovat technickou podporu v rozsahu a za podmínek stanovených tímto dokumentem a Společnou definicí po dobu od 1. 6. 2026 do 31. 5. 2031 (60 měsíců). Dodavatel podpisem smlouvy stvrzuje, že po uvedené období bude plnit sjednané SLA a ostatní povinnosti dle tohoto dokumentu a Společné definice; nesplnění těchto povinností bude posuzováno jako porušení smlouvy se všemi z toho vyplývajícími právními následky podle smlouvy a příslušných právních předpisů.

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

8.1.3. ID03 - Výměna a implementace aktivních síťových prvků

1. Úvod a metodika

Tento dokument definuje předmět a závaznou technickou specifikaci pro dodávku a uvedení do provozu moderních přepínačů s podporou bezpečnostních funkcí na L2/L3 úrovni (např. ACL, mechanismy mitigace L2/L3 útoků, DHCP snooping, ARP inspection) a s možností logické mikrosegmentace. Požadována je plná připravenost na IPv6, podpora 802.1X a centralizovaný management s auditními záznamy změn konfigurace a dohledem nad stavem zařízení.

Součástí plnění je návrh segmentace, zajištění propojení s existující infrastrukturou a předání konfiguračních šablon a provozní dokumentace. Akceptace proběhne ověřením funkčnosti přístupu uživatelů a zařízení podle definovaných politik, testem autentizace 802.1X a kontrolou správné aplikace bezpečnostních pravidel a dohledu v centralizovaném nástroji.

V dodávce je požadované dodání 1 kusu aktivního síťového prvku dle specifikace HW parametrů níže.

2. Specifikace dodávaného hardware, software a služeb instalace, implementace a školení

Dodavatel vyplní následující tabulku specifikace nabízeného plnění. Ve sloupci „Splnění parametrů dodavatele – DOPLNÍ DODAVATEL“ dodavatel doplní:

- ANO/NE v závislosti na tom, zda nabízené plnění či jeho část požadavek zadavatele splňuje/nesplňuje,
- specifikaci konkrétního parametru či popis naplnění požadavku zadavatele,
- číselnou hodnotu v případě požadavku zadavatele, který obsahuje číselně vyjádřitelný parametr
- přesnou specifikaci HW, SW nebo služby
- volitelně odkaz na dodavatelem přiložený dokument ve formátu PDF

Požadavek na funkcionalitu	Minimální požadavky	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
Základní vlastnosti		
Třída zařízení: L3 switch	ano	ano
Formát zařízení: modulární chassi	ano	ano
Počet slotů pro linkové karty: 5	ano	ano
Maximální velikost zařízení: 7U	ano	ano
Počet optických 10/25GE portů s volitelným fyzickým rozhraním	96x 10/25 Gbit/s SFP28	96x 10/25 Gbit/s SFP28
Počet optických 40/100GE portů s volitelným fyzickým rozhraním	12x 40/100Gbit/s QSFP28	12x 40/100Gbit/s QSFP28
Interní hot-swap AC napájecí zdroje	ano, 4x stejný model,	ano, 4x stejný model,
možnost rozšíření o zdroj s vyšším výkonem pro PoE	ano	ano
Podpora PoE+ dle standardu 802.3at na všech portech RJ45 v linkových kartách	ano	ano
Možnost osazení karet s podporou Class 4 a Class 6 PoE	ano	ano

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

Možnost osazení karet s podporou 40 a 100GE interface	ano	ano
Celková propustnost chassis: 14 Tbit/s	ano	ano
Celkový paketový výkon přepínače: 10 Bpps	ano	ano
Paketový buffer: 8 MB per linková karta	ano	ano
Vysoká dostupnost		
Redundantní management modul	ano	ano
Podpora virtualizace funkcí dvou přepínačů - dvojice se chová jako jedno zařízení pro funkce linkové agregace a L3 výchozí brány	ano	ano
Zařízení v rámci virtualizovaného páru si zachovávají vlastní control plane	ano	ano
Virtualizace dvou přepínačů je prováděna přes standardní ethernet porty	ano	ano
Seskupení portů IEEE 802.3ad mezi různými prvky stohu (Multichassis LAG)	ano	ano
Minimální počet seskupení portů napříč různými chassis	256	256
Základní funkce a protokoly		
Podpora "jumbo rámců" včetně velikosti 9198 Byte	ano	ano
Podpora linkové agregace IEEE 802.1AX	ano	ano
Konfigurovatelné rozkládání LACP zátěže podle L2,L3	ano	ano
Počet LACP skupin/linek ve skupině	256/8	256/8
Počet záznamů v tabulce MAC adres	29 000	29 000
Počet záznamů v tabulce ARP	28 000	28 000
Protokol pro definici šířených VLAN	MVRP	MVRP
Podpora VLAN podle IEEE 802.1Q, minimálně 4000 aktivních VLAN	ano	ano
VLAN translace - swap 802.1Q tagů na trunk portu	ano	ano
Podpora zařazování do VLAN podle standardu 802.1v	ano	ano
IEEE 802.1s - Multiple Spanning Tree	ano	ano
STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)	ano	ano
Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED	ano	ano
Detekce jednosměrnosti optické linky (např. UDLD)	ano	ano
DHCP relay pro IPv4 a IPv6	ano	ano
Podpora NTPv4 pro IPv4 a IPv6 včetně VRF a MD5 autentizace	ano	ano
Statické směrování IPv4 a IPv6	ano	ano
Počet záznamů ve směrovací tabulce	64 000	64 000
Dynamické směrování OSPFv2, OSPFv3 a BGP včetně podpory BFD	ano	ano
Podpora BGP a MP-BGP včetně podpory BFD	ano	ano
Podpora Layer-3 routed port	ano	ano

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

IGMP v2 a v3	ano	ano
MLD v1 a v2	ano	ano
Hardware podpora IPv4 a IPv6 ACL	ano	ano
ACL definice na základě skupiny fyzických portů	ano	ano
ACL aplikovatelný na interface, LAG, VLAN	ano	ano
BPDU a Root guard	ano	ano
DHCP snooping pro IPv4 a IPv6	ano	ano
HW ochrana proti zahlcení portu (broadcast/multicast/icmp) nastavitelná na kbps a pps	ano	ano
802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port	ano	ano
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)	ano	ano
Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675	ano	ano
Podpora Critical VLAN	ano	ano
Podpora uživatelských rolí definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely.	ano	ano
Uživatelské role mohou být lokálně definované v přepínači nebo mohou být dynamicky stáhnuty z RADIUS serveru na základě výsledku autorizace.	ano	ano
Podpora IPv6 RA Guard	ano	ano
IP source guard / dynamic IP lockdown	ano	ano
Podpora Dynamic ARP protection	ano	ano
Port security	ano	ano
Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU	ano	ano
Podpora IPv4 a IPv6 QoS	ano	ano
IEEE 802.1p - minimální počet front	8	8
SDN funkce		
Podpora service insertion včetně technologie VXLAN	ano	ano
Podpora BGP EVPN s využitím VXLAN	ano	ano
Podpora tunelování uživatelského provozu pomocí L2 GRE tunelů - schopnost izolololovat více koncových zařízení na jednom portu do unikátních tunelů	ano	ano
Přiřazení koncového zařízení do tunelu na základě výsledku autorizace	ano	ano
Analytické a automatizační nástroje		
Podpora REST API pro automatizaci nastavení sítě.	ano	ano
Podpora skriptování v jazyce Python – lokální interpret jazyka v přepínači	ano	ano
Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní)	ano	ano

Interpretace uživatelských skriptů monitorujících definované parametry síťového provozu s možností automatické reakce na události	ano	ano
Grafické rozhraní pro vynášení výsledků monitorování a analytických skriptů. Možnost vynášení stavu monitorovaných metrik do grafů atp.	ano	ano
Root cause analysis v grafickém rozhraní – možnost vrácení se ke konkrétní funkční konfiguraci a stavu protokolů v čase.	ano	ano
Interní uložiště dat pro sběr provozních dat a pokročilou dignostiku zařízení	ano	ano
Kapacita interního úložiště dat pro analytické účely: 30 GB	30 GB	30 GB
Management		
USB-C konzolový port	ano	ano
1xRJ45 OoB management port s podporou ethernetu	ano	ano
Podpora minimálně 64 virtuálních směrovacích instancí (VRF)	ano	ano
Minimální počet VRF instancí	64	64
Konfigurace zařízení v člověku čitelné textové formě	ano	ano
Podpora automatických i manuálních snapshotů konfigurace systému	ano	ano
USB port pro diagnostiku, přenos konfigurace a firmware	ano	ano
Přímé bezdrátové připojení ke konzoli zařízení skrze bluetooth	ano	ano
Podpora managementu přes IPv4 i IPv6	ano	ano
SSHv2 a HTTPS pro IPv4 a IPv6	ano	ano
Podpora SNMPv2c a SNMPv3	ano	ano
RMON	ano	ano
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano	ano
Lokálně vynucené RBAC na úrovni přepínače	ano	ano
Dualní flash image	ano	ano
Podpora UDP, TCP a TLS SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů	ano	ano
Podpora RADIUS včetně RADIUS CoA (RFC3576)	ano	ano
Podpora TACACS+	ano	ano
Analýza síťového provozu sFlow podle RFC 3176	ano	ano
Port mirroring, alespoň 4 různé obousměrné session: SPAN, ERSPAN	ano	ano
Podpora IP SLA pro měření zpoždění provozu VoIP	ano	ano
Podpora Zero Touch Provisioning (ZTP)	ano	ano

Ostatní podmínky:

- Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství)
- Je-li některý z parametrů vnímán jako proprietární, je možné splnění obdobným parametrem s uvedením příslušné specifikace / standardu.
- Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů.
- Je požadována záruka na hardware s výměnou NBD v délce 60 měsíců. Tato záruka musí být garantovaná výrobcem zařízení.
- Uchazeč je povinen s dodávkou doložit oficiální potvrzení lokálního zastoupení výrobce o všech dodávaných zařízeních (seznam sériových čísel dodávaných zařízení) pro český trh.

2.a. Akceptační kritéria

Akceptace proběhne v souladu s příslušným ustanovením smlouvy a dodavatel mj. dodá a uvede do provozu moderní přepínače s podporou bezpečnostních funkcí na L2/L3 úrovni (např. ACL, mechanismy mitigace L2/L3 útoků, DHCP snooping, ARP inspection) a s možností logické mikrosegmentace.

Součástí plnění je návrh segmentace, zajištění propojení s existující infrastrukturou a předání konfiguračních šablon a provozní dokumentace.

Akceptace proběhne ověřením funkčnosti přístupu uživatelů a zařízení podle definovaných politik, testem autentizace 802.1X a kontrolou správné aplikace bezpečnostních pravidel a dohledu v centralizovaném nástroji.

3. Specifikace služeb technické podpory dodavatele na 60 měsíců od 1. 6. 2026 do 31.5.2031.

Specifikace služeb technické podpory je uvedena v samostatném dokumentu:

- 01 – Technická specifikace – Společná definice technické podpory pro ID01 – ID09

Zadavatel tímto výslovně stanoví, že nepožaduje žádnou záruku nad rámec a mimo rozsah technické podpory vymezený v tomto dokumentu a dokumentu „01 – Technická specifikace – Společná definice technické podpory pro ID01 – ID09“ (dále jen „Společná definice“). Veškeré záruční povinnosti dodavatele, včetně úrovní služeb, reakčních dob, způsobu eskalace, podmínek dostupnosti, režimu aktualizací, EoL/EoS a výluk plnění, se řídí výlučně tímto dokumentem a Společnou definicí. Jakákoli plnění spočívající v rozvojových zásazích, změnových požadavcích, úpravách nad rámec specifikace či integracích nevyplývajících ze Společné definice nejsou součástí záruky, ledaže budou výslovně sjednána zvláštní smlouvou nebo dodatkem.

V případě rozporu nebo kolizního výkladu mezi touto technickou specifikací a Společnou definicí má přednost tato technická specifikace. Společná definice slouží jako doplňující a výkladový dokument a uplatní se pouze v rozsahu, v němž není v rozporu s touto Technickou specifikací.

3.a. Akceptační kritéria

Dodavatel se zavazuje poskytovat technickou podporu v rozsahu a za podmínek stanovených tímto dokumentem a Společnou definicí po dobu od 1. 6. 2026 do 31. 5. 2031 (60 měsíců). Dodavatel podpisem smlouvy stvrzuje, že po uvedené období bude plnit sjednané SLA a ostatní povinnosti dle tohoto dokumentu a Společné definice; nesplnění těchto povinností bude posuzováno jako porušení smlouvy se všemi z toho vyplývajícími právními následky podle smlouvy a příslušných právních předpisů.

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

8.1.4. ID04 - Výměna a implementace Wi-Fi infrastruktury

1. Úvod a metodika

Tento dokument definuje předmět a závaznou technickou specifikaci pro implementaci moderních přístupových bodů a řídicích prvků (kontrolérů) s podporou standardu IEEE 802.11be (Wi-Fi 7) a nasazení bezpečnostních mechanismů dle současných standardů (WPA3) včetně případných nadstaveb pro posílení ochrany přístupu. Infrastruktura bude navržena s oddělenými SSID, vhodnou segmentací provozu a centralizovaným monitoringem a správou přístupových bodů i kontrolérů.

Součástí plnění je kompletní montáž dodávané bezdrátové infrastruktury, implementace politik přístupu, QoS dle potřeb aplikací a dokumentace návrhu, konfigurace a provozu. Akceptace proběhne ověřením autentizace a šifrování dle WPA3, funkčnosti segmentace a dohledové viditelnosti v centrálním systému.

Zadavatel disponuje oddělenou pasivní síťovou infrastrukturou pro zajištění provozu stávající bezdrátové sítě. Tato infrastruktura bude v plném rozsahu využita pro novou WiFi infrastrukturu.

2. Specifikace dodávaného hardware, software a služeb instalace, implementace a školení

Dodavatel vyplní následující tabulku specifikace nabízeného plnění. Ve sloupci „Splnění parametrů dodavatele – DOPLNÍ DODAVATEL“ dodavatel doplní:

- ANO/NE v závislosti na tom, zda nabízené plnění či jeho část požadavek zadavatele splňuje/nesplňuje,
- specifikaci konkrétního parametru či popis naplnění požadavku zadavatele,
- číselnou hodnotu v případě požadavku zadavatele, který obsahuje číselně vyjádřitelný parametr
- přesnou specifikaci HW, SW nebo služby
- volitelně odkaz na dodavatelem přiložený dokument ve formátu PDF

Položka	Minimální požadavek na funkcionalitu	Počet ks	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
Agregační přepínač (10G, L3)	Min. 28× SFP+ (10 Gbps), L2/L3, stohování, redundantní napájení	1	28x SFP+ (10 Gbps); 4x SFP28; L2/L3; redundantní napájení, stohování
Bezpečnostní brána / router	Min. 2× WAN (1/10 Gbps), firewall + IDS/IPS, VPN (IPSec/OpenVPN), centrální správa	1	2× WAN (1/10 Gbps), firewall + IDS/IPS, VPN (IPSec/OpenVPN), centrální správa
Přepínač 8portový (2,5 Gbps, PoE)	8× RJ45 2,5 Gbps, PoE+, uplinky Gigabit/SFP	10	8x1/2,5 GbE RJ 45, PoE+, 2x SFP+ 1/10 Gbps
Wi-Fi AP (802.11be, Wi-Fi 7)	Pásmo 2,4/5/6 GHz, min. 500 klientů, PoE, montáž strop/stěna	60	2,4/5/6 GHz, 500+ klientů, PoE, montáž strop/stěna
DAC kabel SFP+ (10 Gbps)	Pasivní, délky 1 m, 3 m	dle potřeby	DAC délky 1 i 3m
SFP+ modul (10G multimode)	Přenos 10 Gbps, dosah min. 300 m (MM vlákno)	10	SFP+ 10G MM

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

Držák pro montáž AP	Kompatibilní s vybranými přístupovými body	dle potřeby	Kompatibilní s WiFi AP

2.a. Akceptační kritéria

Akceptace proběhne v souladu s příslušným ustanovením smlouvy a dodavatel dodá a implementuje Wi-Fi infrastrukturu s podporou standardu IEEE 802.11be (Wi-Fi 7) a nasazení bezpečnostních mechanismů dle současných standardů (WPA3) včetně případných nadstaveb pro posílení ochrany přístupu. Infrastruktura bude navržena s oddělenými SSID, vhodnou segmentací provozu a centralizovaným monitoringem a správou přístupových bodů i kontrolérů.

Akceptace je dokončena podpisem předávacího protokolu potvrzujícího, že je implementována Wi-Fi infrastruktura a splňuje mj. požadavky uvedené níže.

Specifikace pro naplnění parametrů

Akceptační kritérium	Způsob ověření	Výsledek	Poznámka / Podpis
Podpora standardu IEEE 802.11be (Wi-Fi 7)	Ověření funkcionality přístupových bodů a kontrolérů dle standardu		
Implementace WPA3 a bezpečnostních mechanismů	Test autentizace a šifrování dle WPA3 včetně nadstaveb		
Oddělená SSID a segmentace provozu	Kontrola konfigurace a praktické ověření funkčnosti segmentace		
Centralizovaný monitoring a správa	Ověření dohledové viditelnosti a správy v centrálním systému		
Implementace politik přístupu	Kontrola nastavení politik a praktické testy		
Implementace QoS dle potřeb aplikací	Test funkčnosti QoS pro vybrané aplikace		
Dokumentace návrhu, konfigurace a provozu	Doložení a kontrola úplnosti dokumentace		

3. Specifikace služeb technické podpory dodavatele na 60 měsíců od 1. 6. 2026 do 31.5.2031.

Specifikace služeb technické podpory je uvedena v samostatném dokumentu:

- 01 – Technická specifikace – Společná definice technické podpory pro ID01 – ID09

Zadavatel tímto výslovně stanoví, že nepožaduje žádnou záruku nad rámec a mimo rozsah technické podpory vymezený v tomto dokumentu a dokumentu „01 – Technická specifikace – Společná definice technické podpory pro ID01 – ID09“ (dále jen „Společná definice“). Veškeré záruční povinnosti dodavatele, včetně úrovní služeb, reakčních dob, způsobu eskalace, podmínek dostupnosti, režimu aktualizací, EoL/EoS a výluk plnění, se řídí výlučně tímto dokumentem a Společnou definicí. Jakákoli plnění spočívající v rozvojových zásazích, změnových požadavcích,

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

úpravách nad rámec specifikace či integracích nevyplývajících ze Společné definice nejsou součástí záruky, ledaže budou výslovně sjednána zvláštní smlouvou nebo dodatkem.

V případě rozporu nebo kolizního výkladu mezi touto technickou specifikací a Společnou definicí má přednost tato technická specifikace. Společná definice slouží jako doplňující a výkladový dokument a uplatní se pouze v rozsahu, v němž není v rozporu s touto Technickou specifikací.

3.a. Akceptační kritéria

Dodavatel se zavazuje poskytovat technickou podporu v rozsahu a za podmínek stanovených tímto dokumentem a Společnou definicí po dobu od 1. 6. 2026 do 31. 5. 2031 (60 měsíců). Dodavatel podpisem smlouvy stvrzuje, že po uvedené období bude plnit sjednané SLA a ostatní povinnosti dle tohoto dokumentu a Společné definice; nesplnění těchto povinností bude posuzováno jako porušení smlouvy se všemi z toho vyplývajícími právními následky podle smlouvy a příslušných právních předpisů.

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

8.1.5. ID05 - Výměna a implementace zálohovací infrastruktury

1. Úvod a metodika

Tento dokument definuje předmět a závaznou technickou specifikaci pro náhradu stávající zálohovací infrastruktury moderními systémy a úložišti umožňujícími vysoce dostupný provoz a rychlou obnovu (disková i pásková vrstva). Řešení musí podporovat šifrování záloh, automatizované plánování zálohovacích úloh, průběžnou kontrolu konzistence a pravidelné testování scénářů disaster recovery včetně evidence výsledků testů.

Součástí plnění je nastavení politik záloh s definovanými RPO/RTO pro klíčové služby a předání provozní dokumentace. Akceptace proběhne úspěšným provedením obnovy vybraných systémů dle schválených scénářů, doložením reportů z běhu zálohovacích úloh a ověřením šifrování a integrity záloh.

2. Specifikace dodávaného hardware, software a služeb instalace, implementace a školení

Dodavatel vyplní následující tabulku specifikace nabízeného plnění. Ve sloupci „Splnění parametrů dodavatele – DOPLNÍ DODAVATEL“ dodavatel doplní:

- ANO/NE v závislosti na tom, zda nabízené plnění či jeho část požadavek zadavatele splňuje/nesplňuje,
- specifikaci konkrétního parametru či popis naplnění požadavku zadavatele,
- číselnou hodnotu v případě požadavku zadavatele, který obsahuje číselně vyjádřitelný parametr
- přesnou specifikaci HW, SW nebo služby
- volitelně odkaz na dodavatelem přiložený dokument ve formátu PDF

Deduplikační diskové uložiště

Je požadováno jedno deduplikační diskové pole, níže jsou uvedené minimální parametry, které musí splňovat.

Položka	Parametr	Minimální požadavky	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
1.	Architektura	modulární, minimálně dvou řadičové all flash / hybridní diskové pole active-active designu založené na NVMe architektuře, řešení je koncipováno jako HW, SW a FW od jednoho výrobce	ANO, modulární, dvou řadičové all flash / hybridní diskové pole active-active designu založené na NVMe architektuře, řešení je koncipováno jako HW, SW a FW od IBM
2.	Výkonnost	škálování výkonnosti je možné nativním přidáváním dalších řadičů minimálně do osmi řadičové konfigurace a škálování kapacit pomocí expanzních jednotek. Škálování řadičů ani expanzních jednotek není povoleno řešit pomocí externí virtualizace nebo podvěšením dalšího pole a řadičů	ANO, škálování výkonnosti je možné přidáváním dalších řadičů minimálně do 32 řadičové konfigurace a škálování kapacit pomocí expanzních jednotek
3.	Rozšiřitelnost, podporovan	• celková velikost cache/RAM v jednom řadiči je minimálně 128GB • celková nativní rozšiřitelnost je minimálně 400 disků, v případě	ANO, celková velikost cache/RAM v jednom řadiči je 128 GB

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

	é disky a moduly	nasazení více řadičů minimálně dvojnásobek disků. Jak je popsáno výše na řádku výkonnost, nelze toto řešit pomocí externí virtualizace nebo podvěšením dalšího pole a řadičů • podpora 2,5" nebo 3,5" disků technologie SSD/flash včetně rotačních disků a to současně: - podpora SCM (Storage Class Memory) ○ enterprise úrovně tzn. minimálně eMLC, 3D TLC, SLC nebo eSLC nebo enterprise flash modulů s hodnotou DWPD 1 a vyšší ○ všechny požadované typy SSD musí být NVMe architektury ○ rotační disky minimálně na SAS 3.0 architektuře ○ řešení musí umožňovat nasazení redukce dat tak v reálném čase tak, aby nedošlo k žádnému ovlivnění výkonu jednotlivých řadičů, tzn. je požadována separátní HW technologie, která je nezávislá na výpočetním výkonu jednotlivých řadičů a zajišťuje maximálně efektivní redukci dat nezávisle na typu ukládaných dat • podpora minimálně následujících režimů RAID - 1, 5, 6, 10 nebo minimálně DRAID 1 a 6	ANO, celková rozšiřitelnost je minimálně 440 disků, v případě nasazení více řadičů, více než 30x tolik disků. ANO, podporuje 2,5" nebo 3,5" disků technologie SSD/flash včetně rotačních disků a to současně ANO, podporuje SCM (Storage Class Memory) ANO, podporuje SSD enterprise úrovně 3D TLC, SLC a enterprise flash modulů s hodnotou DWPD minimálně 1 a vyšší ANO, všechny požadované typy SSD jsou NVMe standardu a je možné je současně osadit (mixovat) v rámci jedné diskové police ANO, řešení umožňuje nasazení redukce dat v reálném čase tak, že nedochází k žádnému ovlivnění výkonu jednotlivých řadičů, tzn. je obsažena separátní HW technologie, která je nezávislá na výpočetním výkonu jednotlivých řadičů a zajišťuje maximálně efektivní redukci dat nezávisle na typu ukládaných dat ANO, podporuje DRAID 1, 5 a 6
4.	Minimální požadovaná hrubá kapacita a ochrana dat	Tier 0: minimálně 14 TB na SSD / Flash ve variantě enterprise (DWPD 2 a vyšší, maximální velikost jednoho SSD nebo flash modulu je 2TB)	Tier 0: 15,32 TB na SSD variantě enterprise, velikost jednoho SSD nebo flash modulu je 1,92 TB)
5.	Konektivita k hostitelský m serverům (front-end)	diskové pole obsahuje připojení diskového pole blokovým přístupem pomocí 32Gbit FC. Jsou požadovány min. 4 porty 32Gb FC na řadič, tzn. minimálně 8x 32Gbit FC portů včetně osazených SW SFP převodníky s možností rozšíření 32Gbit FC portů na dvojnásobek a dále možnost osazení minimálně 12 Gbit ethernet portů do nabízených řadičů	ANO, diskové pole obsahuje připojení diskového pole blokovým přístupem pomocí 32Gbit FC. Jsou osazeny 4 porty 32Gb FC na řadič, tzn. 8x 32Gbit FC portů včetně osazených SW SFP převodníky s možností rozšíření 32Gbit FC portů na dvojnásobek a dále možnost osazení minimálně 12 Gbit

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

			ethernet portů do nabízených řadičů
6.	Funkcionality pro efektivní ukládání a správu dat	• vytváření virtuálních logických disků • thin provisioning (včetně detekce a reklamace prázdného prostoru) • komprese dat v reálném čase bez nutnosti dedikování dodatečného diskového prostoru pro post-processing pro celou nabízenou kapacitu včetně patřičného HW akcelerátoru nebo na jednotlivých modulech • deduplikace dat v reálném čase bez nutnosti dedikování dodatečného diskového prostoru pro post-processing pro celou požadovanou kapacitu včetně SW licence • šifrování dat minimálně pro flash kapacitu ve standardu minimálně FIPS 140-2 nebo 3 bez nutnosti přítomnosti speciálních pevných disků včetně příslušné licence. Pokud nabízené řešení neumožňuje šifrování dat nad úrovní disků, jsou požadovány SED disky pro celou nabízenou flash kapacitu, opět minimálně ve standardu FIPS 140-2 nebo 3 • inteligentní správa výkonnostních charakteristik (pro minimálně 3 tiery a to včetně SCM) virtualizovaných diskových prostorů (automatická migrace více utilizovaných dat na rychlejší disky nebo SSD/SCM) • podpora externí storage virtualizace pro stávající disková pole a možnost dalšího připojení externích diskových polí od různých výrobců min. pro účely migrace. Seznam podporovaných diskových systému je veřejně dostupný. • Podpora nástrojů pro sledování historických dat o vytížení datového úložiště (minimálně počet IOps, latence, propustnost, alokovaná kapacita, využití keši) s granularitou	ANO, nabízené doskové pole plně podporuje: - vytváření virtuálních logických disků - Thin provisioning (včetně detekce a reklamace prázdného prostoru) ANO, komprese dat je možná v reálném čase a je bez nutnosti dedikování dodatečného diskového prostoru pro post-processing na jednotlivých FCM modulech ANO, deduplikace dat je v reálném čase bez nutnosti dedikování dodatečného diskového prostoru pro post-processing pro celou požadovanou kapacitu včetně SW licence ANO, šifrování dat pro flash kapacitu je ve standardu FIPS 140-3 Level 1 ANO, v ceně řešení je inteligentní správa výkonnostních charakteristik (pro 3 tiery včetně SCM) virtualizovaných diskových prostorů (automatická migrace více utilizovaných dat na rychlejší disky nebo SSD/SCM) ANO, podporuje externí storage virtualizace pro stávající disková pole a možnost dalšího připojení externích diskových polí od různých výrobců min. pro účely migrace. Seznam podporovaných diskových systému je veřejně dostupný. ANO, obsahuje nástroj pro sledování historických dat o vytížení datového úložiště

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

		na hosta či LUN s historií minimálně 1 rok (možnost řešit externích SW nástrojem v rámci dodávky) • Microsoft VSS podpora • VMware VAAI, VVOL podpora, dále je požadován VASA provider přímo ve FW nabízeného diskového pole	(minimálně počet IOps, latence, propustnost, alokovaná kapacita, využití keší) s granularitou na hosta či LUN s historií minimálně 1 rok pomocí obsažené licence pro Spectrum Control Select Edition / Storage Insights PRO ANO, podporuje Microsoft VSS a VMware VAAI, VASA a VVOL, VASA provider je přímo ve FW nabízeného diskového pole
7.	Podpora operačních systémů a hypervizorů	• IBM AIX 7.1, 7.2 a vyšší • IBM VIOS 2.2 a vyšší • Oracle Enterprise Linux 8.x a vyšší • Oracle DB 11.x a 12.x a vyšší • RHEL 6.x a vyšší • VMware 7 a vyšší včetně VAAI a VASA integrací • Windows server 2016 a vyšší	ANO, podporuje, viz. ZDE
8.	Typ přístupu k datům	• blokový, standard FCP a iSCSI	ANO, podporuje
9.	Bezpečnost	ochrana proti ransomware útokům nativní funkcionalitou nabízeného pole v rámci jeho funkcionalit – řešení z aplikační vrstvy pomocí aplikací třetích stran nebo za asistence zálohovacího SW není přípustné. Řešení musí být pro tento účel jasně popsané a určené, např. ochrana LUNu pouze nastavením do read-only modu není dostatečná pro splnění tohoto požadavku	ANO, ochrana proti ransomware útokům je nativní funkcionalitou nabízeného pole v rámci jeho funkcionalit a je obsažena v nabízeném řešení – Inline Data Corruption Detection a IBM Safeguarded Copy
10.	Bezpečnost	řešení musí umožňovat detekci ransomware v reálném čase na blokové úrovni před uložením na disky / flash moduly	ANO, pomocí integrované funkcionality Inline Data Corruption Detection
11.	Bezpečnost	řešení musí umožňovat kontrolu zapsaných dat (bloků) přímo na jednotlivých SSD / flash modulech	ANO, řešení umožňuje kontrolu zapsaných dat (bloků) přímo na jednotlivých SSD / flash modulech
12.	Kopírovací funkce - licence musí být součástí nabídky a musí být na neomezeno	• zrcadlení virtuálního disku tzn. ochrana virtualizovaných dat v režimu RAID1 (s možností zdvojení dat virtuálního disku i na dvě pole) • možnost vytváření snapshotů (CoW a RoW) a klonů v následujících režimech:	ANO, plně podporuje, licence resp. funkce jsou součástí nabízeného řešení

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

	u kapacitu, počet disků, expanzích jednotek atd.	○ snapshot se po určité době může automaticky stát klonem ○ inkrementální snapshoty, tzn. kopírují se jen rozdílová data mezi dvěma okamžiky iniciace klonu ○ reverzní snapshoty, tzn. lze provést zpětné přesunutí dat z klonu do původního originálního Volume ○ lze udržovat až 4 inkrementálně pořizované klony z jednoho originálu (s možností reverzních snapshotů) • interní/externí zrcadlení logického (virtuálního) disku z jednoho zdroje do dvou cílů pro zvýšení dostupnosti v případě výpadku jednoho cíle	
13.	Zajištění kontinuální dostupnosti dat (DR a HA řešení) - licence musí být součástí nabídky a musí být na neomezeno u kapacitu, počet disků, expanzích jednotek atd.	• upgrade software a hardware u řadičů je proveditelné za chodu a bez ztráty přístupu hostitelských serverů k datum • diskové musí být možné spojit do clusteru, který umožňuje vytvoření jednoho funkčního celku, zrcadlení dat mezi jednotlivými poli apod. • vytvoření HA řešení s automatickým failover bez dalších vícenákladů, které je navíc nezávislé na běžných OS nebo virtualizační platformě včetně příslušných licencí • podpora replikace do třetí lokality • SW pro redundantní datové cesty v ceně řešení • Nabízené řešení musí být plně kompatibilní s VMware Metro Storage Cluster funkcionalitou, tzn. musí být dohledatelné v matici kompatibility na stránkách VMware	ANO, upgrade software a hardware u řadičů je proveditelné za chodu a bez ztráty přístupu hostitelských serverů k datům. ANO, jednotlivá disková pole je možné spojit do clusteru, který umožňuje vytvoření jednoho funkčního celku, zrcadlení dat mezi jednotlivými poli apod. ANO, vytvoření HA řešení s automatickým failover bez dalších vícenákladů, které je navíc nezávislé na OS nebo virtualizační platformě včetně příslušných licencí pro Policy Based HA ANO, podporuje replikace do třetí lokality. ANO, obsahuje SW pro redundantní datové cesty v ceně řešení. ANO, nabízené řešení je plně kompatibilní s VMware Metro Storage Cluster funkcionalitou, tzn. dohledatelná v matici kompatibility na stránkách VMware.
14.	Migrace dat	transparentní migrace (tzn. možnost zdarma migrovat data ze stávajících diskových polí na nová disková úložiště) s možnosti rozšíření o	ANO, obsahuje transparentní migrace (tzn. možnost zdarma migrovat data ze stávajících diskových polí na

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

		synchronní a asynchronní zrcadlení logických (virtuálních) disků v případě více lokalit	nová disková úložiště) s možností rozšíření o synchronní a asynchronní zrcadlení logických (virtuálních) disků v případě více lokalit.
15.	Počet hostitelských serverů připojovaných k diskovému poli	řešení obsahuje licence na neomezený počet připojení hostitelských serverů	ANO, obsahuje
16.	Správa diskového pole a další dostupné funkcionality	• SW pro plnohodnotnou správu diskového pole a diskových subsystémů, možnost ovládání přes CLI, GUI (ze std. web browseru) • Remote Service (call home) v ceně řešení • Příkazy prováděné v GUI jsou uchovávány v tzv. "AuditLogu" v podobě standardních CLI příkazů, které lze později snadno zkopírovat a aplikovat při programování uživatelských skriptů např. pro podporu automatizace zálohování atd. • Je požadováno potvrzení od lokálního zastoupení výrobce, že nabízené řešení je určeno pro český (EU) trh a bude servisním střediskem výrobce plně podporováno. Servisní podpora výrobce bude v českém jazyce	ANO, je obsažen SW pro plnohodnotnou správu diskového pole a diskových subsystémů, možnost ovládání přes CLI, GUI (ze std. web browseru) ANO, Remote Service (call home) je v ceně nabízeného řešení ANO, příkazy prováděné v GUI jsou uchovávány v tzv. "AuditLogu" v podobě standardních CLI příkazů, které lze později snadno zkopírovat a aplikovat při programování uživatelských skriptů např. pro podporu automatizace zálohování atd. ANO, je přiloženo potvrzení od lokálního zastoupení výrobce, nabízené řešení je určeno pro český (EU) trh a bude servisním střediskem výrobce plně podporováno. Servisní podpora výrobce bude v českém jazyce
17.	Příslušenství	Součástí dodávky je veškerá potřebná kabeláž pro plné zapojení všech portů do instalovaného prostředí a potřebná napájecí kabeláž kompatibilní s napájecími lištami v RACK skříních.	ANO, součástí dodávky je veškerá potřebná kabeláž pro plné zapojení všech portů do instalovaného prostředí a potřebná napájecí kabeláž kompatibilní s napájecími lištami v RACK skříních.
18.	Servisní podpora	Minimálně 5 let; v režimu 24x7 s odstraněním závady do 24h od nahlášení.	ANO, obsahuje podporu na 5 let v režimu 24x7 s garantovanou dobou opravy do 24h od nahlášení.

Pásková knihovna

Jsou požadovány dvě modulární páskové knihovny, níže jsou uvedené minimální parametry, které musí splňovat.

Položka	Parametr	Minimální požadavky	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
1	Mechaniky	Modulární pásková knihovna osazená min. 3× LTO9, zalicencovaná a připravená na min. 40 slotů	ANO, nabízena je odulární pásková knihovna osazená 3× LTO9, zalicencovaná a připravená na 40 slotů
2	Podpora mechanik	Možnost připojení HH i FH LTO9 (a vyšších) mechanik	ANO, je možnost připojení HH i FH LTO9 (a vyšších) mechanik, LTO10 bude nejpozději ve 2026
3	Škálovatelnost	Rozšíření až na min. 600 slotů a 45 mechanik	ANO, je možné rozšíření až na 640 slotů a 48 mechanik
4	Velikost	Max. 3U při konfiguraci s min. 40 sloty	ANO, 3U se 40 sloty na média
5	Konektivita	Min. 8 Gbit FC připojení k SAN/backup serveru + optická kabeláž	ANO, 8 Gbit FC připojení k SAN/backup serveru + optická kabeláž obsažena
6	I/O sloty	Min. 5 I/O slotů při konfiguraci s min. 40 sloty	ANO, 5 I/O slotů při konfiguraci se 40 sloty
7	Čtečka	Integrovaná čtečka čárových kódů	ANO, obsažena
8	Redundance cest	Podpora redundantních cest	ANO, Path failover obsažen v nabídce
9	Logické dělení	Podpora rozdělení knihovny na více celků (při více mechanikách)	ANO, podporuje rozdělení knihovny na více celků, 3 mechaniky = až 3 logické rozdělení
10	Napájení	Redundantní napájecí zdroje	ANO, obsahuje
11	Rack montáž	Potřebné komponenty pro zabudování do racku	ANO, obsahuje
12	Čistící média	Min. 3 ks čisticích pásek	ANO, obsahuje
13	Šifrování	Možnost šifrování pásek prostřednictvím mechanik	ANO, licence obsažena
14	Reportování	Pokročilé reporty bez omezení, min. analýza trendů, využití mechanik, čitelnost médií, logování chyb	ANO, umožňuje
15	Monitoring	SW pro health monitoring dostupnosti a částí knihovny	ANO, umožňuje
16	Obnova	Automatické obnovení po chybových stavech	ANO, podporuje
17	Servis	Servisní podpora min. 5 let, online 24×7, odezva tentýž den	ANO, obsahuje servisní podporu na 5 let, online 24×7, s odezvou tentýž den (SD)

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

Server pro zálohování

Je požadován jeden server pro zálohování, níže jsou uvedené minimální parametry, které musí splňovat.

Minimální technické parametry – 1 ks serveru včetně licencí a implementace

Parametr	Minimální požadavky	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
1.	Server – velikost a vnitřní uspořádání: Rack provedení, 1U, min. 8 diskových slotů s možností rozšíření na 10 diskových pozic. Pro přístup ke všem komponentám serveru není nutné nářadí, barevně značené hot-plug vnitřní komponenty. Pojízdné ližiny pro osazení do rozvaděče a rameno na kabeláž.	ANO
2.	Server – procesor: 1-socketový systém osazený jedním procesorem s parametry min. 2.6 GHz, min. 8 core, min. 22.5MB L3 cache a podporou sběrnice DDR5 4400 MT/s s maximálním příkonem 125W https://www.spec.org/cpu2017/results/cpu2017.html Floating Rates Base: min. 135 bodů Integer Rates Base: min. 87,2	ANO - INT Xeon-S 4509Y CPU
3.	Server – rychlost RAM – min. 5600 MHz DDR5	ANO
4.	Server – velikost RAM – min. 64 GB, osazeno 2x32 GB moduly, celkově rozšiřitelná až na 2TB typu DDR5	ANO
5.	2x M.2 SSD disk 480 GB v RAID 1 pro instalaci VMware ESXi	ANO
6.	Server – síťový interface: Min. 2x 25Gbit SFP28 LAN na kartě nezabírající místo v PCIE slotu včetně 2ks SFP28 Transcieverů	2x25Gb
7.	Server – management konzole: Vyžadována je schopnost monitorovat a spravovat server out-of-band bez nutnosti instalace agenta do operačního systému. Možnost vzdáleného managementu skrze cloud konzoli, bez nutnosti lokálního přístupu. Pokud je k tomuto přístupu třeba licence, musí být součástí konfigurace serveru. Management serveru nezávislý na operačním systému Možnost stažení aktualizací lokálně z internetu (FTP, nebo HTTP) IPMI 2.0 Vestavěná diagnostika komponent Web GUI management vestavěný v managementu Možnost přesměrování sériové linky managementu po LAN Zabezpečená komunikace SSH/HTTPS Podpora SNMP, HTML5 Vícefaktorové ověřování přístupu k managementu serveru	ANO

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

	Záznam a přehrání záznamu situace posledního crash-screen operačního systému Integrace s Directory Services (AD, LDAP) Management nástroje musí umět poskytovat ovladače instalovaným operačním systémům bez speciální dedikované partition na interních discích serveru a nezávisle na těchto discích (úložiště nezávislé na OS) Nezávislý management musí disponovat dedikovaným ethernet portem, který není součástí požadovaných ethernet portů s možností failover konfigurace na jeden z portů na základní desce (LOM) Firmware všech součástí serveru musí být kryptograficky podepsán tak, aby v rámci distribučního řetězce nemohlo dojít k jeho narušení nebo jeho alternaci. Při zapnutí serveru musí proběhnout kontrola kryptografických podpisů a skutečného obsahu firmwarů jednotlivých komponent. V případě, že jsou některé z nich narušeny, musí server umožnit automatický návrat k posledním validním firmware, či zastavit boot a umožnit administrátorovi přes vzdálené rozhraní nápravu nahráním autentické verze firmware. Možnost integrace do prostředí VMware vCenter Lifecycle Manager (vLCM) pro zjednodušení správy životního cyklu serverů přímo z konzole VMware vCenter	
8.	Server – zdroje/napájení: redundantní síťové napájecí zdroje min. 1000W Titanium s možností nastavení limitů výkonu a spotřeby v BIOSu (Power Budgeting)	ANO
9.	Server – podpora výrobce: Záruka vč. technické podpory na 5 let v režimu NBD, započetí opravy nejpozději následující pracovní den od nahlášení závady, oprava v místě instalace serveru, servis je poskytován výrobcem serveru, jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému, v případě poruchy a výměny SSD disků požadujeme ponechání vadných disků, možnost stažení ovladačů a management software na webových stránkách, doprava serveru do místa v ČR specifikovaného zadavatelem v ceně serveru	ANO
10.	Server – Interface: 4x USB + 1 volitelný, 1x VGA, 1x Display port volitelný, 1x RJ45 dedikovaný pro vzdálenou správu	ANO
11.	Podpora všech běžných OS: Microsoft, VMware, Red Hat, SUSE, Canonical Ubuntu, Oracle Linux and Oracle VM, XenServer a další	ANO
12.	Server – licence, které budou kompatibilní nebo budou technicky i kvalitativně srovnatelné s níže uvedeným výčtem potřebných licencí pro správný chod serveru: 1 x MS Windows Server 2025 Standard	ANO

13.	Server – dodání a nastavení: Zboží musí být nové, nepoškozené a určené přímo pro „zákazníka“ s garancí výrobce serveru. Příprava nového serveru Instalace a konfigurace virtualizační platformy Instalace a konfigurace Serverů, které budou kompatibilní se současným využívaným systémem ve společnosti. (Windows) migrace firemního prostředí na nové servery asistence s nasazením aplikací 3. stran vytvoření a nastavení zálohovacího scénáře nové serverové infrastruktury propojení na vzdálený replikační server v jiné lokalitě s úložištěm a kopií všech dat pro obnovu v případě havárie primární lokality provedení testovací obnovy infrastruktury doložené protokolem	ANO

Zálohovací software

Je požadovaný zálohovací software, níže jsou uvedené minimální parametry, které musí splňovat.

Položka	Parametr	Minimální požadavky	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
1	Prostředí	Kompletní pokrytí hybridního prostředí (fyzické servery, virtuály, cloud)	Pokrytí hybridního prostředí (fyzické servery, virtuály, cloud)
2	Úložiště	Podpora zálohování na disk, pásku i cloudové úložiště	Podpora zálohování na disk, pásku i cloudové úložiště
3	Optimalizace	Možnost deduplikace a komprese	Možnost deduplikace a komprese
4	Obnova	Granulární obnova (soubor, databáze, e-mail, celá VM)	Granulární obnova (soubor, databáze, e-mail, celá VM)
5	Správa	Centralizovaná správa a reporting	Centralizovaná správa a reporting
6	Bezpečnost	Šifrování dat i při přenosu	Šifrování dat i při přenosu
7	DR scénáře	Podpora disaster recovery scénářů	Podpora disaster recovery scénářů
8	Licence	Licence na 60 měsíců (5 let)	Licence na 60 měsíců (5 let)
9	Počet lokalit	1 lokalita	1 lokalita
10	Počet virtuálních serverů	100 virtuálních serverů	100 virtuálních serverů
11	Počet fyzických serverů	30 fyzických serverů	30 fyzických serverů
12	Počet uživatelů	250 uživatelů cloudové služby	250 uživatelů cloudové služby

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

Ostatní podmínky:

- Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství)
- Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů.
- Je požadována záruka na hardware, tato záruka musí být garantovaná výrobcem zařízení.
- Uchazeč je povinen s dodávkou doložit oficiální potvrzení lokálního zastoupení výrobce o všech dodávaných zařízeních (seznam sériových čísel dodávaných zařízení) pro český trh.

2.a. Akceptační kritéria

Akceptace proběhne v souladu s příslušným ustanovením smlouvy a dodavatel mj. dodá a uvede do provozu novou zálohovací infrastrukturu která umožní vysoce dostupný provoz a rychlou obnovu (disková i pásková vrstva). Řešení musí podporovat šifrování záloh, automatizované plánování zálohovacích úloh, průběžnou kontrolu konzistence a pravidelné testování scénářů disaster recovery včetně evidence výsledků testů.

Akceptace je dokončena podpisem předávacího protokolu potvrzujícího, že nástroj pro správu logů splňuje požadavky uvedené níže.

Specifikace pro naplnění parametrů

Akceptační kritérium	Způsob ověření	Výsledek	Poznámka / Podpis
Šifrování záloh	Ověření aktivního šifrování záloh a správné konfigurace		
Automatizované plánování zálohovacích úloh	Demonstrace funkčního plánovače zálohovacích úloh		
Průběžná kontrola konzistence záloh	Ověření pravidelné kontroly konzistence a evidence výsledků		
Testování disaster recovery scénářů	Praktické provedení DR testů dle schválených scénářů, doložení evidence		
Nastavení politik záloh (RPO/RTO)	Kontrola konfigurace a nastavení RPO/RTO pro klíčové služby		
Předání provozní dokumentace	Dodání a kontrola úplnosti provozní dokumentace		
Obnova vybraných systémů	Úspěšná obnova vybraných systémů dle schválených scénářů		
Reporty z běhu zálohovacích úloh	Doložení a ověření reportů o průběhu zálohování		
Integrita záloh	Ověření čitelnosti a nemožnosti neoprávněných změn záloh		

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

3. Specifikace služeb technické podpory dodavatele na 60 měsíců od 1. 6. 2026 do 31.5.2031.

Specifikace služeb technické podpory je uvedena v samostatném dokumentu:

- 01 – Technická specifikace – Společná definice technické podpory pro ID01 – ID09

Zadavatel tímto výslovně stanoví, že nepožaduje žádnou záruku nad rámec a mimo rozsah technické podpory vymezený v tomto dokumentu a dokumentu „01 – Technická specifikace – Společná definice technické podpory pro ID01 – ID09“ (dále jen „Společná definice“). Veškeré záruční povinnosti dodavatele, včetně úrovní služeb, reakčních dob, způsobu eskalace, podmínek dostupnosti, režimu aktualizací, EoL/EoS a výluk plnění, se řídí výlučně tímto dokumentem a Společnou definicí. Jakákoli plnění spočívající v rozvojových zásazích, změnových požadavcích, úpravách nad rámec specifikace či integracích nevyplývajících ze Společné definice nejsou součástí záruky, ledaže budou výslovně sjednána zvláštní smlouvou nebo dodatkem.

V případě rozporu nebo kolizního výkladu mezi touto technickou specifikací a Společnou definicí má přednost tato technická specifikace. Společná definice slouží jako doplňující a výkladový dokument a uplatní se pouze v rozsahu, v němž není v rozporu s touto Technickou specifikací.

3.a Akceptační kritéria

Dodavatel se zavazuje poskytovat technickou podporu v rozsahu a za podmínek stanovených tímto dokumentem a Společnou definicí po dobu od 1. 6. 2026 do 31. 5. 2031 (60 měsíců). Dodavatel podpisem smlouvy stvrzuje, že po uvedené období bude plnit sjednané SLA a ostatní povinnosti dle tohoto dokumentu a Společné definice; nesplnění těchto povinností bude posuzováno jako porušení smlouvy se všemi z toho vyplývajícími právními následky podle smlouvy a příslušných právních předpisů.

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

8.1.6. ID06 - Zavedení systému řízení kybernetické bezpečnosti a výkon role manažera KB

1. Úvod a metodika

Tento dokument definuje předmět a závaznou technickou specifikaci na zavedení systému řízení kybernetické bezpečnosti včetně vytvoření a aktualizace dokumentace, nastavení procesů a rolí tak, aby zadavatel dosáhl souladu s požadavky směrnice (EU) 2022/2555 (NIS2) a zákona č. 264/2025 Sb., ve znění pozdějších předpisů. Systém bude provozován v online nástroji, který usnadní správu aktiv, rizik a opatření a umožní dynamicky definovat a aktualizovat normativní požadavky prostřednictvím katalogů hrozeb, zranitelností a opatření.

Součástí plnění je zajištění výkonu role osoby odpovědné za kybernetickou bezpečnost (manažer KB) po dobu implementace a stabilizace, včetně metodického vedení, nastavení metrik a vedení registru rizik. Akceptace proběhne předáním schválené dokumentace, prokázáním funkčnosti nástroje (evidence aktiv, rizik, opatření, workflow) a předložením plánu dalšího rozvoje souladu a auditní připravenosti.

2. Specifikace dodávaného hardware, software a služeb instalace, implementace a školení

Řízení aktiv

- **Evidence aktiva** (sada povinných a nepovinných atributů).
- **Hodnocení aktiva** dle komponent zvoleného algoritmu, typicky C(důvěrnost), I(integrita), A(dostupnost).
- **Dědění hodnoty** z nadřízených aktiv. Z jednoho nebo více nadřízených aktiv se dědí vždy nejvyšší hodnota komponenty C, I, A.
- **Definice vazeb** mezi aktivy včetně určení síly vazby. Aktivum může mít 1..N vazeb na aktiva, která ho využívají a 0..N vazeb na aktiva, která aktivum využívá.
- **Hodnocení kontinuity**. Definice RTO (požadavek garanta a možnosti IT), RPO (požadavek garanta a požadavek IT). Dále je možné definovat Minimální Úroveň poskytovaných služeb.
- Jednoduché nebo **hromadné zakládání rizik** k aktivu. Lze hromadně založit všechna, nebo jen vybraná rizika z katalogu rizikových situací ze stromu hrozeb a zranitelností. Tato rizika lze při výběru rovnou ohodnotit.
- Možnost integrace na **Asset management** nebo jiné systémy pro evidenci.
- **Kopírování** aktiv.
- Ukládání aktiva jako **šablony**.
- Možnost tvorby aktiv z připravených šablon.

Štítky a vlastní atributy

- Spravované objekty lze označoval uživatelsky definovanými **štítky**.
- Atributy spravovaných objektů lze rozšířit o **Vlastní atributy**. Je možné definovat název a typ vlastního atributu. Tyto atributy lze přiřadit také šabloně aktiva.

Mapa aktiv

- Vizuální mapa všech aktiv a jejich vazeb včetně možnosti vytvářet a upravovat vazby a zakládat či mazat aktiva.
- Filtrování na vybraná aktiva se zobrazením vlastního stromu vazeb.

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

- Možnost zobrazení směru vazeb (směr závislosti).
- Zvýraznění nejbližších vazeb v případě označení dotčeného aktiva.
- Zakládání, editace nebo mazání aktiv rovnou z mapy aktiv včetně vazeb.
- Vizuální indikace, zdali je nebo není aktivum hodnoceno, zdali má rizika a opatření a jaká je hodnota těchto atributů
- Odlišení primárních a podpůrných aktiv.
- Po výběru aktiva je zobrazena mapa aktiv a navázaných opatření.
- Možnost založit riziko k aktivu.
- Možnost přidat opatření k zobrazenému riziku v mapě rizik a opatření.

Vzorové katalogy

Katalog hrozeb

- Správa katalogu hrozeb.
- Katalog je nastaven od výrobce s možností jeho úprav.
- Definice výchozích pravděpodobností hrozeb.
- Možnost definovat vlastní hrozby specifické pro obor nebo organizaci.

Katalog zranitelností

- Správa katalogu hrozeb.
- Katalog je nastaven od výrobce s možností jeho úprav.
- Definice výchozích pravděpodobností hrozeb.
- Možnost definovat vlastní zranitelnosti specifické pro obor nebo organizaci.

Katalog rizikových scénářů

- Definice smysluplných kombinací hrozeb a zranitelností pro daný typ aktiva. Tyto kombinace jsou pak nabízeny při manuálním nebo hromadném zakládání rizik.
- Katalog je nastaven od výrobce s možností jeho úprav.
- S možností hromadného výběru ze stromu hrozeb a zranitelností. Tím je vytvořena sada potenciálních rizik pro přiřazení konkrétním aktivům.
- Díky tomuto katalogu lze následně vytvářet rizika pro dané aktivum zcela automaticky pouze na základě typu aktiva.

Katalog vzorových opatření

- Definice **vzorových organizačních a technických opatření** dle jednotlivých norem.
- Možnost určit jaké zranitelnosti dané opatření snižuje.
- Katalog je nastaven od výrobce s možností jeho úprav.

Rizika

- Podpora jak **individuálního založení** jednoho rizika, tak i **hromadného založení** rizika prostřednictvím výběru ze stromu hrozeb a zranitelností pro konkrétní vybrané aktivum
- V rámci aktiva lze rizika zcela **automaticky vygenerovat** dle katalogu rizikových scénářů (viz řízení aktiv).
- Hodnocení rizika dle vybraného algoritmu s **automatickým výpočtem**.
- Zobrazení původního, aktuálního a cílového rizika dle stavu opatření.

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

- Přiřazení relevantních opatření a provedení výpočtu po jeho aplikaci.

Zvládání rizik

- Evidence a tvorba zvládání rizik se související sadou atributů.
- Zvládání rizika může být organizační opatření, technické opatření, akceptace rizika, eliminace aktiva, eliminace hrozby, pojištění aktiva, sdílení rizika, přenesení rizika.
- Evidence dílčích finančních a lidských nákladů pro aplikací zvládání jednotlivých rizik a zobrazení součtu dílčích nákladů.
- Přiřazení zvládání rizik (systém může automaticky filtrovat pouze relevantní rizika) na konkrétní vybraná rizika. V souvislosti s přiřazením je k dispozici sada atributů, včetně stavu zavedení opatření.
- Zvládání rizika může pokrývat více rizik. Jedno riziko může být pokryto více zvládáními.
- Definice účinnosti zvládání rizika a přepočet hodnoty rizika na základě přiřazeného zvládání.
- Hromadná akceptace rizik s možností volby hodnoty rizika, které má být akceptováno.

Evidence subjektů

- Evidence komerčních subjektů (dodavatel, odběratel, provozovatel) s příslušnou sadou atributů.
- Označení významnosti subjektu s evidencí datumu o oznámení o významnosti.
- Hodnocení subjektu.
- Možnost vytvořit a spravovat subjekt jako aktivum.
- Uložení související dokumentace.
- V rámci evidence subjektů lze tvořit štítky a vlastní atributy, viz kapitola 1.1.1.

Evidence organizační struktury

- Evidence organizačních jednotek ve stromové struktuře.
- Evidence osob s možností zařazení do organizačních jednotek.
- Evidované osoby slouží jako zdroj osob pro určení odpovědných pracovníků na aktiva, rizika, zvládání rizik a komerční subjekty.
- Možnost integrace se systémy pro správu identit.

Dokumentové výstupy

Systém generuje následující typy dokumentů:

- Prohlášení o aplikovatelnosti,
- Plán zvládání rizik,
- Zhodnocení rizik.

Systém umožňuje generovat další typy dokumentů dle zadání.

Funkce pro všechny evidenční objekty nebo funkce systému

- Definice oprávnění na evidované objekty pro uživatele nebo skupiny uživatelů.
- Definice oprávnění na aplikační funkce pro aplikační role nebo skupiny uživatelů.
- Historie objektů.
- Úkoly pro definici aktivit či workflow se sledováním stavů.

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

- Možnost definovat metodiky dle normy.
- Odběr notifikací s přehledem nestandardních stavů v evidenci. Jedná se typicky o aktiva bez rizik, rizika bez zvládání rizik, nehodnocená aktiva a rizika, blížící se a uplynulé termíny pro zavádění zvládání rizika, změnu hodnoty akceptovaného rizika nad definovanou úroveň apod.
- Zobrazení záznamů v přehledných tabulkách, s definicí sloupců potřebných atributů.
- Vícenásobné filtrování a řazení záznamů. Ukládání uživatelských filtrů.
- Exporty a reporting dat.
- Fulltextové vyhledávání na atributy a obsah dokumentů.
- Ukládání dokumentů.
- MFA autentizace.
- API pro funkce aplikace a integrace.
- Kontinuální přepočet hodnocení aktiv, rizik i zvládání rizika dle potřeby během provádění změn na těchto objektech.
- Systém disponuje aparátem uživatelských notifikací, které jsou dohledatelné v uživatelském rozhraní systému nebo doručitelné externím kanálem jako je například e-mail.
- Systém obsahuje aparát umožňující definovat, plánovat a automaticky spouštět pravidelné úlohy.

Funkce pro administraci systému

- Správa uživatelů.
- Tvorba šablon pro aktiva.
- Definice vlastních atributů.
- Definice číselníků
- Definice úrovní pro parametry hodnocení (pro aktiva včetně výsledné hodnoty, rizika včetně pro výsledné hodnoty, subjekty, síly vazeb).
- Definice algoritmů pro výpočet hodnoty aktiva a rizika.

Technologie, provoz, bezpečnost

Podpora operačních systémů

Systém je možno provozovat na jakémkoli systému i HW platformě, kde je podporován systém docker a existují docker image pro tuto platformu.

Docker

Všechny komponenty systému, tedy front-end, back-end komponenty i aplikace třetích stran, jsou dodávány a provozovány jako Docker container pro snadnou instalaci a orchestraci provozu. Veškeré komponenty budou provozovány v plně virtualizovaném prostředí a distribuovány formou Docker kontejnerů.

Multi-tenantní provoz

Systém bude navržen s důrazem na flexibilní podporu multitenantního provozu, tedy možnosti využití jednoho společného aplikačního prostředí pro více vzájemně nezávislých organizací či jejich jednotlivých částí. Každý tenant bude mít k dispozici vlastní izolovanou databázi pro zajištění bezpečnosti a integrity dat. Zároveň systém umožní nasazení databází jednotlivých

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

tenantů na samostatné databázové servery, které mohou být umístěny v různých lokalitách či segmentech IT infrastruktury.

Horizontální i vertikální škálovatelnost

Systém bude navržen tak, aby umožňoval jak horizontální, tak vertikální škálovatelnost pro možnost přizpůsobení výkonu momentálním potřebám.

LDAP Integrace

Systém bude obsahovat vlastní aparát pro správu uživatelů, ale zároveň bude podporovat plnou integraci s externími identity providery prostřednictvím protokolu LDAP. Systém umožní nastavení plné synchronizace uživatelů a uživatelských skupin z těchto externích zdrojů a zároveň umožní externí LDAP servery využívat jako centrální zdroj autentizace.

REST API - dokumentace API

Systém poskytne robustní REST API, jehož struktura bude kompletně zdokumentována ve formátu OpenAPI 3 (nebo obdobné). Veškerá komunikace mezi uživatelským rozhraním a servery, stejně jako mezi jednotlivými komponentami uvnitř serveru, bude zabezpečena například JWT (JSON Web Token) nebo obdobným.

OAuth2 autentizace

Systém bude využívat standardní OAuth2 autentizaci doplněnou o zabezpečení pomocí JWT (JSON Web Token) nebo obdobné. Zároveň bude umožňovat plnou integraci s externími poskytovateli identit a bude možné využít existující externí služby pro autentizaci uživatelů a správu jejich přístupových oprávnění.

Plánované úlohy

Systém bude obsahovat aparát umožňující definovat, plánovat a automaticky spouštět pravidelné úlohy. Každá úloha může být nakonfigurována ve více instancích, přičemž každá instance může mít samostatně nastavenou frekvenci či harmonogram spouštění. K dispozici bude rovněž monitoring těchto úloh, který poskytuje informace o jejich průběhu, historii spouštění, délce trvání a dosažených výsledcích, včetně případných chyb či upozornění.

Typické příklady naplánovaných úloh zahrnují například:

- **Rozesílání notifikací** (upozornění, oznámení, reporty uživatelům)
- **Importy a exporty dat** (automatizovaná integrace s externími systémy, výměna datových sad)
- **Synchronizaci uživatelských účtů** (např. s externími LDAP servery či jinými poskytovateli identity)
- **Pravidelné odmazávání starých či neaktuálních dat** (optimalizace databáze a správy úložiště)

Transakční protokol

Systém bude umožňovat evidence transakčních protokolů. Transakční protokol představuje speciální typ auditního záznamu, jehož hlavním účelem je podrobná evidence všech změn prováděných nad objekty, které systém spravuje. Tyto změny budou zaznamenávány přímo v podobě, v jaké proběhly v databázi, což umožní přesné dohledání historie jakékoli modifikace – kdy k ní došlo, který uživatel ji provedl, jaká konkrétní změna nastala a jak se změnil stav objektu.

Full-Text nad objekty a obsahem dokumentů.

Veškerý obsah spravovaný systémem bude patřičně indexován a připraven na full-textové vyhledávání. Vyhledávat lze byznysové objekty dle jejich metadatových popisů a přiložené textové dokumenty typu PDF, MS Word a další strojově čitelné textové formáty. Uživatel může

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

full-textově vyhledat jen takový obsah, na který má oprávnění udělené mu přímo nebo získané členstvím ve skupinách uživatelů a aplikačních rolích.

MFA

Systém bude podporovat více faktorovou autentizaci (MFA) formou jednorázových hesel (One-Time Password, OTP), generovaných pomocí standardních aplikací, jako jsou Microsoft Authenticator nebo Google Authenticator. Tento způsob autentizace zvyšuje bezpečnost uživatelských účtů tím, že kromě běžného hesla vyžaduje ještě druhý, dynamicky generovaný faktor, platný pouze po velmi krátkou dobu.

Šifrování

Systém zajistí komplexní zabezpečení dat jak při jejich přenosu, tak i při jejich ukládání. Veškerá komunikace bude zabezpečena protokolem HTTPS, který garantuje integritu a šifrování dat při přenosu mezi uživatelem a serverem.

Na úrovni datových úložišť systém bude podporovat šifrování disků, pro případ fyzického nebo neoprávněného přístupu k infrastruktuře. Další bezpečnostní vrstvou bude šifrování dokumentů, které jsou přílohami obchodních objektů spravovaných systémem. Tyto přílohy budou ukládány v zašifrované podobě a jejich dešifrování probíhá výhradně v okamžiku autorizovaného přístupu oprávněným uživatelem při jejich zobrazení či stažení.

Kontinuální sken zdrojových kódů

V rámci automatizovaných CD/CI procesů budou zdrojové kódy systému kontinuálně skenovány. Toto skenování bude zaměřené na identifikaci bezpečnostních zranitelností podle doporučení OWASP (Open Web Application Security Project).

2.a. Akceptační kritéria

Akceptace proběhne v souladu s příslušným ustanovením smlouvy a akceptace aplikace pro řízení aktiv proběhne předáním zprovozněného systému včetně dokumentace a uživatelských příruček. Dodavatel doloží protokoly o provedených funkčních a bezpečnostních testech a potvrzení o úspěšné integraci. Akceptace je dokončena podpisem předávacího protokolu, který stvrzuje, že systém splňuje požadavky dle smlouvy.

Výkon bezpečnostní role osoby odpovědné za kybernetickou bezpečnost (dodání služeb)

Služby v rozsahu popisu specifikace služeb osoby odpovědné za kybernetickou bezpečnost, která bude zajišťovat jak komunikaci s dozorovými a kontrolními orgány, tak i interní procesní a organizační opatření u klienta.

1. Specifikace služeb kybernetického manažera

Komunikace a reporting:

- Pasivně přijímá a sleduje sdělení NÚKIB a dalších orgánů.
- Aktivně komunikuje s orgány veřejné správy a NÚKIB, zejména při hlášení změn a kybernetických incidentů.
- Poskytuje varování v oblasti nových hrozeb, změn legislativy či metodických pokynů.

Incident management:

- Zajišťuje procesní část hodnocení a hlášení incidentů, včetně jejich dokumentace a archivace.
- Funguje jako kontaktní místo pro zaměstnance klienta a jako informační kanál vůči nim.

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

- Přijímá a vyhodnocuje podněty o nestandardním chování, včetně kontroly podezřelých e-mailů a příloh.

Dokumentace a compliance:

- Vede a řídí dokumentaci odpovídající povinnostem ze zákona o kybernetické bezpečnosti (ZoKB).
- Zajišťuje auditní stopu a verzování všech změn a úkonů.
- Odpovídá za soulad dokumentace se zákonem a metodikami NÚKIB.
- Každoročně provádí přezkum aktuálnosti dokumentace a zajišťuje potvrzení o seznámení klienta.
- Organizuje revize bezpečnostních opatření a vedení evidence aktiv.
- Připravuje vzorové smluvní doložky dle povinných ujednání a doporučení NÚKIB.

Školení a osvěta:

- Vede přehledy o absolvovaných školeních v oblasti kybernetické bezpečnosti.
- Zajišťuje vstupní i pravidelná školení formou e-learningu.
- Doporučuje odborná teoretická i praktická školení pro administrátory a další osoby odpovědné za kybernetickou bezpečnost.

Kontroly a vyhodnocování:

- Každoročně provádí a dokumentuje vyhodnocení účinnosti zavedených bezpečnostních opatření, včetně jejich aktualizace.
- Pravidelně přezkoumává nastavení přístupových oprávnění.
- Zajišťuje plánování a dokumentování auditů, penetračních testů a skenů zranitelností.

2. Akceptace služeb kybernetického manažera

2.b. Akceptační kritéria

Akceptace proběhne v souladu s příslušným ustanovením smlouvy a akceptace služeb probíhá předáním dokumentace a reportů prokazujících splnění sjednaných činností. Dodavatel předkládá aktuální dokumentaci v souladu se zákonem o kybernetické bezpečnosti a metodikami NÚKIB, včetně evidence aktiv, přehledů incidentů a komunikace s NÚKIB, záznamů o školeních zaměstnanců a výsledků provedených kontrol a testů (vyhodnocení opatření, přezkum přístupových oprávnění, audity, penetrační testy a skeny zranitelností).

Akceptace je dokončena podpisem předávacího protokolu potvrzujícího, že služby byly poskytnuty v plném rozsahu a v souladu se smlouvou.

Specifikace pro naplnění parametrů

Dodavatel vyplní následující tabulku specifikace nabízeného plnění. Ve sloupci „Splnění parametrů dodavatele – DOPLNÍ DODAVATEL“ dodavatel doplní:

- ANO/NE v závislosti na tom, zda nabízené plnění či jeho část požadavek zadavatele splňuje/nesplňuje,
- specifikaci konkrétního parametru či popis naplnění požadavku zadavatele,
- číselnou hodnotu v případě požadavku zadavatele, který obsahuje číselně vyjádřitelný parametr
- přesnou specifikaci HW, SW nebo služby

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

- volitelně odkaz na dodavatelem přiložený dokument ve formátu PDF

Specifikace systému ISMS (implementace SW)

#	Minimální požadavky	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
1	Systém řízení rizik musí správu případných podřízených nebo přímo řízených organizací.	ANO
2	Systém musí mít možnost importu a exportu informací ve formátu MS Excel nebo CSV.	ANO
3	Systém musí podporovat češtinu, a to jak v části popisné (obsah jednotlivých polí), tak v části funkční (menu, funkce, popisy)	ANO
4	Systém musí mít své vlastní řízení rolí a přístupů s tím, že integrační napojení na systémy AD/LDAP jsou povinností.	ANO
5	Musí být schopen pracovat s identitami i samostatně, bez tohoto napojení na systémy AD/LDAP	ANO
6	Systém musí být připraven na implementaci dle nového zákona o kybernetické bezpečnosti.	ANO
7	Systém umožní odběry pravidelných notifikaci pro následující oblasti: - nehodnocená aktiva - aktiva bez evidovaných rizik - nehodnocená rizika - rizika bez aplikovaných opatření - blížící se a uplynulé termíny	ANO
8	Systém umožní definovat a evidovat vlastní atributy k libovolnému základnímu prvku rizikového řízení	ANO
9	Systém umožní definovat oprávnění na evidenční oblasti pro uživatele nebo skupiny uživatelů.	ANO
10	Systém umožní definovat oprávnění na aplikační funkce pro aplikační role nebo skupiny uživatelů.	ANO
11	Systém zajistí u každé evidované oblasti (aktiva, rizika, opatření) vlastní auditní stopu.	ANO
12	Systém umožní u každé evidované oblasti úkoly pro definici aktivit se sledováním stavů	ANO
13	Systém zajistí zobrazení seznamu záznamů v přehledných tabulkách.	ANO
14	Systém zajistí fulltextové vyhledávání dle atributů uložených objektů a obsahu uložených dokumentů.	ANO
15	Systém umožní Více faktorovou autentizaci.	ANO
16	Systém bude poskytovat API pro funkce aplikace a integrace.	ANO
17	Systém zajistí kontinuální přepočet hodnocení aktiv, rizik a opatření dle potřeby během provádění změn.	ANO

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

	Řízení rizik	
18	Systém umožní evidenci rizik, který umožní evidenci rizika dle vybraných hrozeb a zranitelností jejichž kombinace je validována proti katalogu kombinací hrozeb a zranitelností pro daný typ aktiva.	ANO
19	Systém umožní hodnocení rizika dle zvoleného algoritmu pro výpočet hodnocení rizika.	ANO
20	Systém umožní mitigaci rizika formou vazby opatření na riziko s možností zvolit účinnost tohoto opatření na riziko.	ANO
21	Systém umožní aplikaci opatření na riziko formou evidence stavu zavedení.	ANO
22	Systém umožní párovat jedno opatření s více riziky.	ANO
23	Systém umožní párovat více opatření s jedním rizikem.	ANO
24	Systém umožní definovat pro každé navázané riziko vlastní účinnost (velikost mitigace).	ANO
25	Historie rizika. Možnost u každého rizika zobrazit vývoj jeho hodnoty v čase.	ANO
26	Systém umožní definici stupnice pro hodnocení rizik.	ANO
27	Systém zajistí zobrazení základních údajů o evidovaných záznamech rizik.	ANO
28	Systém umožní seskupování rizik dle zvolených štítků.	ANO
29	Systém zajistí provázání rizik na: - aktiva - osobu v rámci organizační struktury - úkoly - incidenty	ANO
	Řízení incidentů	
30	Systém umožní vedení registru incidentů.	ANO
31	Systém umožní evidovat průběh investigace incidentu formou komentářů k incidentu.	ANO
32	Systém umožní řídit řešení incidentu formou vzorových úkolů.	ANO
33	Systém umožní evidovat vazbu mezi incidentem a následnými opatřeními k incidentům.	ANO
34	Systém umožní evidovat vazbu incidentu na riziko.	ANO
35	Systém umožní rozesílat notifikaci na vznik incidentu.	ANO
	Řízení auditu	
36	Systém umožní evidovat audity a bezpečnostní výbory.	ANO
37	Systém umožní plánovat audity a bezpečnostní výbory.	ANO
38	Systém umožní přidělit odpovědné osoby za audit a bezpečnostní výbor.	ANO
39	Systém umožní připojit dokumentaci k bezpečnostnímu výboru a auditu.	ANO
	Vzorové katalogy	
40	Systém umožní vedení vzorového katalogu hrozeb a zranitelností s možností vkládání nových uživatelských hrozeb a zranitelností. Možnost definovat výchozí pravděpodobnost hrozby a velikost zranitelnosti.	ANO

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

41	Systém umožní vedení vzorového katalogu praktických kombinací hrozeb a zranitelností pro jednotlivé typy aktiv. Tyto kombinace budou použity při validaci kombinace hrozby a zranitelnosti při vytváření rizik.	ANO
42	Systém umožní tvorbu katalogu vzorových opatření z možností definice jeho účinnosti na vybrané zranitelnosti.	ANO
43	Systém umožní tvorbu katalog vzorových aktiv.	ANO
	Řízení aktiv (Asset)	
44	Systém umožní evidovat aktiva dle zákona o kybernetické bezpečnosti.	ANO
45	Systém umožní evidovat základní evidenční údaje o aktivech (majetkového charakteru).	ANO
46	Systém umožní vytvářet vazby aktiva na riziko.	ANO
47	Vazba aktiva na incident	ANO
48	Evidenční údaje aktiva z hlediska kybernetického zákona (dostupnost, důvěrnost, integrita)	ANO
49	Systém umožní tvorbu vazby aktiva na organizační strukturu (zodpovědného pracovníka (roli)).	ANO
50	Systém umožní vytvořit report o aktivech.	ANO
51	Systém umožní evidenci parametrů kontinuity minimálně na úrovni evidence PRO, RTO, MÚPS	ANO
	Dokumenty	
52	Systém umožní připojovat dokumentaci k libovolné evidované oblasti.	ANO
	Integrace	
53	Systém bude možné integrovat na systémy řízení přístupu (AD, LDAP)	ANO
	Compliance	
54	Systém bude umožňovat vytváření následujících výstupů: - Prohlášení o aplikovatelnosti - Zpráva o zhodnocení rizik - Plá zvládání rizik	ANO
	Vizualizace vazeb	
55	Systém vytvoří vizuální mapu všech aktiv a jejich vazeb včetně možnosti vytvářet a upravovat vazby a zakládat či mazat aktiva.	ANO
56	Systém umožní filtrování aktiv v rámci mapy aktiv.	ANO
57	Systém v rámci vizualizace zajistí indikaci, zdali je nebo není aktivum hodnoceno, zdali má rizika a opatření a jaká je hodnota těchto atributů.	ANO
58	V rámci mapy bude k dispozici barevné odlišení primárních a podpůrných aktiv.	ANO
59	V rámci mapy aktiv bude po výběru aktiva zobrazena mapa rizik a navázaných opatření.	ANO
60	V rámci mapy rizik bude možnost založit riziko k aktivu.	ANO
61	V rámci mapy rizik bude možnost přidat opatření k zobrazenému riziku.	ANO
62	V rámci mapy aktiv bude k dispozici zvýraznění nejbližších vazeb v případě označení dotčeného aktiva.	ANO

63	V rámci mapy aktiv bude možné vytvářet nebo rušit vazby mezi aktivy.	ANO
	Možnosti konfigurace	
64	Systém umožní nastavit vlastní úrovně pro hodnocení aktiv (C, I, A)	ANO
65	Systém umožní výběr algoritmu pro výpočet hodnoty aktiva minimálně v rozsahu: Součet CIA, Maximum z CIA	ANO
66	Systém umožní nastavit vlastní úrovně pro hodnoty hrozby a zranitelnosti.	ANO
67	Systém umožní výběr algoritmu pro výpočet hodnoty rizika minimálně v rozsahu: Součin (hrozba, zranitelnost), Součin (hrozba, zranitelnost, dopad)	ANO
68	Systém bude mít k dispozici správu uživatelů.	ANO
	Řízení dodavatelského řetězce	
69	Systém umožní vést evidenci dodavatelů.	ANO
70	Systém umožní hodnotit dodavatele.	ANO
71	Systém umožní označit významného dodavatele.	ANO
72	Systém umožní vytvořit dodavatele jako aktivum a odkazovat na aktivum spojené s dodavatelem.	ANO
73	Systém umožní uložení související dokumentace k dodavateli.	ANO

Výkon bezpečnostní role osoby odpovědné za kybernetickou bezpečnost (dodání služeb)

	Minimální požadavky	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
1	Výkon bezpečnostní role osoby odpovědné za kybernetickou bezpečnost	ANO
2	Pasivní komunikace s NÚKIB a případně dalšími orgány	ANO
3	Aktivní komunikace vůči orgánům veřejné správy	ANO
4	Aktivní komunikace vůči NÚKIB - hlášení změn, incidentů apod.	ANO
5	Alerting v oblasti hrozeb, změn legislativy a metodik	ANO
6	Zajišťuje procesní část hodnocení a hlášení incidentu včetně dokumentace a archivace	ANO
7	Individuální komunikace administrátora s klientem	ANO
8	Kontaktní místo pro zaměstnance klienta	ANO
9	Informační kanál vůči zaměstnancům klientů	ANO
10	Kontaktní bod pro informace o nestandardním chování	ANO
11	Kontrola podezřelých e-mailů a příloh	ANO
12	Obsahuje a řídí dokumentaci odpovídající povinnostem ze ZoKB	ANO
13	Veškeré změny a úkony mají prokazatelnou auditní stopu, dokumentace je verzovaná	ANO
14	Odpovědnost za soulad dokumentace se zákonem a metodikami NÚKIB	ANO
15	Zajišťuje každoroční přezkum aktuálnosti dokumentace	ANO

16	Zajišťuje záznam o seznámení klienta s dokumentací	ANO
17	Zajišťuje revize bezpečnostních opatření vedením klienta	ANO
18	Zajišťuje vedení a revize evidence aktiv	ANO
19	Zajišťuje vzorové smluvní doložky pro povinná smluvní ujednání a dle doporučení NÚKIB	ANO
20	Vede přehledy o školeních kybernetické bezpečnosti	ANO
21	Zajišťuje vstupní školení v oblasti kybernetické bezpečnost formou e-learningu,	ANO
22	Provádí pravidelná školení v oblasti kybernetické bezpečnosti formou e-learningu,	ANO
23	Doporučuje potřebná odborná teoretická i praktická školení administrátorů a osoby odpovědné za kybernetickou bezpečnost v souladu s jejich pracovní náplní,	ANO
24	Jednou ročně provede a dokumentuje vyhodnocení účinnosti zavedených bezpečnostních opatření, včetně aktualizace přehledu bezpečnostních opatření,	ANO
25	Provede pravidelné přezkoumání nastavení veškerých přístupových oprávnění,	ANO
26	Zajišťuje plánování a dokumentování auditů, penetračních testů a scanů zranitelnosti	ANO

3. Specifikace služeb technické podpory dodavatele na 60 měsíců od 1. 6. 2026 do 31.5.2031.

Specifikace služeb technické podpory je uvedena v samostatném dokumentu:

- 01 – Technická specifikace – Společná definice technické podpory pro ID01 – ID09

Zadavatel tímto výslovně stanoví, že nepožaduje žádnou záruku nad rámec a mimo rozsah technické podpory vymezený v tomto dokumentu a dokumentu „01 – Technická specifikace – Společná definice technické podpory pro ID01 – ID09“ (dále jen „Společná definice“). Veškeré záruční povinnosti dodavatele, včetně úrovní služeb, reakčních dob, způsobu eskalace, podmínek dostupnosti, režimu aktualizací, EoL/EoS a výluk plnění, se řídí výlučně tímto dokumentem a Společnou definicí. Jakákoli plnění spočívající v rozvojových zásazích, změnových požadavcích, úpravách nad rámec specifikace či integracích nevyplývajících ze Společné definice nejsou součástí záruky, ledaže budou výslovně sjednána zvláštní smlouvou nebo dodatkem.

V případě rozporu nebo kolizního výkladu mezi touto technickou specifikací a Společnou definicí má přednost tato technická specifikace. Společná definice slouží jako doplňující a výkladový dokument a uplatní se pouze v rozsahu, v němž není v rozporu s touto Technickou specifikací.

3.a. Akceptační kritéria

Dodavatel se zavazuje poskytovat technickou podporu v rozsahu a za podmínek stanovených tímto dokumentem a Společnou definicí po dobu od 1. 6. 2026 do 31. 5. 2031 (60 měsíců). Dodavatel podpisem smlouvy stvrzuje, že po uvedené období bude plnit sjednané SLA a ostatní povinnosti dle tohoto dokumentu a Společné definice; nesplnění těchto povinností bude posuzováno jako porušení smlouvy se všemi z toho vyplývajícími právními následky podle smlouvy a příslušných právních předpisů.

8.1.7. ID07 - Firewally pro detašovaná pracoviště

1. Úvod a metodika

Tento dokument definuje předmět a závaznou technickou specifikaci pro dodávku a nasazení dedikovaného NGFW s centrálním managementem pro vzdálené lokality (detašovaná pracoviště), včetně návrhu a implementace bezpečnostních pravidel, VPN spojení šifrovaným tunelem do centrály a jednotných pravidel pro přístup k aplikacím. Řešení musí integrovat IPS/IDS pro zachycení útoků v reálném čase, vycházet z principů NIST CSF a uplatňovat osvědčené postupy pro ochranu perimetru.

Bude dodáno minimálně 8 ks NGFW pro lokality: Plechárna, KD Kyje, Gen. Jan., G14, KC Kardašovská, H55, Polyfunkční budova a Správa majetku, včetně odpovídajících softwarových licencí a centralizovaného dohledového rozhraní. Akceptace proběhne ověřením provozu VPN, aplikace politik, centrální správy a dohledu a předáním konfigurační a provozní dokumentace.

2. Specifikace dodávaného hardware, software a služeb instalace, implementace a školení

Dodavatel vyplní následující tabulku specifikace nabízeného plnění. Ve sloupci „Splnění parametrů dodavatele – DOPLNÍ DODAVATEL“ dodavatel doplní:

- ANO/NE v závislosti na tom, zda nabízené plnění či jeho část požadavek zadavatele splňuje/nesplňuje,
- specifikaci konkrétního parametru či popis naplnění požadavku zadavatele,
- číselnou hodnotu v případě požadavku zadavatele, který obsahuje číselně vyjádřitelný parametr
- přesnou specifikaci HW, SW nebo služby
- volitelně odkaz na dodavatelem přiložený dokument ve formátu PDF

Firewall pro střední zátěž (7 ks)

Požadavek na funkcionalitu	Minimální požadavky	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
Počet kusů	7	7
Výkon firewallu	min. 4 Gbps	5 Gbps
Výkon NGFW (aplikace + IPS)	min. 1,2 Gbps	1,25 Gbps
Výkon IPSec VPN	min. 4,5 Gbps	4,5 Gbps
Rozhraní	min. 5× GE RJ45	5x GE RJ45
Základní funkce	Stateful FW, Application Control, Web filtering, IPS, Anti-Malware, Anti-Spam, SSL inspection	Stateful FW, Application Control, Web filtering, IPS, Anti-Malware, Anti-Spam, SSL inspection
Vysoká dostupnost	Podpora HA (Active/Passive)	Podpora HA (HA (Active/Active, Active/Passive)
Síťová segmentace	Podpora VLAN	Podpora VLAN
SD-WAN	Integrovaná funkcionalita SD-WAN	Integrovaná funkcionalita SD-WAN
IPv4 / IPv6	Plná podpora obou protokolů	Plná podpora IPv4/IPv6
Autentizace uživatelů	LDAP, RADIUS, MFA	LDAP, RADIUS, MFA

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

Licence	Unified Threat Protection (UTP) na 5 let	Unified Threat Protection (UTP) na 5 let
Podpora	24/7 na 5 let	24/7 na 5 let

Firewall pro vyšší zátěž (1 ks)

Požadavek na funkcionalitu	Minimální požadavky	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
Počet kusů	1	1
Výkon firewallu	min. 10 Gbps	10 Gbps
Výkon NGFW (aplikace + IPS)	min. 1,5 Gbps	2,5 Gbps
Výkon IPSec VPN	min. 7 Gbps	7,1 Gbps
Rozhraní	min. 10× GE RJ45	10x GE RJ45
Základní funkce	Stateful FW, Application Control, Web filtering, IPS, Anti-Malware, Anti-Spam, SSL inspection	Stateful FW, Application Control, Web filtering, IPS, Anti-Malware, Anti-Spam, SSL inspection
Vysoká dostupnost	Podpora HA (Active/Passive)	Podpora HA (Active/Active, Active/Passive)
Síťová segmentace	Podpora VLAN	Podpora VLAN
SD-WAN	Integrovaná funkcionalita SD-WAN	Integrovaná funkcionalita SD-WAN
IPv4 / IPv6	Plná podpora obou protokolů	Plná podpora IPv4/IPv6
Autentizace uživatelů	LDAP, RADIUS, MFA	LDAP, RADIUS, MFA
Licence	Unified Threat Protection (UTP) na 5 let	Unified Threat Protection (UTP), 5 let
Podpora	24/7 na 5 let	24/7, 5 let

Centralizovaný management (SW, 1 ks)

Požadavek na funkcionalitu	Minimální požadavky	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
Počet kusů	1	1 VM
Podpora správy zařízení	Min. 10 zařízení	10
Centrální správa politik	Správa politik, konfigurace a aktualizací FW	Správa politik, konfigurace a aktualizací FW
Správa VPN	Podpora správy VPN tunelů a certifikátů	Podpora správy VPN tunelů a certifikátů
Reportování	Generování reportů a log management	Generování reportů a log management
Přístupová práva	Role-based Access Control (RBAC)	Role-based Access Control (RBAC)
Vysoká dostupnost	Podpora HA management serveru	Podpora HA management serveru
Licence	Min. 5 let	5 let
Podpora	Aktualizace a podpora výrobce min. 5 let	Aktualizace a podpora výrobce 5 let

Ostatní podmínky:

- Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství)
- Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů.
- Je požadována záruka na hardware s výměnou NBD v délce 60 měsíců. Tato záruka musí být garantovaná výrobcem zařízení.
- Uchazeč je povinen s dodávkou doložit oficiální potvrzení lokálního zastoupení výrobce o všech dodávaných zařízeních (seznam sériových čísel dodávaných zařízení) pro český trh.

2.a. Akceptační kritéria

Akceptace proběhne v souladu s příslušným ustanovením smlouvy a dodavatel mj. dodá a uvede do provozu NGFW s centrálním managementem pro vzdálené lokality (detašovaná pracoviště), včetně návrhu a implementace bezpečnostních pravidel, VPN spojení šifrovaným tunelem do centrály a jednotných pravidel pro přístup k aplikacím. Řešení musí integrovat IPS/IDS pro zachycení útoků v reálném čase, vycházet z principů NIST CSF a uplatňovat osvědčené postupy pro ochranu perimetru.

Akceptace je dokončena podpisem předávacího protokolu potvrzujícího, že bylo dodáno 8ks firewallů a implementace splňuje požadavky uvedené níže.

Specifikace pro naplnění parametrů

Akceptační kritérium	Způsob ověření	Výsledek	Poznámka / Podpis
Zprovoznění VPN tunelů do centrály	Ověření funkčního VPN spojení šifrovaným tunelem		
Aplikace bezpečnostních politik	Test správného uplatnění definovaných politik v síti		
Centrální správa NGFW	Praktická demonstrace centrální správy všech nasazených NGFW		
Centrální dohled a monitoring	Ověření funkčnosti centrálního dohledového rozhraní		
Integrace IPS/IDS	Test zachycení a vyhodnocení útoku v reálném čase		
Soulad s NIST CSF a osvědčenými postupy	Kontrola nastavení a konfigurace dle principů NIST CSF		
Dodávka všech požadovaných NGFW	Fyzické předání min. 8 ks zařízení včetně licencí		
Předání dokumentace	Kontrola úplnosti konfigurační a provozní dokumentace		

3. Specifikace služeb technické podpory dodavatele na 60 měsíců od 1. 6. 2026 do 31.5.2031.

Specifikace služeb technické podpory je uvedena v samostatném dokumentu:

- 01 – Technická specifikace – Společná definice technické podpory pro ID01 – ID09

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

Zadavatel tímto výslovně stanoví, že nepožaduje žádnou záruku nad rámec a mimo rozsah technické podpory vymezený v tomto dokumentu a dokumentu „01 – Technická specifikace – Společná definice technické podpory pro ID01 – ID09“ (dále jen „Společná definice“). Veškeré záruční povinnosti dodavatele, včetně úrovní služeb, reakčních dob, způsobu eskalace, podmínek dostupnosti, režimu aktualizací, EoL/EoS a výluk plnění, se řídí výlučně tímto dokumentem a Společnou definicí. Jakákoli plnění spočívající v rozvojových zásazích, změnových požadavcích, úpravách nad rámec specifikace či integracích nevyplývajících ze Společné definice nejsou součástí záruky, ledaže budou výslovně sjednána zvláštní smlouvou nebo dodatkem.

V případě rozporu nebo kolizního výkladu mezi touto technickou specifikací a Společnou definicí má přednost tato technická specifikace. Společná definice slouží jako doplňující a výkladový dokument a uplatní se pouze v rozsahu, v němž není v rozporu s touto Technickou specifikací.

3.a. Akceptační kritéria

Dodavatel se zavazuje poskytovat technickou podporu v rozsahu a za podmínek stanovených tímto dokumentem a Společnou definicí po dobu od 1. 6. 2026 do 31. 5. 2031 (60 měsíců). Dodavatel podpisem smlouvy stvrzuje, že po uvedené období bude plnit sjednané SLA a ostatní povinnosti dle tohoto dokumentu a Společné definice; nesplnění těchto povinností bude posuzováno jako porušení smlouvy se všemi z toho vyplývajícími právními následky podle smlouvy a příslušných právních předpisů.

8.1.8. ID08 - Kompletní správa životního cyklu logů

1. Úvod a metodika

Tento dokument definuje předmět a závaznou technickou specifikaci na implementaci pokročilého nástroje pro správu logů (log management) zajišťujícího automatizovaný sběr, normalizaci a archivaci provozních i bezpečnostních záznamů ze všech relevantních infrastrukturních i aplikačních systémů. Systém využije metody strojového učení k přesnému parsování a klasifikaci, zajistí ochranu uložených logů proti neoprávněným změnám i při archivaci a umožní kompresi archivovaných logů na úroveň nejvýše 10% jejich původní velikosti.

Musí být umožněno rychlé vícekriteriální vyhledávání napříč zdroji včetně logů uložených v komprimovaném archivu a k dispozici bude reportovací a notifikační systém s napojením na provozní a bezpečnostní události. Akceptace proběhne demonstrací příjmu a zpracování logů z definovaných zdrojů, ověřením vyhledávání v historických archivovaných datech, testem neměnnosti uložených záznamů a předáním provozní dokumentace.

2. Specifikace dodávaného hardware, software a služeb instalace, implementace a školení

Dodavatel vyplní následující tabulku specifikace nabízeného plnění. Ve sloupci „Splnění parametrů dodavatele – DOPLNÍ DODAVATEL“ dodavatel doplní:

- ANO/NE v závislosti na tom, zda nabízené plnění či jeho část požadavek zadavatele splňuje/nesplňuje,
- specifikaci konkrétního parametru či popis naplnění požadavku zadavatele,
- číselnou hodnotu v případě požadavku zadavatele, který obsahuje číselně vyjádřitelný parametr
- přesnou specifikaci HW, SW nebo služby
- volitelně odkaz na dodavatelem přiložený dokument ve formátu PDF

Architektura

Minimální požadavky	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
Systém musí být navržen ve vysoké dostupnosti, tj. odolné proti výpadkům a poruchám jednotlivých částí Systému tzv. HA.	ANO Systém plně podporuje režim vysoké dostupnosti (HA), a to jak na úrovni infrastruktury, tak na úrovni softwarových komponent odolné proti výpadkům a poruchám jednotlivých částí Systému.
Systém musí být postaven na moderní clusterové architektuře za účelem dosažení vysoké dostupnosti	ANO Nástroj je postaven na moderní clusterové architektuře.
Účastník zadávacího řízení uvede v nabídce podrobné blokové schéma zapojení Systému, kterým osvědčí naplnění tohoto požadavku zadavatele	ANO Účastník zadávacího řízení uvedl v nabídce podrobné blokové schéma zapojení Systému.
Více-uzlový nástroj se musí chovat jako 1 celek	ANO Nástroj umožňuje rozšiřování kapacity i navyšování výkonu přidáváním dalších uzlů do clusteru, přičemž celý víceuzlový systém se chová jako jeden celek.

V případě rozšíření clusteru (přidání dalšího uzlu) je podporována funkce virtuální IP adresy – z datových zdrojů se události posílají na jedinou IP adresu a cluster zajišťuje synchronizaci událostí mezi jednotlivými uzly	ANO Při rozšíření clusteru (přidání uzlu) zůstává pro zdroje jediná cílová IP díky virtuální IP adrese. ANO VIP se transparentně přesouvá mezi uzly a cluster si interně synchronizuje události i stavy, takže není potřeba měnit nastavení na datových zdrojích.
Systém musí být odolný vůči výpadku jednoho datového centra nebo lokality	ANO Nástroj navržen jako vysoce dostupné (HA) řešení, které zajišťuje odolnost proti výpadku datového centra nebo lokality.
Implementace systému musí být provedena jako „on premise“	ANO Implementace bude provedena jako „on premise“.
Řešení musí běžet v provedení aktivního clusteru, tj. po celou dobu běhu aktivně využívat všech hardwarových zdrojů, které jsou k dispozici	ANO Nástroj podporuje provoz v aktivním clusteru, kde jsou všechny dostupné hardwarové uzly aktivně využívány současně.
Zadavatel vylučuje nasazení v Režimu aktive/pasiv	ANO Nástroj bude nasazen v režimu active-active.
Systém nesmí obsahovat "single-point-of-failure", tj. nesmí obsahovat žádný prvek, jehož výpadek by způsobil ztrátu funkčnosti celého Systému, tj. požadovaný hardware bude dodán v počtech kusů umožňujících redundanci odpovídající High Availability clusteru a bude takto zapojen a konfigurován	ANO Nástroj je koncipován jako plně vysokodostupné (High Availability – HA), s architekturou active-active clusteru, která zajišťuje plynulý a bezpečný provoz bez jediného bodu selhání (Single Point of Failure – SPOF). Každá komponenta systému – od kolektorů přes zpracování až po úložiště – je nasazena v redundantním režimu s možností dynamického přebírání zátěže. Hardware bude dodán v potřebném počtu kusů aby byl požadavek naplněn.
Systém musí být nasazen v konfiguraci minimálně 2x 1U server s nejméně 100TB datového prostoru v každém serveru pro archivaci logů	ANO Systém bude nasazen v konfiguraci minimálně 2x 1U server s nejméně 100TB datového prostoru v každém serveru pro archivaci logů
Zadavatel nepřipouští využití pro provoz Systému jeho stávajících hardwarových zařízení (serverů, virtualizačních platforem, sond, kolektorů apod	Systém nebude provozován na stávajících hardwarových zařízeních zadavatele a to včetně (serverů, virtualizačních platforem, sond, kolektorů apod.
Systém musí být dodán jako kompletní řešení složené z hardware a software, to bez dalších nároků na ICT zdroje zadavatele	ANO Systém bude dodán jako kompletní řešení složené z hardware a software, to bez dalších nároků na ICT zdroje zadavatele
Řešení musí poskytovat možnosti distribuované architektury, kde pomocí kolektorů v jednotlivých prostředích a lokalitách bude docházet ke sběru logů a následnému transportu do centrální komponenty ke zpracování a archivaci logů.	ANO Nástroj podporuje plně distribuovanou architekturu, která je navržena pro nasazení ve složitých a víceúrovňových prostředích s více lokalitami. Tato architektura umožňuje, aby v každé lokalitě nebo prostředí fungovaly lokální kolektory, které zajišťují sběr logů bez nutnosti přímého připojení každého zdroje do centrálního systému.
Aktualizace nástroje jsou možné distribuovat online i offline	ANO Aktualizace nástroje jsou možné distribuovat online i offline.

Upgrade i downgrade verzí nástroje musí probíhat bez restartu či rebootu, a to za účelem poskytování nepřetržité funkce nástroje i průběhu upgrade and downgrade	ANO Nástroj podporuje upgrade i downgrade komponent systému za běhu, tedy bez nutnosti restartu nebo rebootu celého nástroje či jeho částí.
Řešení musí podporovat tzv. rolling upgrade, tj. postupný upgrade jednotlivých uzlů clusteru bez celkového downtime systému minimálně z pohledu příjmu logů	ANO Nástroj plně podporuje tzv. rolling upgrade, tedy postupnou aktualizaci jednotlivých uzlů clusteru bez nutnosti zastavení celého systému. Příjem logů zůstává vždy zachován.
Veškerá konfigurace, musí být verzována ve version control systému (např. Git) tak, aby byla zajištěná vysoká úroveň kontroly nad provozním nastavením systému včetně možnosti návratu k předchozí verzi konfigurace	ANO Nástroj podporuje verzování veškeré konfigurace systému prostřednictvím integrace s version control systémem, jako je např. Git.
Nástroj musí mít podporu zrcadlení a clusteru – 2 a více zařízení v režimu active / active	ANO Nástroj podporuje zrcadlení a provoz v clusteru v režimu active/active, tedy s dvěma a více zařízeními, která jsou aktivně využívána současně.
Nástroj musí být nasazen v nativním plnohodnotném active-active clusteru	ANO Nástroj podporuje nasazení v nativním plnohodnotném active-active clusteru
Nástroj musí v případě havárie libovolného uzlu clusteru podporovat přepojení zdrojů logů na zbylé aktivní uzly clusteru bez zásahu administrátora	ANO Nástroj podporuje v případě havárie libovolného uzlu clusteru přepojení zdrojů logů na zbylé aktivní uzly clusteru bez zásahu administrátora.
Administrátor musí mít přístup ke všem komponentám systému, a to až na úroveň příkazové řádky	ANO Nástroj poskytuje administrátorům plnohodnotný přístup ke všem komponentám systému, včetně možnosti přímého přístupu na úrovni příkazové řádky.
Nástroj musí mít mikroservisovou architekturu	ANO Nástroj je postaven na mikroservisové architektuře, která zajišťuje modularitu, flexibilitu a vysokou dostupnost celého systému.
Nástroj musí mít oddělené systémové datové úložiště (s aplikací a operačním systémem) od uložišť logů	ANO Nástroj podporuje oddělení systémového úložiště (pro operační systém a aplikační komponenty) od úložišť určených pro logy.

Licencování

Minimální požadavky	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
Licence neomezuje počet připojených zdrojů logů	ANO Licence nijak neomezuje počet zdrojů logů.
Licence umožňuje generovat neomezený počet reportů	ANO Licence umožňuje generovat neomezený počet reportů.
Licence umožňuje tvorbu neomezeného množství dashboardů	ANO Licence umožňuje tvorbu neomezeného množství dashboardů.
Licence umožňuje tvorbu neomezeného množství parserů logů	ANO Licence umožňuje tvorbu neomezeného množství parserů logů.
Licence umožňuje nasazení jako virtuální appliance do cloudu	ANO Licence umožňuje nasazení jako virtuální appliance do cloudu.

Licence umožňuje nasazení v tzv. multi-tenancy módu. Systém musí poskytovat logicky oddělené samostatné datové prostory, tzv. tenanty	ANO Licence umožňuje nasazení v tzv. multi-tenancy módu a systém poskytuje logicky oddělené samostatné datové prostory, tzv. Tenanty.
Systém nesmí být zcela uzavřená aplikace, ale musí být možné jej integrovat nejenom s různými zdroji, ale i s kontextovými informacemi pomocí skriptů	ANO Nástroj není uzavřenou aplikací, ale naopak je navržen jako otevřená, modulární a flexibilní platforma, která umožňuje snadnou integraci se zdroji dat i kontextovými systémy a podporuje skriptovatelnost a komunitní rozšiřitelnost.
Systém musí umožňovat integrace tak, aby bylo možné čerpat zkušenosti a návody z internetových komunit a tím zefektivnit provoz a rozšiřovaní systému.	ANO Systém umožňuje integrace tak, že je možné čerpat zkušenosti a návody z internetových komunit a tím zefektivnit provoz a rozšiřovaní systému.
Systém musí umožňovat trvale zpracovávat nejméně 2 000 EPS (Events Per Second) a nepřetržitě výkonovou špičku po dobu alespoň 60 minut nejméně 8 000 EPS bez ztráty dat	ANO Systém umožňuje trvale zpracovávat nejméně 2 000 EPS (Events Per Second) a nepřetržitě výkonovou špičku po dobu alespoň 60 minut nejméně 8 000 EPS bez ztráty dat.
Při překročení maximálního zakoupeného objemu zpracovaných dat nesmí dojít ke ztrátě či k zahození dat, nebo k omezení funkčnosti nástroje	ANO Při překročení maximálního zakoupeného objemu nedojde k zahození nebo ztrátě událostí, nebo omezení funkčnosti řešení.
Při opakovaném překročení maximálního zakoupeného objemu zpracovaných dat musí nástroj upozornit na překročení limitu	ANO Při opakovaném překročení maximálního zakoupeného objemu zpracovaných dat je administrátor informován prostřednictvím varování v konzoli, e-mailu nebo jiného zvoleného notifikačního kanálu.
Systém musí být schopen zaznamenávat a vyhodnocovat vlastní logy stejným způsobem jako logy ostatních Zdrojů	ANO Systém je schopen zaznamenávat a vyhodnocovat vlastní logy stejným způsobem jako logy ostatních Zdrojů
Způsob zpracování: logy jsou zpracovávány pomocí parsingu do strukturovaných eventů, které jsou normalizovány do některého z obecně známých a rozšířených schémat (např. CEF, LEEF, Sigma, ECS);	ANO Nástroj podporuje minimálně dvě obecně rozšířená schémata polí – konkrétně Elastic Common Schema (ECS) a formát CEF (Common Event Format). Kromě toho je možné pracovat také s dalšími standardy, jako jsou LEEF (Log Event Extended Format) a Sigma, buď nativně, nebo prostřednictvím transformačních pravidel.

Základní požadavky

Minimální požadavky	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
Nástroj musí umožnit přístup více uživatelů současně, a to jak na úrovni přístupu ke vstupním/zdrojovým datům systému, tak i k incidentům	ANO Nástroj umožňuje současný přístup více uživatelů, a to jak k vstupním/zdrojovým datům, tak i k incidentům a jejich správě.
Nástroj umožňuje snadné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem a jednotlivým konfiguračním komponentám nástroje	ANO Nástroj umožňuje snadné a flexibilní vytváření uživatelských rolí, které definují přístupová práva k uloženým událostem i ke konfiguračním komponentám systému.

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

Přístup uživatelů musí být založen na volně definovaných, oddělených rolích s možností granulárního přidělování práv v rámci každé role, dle zdrojových dat, identifikace monitorovaných zařízení, skupin zařízení a serverů, typu vstupních dat, apod.	ANO Přístup je řízen volně definovatelnými a vzájemně oddělenými rolemi (RBAC), kterým lze granularně přidělovat práva k datům i funkcím. Oprávnění se nastavují podle zdrojových dat a jejich identifikátorů (hostname, IP, IP rozsahy, tagy), podle skupin a konkrétních zařízení/serverů, podle typu vstupních dat (např. Windows EventLog, Syslog, NGFW, databázové či aplikační logy) a také podle tenantu či lokality. U každé role lze určit akce (čtení, tvorba/úprava/mazání konfigurace, export, správa pravidel a parserů, správa alertů), omezit přístup na vybraná pole či povolit zobrazení deanonymizovaných hodnot jen oprávněným uživatelům. Role lze kombinovat (uživatel může mít více rolí), nástroj podporuje dědičnost i výjimky, hromadnou správu práv, kompletní auditní stopu změn a plnou správu přes GUI, CLI i REST API. Oprávnění se automaticky promítají do GUI objektů (vyhledávání, dashboardy, reporty, alerty), takže každý uživatel vidí pouze data a funkce v rámci své role.
Role nesmí být vázány na AD, musí být spravovatelné interně	ANO Nástroj umožňuje plnohodnotnou správu uživatelských rolí přímo v rámci nástroje, bez nutnosti napojení na Active Directory nebo jiný externí systém identity.
Nástroj musí podporovat kompletní oddělení přístupu skupin uživatelů k odlišným datům a konfiguracím (multi-tenantnost), kdy jednotlivé instance mají vlastní konfigurace a samostatně oddělená uložiště logů	ANO Nástroj plně podporuje multi-tenantní architekturu, která umožňuje kompletní oddělení skupin uživatelů, jejich dat, konfigurací i přístupových oprávnění v rámci jednoho systému.
Nástroj podporuje ověřování uživatelů nástroje na externím AD / LDAP serveru. V případě výpadku externího LDAP, nástroj musí podporovat ověření z lokální databáze.	ANO Nástroj podporuje ověřování uživatelů vůči externím AD / LDAP serverům, a zároveň je vybaven mechanismem záložního ověření přes interní lokální databázi, pro případ nedostupnosti externího ověřovacího systému.
Nástroj musí podporovat vícefaktorovou autentikaci uživatelů systému	ANO Nástroj podporuje vícefaktorovou autentikaci uživatelů systému tak, aby se vyloučil neoprávněny přístup do konsole skrze odcizené heslo.
Vyžaduje se zejména vícefaktorová autentikace pomocí hardwarového tokenu, TOTP a hardwarového klíče v mobilním telefonu podle speficikace FIDO2.	ANO Nástroj podporuje vícefaktorovou autentizaci včetně podpory FIDO2, TOTP a hardwarových tokenů.

Nástroj umožňuje definování uživatelských rolí s možností nastavení přístupových práv (možností granulárního přidělování práv v rámci role podle zdrojů logů, skupin zařízení, jednotlivých serverů, typu logu apod.).	ANO Nástroj umožňuje definování uživatelských rolí s detailním (granulárním) nastavením přístupových práv na základě široké škály kritérií. Minimálně ale podle zdrojů logů – IP rozsahy, hostname, název agenta nebo kolektoru. Podle skupin zařízení nebo konkrétních serverů – např. aplikační servery, firewall, databázové uzly. Podle typu logu nebo události – např. autentizační logy, síťové události, systémové chyby. Podle geografické nebo organizační lokality – pobočky, datová centra, oddělení. Podle datové kritičnosti či klasifikace – auditní, provozní, osobní, bezpečnostní logy. Kombinace pravidel umožňuje velmi přesné přidělování přístupů např. jen ke čtení určitého typu logů z konkrétní sítě. Role jsou plně spravovatelné z uživatelského rozhraní. Lze vytvářet libovolné množství rolí. Jeden uživatel může být přiřazen k více rolím současně. Přístupy mohou být automaticky uplatňovány napříč GUI i API rozhraním.
Nástroj umožňuje nastavit pravidelné automatické přesuny dat z interního do externího úložiště, resp. archivu podle definovaných pravidel, a bez vzniku neautorizovaných změn	ANO Nástroj umožňuje nastavit pravidelné a automatické přesuny dat z interního úložiště do externího archivu, a to na základě uživatelsky definovaných pravidel (např. dle stáří dat, typu zdroje nebo úrovně kritičnosti). Nezměnitelnost je garantována pomocí digitálních podpisů.
Nástroj podporuje nastavení retence dat s možností nastavení pravidel pro automatické mazání dat	ANO Nástroj podporuje nastavení retenční politiky s možností automatického a bezpečného mazání dat po uplynutí definované doby uchování.
Nástroj umožňuje retenci (uložení logů) minimálně na 6 měsíců v režimu přímého prohledávání	ANO Nástroj umožňuje retenci logů po dobu minimálně 6 měsíců v režimu okamžitého a přímého prohledávání. Retenční doba je uživatelsky konfigurovatelná – lze prodloužit dle kapacity a politik organizace.
Nástroj umožňuje retenci (uložení logů) minimálně 18 měsíců v archivu	ANO Nástroj umožňuje retenci (uložení) logů po dobu minimálně 18 měsíců v archivu.
Nástroj umožňuje nastavit nezávislé retenční politiky pro jednotlivá úložiště logových dat	ANO Nástroj umožňuje nastavit nezávislé retenční politiky pro jednotlivá úložiště log dat, a to dle provozních, právních nebo bezpečnostních požadavků.
Nástroj umožňuje snadnou obnovu historických dat z archivu pro zpětnou analýzu	ANO Nástroj umožňuje snadnou a bezpečnou obnovu historických dat z archivu pro zpětnou analýzu. Obnova je možná i selektivně – dle časového období, zdroje nebo typu událostí. Celý proces je řízený a auditovaný, s důrazem na zachování integrity dat.

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

Nástroj podporuje provoz v prostředí TCP/IP IPv4 i IPv6	ANO Nástroj plně podporuje provoz v prostředí sítě TCP/IP, a to jak v protokolu IPv4, tak i IPv6, včetně jejich souběžného (dual-stack) nasazení. Všechny komponenty systému – sběr, přenos, zpracování i přístup uživatelů – fungují bez omezení v obou verzích IP protokolu.
Nástroj umožňuje synchronizaci interního času nástroje s externím NTP serverem	ANO Nástroj umožňuje synchronizaci systémového času všech svých komponent s externím NTP serverem určeným uživatelem. Synchronizace je plně konfigurovatelná a podporuje více redundantních NTP serverů.
Nástroj musí pro veškerou kryptografii využívat kryptografickou komponentu, která splňuje platné doporučení NÚKIB pro kryptografické prostředky „Doporučení v oblasti kryptografických prostředků verze 3.0“	ANO Nástroj využívá pro veškeré kryptografické operace (šifrování, digitální podpisy, hashování, integritu logů) kryptografické prostředky, které odpovídají platnému doporučení NÚKIB – „Doporučení v oblasti kryptografických prostředků verze 3.0".
Nástroj poskytuje vlastní provozní a auditní log o aktivitě uživatelů alespoň v rozsahu přihlášení, odhlášení uživatele do/z centrální konzole nástroje, evidence provedených konfiguračních změn a varovná nebo chybová hlášení	ANO Nástroj poskytuje vlastní provozní a auditní log, který detailně zaznamenává aktivitu uživatelů a události systému. Zaznamenává mimo jiné přihlášení a odhlášení uživatelů do/z centrální konzole (včetně času, IP adresy, způsobu ověření), provedené konfigurační změny, včetně informace kdo, kdy a co změnil, systémová varování a chybová hlášení (např. nedostupnost komponent, chyby synchronizace, selhání přenosu dat), přístup k citlivým částem systému nebo logům. Auditní logy jsou chráněny proti modifikaci, indexovány, vyhledatelné a lze je také exportovat pro externí audit nebo korelaci s dalšími nástroji.
Konfigurační a nástrojové rozhraní a dokumentace musí být identické v českém nebo anglickém jazyce	ANO Konfigurační a nástrojové rozhraní a dokumentace jsou k dispozici identické v českém a anglickém jazyce.
Nástroj musí podporovat tmavý a světlý mód uživatelského rozhraní pro dobrou ergonomii práce s nástrojem v různých světelných podmínkách	ANO Nástroj podporuje tmavý a světlý mód uživatelského rozhraní pro dobrou ergonomii práce s nástrojem v různých světelných podmínkách.
Všechny komponenty nástroje, včetně komponent třetích stran, musí být aktuální a nesmí obsahovat zastaralé verze. Za zastaralou verzi komponenty se považuje taková, pro kterou výrobce nebo správce již nevydává nové vyšší „major“ verze, které řeší např. bezpečnostní chyby či jiné zásadní problémy.	ANO Nástroj je navržen tak, aby všechny jeho komponenty – včetně těch třetích stran – byly pravidelně aktualizovány a neobsahovaly zastaralé verze. Komponenty jsou monitorovány z hlediska vydaných „major” verzí a známých bezpečnostních zranitelností.
Zadavatel požaduje doložit použité verze u všech komponent	ANO Seznam použitých verzí u všech component je součástí podání.

Bezpečnost systémů

Minimální požadavky	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
Systém musí umožňovat ochranu integrity "raw" logů digitálními podpisy, přičemž použitý kryptografický algoritmus musí splňovat platná doporučení NÚKIB pro kryptografické prostředky „Doporučení v oblasti kryptografických prostředků verze 3.0“	ANO Nástroj využívá pro veškeré kryptografické operace (šifrování, digitální podpisy, hashování, integritu logů) kryptografické prostředky, které odpovídají platnému doporučení NÚKIB – „Doporučení v oblasti kryptografických prostředků verze 3.0".
Systém musí pro sběr logů musí používat výhradně silné autentizované spojení pro odesílání logů, např. Mutual SSL/TLS tak, aby se vyloučila manipulace se vstupními logy během jejich transportu	ANO Nástroj při sběru a přenosu logů používá výhradně silné autentizované spojení, typicky ve formě vzájemně ověřovaného šifrovaného spojení Mutual SSL/TLS. Tento způsob přenosu zajišťuje důvěryhodnost komunikujících stran, šifrování přenášených dat a integritu logů během celého transportu. Tím je plně vyloučena možnost manipulace, podvržení nebo zachycení logů mezi zdrojem a centrálním systémem.
Účastník zadávacího řízení popíše, jaký bude nabízený Systém využívat kryptografický algoritmus pro zajištění integrity uložených logů	ANO K zajištění bezpečnosti logů nástroj používá následující kryptografické algoritmy: SHA256, ECDSA.
Systém umožňuje řídit přístupy uživatelů např. pomocí systému RBAC (Role-based Access Control).	ANO Nástroj umožňuje detailní řízení přístupových práv uživatelů pomocí systému RBAC (Role-Based Access Control). Každému uživateli může být přiřazena jedna nebo více rolí, které určují, k jakým funkcím systému má přístup – včetně přístupu k uloženým datům, konfiguračním možnostem, typům zobrazení nebo správě alertů. Přístupy lze definovat granulárně až na úroveň jednotlivých typů logů, zdrojů dat, skupin zařízení nebo specifických funkcí nástroje. Systém rovněž umožňuje snadné vytváření a správu vlastních rolí podle provozních nebo bezpečnostních požadavků organizace.
Systém musí řídit přístupová práva uživatelů pro konkrétní tenanty, tj. uživatel může mít jiná práva v různých tenantech	ANO Nástroj umožňuje řídit přístupová práva uživatelů samostatně pro každý tenant. To znamená, že jeden uživatel může mít odlišná oprávnění v různých tenantech – například v jednom může být administrátorem s plným přístupem ke konfiguraci a logům, zatímco v jiném pouze pozorovatelem s omezeným přístupem k datům.
Systém musí nabízet přístup k datům prostřednictvím API pro integraci s dalšími systémy.	ANO Řešení poskytuje plně dokumentované a bezpečné API rozhraní, které umožňuje autorizovaný přístup k funkcím systému a uloženým datům, a je

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

	určené pro integraci s externími nástroji a systémy třetích stran.
Součástí dodávky musí být podrobná dokumentace API v českém jazyce nebo i anglickém jazyce	ANO Součástí dodávky bude podrobná dokumentace API v českém jazyce.
Systém musí být otevřený pro administrátorské zásahy i z příkazové řádky	ANO Systém poskytuje administrátorům plnohodnotný přístup ke všem komponentám systému, včetně možnosti přímého přístupu na úrovni příkazové řádky.
Součástí dodávky musí být podrobná administrátorská, provozní a bezpečnostní dokumentace v českém jazyce	ANO Podrobná produktová, provozní a bezpečností dokumentace v českém jazyce je součástí dodávky.
Systém musí dimenzován tak, aby umožňoval následující retenci logů: • zpracované (parsované) logy musí být dostupné po dobu minimálně 3 měsíce pro vyhledávání a další analytickou práci; • "raw" logy musí být uloženy po 18 měsíců v archivu, tj. úložišti kde je dostupnost archivovaných dat zajištěna alespoň na úrovni zrcadlení úložiště, tj. toto úložiště musí být integrální součástí Systému. • Archiv musí být nezávislý na databázi použité pro ukládání zpracovaných logů • Při archivovaní musí být zajištěno, že nedojde ke změně logů, jejich integrity, ani k změně hashů • Účastník zadávacího řízení popíše specifikaci této ochrany s ohledem na platné doporučení NÚKIB pro kryptografické prostředky „Doporučení v oblasti kryptografických prostředků verze 3.0“ • Integritu logů v archivu lze ověřit pomocí běžných nástrojů, ověření může provést třetí strana bez přístupu k nástroji • Systém musí být topologicky distribuovaný, komponenty sběru a zpracování musí být funkčně i technicky oddělené od ostatních částí Systému, přičemž splnění tohoto požadavku musí vyplývat z předloženého blokového schématu	• zpracované (parsované) logy jsou v systému dostupné po dobu minimálně 3 měsíce pro vyhledávání a další analytickou práci; • "raw" logy jsou uloženy po 18 měsíců v archivu, tj. úložišti kde je dostupnost archivovaných dat zajištěna alespoň na úrovni zrcadlení úložiště, tj. toto úložiště je integrální součástí Systému. • Archiv je nezávislý na databázi použité pro ukládání zpracovaných logů • Při archivovaní je zajištěno, že nedojde ke změně logů, jejich integrity, ani k změně hashů • Nástroj využívá pro veškeré kryptografické operace (šifrování, digitální podpisy, hashování, integritu logů) kryptografické prostředky, které odpovídají platnému doporučení NÚKIB – „Doporučení v oblasti kryptografických prostředků verze 3.0". • Integritu logů v archivu lze ověřit pomocí běžných nástrojů, ověření může provést třetí strana bez přístupu k nástroji • Systém je topologicky distribuovaný, komponenty sběru a zpracování jsou funkčně i technicky oddělené od ostatních částí Systému, přičemž splnění tohoto požadavku vyplývá předloženého blokového schématu

Sběr a zpracování logů

Minimální požadavky	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
Systém musí nabízet konfigurovatelné rozhraní (musí obsahovat alespoň API a vlastní parsery) pro uzpůsobení odlišnostem jednotlivých zdrojů	ANO Systém obsahuje konfigurovatelné rozhraní (API a vlastní parsery) pro uzpůsobení odlišnostem jednotlivých zdrojů.

sběr logů alespoň pomocí protokolů Syslog (UDP, TCP, TLS), SNMP, CEF, LEEF, HTTP/S	ANO Sběr logů probíhá pomocí protokolů Syslog (UDP, TCP, TLS), SNMP, CEF, LEEF, HTTP/S
Systém musí poskytovat bezagentový sběr logů (sběr bez nutnosti instalovat agenta na cílový systém)	ANO Systém podporuje bezagentní sběr dat, tedy sběr bez nutnosti instalace jakéhokoliv agenta na zdrojové systémy nebo zařízení.
Systém musí poskytovat sběr Windows Events pomocí WEC/WEF a centralizované konfigurace doménového řadiče, vylučuje se použití agenta instalovaného na počítače s OS Windows	ANO Sběr Windows Events v prostředí Windows probíhá přes WEC/WEF a centralizované konfigurace doménového řadiče.
Systém musí poskytovat sběru logů samostatným kolektorem, který přeposílá logy do centrálního systému	ANO Nástroj umožňuje sběr logů samostatným kolektorem, který přeposílá logy do centrálního systému.
Systém musí poskytovat sběr logů z dalších bezpečnostních a síťových systémů (alespoň firewall, IDS/IPS, routery, switche, AP controllery, Network Access Control);	ANO Nástroj poskytuje přijímání a zpracovávání logů, událostí a dalších strojově generovaných dat prostřednictvím bezpečnostních a síťových systémů (firewall, IDS/IPS, routery, switche, AP controllery, Network Access Control).
Systém musí poskytovat možnost agregace událostí z logů i podle položek, které nejsou standardně zahrnuty v Systému, tj. Systém musí umožňovat uživatelsky vytvářet vlastní parsery;	ANO Nástroj poskytuje možnost agregace událostí z logů i podle položek, které nejsou standardně zahrnuty v Systému, tj. Systém umožňuje uživatelsky vytvářet vlastní parsery.
Systém musí poskytovat sběr textových logů ze souborů;	ANO Nástroj podporuje přijímání a zpracovávání textových logů ze souborů.
Systém musí poskytovat sběr logů z databází minimálně pomocí ODBC a JDBC;	ANO Nástroj podporuje přijímání a zpracovávání logů, událostí a dalších strojově generovaných dat prostřednictvím databází minimálně pomocí ODBC a JDBC.
Systém musí poskytovat sběr log záznamů z prostředí Windows a Linux/Unix;	ANO Nástroj podporuje přijímání a zpracovávání logů, událostí a dalších strojově generovaných dat prostřednictvím prostředí Windows a Linux/Unix
Systém musí poskytovat sběr logů z API rozhraní v podobě REST-API i SOAP;	ANO Nástroj podporuje přijímání a zpracovávání logů, událostí a dalších strojově generovaných dat prostřednictvím API rozhraní v podobě REST-API i SOAP.
Systém musí poskytovat sběr logů z XML i JSON souborů;	ANO Nástroj podporuje přijímání a zpracovávání logů, událostí a dalších strojově generovaných dat prostřednictvím XML i JSON souborů.
Systém musí uchovávat logy jak v normalizovaném formátu, tak i v „raw“ formátu a to v technologicky oddělených uložištích	ANO Nástroj uchovává logy jak v normalizovaném formátu, tak i v „raw“ formátu, a to v technologicky oddělených uložištích.

Při přetížení Systému nesmí dojít ke ztrátě přijímaných zpráv. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti (např. kolektoru) pro následné zpracování	ANO Při přetížení systému nedochází ke ztrátě přijímaných zpráv. Všechny nezpracované logy a události jsou automaticky ukládány do vyrovnávací paměti (bufferu) na úrovni kolektoru nebo jiných vstupních komponent. Po obnovení kapacity systému jsou tyto zprávy z bufferu postupně zpracovány a doručeny do centrální části bez ztráty či duplicit.
Systém provádí normalizaci přijímaných událostí a logů minimálně v rozsahu typ činnosti, datum a čas, identifikaci datového zdroje, identifikaci původce a místa činnosti záznamu, úspěšnost nebo neúspěšnost činnosti	ANO Nástroj provádí automatickou normalizaci všech přijímaných událostí a logů. Minimálně jsou při normalizaci extrahovány a uchovávány údaje jako typ činnosti, datum a čas události, identifikace datového zdroje (např. zařízení, aplikace), identita původce (uživatel, proces), místo provedení akce (např. IP adresa nebo zařízení) a informace o úspěchu nebo neúspěchu operace.
Systém provádí automatické doplňování GeoIP informací k událostem	ANO Nástroj provádí automatické doplňování geolokačních informací (GeoIP) k událostem obsahujícím veřejné IP adresy. Geolokační data jsou následně vizualizována přímo v analytickém rozhraní pomocí interaktivní mapy, kde je možné zobrazit rozmístění událostí dle geografického původu.
Systém provádí automatické doplňování výrobce zařízení z MAC adres v událostech	ANO Nástroj automaticky doplňuje informaci o výrobci zařízení na základě MAC adres obsažených v událostech. Využívá k tomu databázi OUI (Organizationally Unique Identifier), která umožňuje rozpoznat výrobce zařízení podle prvních bajtů MAC adresy. Tato informace je přidána k logu jako obohacující údaj (enrichment).
Nástroj obsahuje kolektor, který umožňuje sběr událostí ve vzdálených lokalitách a jejich odeslání po saturované lince bez ztráty dat	ANO Nástroj obsahuje kolektor, který sbírá události ve vzdálených lokalitách a umožnuje jejich odeslání po saturované lince bez ztráty dat.
Kolektor logů lze provozovat mimo centrální instalaci	ANO Součástí nástroje je kolektor logů, který lze plnohodnotně provozovat mimo centrální instalaci, například v oddělené lokalitě, pobočce nebo DMZ zóně.
Kolektor musí být k dispozici jako virtuální a hardwarová appliance.	ANO Kolektory jsou k dispozici jako virtuální a hardwarová appliance.

Nástroj musí podporovat sběr logů v režimu vysoké dostupnosti (HA), tj: • Zasílání logů ze zdroje logů na dvě a více instancí kolektorů (push) • Odebíraní logů ze zdroje dvěmi a více instancemi kolektorů (pull)	ANO Nástroj plně podporuje sběr logů v režimu vysoké dostupnosti (HA), a to jak na úrovni infrastruktury, tak na úrovni softwarových komponent. • Nástroj podporuje zasílání logů (push) ze zdrojů logů na dvě a více instancí kolektorů současně. • Nástroj podporuje režim odebírání logů (pull) ze zdrojových systémů pomocí dvou a více instancí kolektorů současně.
Kolektor musí podporovat připojení k centrálnímu systému v režimu vysoké dostupnosti, konkrétně se kolektor musí umět v případě ztráty spojení automaticky připojit na další dostupný uzel a tudíž je zajištěn bezvýpadkový sběr logů	ANO Kolektor podporuje režim vysoké dostupnosti (HA) při připojení k centrálnímu systému. Automatické přepínání (failover): Pokud kolektor ztratí spojení s jedním uzlem centrálního systému, automaticky se přepojí na další dostupný uzel bez přerušení sběru. Seznam dostupných uzlů: Kolektor má nakonfigurován seznam více centrálních uzlů, ke kterým se může připojit.
Nástroj šifruje a komprimuje posílaná data a zabezpečuje je proti jejich modifikaci nebo smazání. Je garantováno doručení do centrálního prvku	ANO Nástroj zajišťuje, že veškerá data odesílaná kolektory nebo agenty do centrálního systému jsou šifrována, komprimována a chráněna proti neoprávněné změně nebo ztrátě. Je garantováno doručení do centrálního prvku.
Nástroj podporuje centralizovanou správu sběru dat přímo z centrální konzole bez ohledu, zda sběr probíhá nebo neprobíhá přes kolektor	ANO Nástroj podporuje centralizovanou správu sběru dat prostřednictvím jediné centrální konzole, a to bez ohledu na to, zda je sběr realizován přímo, nebo přes kolektory.
Kolektor je schopen automaticky navázat spojení (po instalaci nebo po výpadku) s centrálním nástrojem a přenášená data šifrovat	ANO Kolektor po instalaci nebo výpadku automaticky naváže zabezpečené spojení s centrálním systémem, bez nutnosti zásahu administrátora. Veškerá přenášená data jsou automaticky šifrována.
Nástroj komunikuje po definovaném IP protokolu s možností nastavení sítě pro zajištění kvality služeb (QoS) pro přenos událostí	ANO Nástroj umožňuje komunikaci po definovaném IP protokolu (IPv4 i IPv6) a zároveň podporuje konfigurovatelné síťové nastavení pro zajištění kvality služeb (QoS) při přenosu událostí.
Kolektor poskytuje kapacitu vyrovnávací paměti pro minimálně 1 TB dat pro jejich uchování během výpadku spojení s centrálním nástrojem/serverem	ANO Kolektor disponuje lokálním úložištěm pro případný dočasný výpadek konektivity pro minimálně 1 TB dat, a po jejím obnovení data doručí do centrálního nástroje/serveru.

Nástroj v centrální uživatelské konzoli poskytuje online přehled připojených a nepřipojených kolektorů, včetně přehledového monitoru aktivity přijmu logů na jednotlivých kolektorech.	ANO Nástroj poskytuje v centrální uživatelské konzoli okamžitý přehled o stavu všech kolektorů, a to včetně informace, zda jsou připojené či nepřipojené. Součástí konzole je také přehledový monitor aktivity příjmu logů na jednotlivých kolektorech, který umožňuje sledovat jejich aktuální zátěž, stav komunikace a objem zpracovaných událostí v reálném čase.
Sběr dat probíhá bez-agentním způsobem, tj. bez instalace agenta na zdrojové systémy a zařízení.	ANO Nástroj podporuje bezagentní sběr dat, tedy sběr bez nutnosti instalace jakéhokoliv agenta na zdrojové systémy nebo zařízení.
Komponenty nástroje musí být schopny komunikovat s centrálním nástrojem i přes vícenásobný překlad adres (NAT) včetně managementu	ANO Komponenty nástroje jsou navrženy tak, aby byly schopny spolehlivě komunikovat s centrálním systémem i přes vícenásobný překlad adres (NAT). Tato schopnost platí jak pro samotný sběr a přenos logů, tak i pro vzdálenou správu a centrální management kolektorů, agentů a dalších komponent.
Nástroj nevyžaduje instalaci dalších podpůrných nástrojů a aplikací na zdrojové systémy (kompletně bez-agentový sběr)	ANO Nástroj umožňuje plně bezagentní sběr dat, a to bez nutnosti instalace jakýchkoliv podpůrných nástrojů nebo aplikací na zdrojové systémy.
Nástroj podporuje načítání log souborů (jedno a víceřádkové textové logy), kde tyto soubory mají stanovenu strukturu a význam dat.	ANO Nástroj podporuje načítání log souborů, včetně jednořádkových i víceřádkových textových logů, a to i v případech, kdy tyto soubory mají definovanou strukturu a význam dat.
Nástroj umožňuje přijímat logy i na uživatelsky definovaných UDP a TPC portech.	ANO Nástroj umožňuje přijímat logy i na uživatelsky definovaných UDP a TPC portech.
Sběr logů v prostředí Windows musí probíhat přes technologii WEC/WEF.	ANO Sběr logů v prostředí Windows probíhá přes WEC/WEF.
Kolektor musí podporovat připojení do Microsoft Windows AD domény pomocí Kerberos.	ANO Nástroj podporuje připojení do Microsoft Windows AD domény pomocí Kerberos autentizace.
Nástroj umožňuje zobrazit logy v původní formě jak byly přijaty, tzv. raw message.	ANO Nástroj umožňuje zobrazit každý log v jeho původní podobě, tzv. raw message, přesně tak, jak byl přijat ze zdrojového systému.
Při přetížení nástroje nesmí dojít ke ztrátě přijímaných zpráv. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti (např. kolektoru) pro následné zpracování.	ANO Při přetížení systému nedochází ke ztrátě přijímaných zpráv. Všechny nezpracované logy a události jsou automaticky ukládány do vyrovnávací paměti (bufferu) na úrovni kolektoru nebo jiných vstupních komponent. Po obnovení kapacity systému jsou tyto zprávy z bufferu postupně zpracovány a doručeny do centrální části bez ztráty či duplicit.

Nástroj umožňuje uložit různé druhy logů po různě dlouhou dobu (retenční perioda). Nástroj musí poskytovat neomezené množství těchto skupin	ANO Nástroj umožňuje nastavit rozdílné retenční periody pro různé druhy logů, zdroje nebo datové skupiny. Pro každou skupinu lze definovat vlastní dobu uchování podle typu dat, jejich významu nebo regulatorních požadavků. Nástroj nemá omezení v počtu těchto retenčních skupin a umožňuje jejich snadnou správu prostřednictvím centrální konzole.
Nástroj je schopen detekovat výpadek zdrojů logů (jak typu, tak jednotlivých serverů) v centrální konzoli, včetně upozornění na tento stav	ANO Nástroj je schopen detekovat výpadek logovacích zdrojů – jak na úrovni celého typu zařízení, tak konkrétních serverů nebo služeb. V případě, že přestane přicházet očekávaný objem dat z určitého zdroje, systém tento stav automaticky identifikuje a zobrazí upozornění v centrální konzoli. Upozornění může být doplněno vizuálním indikátorem, e-mailem nebo jinou notifikací dle nastavení.
Nástroj musí detekovat i anomálie ve sběru logů, zejména např. výrazně vyšší příjem logů z konkrétních zařízení, než je předpokládaný příjem na základě historických dat	ANO Nástroj obsahuje mechanismy pro detekci anomálií ve sběru logů, včetně identifikace náhlého nárůstu objemu událostí z konkrétních zařízení nebo systémů. Systém průběžně vyhodnocuje chování jednotlivých logovacích zdrojů a porovnává aktuální vstup s historickými vzorci. V případě výrazné odchylky, například při neobvykle vysokém příjmu logů, dojde k vyhodnocení situace jako anomálie a uživatel je o tom informován formou upozornění v centrální konzoli nebo e-mailovou notifikací.
Sběr logů musí používat výhradně silné autentizované spojeni pro odesílání logů, např. Mutual SSL/TLS tak, aby se vyloučila manipulace se vstupními logy během jejich transportu.	ANO Nástroj při sběru a přenosu logů používá výhradně silné autentizované spojení, typicky ve formě vzájemně ověřovaného šifrovaného spojení Mutual SSL/TLS. Tento způsob přenosu zajišťuje důvěryhodnost komunikujících stran, šifrování přenášených dat a integritu logů během celého transportu.
Kolektor logů musí podporovat automatizovanou obnovu klientských certifikátů. Maximální platnost klientského certifikátu kolektoru logů je 6 měsíců	ANO Kolektor logů podporuje automatizovanou správu a obnovu klientských certifikátů. Certifikáty jsou pravidelně kontrolovány a v případě blížícího se konce jejich platnosti je proces obnovy řízen centrálně, bez potřeby manuálního zásahu. Nástroj umožňuje nastavit maximální platnost klientského certifikátu kolektoru na 6 měsíců a zajišťuje, že po jejím uplynutí dojde k jeho bezpečné a bezvýpadkové výměně.

Nástroj provádí normalizaci přijímaných událostí a logů minimálně v rozsahu typ činnosti, datum a čas, identifikaci datového zdroje, identifikaci původce a místa činnosti záznamu, úspěšnost nebo neúspěšnost činnosti	ANO Nástroj provádí automatickou normalizaci všech přijímaných událostí a logů. Minimálně jsou při normalizaci extrahovány a uchovávány údaje jako typ činnosti, datum a čas události, identifikace datového zdroje (např. zařízení, aplikace), identita původce (uživatel, proces), místo provedení akce (např. IP adresa nebo zařízení) a informace o úspěchu nebo neúspěchu operace.

Nástroj musí podporovat přijímání a zpracovávání logů, událostí a další strojově generovaných data prostřednictvím minimálně následujících protokolů a formátů:
• Syslog RFC3164 přes UDP, TCP a SSL
• Syslog RFC5424 přes UDP, TCP a SSL
• Syslog RFC3195 BEEP přes TCP a SSL
• Syslog RFC6587 přes TCP a SSL
• Windows Event Collection (WEC/WEF)
  ○ s autentizací pomocí SSL certifikátů
  ○ s autentizací pomocí Kerberos
• FTP
• SFTP
• SNMP
• ODBC nebo JDBC
• Apache Kafka
• Rest API
• CEF
• LEEF
• JSON
• XML
• Text file, single line
• Text file, multiline
	ANO Nástroj podporuje přijímání a zpracovávání logů, událostí a dalších strojově generovaných dat prostřednictvím všech uvedených protokolů a formátů.

Zpracování logů

Minimální požadavky	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
Přijaté logy nástroj standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu se současným uchováním originální verze zpráv	ANO Nástroj standardizuje všechny přijaté logy do jednotného interního formátu, který umožňuje jednotné zpracování napříč různými zdroji a formáty. Každý log je při zpracování automaticky normalizován – to znamená, že jsou z něj extrahována jednotlivá datová pole podle typu zprávy (např. časová značka, identita uživatele, IP adresa, typ činnosti apod.). Zároveň je vždy zachována i původní, neupravená verze zprávy (tzv. raw log), která zůstává dostupná pro auditní účely, forenzní analýzu nebo zpětné ověření.

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

Nástroj zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje jí a vytváří vlastní důvěryhodné časové razítko ke každému logu, kterým se nástroj defaultně řídí	ANO Nástroj při zpracování každého logu zachovává původní časovou značku tak, jak byla odeslána ze zdrojového systému. Zároveň však nástroj automaticky vytváří vlastní důvěryhodné časové razítko při přijetí logu do systému. Toto vnitřní časové razítko je generováno na základě synchronizovaného systémového času (např. přes NTP) a slouží jako primární údaj pro časové třídění, analýzu a korelaci událostí.
Nástroj musí podporovat minimálně dvě obecně rozšířená schémata polí, např. ECS, CEF, LEEF, Sigma	ANO Nástroj podporuje minimálně dvě obecně rozšířená schémata polí – konkrétně Elastic Common Schema (ECS) a formát CEF (Common Event Format). Kromě toho je možné pracovat také s dalšími standardy, jako jsou LEEF (Log Event Extended Format) a Sigma, buď nativně, nebo prostřednictvím transformačních pravidel.
Všechna pole a položky přijaté nástrojem jsou automaticky indexovány s možností okamžitého vyhledávání bez nutnosti dodatečného ručního indexování administrátorem	ANO Nástroj automaticky indexuje všechna pole a položky přijaté v rámci zpracování logů bez nutnosti jakéhokoli ručního zásahu ze strany administrátora. To umožňuje okamžité a efektivní vyhledávání nad všemi dostupnými daty, a to i ve velkých objemech. Vyhledávání probíhá v reálném čase a podporuje pokročilé dotazy, filtrování, regex i full-textové hledání.
Nástroj provádí automatické doplňování GeoIP informací k událostem a jejich grafické znázornění na mapě	ANO Nástroj provádí automatické doplňování geolokačních informací (GeoIP) k událostem obsahujícím veřejné IP adresy. Geolokační data jsou následně vizualizována přímo v analytickém rozhraní pomocí interaktivní mapy, kde je možné zobrazit rozmístění událostí dle geografického původu.
Nástroj provádí automatické doplňování výrobce zařízení z MAC adres v událostech	ANO Nástroj automaticky doplňuje informaci o výrobci zařízení na základě MAC adres obsažených v událostech. Využívá k tomu databázi OUI (Organizationally Unique Identifier), která umožňuje rozpoznat výrobce zařízení podle prvních bajtů MAC adresy. Tato informace je přidána k logu jako obohacující údaj (enrichment).

Nástroj provádí automatické doplňování dle informací z externích zdrojů (doplnění hostname k IP, doplnění Jména k ID uživatele, doplnění identifikace lokality k ID čtečky karet apod.)	ANO Nástroj provádí automatické doplňování dat k událostem pomocí informací z externích zdrojů. Mezi tyto obohacující údaje patří například doplnění názvu hostitele (hostname) k IP adrese prostřednictvím reverzního DNS záznamu, doplnění jména uživatele k jeho ID získanému z logu (např. z propojení na LDAP/AD), nebo identifikace lokality zařízení podle ID čtečky karet či IP rozsahu. Tyto informace jsou přiřazovány automaticky podle předem nastavených pravidel nebo připojených externích datových tabulek.
Přijímané události jsou automaticky kategorizovány pomocí sady přednastavených tzv. značek. (přihlášení, změna atd. včetně výsledku operace, úspěšná, neúspěšná apod.)	ANO Nástroj automaticky kategorizuje přijímané události pomocí sady přednastavených značek (tags), které jsou přiřazovány na základě obsahu a typu logu. Tyto značky zahrnují například typ činnosti jako přihlášení, odhlášení, změna konfigurace, vytvoření objektu, pokus o přístup a další. Dále je ke každé události přiřazen výsledek operace, tedy zda byla akce úspěšná nebo neúspěšná.

Archivace logů

Minimální požadavky	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
Nástroj musí umožňovat efektivní archivaci logů a všech ostatních zpracovávaných událostí na dobu minimálně 18 měsíců. Efektivita je definována jako poměr místa, které zabírají archivované logy a velikosti logů na vstupu. Požadován je poměr alespoň 1:10, tj. logy jsou při archivaci zkomprimovány alespoň na 10 procent jejich vstupní velikosti, a to včetně všech potřebných metadat.	ANO Nástroj umožňuje efektivní archivaci logů a všech zpracovávaných událostí s cílem uchovávat data po dobu minimálně 18 měsíců. Archivace probíhá s využitím pokročilé komprese, která dosahuje požadovaného poměru minimálně 1:10 – tedy archivované logy včetně všech potřebných metadat zabírají maximálně 10 % původní velikosti vstupních dat. Komprimace je prováděna automaticky a transparentně, přičemž jsou zachovány veškeré vlastnosti potřebné pro forenzní analýzu, audit i integritu dat.
Data v archivu musí být komprimovány s účinností minimálně 90%	ANO Nástroj umožňuje kompresi dat v archivu s účinností minimálně 90%.
Archiv musí podporovat připojení externích uložišť NAS, SAN atp.	ANO Archivní komponenta nástroje podporuje ukládání archivních souborů na síťová úložiště typu NAS (Network Attached Storage) a SAN (Storage Area Network). Archivní data jsou uložena ve vysoce komprimovaném a šifrovaném formátu, přičemž přístupová práva a integrita dat jsou nadále plně řízena a monitorována centrálním systémem.

Logy jsou do archivu ukládány ihned po vstupu do centrální komponenty, nezávisle na další zpracování v nástroji, jako je parsing, enrichment atd.	ANO Nástroj ukládá logy do archivu ihned po jejich vstupu do centrální komponenty, tedy ještě před jakýmkoli dalším zpracováním, jako je parsing, enrichment nebo normalizace. Tento přístup zajišťuje uchování původní, nezměněné podoby zpráv (raw logů), včetně časové konzistence a integrity dat. Archivace probíhá paralelně s ostatními procesy, což zajišťuje, že ani při zátěži nebo dočasném výpadku zpracovacích modulů nedojde ke ztrátě či opožděnému uložení logů.
Archiv musí podporovat ukládání archivních souborů na NAS, SAN.	ANO Archivní komponenta nástroje podporuje ukládání archivních souborů na síťová úložiště typu NAS (Network Attached Storage) a SAN (Storage Area Network). Archivní data jsou uložena ve vysoce komprimovaném a šifrovaném formátu, přičemž přístupová práva a integrita dat jsou nadále plně řízena a monitorována centrálním systémem.
Archiv musí podporovat ukládání archivních souborů na pásky, pomocí páskové mechaniky, a to důvodu požadavku na dvě různé technologie pro dlouhodobou archivaci.	ANO Archivní komponenta nástroje podporuje také ukládání archivních souborů na páskové mechaniky, čímž umožňuje využití dvou různých technologií pro dlouhodobou archivaci – například kombinaci NAS/SAN a LTO páskových systémů. Archivní komponenta dokáže exportovat archivní balíky ve formátu vhodném pro zápis na pásky a zároveň uchovat metadata o jejich umístění a obsahu pro budoucí vyhledávání a zpětnou obnovu.
Archiv musí podporovat ukládání archivních souborů na veřejné cloudy, minimálně Microsoft Azure a AWS S3.	ANO Archivní komponenta nástroje podporuje ukládání archivních souborů do veřejných cloudových úložišť, a to minimálně do Microsoft Azure Blob Storage a Amazon AWS S3. Archivace do těchto cílů probíhá s využitím silného šifrování dat před jejich odesláním a s podporou ověřených metod autentizace (např. klíče, tokeny). Zároveň je uchována integrita archivních souborů a metadata potřebná pro rychlé dohledání a obnovu.
Nástroj musí podporovat řízení životního cyklu archivovaných dat, ve kterém se stanovuje, kde jsou archivní soubory uloženy a případně kdy se mají přesouvat.	ANO Nástroj podporuje řízení životního cyklu archivovaných dat, kdy je možné přesně definovat, kde budou archivní soubory uloženy a kdy se mají podle stanovených pravidel přesouvat mezi jednotlivými typy úložišť. Celý proces probíhá za plného zajištění integrity dat, šifrování, sledování přístupových oprávnění a s evidencí všech změn.

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

Archiv musí podporovat repliky archivních souborů tak, aby data mohla být uložena ve více kopiích na různých uložištích a fyzických místech.	ANO Nástroj podporuje vytváření replik archivních souborů, což umožňuje ukládání dat ve více kopiích na různých úložištích a fyzicky oddělených lokalitách. Tato funkcionalita je součástí politik archivace a řízení životního cyklu dat a zajišťuje vysokou dostupnost, odolnost proti ztrátě dat a splnění požadavků na geografickou redundanci. Replikace může probíhat mezi lokálními úložišti, vzdálenými datacentry nebo cloudovými službami a je prováděna automatizovaně a bezpečně, včetně šifrování a kontroly integrity archivovaných dat.
Nástroj garantuje integritu uložených dat v archivu. Nesmí umožnit mazání nebo modifikování již uložených logů. Každý log musí mít unikátní identifikátor, který umožní jeho jednoznačnou identifikaci.	ANO Nástroj garantuje integritu všech uložených dat v archivu. Jakmile jsou logy jednou archivovány, nelze je zpětně mazat ani upravovat. Každý log je opatřen unikátním identifikátorem, který umožňuje jeho jednoznačnou identifikaci a zpětnou dohledatelnost. Systém zároveň využívá kryptografické kontroly integrity (např. hashovací otisky) k detekci jakékoli neoprávněné změny a všechny operace s archivními daty jsou auditovány.
Pro garanci integrity logů v archivu se využívají kryptografické algoritmy (digitální podpisy, hašovací funkce), které vyhovují platným požadavků organizace ENISA.	ANO Nástroj využívá pro zajištění integrity logů v archivu moderní kryptografické algoritmy, jako jsou digitální podpisy a hašovací funkce, které splňují platná doporučení organizací jako je ENISA a také NÚKIB. Každý archivní soubor je při uložení kryptograficky označen, což umožňuje následné ověření, že nedošlo k žádné změně jeho obsahu. Tato kontrola integrity probíhá pravidelně a systém zaznamenává jakýkoli pokus o neautorizovanou manipulaci.
Integritu logů lze ověřit pomocí běžných nástrojů, aby toto ověření mohla provést třetí strana bez přístupu k nástroji.	ANO Nástroj ukládá logy do archivu takovým způsobem, že jejich integritu lze ověřit i pomocí běžně dostupných nástrojů bez nutnosti přístupu k samotnému systému. Každý archivní soubor je doplněn o kryptografický otisk (např. pomocí algoritmů SHA-2) a případně digitální podpis. Tyto informace jsou uloženy odděleně nebo jako součást metadat, a mohou být ověřeny třetí stranou pomocí standardních nástrojů pro kontrolu hashů nebo ověření podpisu.

Logy v archivu je možné prohledávat pomocí standardních možností z konzole bez nutnosti je importovat zpět do nástroje.	ANO Nástroj umožňuje prohledávání logů přímo v archivu bez nutnosti jejich importu zpět do systému. Archivované logy jsou uloženy ve strukturovaném a indexovaném formátu, který je dostupný z konzole nástroje a lze nad ním provádět standardní dotazy, včetně filtrování, fulltextového vyhledávání nebo časového ohraničení.
Nástroj obsahuje přehled logů uložených v archivu, ze kterého je možné snadno dohledat, které archivní soubory obsahují logy ze zvoleného časového intervalu a kde jsou tyto archivní soubory uloženy.	ANO Nástroj obsahuje přehledové rozhraní pro správu archivních logů, které umožňuje snadno identifikovat, které archivní soubory obsahují logy ze zvoleného časového intervalu. Uživatel má k dispozici seznam archivních bloků s metadaty, jako je časový rozsah, typ logů, velikost a umístění na úložišti (např. disk, NAS, cloud, páska). Díky tomu je možné rychle a přehledně dohledat relevantní archivované údaje bez nutnosti procházet celý archiv ručně
Logy lze z archivu znovu v případě potřeby nahrát do nástroje. Při takovém nahrávání nástroj volitelně aplikuj e detekční pravidla atd.	ANO Nástroj umožňuje znovunačtení archivovaných logů zpět do systému v případě potřeby, například při forenzní analýze, auditu nebo vyšetřování incidentu. Při opětovném načtení lze volitelně aktivovat zpracování těmito daty, včetně aplikace detekčních pravidel, korelačních scénářů, enrichmentu a vizualizačních funkcí. Uživatel má plnou kontrolu nad tím, zda budou znovunačtená data analyzována stejně jako běžný živý provoz, nebo zda budou pouze přístupná k ručnímu procházení. Tento proces je bezpečný, auditovaný a nedochází při něm ke změně původních archivovaných dat.

Úpravy a přizpůsobení

Minimální požadavky	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
Nástroj umožňuje dopsání parsovacích pravidel odpovědným administrátorem za nástroj bez nutnosti spolupráce s výrobcem nebo dodavatelem. Nástroj obsahuje nástroje pro jejich testování a optimalizaci bez rizika negativního dopadu na ostatní funkce nástroje.	ANO Nástroj umožňuje odpovědnému administrátorovi samostatně vytvářet a upravovat parsovací pravidla bez nutnosti zásahu výrobce nebo dodavatele. K dispozici jsou integrované nástroje pro tvorbu, testování a ladění těchto pravidel v izolovaném prostředí, které umožňují ověřit funkčnost nových pravidel nad reálnými nebo testovacími daty bez jakéhokoliv dopadu na provozní prostředí.

Vlastní zdroje logů, pro které je vyvinuté vlastní parsování, mají stejnou sadu funkcí a vlastností, jako ty nativně podporované výrobcem (sběr, parsování, doplňování dalších informací, filtrace, kategorizace atd.).	ANO Vlastní zdroje logů, pro které je vyvinuté vlastní parsování mají stejnou sadu funkcí a vlastností jako ty nativně podporované výrobcem. To zahrnuje standardní procesy jako sběr a příjem dat, parsování a normalizaci, doplňování kontextových informací (enrichment), filtrování, kategorizaci událostí, aplikaci bezpečnostních pravidel a vizualizaci.
Možnost on-line uprav parsovacích pravidel – při jejich vytváření je možné vložit vlastní testovací zprávy, přičemž je okamžitě zobrazena výsledná podoba rozparsovaných dat a případná chybová hlášení.	ANO Nástroj umožňuje online úpravu parsovacích pravidel přímo v administrátorské konzoli. Při jejich vytváření nebo úpravě lze vložit vlastní testovací zprávy, nad kterými je ihned zobrazena výsledná struktura rozparsovaných dat včetně všech rozpoznaných polí. Systém zároveň okamžitě upozorní na případné chyby nebo nesoulad s definicí.
Nástroj pro vývoj parsovacích pravidel musí podporovat automatizované testování vytvořených pravidel tzv. jednotkový test (unit test) a zařazení tohoto nástroje do CI/CD (continuous intergration/continous delivery) nástrojů.	ANO Nástroj poskytuje nástroj pro vývoj parsovacích pravidel, který podporuje automatizované testování formou jednotkových testů (unit testů). Administrátor může definovat vstupní zprávy a očekávaný výstup parsování, přičemž systém automaticky ověří správnost výsledků. Tento nástroj je navržen tak, aby byl plně integrován do CI/CD nástrojů, což umožňuje začlenit testování parsovacích pravidel do automatizovaného procesu nasazení a aktualizace konfigurace.
Nástroj má možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování.	ANO Nástroj umožňuje uživatelům vytvářet vlastní pohledy na data ve formě dashboardů a tyto pohledy následně ukládat pro budoucí použití. Uživatelé si mohou nakonfigurovat vizualizace, filtry, metriky a rozložení komponent podle svých potřeb a uložené dashboardy pak kdykoli znovu otevřít, sdílet nebo dále upravovat.
Text alertu lze uživatelsky definovat a je možné jej doplnit proměnnými z podkladové zprávy.	ANO Nástroj umožňuje uživatelsky definovat text alertu a doplňovat jej o dynamické proměnné přímo z podkladové zprávy, která výstrahu vyvolala. Uživatel si tak může přesně upravit podobu upozornění, včetně vložení informací jako je IP adresa, název zařízení, typ události, čas a další relevantní pole z původního logu.

Nástroj je dodáván se sadou předpřipraveného obsahu. Uživatelé mohou bez omezení přistupovat k předpisům předpřipraveného obsahu a případně tento obsah měnit nebo rozšiřovat.	ANO Nástroj je dodáván se sadou předpřipraveného obsahu, který zahrnuje detekční pravidla, parsovací šablony, vizualizační dashboardy, dotazy, korelace a další analytické komponenty. Uživatelé mají plný přístup k tomuto obsahu a mohou jej bez omezení upravovat, rozšiřovat nebo přizpůsobovat svému prostředí a potřebám.
Nástroj musí podporovat full-textové vyhledávání v předpřipraveném a uživatelském obsahu.	ANO Nástroj podporuje full-textové vyhledávání v předpřipraveném i uživatelsky vytvořeném obsahu. Uživatelé mohou jednoduše vyhledávat napříč detekčními pravidly, dashboardy, dotazy, parsovacími šablonami a dalšími prvky podle klíčových slov, názvů, proměnných nebo konkrétního obsahu.

Vyhledávání, zobrazení a reporting

Minimální požadavky	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
Nástroj poskytuje centrální webové rozhraní pro přístup k logům, alertům, reportům a pro správu nástroje. Z této konzole se provádí veškerá konfigurace, správa a analýza uložených dat.	ANO Nástroj poskytuje centralizované webové rozhraní, které slouží jako jednotná přístupová konzole pro práci s logy, alerty, reporty i správu celého nástroje. Z této konzole lze provádět kompletní konfiguraci systému, správu datových toků, definování pravidel, tvorbu dashboardů, spouštění vyhledávacích dotazů, správu uživatelů a jejich oprávnění, sledování systémového stavu i provozních statistik.
Nástroj umožňuje snadné vyhledávání událostí bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce.	ANO Nástroj umožňuje snadné a intuitivní vyhledávání událostí bez nutnosti psaní SQL dotazů nebo programování. Vyhledávání probíhá prostřednictvím grafického rozhraní, kde lze využít interaktivní filtry, fulltextové vyhledávání, přednastavené šablony nebo dynamické vizualizační prvky. Uživatelé tak mohou efektivně analyzovat a třídit události podle typu, času, zdroje, IP adresy, uživatele nebo dalších atributů i bez znalosti dotazovacího jazyka.
Nástroj umožňuje rychlé vyhledávání na základě fulltext indexace (vyhledávaní bez nutnosti tvorby parserů), tzn. že velké objemy dat se neprohledávají formou „grep like“ prohledávání po řádcích.	ANO Nástroj podporuje rychlé vyhledávání díky integrované fulltextové indexaci všech přijatých logů a událostí. To znamená, že i velké objemy dat lze prohledávat bez nutnosti předchozího parsování a bez zdlouhavého lineárního „grep-like” prohledávání po řádcích. Uživatel může okamžitě vyhledávat jakýkoliv výraz nebo hodnotu v celém datovém souboru a výsledky jsou vraceny v reálném čase.

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

Nástroj umožňuje unifikované vyhledávání napříč všemi typy uložených dat (filtrování).	ANO Nástroj umožňuje unifikované vyhledávání napříč všemi typy uložených dat bez ohledu na jejich původní formát nebo zdroj. Díky jednotné datové struktuře a automatické indexaci lze vyhledávat a filtrovat události podle libovolných atributů – například časového razítka, typu události, zdroje logu, IP adresy, uživatele, výsledku operace a dalších. Vyhledávání je možné kombinovat s logickými operátory, přednastavenými filtry i vlastními dotazy.
Nástroj obsahuje reportovací nástroj se sadou přednastavených reportů a možností vlastních úprav a vytvoření nových pohledů a reportů.	ANO Nástroj obsahuje integrovaný reportovací nástroj, který je dodáván se sadou přednastavených reportů pokrývajících běžné scénáře bezpečnostního a provozního dohledu. Uživatelé mají možnost tyto reporty upravovat, přizpůsobovat svému prostředí nebo vytvářet zcela nové pohledy a výstupy dle vlastních požadavků. Reporty lze generovat automaticky dle plánu nebo ad-hoc, exportovat do běžných formátů (PDF, HTML, CSV, XLS) a distribuovat určeným adresátům. Vše je dostupné přímo z centrální webové konzole.
Prezentace dat musí být proveditelná v grafické podobě, prezentační rozhraní musí být multiplatformní nebo platformě nezávislé a plně funkční na platformách Windows, Linux, Apple OSX.	ANO Prezentace dat v nástroji je dostupná v plně grafické podobě prostřednictvím interaktivních dashboardů, tabulek, grafů a vizualizačních prvků. Prezentační rozhraní je platformově nezávislé – jedná se o webové rozhraní, které je plně funkční na všech běžných operačních systémech včetně Windows, Linux a macOS. Není nutná žádná instalace klientských komponent, vše je dostupné přes standardní webový prohlížeč.
Nástroj obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění.	ANO Nástroj obsahuje předpřipravené pohledy na uložená data, které jsou rozděleny jak podle kategorií zdrojových zařízení (např. firewall, IDS/IPS, operační systémy, aplikace), tak i podle logického členění (např. autentizace, síťové události, správa systémů, bezpečnostní incidenty). Tyto pohledy umožňují rychlou orientaci v datech, usnadňují analýzu a poskytují uživatelům relevantní výstupy bez nutnosti ruční konfigurace. Pohledy lze dále přizpůsobovat a ukládat pro opakované použití.

Nástroj zajišťuje automatické spouštění definovaných reportů (měsíčně, týdně, denně, nebo v definovaném čase), ukládání na síťové úložiště a jejich zasílání e-mailem přímo ze systému.	ANO Nástroj umožňuje plně automatizované spouštění definovaných reportů v pravidelných intervalech – denně, týdně, měsíčně nebo v přesně definovaném čase. Reporty lze po vygenerování automaticky ukládat na zvolené síťové úložiště (např. NAS, SMB share) a zároveň je distribuovat e-mailem přímo ze systému vybraným adresátům.
Nástroj podporuje i automatizuje průběžné aktualizace reportů a pohledů výrobcem.	ANO Nástroj podporuje a automatizuje průběžné aktualizace předpřipravených reportů a analytických pohledů výrobcem. Tyto aktualizace reflektují aktuální bezpečnostní hrozby, nové technologie a změny v logovacích formátech. Aktualizace mohou být aplikovány automaticky nebo podle nastavené politiky správcem systému a umožňují tak udržovat obsah nástroje stále aktuální bez nutnosti ručního zásahu.
Nástroj umožňuje vytvářet reporty ve formátech PDF, HTML a CSV, popř. dalších.	ANO Nástroj umožňuje vytváření a export reportů ve formátech PDF, HTML a CSV a dalších.
Nástroj umožňuje zobrazení přehledu o využití diskového prostoru v interním úložišti nástroje.	ANO Nástroj poskytuje přehledné zobrazení o využití diskového prostoru v interním úložišti nástroje. Uživatelé mají k dispozici grafické rozhraní, ve kterém lze sledovat aktuální stav využití úložiště, historický vývoj spotřeby, predikce budoucího zaplnění a rozdělení podle jednotlivých komponent, zdrojů logů nebo typů dat.
Nástroj podporuje export vybraných dat přes rozhraní centrální konzole.	ANO Nástroj umožňuje export vybraných dat přímo z centrální konzole. Uživatel si může zvolit konkrétní časový rozsah, datové zdroje nebo filtry a následně exportovat výsledná data ve zvoleném formátu (např. CSV, JSON, PDF). Export je dostupný jak pro jednotlivé události, tak pro výsledky vyhledávání, reporty nebo analytické výstupy. Tento proces je plně integrovaný do GUI a nevyžaduje žádné externí nástroje.
Nástroj podporuje export a sdílení log dat v originálním i ve strukturovaném tvaru.	ANO Nástroj podporuje export a sdílení log dat jak v jejich originálním (raw) tvaru, tak i ve strukturované podobě po normalizaci. Uživatelé si mohou zvolit formát exportu podle potřeby – například pro forenzní analýzu lze využít surová data, zatímco pro další zpracování nebo integraci je možné využít strukturovaný výstup (např. CSV, JSON). Export lze provádět ručně i automatizovaně.

Nástroj umožňuje anonymizovat některá vybraná pole (sloupce). Např. z důvodu ochrany citlivých informací, osobních údajů apod. Jejich neanonymizovaná hodnotu je možné zobrazit přímo ve výsledcích vyhledávání pouze vybraným uživatelům s oprávněním k této činnosti.	ANO Nástroj umožňuje anonymizaci vybraných polí (např. uživatelských jmen, IP adres, e-mailů) s cílem chránit citlivé nebo osobní údaje v souladu s legislativními požadavky (např. GDPR). Anonymizovaná data jsou zobrazena všem uživatelům, kteří nemají oprávnění pro přístup k původním hodnotám. Neanonymizovaná (dešifrovaná) hodnota se zobrazí pouze uživatelům s odpovídajícími přístupovými právy, přímo ve výsledcích vyhledávání nebo analytických náhledech.
Nástroj musí nabízet sadu algoritmů pro deidentifikaci dat za účelem odstranění osobních informací z přijímaných logů. Požadované možnosti jsou: pseudoanynimizace, anonymizace, šifrování, maskování dat a šifrování se zachováním formátu (FPE).	ANO Nástroj podporuje pokročilé techniky deidentifikace dat přímo při zpracování logů. K dispozici jsou funkce pro pseudonymizaci, anonymizaci, šifrování, maskování i šifrování se zachováním formátu (FPE – Format Preserving Encryption). Tyto metody umožňují efektivní odstranění nebo ochranu osobních a citlivých údajů obsažených v datech. Deidentifikaci lze nastavit selektivně pro vybraná pole, přičemž přístup k původním hodnotám je možný pouze pro uživatele s příslušným oprávněním. Vše probíhá automatizovaně dle předem definovaných pravidel bez nutnosti zásahu výrobce.
Nástroj umožňuje drill-down prohlížení logů a eventů a identifikovaných stavů přímo překlikem z jednotlivých položek dashboardu	ANO Nástroj umožňuje plnohodnotné drill-down prohlížení logů, událostí a identifikovaných stavů přímo z jednotlivých vizuálních prvků na dashboardu. Uživatel může kliknutím na konkrétní položku grafu, tabulky nebo jiné vizualizace okamžitě přejít na podrobné zobrazení souvisejících událostí nebo surových logů. Tato funkce zajišťuje rychlý a efektivní přechod z agregovaných přehledů do detailní analytiky bez nutnosti složitého vyhledávání.
Řešení poskytuje analýzu dlouhodobých trendů událostí (vč. reportingu) v rozsahu dvou let.	ANO Nástroj umožňuje analýzu dlouhodobých trendů událostí včetně tvorby přehledných vizualizací a reportů na základě historických dat v rozsahu minimálně dvou let. Díky optimalizovanému způsobu ukládání, archivace a indexace dat je možné efektivně vyhodnocovat vývoj událostí v čase, identifikovat opakující se vzory nebo odchylky a vytvářet dlouhodobé statistiky pro auditní a bezpečnostní účely. Vše je dostupné přímo z centrální konzole, bez nutnosti dodatečného importu dat.

Nástroj obsahuje monitor právě přijímaných logů (tzv. tail -f), který průběžně a v reálném čase zobrazuje příchozí logy včetně možnosti filtrování podle všech atributů obsažených v logových datech.	ANO Nástroj obsahuje nástroj pro sledování právě přijímaných logů v reálném čase, který je známý jako příkaz tail -f. Tento náhled umožňuje průběžné zobrazení příchozích událostí tak, jak do systému přicházejí, a zároveň nabízí možnost okamžitého filtrování podle libovolných atributů obsažených v datech, jako je například zdroj, typ události, IP adresa nebo časová značka. Funkce je plně integrovaná do centrálního rozhraní a slouží jak pro online monitoring, tak i pro operativní analýzu incidentů.
Nástroj poskytuje světlý a tmavý režim zobrazení pro uživatele kvůli větší ergonomice uživatelské práce.	ANO Nástroj nabízí přepínatelné uživatelské rozhraní ve světlém i tmavém režimu. Každý uživatel si může individuálně zvolit vzhled rozhraní přímo v nastavení svého profilu.

Detekce

Minimální požadavky	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
Nástroj umožňuje detekce bezpečnostních hrozeb v reálném čase pomocí detekčních pravidel.	ANO Nástroj umožňuje detekci bezpečnostních hrozeb v reálném čase prostřednictvím pokročilého systému detekčních pravidel. Tato pravidla lze definovat na základě libovolných parametrů logovaných událostí, jako jsou IP adresy, porty, typy činností, časové souvislosti nebo sekvence událostí. Detekce probíhá okamžitě při příjmu události, což umožňuje rychlou reakci na potenciální incidenty. Pravidla lze upravovat, rozšiřovat a automatizovat bez nutnosti programování a lze je kombinovat s funkcemi enrichmentu a kategorizace pro vyšší přesnost detekce.
Detekční pravidla jsou dodávány výrobcem nástroje a to průběžně, pomocí online aktualizace.	ANO Nástroj je dodáván se sadou předdefinovaných detekčních pravidel, která jsou průběžně aktualizována výrobcem prostřednictvím online aktualizačního mechanismu. Tento systém zajišťuje, že nástroj reaguje na nové typy bezpečnostních hrozeb a techniky útočníků v reálném čase bez nutnosti manuálního zásahu. Aktualizace pravidel probíhá bezpečným způsobem a je plně integrována do správy systému, přičemž si uživatelé mohou zvolit, zda nové detekce aplikovat automaticky, nebo je nejprve ručně zkontrolovat a upravit.

Uživatel si může tvořit vlastní bezpečnostní pravidla, jakožto i uzpůsobovat pravidla dodávaná výrobcem.	ANO Nástroj umožňuje uživatelům vytvářet vlastní detekční pravidla pro identifikaci bezpečnostních hrozeb dle specifických potřeb prostředí. Kromě toho lze libovolně upravovat a rozšiřovat pravidla dodávaná výrobcem, a to prostřednictvím intuitivního editoru pravidel dostupného v centrálním rozhraní. Práce s pravidly nevyžaduje pokročilé programátorské dovednosti a je doplněna nástroji pro jejich testování a validaci, čímž se minimalizuje riziko chyb a zajišťuje vysoká flexibilita při nastavování bezpečnostní politiky.
Detekce jsou minimálně následujících typů: • Detekce na základě obsahu jednotlivých políček logu nebo jejich kombinací. • Detekce v časovém okně (tzv. korelace), tj takové, které sdružují (agregují) události pro specifikovaný sledovaný objekt (uživatele, IP adresu, hosta atd.) v časovém rozsahu. • Detekce anomálií s využitím mechanismů zdrojového učení. • Detekce s použitím Threat Intelligence vstupů, konkrétně IP adresy, hashe souborů, obsahy příkazových řádek a URL	ANO Nástroj podporuje detekci hrozeb v reálném čase prostřednictvím několika typů detekčních mechanismů, které pokrývají široké spektrum scénářů. Prvním typem je detekce na základě obsahu jednotlivých polí logu nebo jejich kombinací, která umožňuje identifikaci konkrétních hodnot či vzorců v datech. Druhým typem jsou korelační detekce v časovém okně, které analyzují posloupnosti událostí v rámci definovaného intervalu a sledovaného objektu (např. uživatel, IP adresa, zařízení). Nástroj dále nabízí detekci anomálií využívající mechanismy strojového učení pro identifikaci neobvyklého chování oproti historickým vzorcům. Posledním typem jsou detekce založené na Threat Intelligence datech – např. indikátory kompromitace jako IP adresy, hash hodnoty souborů, příkazy či URL adresy, které systém automaticky porovnává se vstupy z důvěryhodných TI zdrojů. Všechny tyto mechanismy lze kombinovat pro zvýšení přesnosti a snížení počtu falešných poplachů.
Detekce je možno řetězit, tj. vystup jedné detekce lze použít v jiné detekci.	ANO Nástroj umožňuje řetězení detekcí, kdy výstup jednoho detekčního pravidla (např. alert nebo označená událost) lze využít jako vstup pro další detekční pravidlo. Tento mechanismus umožňuje vytvářet vícevrstvé, pokročilé detekční scénáře, kde lze například sledovat následné aktivity po detekované události nebo eskalovat incidenty na základě kombinace různých typů chování.

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

Výstupy detekce lze odesílat emailem, nástrojem Slack, Microsoft Teams nebo pomocí protokolu Syslog do nástrojů třetích stran.	ANO Výstupy detekcí v nástroji lze automaticky odesílat prostřednictvím několika komunikačních kanálů. Podporováno je zasílání e-mailových notifikací s možností vlastního formátování zprávy a využitím proměnných z detekované události. Dále je možné odesílat upozornění do nástrojů pro týmovou spolupráci jako Slack a Microsoft Teams, a to pomocí integrovaných konektorů nebo webhooků. Výstupy detekcí je rovněž možné předávat pomocí protokolu Syslog (včetně šifrovaného přenosu) do dalších SIEM nebo bezpečnostních nástrojů třetích stran.
Detekce dále mohou zakládat alerty v alert managementu.	ANO Detekce v nástroji mohou automaticky zakládat alerty v integrovaném systému pro správu alertů (alert management). Každý alert je vytvářen na základě detekčního pravidla a obsahuje veškeré potřebné informace pro jeho rychlé vyhodnocení a eskalaci – například čas události, dotčený systém nebo uživatele, závažnost a detailní popis. Alerty lze dále kategorizovat, přiřazovat konkrétním uživatelům nebo týmům a sledovat jejich stav v rámci celého životního cyklu incidentu.
Detekce mohou spouštět uživatelem definované scripty za účelem automatizace.	ANO Detekce v nástroji podporují spouštění uživatelsky definovaných skriptů, což umožňuje ANO vysokou míru automatizace reakce na bezpečnostní události. Při splnění podmínek detekčního pravidla může systém automaticky vykonat předdefinovaný skript, který může například upravit konfiguraci zařízení, izolovat koncový bod, upozornit další systém, vytvořit záznam v helpdesku nebo provést jakoukoli jinou akci dle definice. Skripty je možné psát v podporovaných jazycích (např. Bash, PowerShell nebo Python) a jejich spouštění je zabezpečeno pomocí kontrol oprávnění a auditovatelnosti každého provedení.

Nástroj obsahuje grafický nástroj pro tzv. Machine Learning, tj. vyhodnocování dat s využitím pokročilých matematických analýz, typicky využívající historická data uložená v systému.	ANO Nástroj obsahuje integrovaný grafický nástroj pro strojové učení (Machine Learning), který umožňuje analýzu dat pomocí pokročilých matematických a statistických metod. Tento nástroj využívá historická data uložená v systému k trénování modelů pro detekci anomálií, identifikaci neobvyklého chování a predikci budoucích hrozeb. Uživatelé mohou snadno vytvářet, upravovat a vizualizovat modely prostřednictvím intuitivního grafického rozhraní bez nutnosti pokročilého programování. Součástí jsou i šablony a předpřipravené scénáře, které urychlují nasazení pokročilé analytiky do provozu. Výsledky analýz lze následně propojit s detekčními pravidly a automatizačními nástroji systému.
Detekce anomálií musí být schopná využívat existující historické logy a jiné události pro stanovení běžných vzorů chování a ty pak aplikovat na aktuální vstupy. Odchylky jsou indikovány jako nálezy detekce.	ANO Detekce anomálií v nástroji je schopna využívat historických logů a událostí ke stanovení běžných vzorů chování (tzv. baseline). Tyto vzory jsou dynamicky vytvářeny pomocí strojového učení a statistických analýz bez nutnosti ručního nastavování prahových hodnot. Systém následně tyto vzory aplikuje na aktuální příchozí data v reálném čase a v případě detekce významných odchylek generuje nálezy (detections), které mohou být dále využity k tvorbě alertů nebo jako vstupy do dalších automatizačních nebo analytických procesů.
Nástroj musí detekovat provoz z tzv. exit uzlů známých VPN poskytovatelů	ANO Nástroj obsahuje podporu pro detekci provozu z tzv. exit uzlů známých VPN poskytovatelů. Tento typ provozu je identifikován prostřednictvím Threat Intelligence databází, které jsou průběžně aktualizovány a obsahují seznamy IP adres používaných VPN službami. Detekční pravidla pak porovnávají IP adresy v přijatých událostech s těmito seznamy a v případě shody generují příslušné nálezy.
Nástroj musí detekovat aktivitu z IP adres, které jsou označeny jako nebezpečné. Seznam nebezpečných IP adres poskytuje průběžně výrobce nástroje.	ANO Nástroj podporuje detekci aktivity z IP adres, které jsou označeny jako nebezpečné. Seznam těchto IP adres je součástí Threat Intelligence feedu, který je průběžně aktualizován výrobcem nástroje. Při příjmu událostí jsou IP adresy automaticky porovnávány s tímto seznamem, a v případě shody je událost označena, klasifikována a zpracována podle příslušného detekčního pravidla.

Nástroj musí umožňovat nasazení detekcí založených na Sigma pravidlech, https://github.com/SigmaHQ/sigma	ANO Nástroj plně podporuje nasazení detekcí založených na pravidlech Sigma. Umožňuje import a převod pravidel ve formátu definovaném iniciativou SigmaHQ do nativní podoby detekčního systému. Pravidla lze zároveň doplnit o vlastní enrichments nebo napojit na výstupy alertingu, včetně automatických akcí.

Funkčnost systému

Minimální požadavky	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL

centrální management:
• umožňuje správu sběru logů, distribuci a oprávnění v rámci logování jednotlivých zdrojů
• umožňuje provádění analýz, reportingů a diagnostiky Systému
• umožňuje správu všech komponent a administrativních funkcí ve webovém uživatelském rozhraní
• umožňuje poskytování interní kontroly stavu Systému a upozornění uživatele v případě problému
• možnost ladění upozornění, alertů a vlastních parserů
• sofistikované vyhledávací funkce včetně možnosti rozčlenění vyhledaných dat až na detailní úroveň všech typových polí dostupných ze zdroje událostí
  ○ způsob zadávání vyhledávání: vyhledávací rozhraní musí poskytovat podporu jak pro zadání dotazu s použitím Booleovské logiky, tak i pro regulární výrazy
  ○ poskytování rozhraní pro reporting, pomocí kterého lze vytvářet nové reporty bez vlivu na již existující
	ANO Nástroj splňuje vše zde uvedené.

procesně vícestupňová aktualizace s podporou testování aktualizované verze před přechodem do produkčního provozu, a to bez přerušení provozu Systému a bez ztráty dat v jakékoliv jeho části	ANO
všechna pole vyparsovaná z logů musejí být indexovaná	V ANO šechna pole vyparsovaná z logů jsou indexovaná.
generování alertu při výpadku logů z konkrétního zdroje	ANO Systém vygeneruje alert při výpadku logů z konkrétního zdroje.

schopnost odesílat nasbírané logy na více míst ke zpracování najednou	ANO Systém má schopnost odesílat nasbírané logy na více míst ke zpracování najednou.
Systém musí detekovat anomálie v příjmu logů (výpadek logů, větší než obvyklé množství logů, anomální počty chybových úrovní atp) a to v reálném čase, na základě predikcí průběžně vytvářených z historických dat	ANO Systém detekuje anomálie v příjmu logů (výpadek logů, větší než obvyklé množství logů, anomální počty chybových úrovní atp) a to v reálném čase, na základě predikcí průběžně vytvářených z historických dat
Systém musí podporovat tmavý a světlý mód uživatelského rozhraní pro dobrou ergonomii práce s nástrojem v různých světelných podmínkách	ANO Systém podporuje tmavý a světlý mód uživatelského rozhraní pro dobrou ergonomii práce s nástrojem v různých světelných podmínkách.
Logy v archivu je možné prohledávat pomocí standardních možností z příkazové řádky bez nutnosti je importovat zpět do Systému	ANO Logy v archivu je možné prohledávat pomocí standardních možností z příkazové řádky bez nutnosti je importovat zpět do Systému.

Konfigurace a integrace

Minimální požadavky	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
Zadavatel požaduje provedení instalace, implementace, integrace včetně napojení na Zdroje, montáže a konfigurace Systému tak, aby bylo plně provozuschopné v síťové infrastruktuře zadavatele.	ANO Dodavatel provede instalaci, implementaci, integraci včetně napojení na Zdroje, montáže a konfigurace Systému tak, aby byl plně provozuschopný v síťové infrastruktuře zadavatele.
Zadavatel dále požaduje, aby Systém splňoval následující požadavky:	
Systém musí podporovat napojení na SIEM systém bez nutnosti rozšiřovat licenci Systému nebo významné rekonfigurace Systému	ANO
Systém musí podporovat rychlé a snadné získávání "raw" logů z archivu v podobě souborů (a to i v případě nefunkčnosti Systému) a jejich následné načtení do technologií na práci s historickými daty.	ANO
Archiv logů musí být dostupný i v případě nedostupnosti systému.	ANO
Archivace se řídí konfigurovatelnou retenční politikou	ANO
Retenční politiku archivace logů lze konfigurovat odlišnou pro různé typy logů	ANO
Systém musí podporovat integraci s adresářovým systémem Microsoft AD/LDAP pro potřeby autentizace a autorizace uživatelů, přičemž součástí požadavku je rovněž, aby Systém musí tyto funkce podporovat včetně funkcí SSO a vícefaktorové autentizace	ANO
Vyžaduje se zejména vícefaktorová autentikace pomocí hardwarového tokenu případně pomocí hardwarového klíče v mobilním telefonu podle specifikace FIDO2	ANO

Systém musí podporovat zabezpečení kryptografickými algoritmy pro uživatelská hesla pro lokální účty uložená v Systému	ANO
Použité algoritmy musí splňovat platné požadavky NÚKIB na tyto algoritmy	ANO

Podpora provozu

Minimální požadavky	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
Dodavatel musí v rámci placené podpory Systému poskytovat pravidelné profylaktické prohlídky a to nejméně jedenkrát měsíčně. Výstupem profylaktické prohlídky je souhrnná zpráva o stavu systému doplněná o případné nálezy a nápravná opatření	V rámci placené podpory Systému budou poskytovány pravidelné profylaktické prohlídky a to nejméně jedenkrát měsíčně. Výstupem profylaktické prohlídky bude souhrnná zpráva o stavu systému doplněná o případné nálezy a nápravná opatření.
Dodavatel v rámci placené podpory Systému implementuje nápravná opatření, v součinnosti se Zadavatelem	ANO
Dodavatel rámci placené podpory Systému nasazuje nové verze Systému.	ANO
Aktualizace nástroje musí být distribuovány online	ANO
Podpora výrobce je požadována na období 60 měsíců	ANO

2.a. Akceptační kritéria

Akceptace proběhne v souladu s příslušným ustanovením smlouvy a dodavatel mj. dodá pokročilý nástroje pro správu logů (log management), zajišťujícího automatizovaný sběr, normalizaci a archivaci provozních i bezpečnostních záznamů ze všech relevantních infrastrukturních i aplikačních systémů. Systém využije metody strojového učení k přesnému parsování a klasifikaci, zajistí ochranu uložených logů proti neoprávněným změnám i při archivaci a umožní kompresi archivovaných logů na úroveň nejvýše 10% jejich původní velikosti.

Akceptace je dokončena podpisem předávacího protokolu potvrzujícího, že nástroj pro správu logů splňuje požadavky uvedené níže.

Specifikace pro naplnění parametrů

Akceptační kritérium	Způsob ověření	Výsledek	Poznámka / Podpis
Rychlé vícekriteriální vyhledávání napříč zdroji	Demonstrace funkčního vyhledávání v datech ze všech relevantních zdrojů, včetně logů z komprimovaného archivu		
Reportovací a notifikační systém	Ověření generování reportů a notifikací při provozních a bezpečnostních událostech		
Příjem a zpracování logů z definovaných zdrojů	Praktická demonstrace sběru a zpracování logů ze stanovených infrastrukturních a aplikačních systémů		
Vyhledávání v historických	Test vyhledávání konkrétních záznamů v archivovaných a komprimovaných logech		

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

archivovaných datech			
Neměnnost uložených záznamů	Ověření integrity a nemožnosti neoprávněných změn uložených logů		
Předání provozní dokumentace	Dodání a kontrola úplnosti dokumentace architektury, konfigurace a provozních postupů		

3. Specifikace služeb technické podpory dodavatele na 60 měsíců od 1. 6. 2026 do 31.5.2031.

Specifikace služeb technické podpory je uvedena v samostatném dokumentu:

- 01 – Technická specifikace – Společná definice technické podpory pro ID01 – ID09

Zadavatel tímto výslovně stanoví, že nepožaduje žádnou záruku nad rámec a mimo rozsah technické podpory vymezený v tomto dokumentu a dokumentu „01 – Technická specifikace – Společná definice technické podpory pro ID01 – ID09“ (dále jen „Společná definice“). Veškeré záruční povinnosti dodavatele, včetně úrovní služeb, reakčních dob, způsobu eskalace, podmínek dostupnosti, režimu aktualizací, EoL/EoS a výluk plnění, se řídí výlučně tímto dokumentem a Společnou definicí. Jakákoli plnění spočívající v rozvojových zásazích, změnových požadavcích, úpravách nad rámec specifikace či integracích nevyplývajících ze Společné definice nejsou součástí záruky, ledaže budou výslovně sjednána zvláštní smlouvou nebo dodatkem.

V případě rozporu nebo kolizního výkladu mezi touto technickou specifikací a Společnou definicí má přednost tato technická specifikace. Společná definice slouží jako doplňující a výkladový dokument a uplatní se pouze v rozsahu, v němž není v rozporu s touto Technickou specifikací.

3.a. Akceptační kritéria

Dodavatel se zavazuje poskytovat technickou podporu v rozsahu a za podmínek stanovených tímto dokumentem a Společnou definicí po dobu od 1. 6. 2026 do 31. 5. 2031 (60 měsíců). Dodavatel podpisem smlouvy stvrzuje, že po uvedené období bude plnit sjednané SLA a ostatní povinnosti dle tohoto dokumentu a Společné definice; nesplnění těchto povinností bude posuzováno jako porušení smlouvy se všemi z toho vyplývajícími právními následky podle smlouvy a příslušných právních předpisů.

8.1.9. ID09 - Automatická, periodická kontrola stavu bezpečnosti IT systémů a aplikací

1. Úvod a metodika

Tento dokument definuje předmět a závaznou technickou specifikaci pro nasazení a zprovoznění systému řízeného vulnerability managementu zahrnujícího periodické automatizované prověřování stavu bezpečnosti komponent infrastruktury (interní i externí testování), správu zjištěných zranitelností po celý jejich životní cyklus a reporting pro potřeby řízení nápravných opatření. Řešení bude schopno zahrnout i zařízení bez tradičního operačního systému, která nepodporují instalaci agentů.

Součástí plnění je definice plánů a periodicity skenů, nastavení prioritizace dle rizika, napojení na stávající procesy a nástroje (např. ticketing, SOC/SIEM) a předání provozní dokumentace. Akceptace proběhne doložením běhu pravidelných skenů, přehledů zranitelností a jejich stavu, metrik doby nápravy a funkční integrace do procesů řízení bezpečnostních incidentů a změn.

2. Specifikace dodávaného hardware, software a služeb instalace, implementace a školení

Dodavatel vyplní následující tabulku specifikace nabízeného plnění. Ve sloupci „Splnění parametrů dodavatele – DOPLNÍ DODAVATEL“ dodavatel doplní:

- ANO/NE v závislosti na tom, zda nabízené plnění či jeho část požadavek zadavatele splňuje/nesplňuje,
- specifikaci konkrétního parametru či popis naplnění požadavku zadavatele,
- číselnou hodnotu v případě požadavku zadavatele, který obsahuje číselně vyjádřitelný parametr
- přesnou specifikaci HW, SW nebo služby
- volitelně odkaz na dodavatelem přiložený dokument ve formátu PDF

Je požadována dodávka a implementace SW pro automatické, periodické testování, níže jsou uvedené minimální parametry, které musí splňovat.

Parametr	Minimální požadavky	Splnění parametrů dodavatele – DOPLNÍ DODAVATEL
Rozsah	Řešení musí podporovat monitoring do 700 zařízení bez omezení počtu skenovaných IP	**ANO**, 700+ cílů je reálných dle profilu skenů/HW.
Implementace	Dodavatel musí zajistit kompletní instalaci a implementaci v místě instalace	**ANO**, lokální instalace Windows/Linux/macOS a rychlý deploy.
Automatizované skenování	Řešení musí provádět pravidelné automatizované vyhledávání známých zranitelností (CVE) ve vnitřních i vnějších systémech a využívat aktuální databáze zranitelností	**ANO**, *plánovač + auto-update pluginů (aktuální CVE) pro interní i externí cíle.*
Agentless i agent-based režim	Řešení musí podporovat skenování zařízení bez OS nebo bez možnosti instalace agentů (např. tiskárny, UPS, IP kamery) i možnost autentizovaných skenů	**ANO**, credentialed/agentless skeny včetně bez-OS zařízení.

Správa zranitelností	Řešení musí umožňovat evidenci nalezených zranitelností po celý životní cyklus, klasifikaci dle závažnosti (CVSS) a poskytovat doporučení k nápravě včetně prioritizace	**ANO**, detekce, CVSS a doporučení.
Reportování a vizualizace	Řešení musí poskytovat generování přehledů a dashboardů o zranitelnostech, export výsledků do formátů PDF, HTML, CSV, XML a podporovat přehledné seskupování výsledků	**ANO**, export HTML/CSV/XML/PDF a dashboardy.
Integrace s ticketovacím systémem	Řešení musí umožnit přímé vytváření úkolů v ticketovacím systému, sledování jejich řešení a napojení na SOC/SIEM a případně patch management	**ANO**, napojení přes export/API na ticketing/SIEM/patch management.
Soulad se standardy	Řešení musí být v souladu s ISO/IEC 27002 (řízení technických zranitelností) a NIST SP 800-40; musí podporovat auditní šablony a compliance frameworky	**ANO**, audit šablony (CIS/DISA) a compliance reporting.
Bezpečnostní a provozní požadavky	Řešení musí umožnit definici plánů a periodicity skenů, nastavení prioritizace dle rizika, eskalační postupy pro závažné nálezy a zajištění ochrany osobních údajů	**ANO**, plánování, periodicita, prioritizace skenů pro eskalaci.
Provozní dokumentace	Dodavatel musí dodat kompletní provozní dokumentaci systému včetně návrhu, konfigurace a provozu	**ANO**, instalační a provozní dokumentace (postupy) dodáme.
Pokrytí technologií	Řešení musí podporovat skenování OS, databází, síťových prvků, hypervizorů, cloudových prostředí a ICS/SCADA	**ANO**, OS/DB/síť/hypervizory/cloud/ICS, SCADA
Automatické aktualizace	Řešení musí obsahovat mechanismus pravidelných a automatických aktualizací knihovny pluginů a detekčních pravidel	**ANO**, automatické aktualizace pluginů (online nebo přes interní mirror).
Detekce malwaru a botnetů	Řešení musí být schopno identifikovat škodlivé procesy, podezřelé komunikace a indikátory kompromitace (IoC)	**ANO**, indikace známých IoC/misconfig a podezřelých bannerů apod.
Auditní šablony	Řešení musí podporovat využití a úpravu auditních šablon pro různé standardy a umožnit přidání vlastních pluginů	**ANO**, úprava .audit a vlastní kontroly/NASL v mezích Pro.
Skórování zranitelností	Řešení musí podporovat více metod hodnocení závažnosti zranitelností (např. CVSS v4, EPSS, VPR) pro efektivní prioritizaci	**ANO**, CVSS v2/v3//EPSS/VPR.
Seskupování výsledků	Řešení musí poskytovat možnost seskupování nalezených zranitelností pro snadnější přehled a rychlejší analýzu	**ANO**, filtry, group-by řazení, různé pohledy na data.
Škálovatelnost a mobilita	Řešení musí umožňovat snadné přenášení licence a škálování nasazení (od malých prostředí až po rozsáhlou infrastrukturu)	**ANO**, licenci lze přesunout. Škálovatelnost na úrovni skenování target seznamů a díky přenositelnosti řešení.

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

2.a. Akceptační kritéria

Akceptace proběhne v souladu s příslušným ustanovením smlouvy a dodavatel mj. zajistí implementaci systému řízeného vulnerability managementu zahrnujícího periodické automatizované prověřování stavu bezpečnosti komponent infrastruktury (interní i externí testování), správu zjištěných zranitelností po celý jejich životní cyklus a reporting pro potřeby řízení nápravných opatření. Řešení bude schopno zahrnout i zařízení bez tradičního operačního systému, která nepodporují instalaci agentů.

Akceptační parametry

Akceptační kritérium	Způsob ověření	Výsledek	Poznámka / Podpis
Nasazení a zprovoznění systému vulnerability managementu	Ověření funkčnosti systému v prostředí zadavatele		
Periodické automatizované skeny infrastruktury (interní i externí)	Doložení běhu pravidelných skenů a jejich výsledků		
Správa zjištěných zranitelností po celý životní cyklus	Kontrola evidence zranitelností a jejich stavů		
Reporting pro řízení nápravných opatření	Předložení přehledů a reportů o zranitelnostech		
Podpora zařízení bez OS (bez agentů)	Ověření funkčnosti skenů zařízení bez možnosti instalace agentů		
Definice plánů a periodicity skenů	Kontrola nastavení harmonogramů a plánů skenů		
Prioritizace dle rizika	Ověření nastavení prioritizace v systému		
Integrace s procesy a nástroji (ticketing, SOC/SIEM)	Ověření funkční integrace se stávajícími nástroji		
Provozní dokumentace	Doložení a kontrola úplnosti provozní dokumentace		
Metriky doby nápravy	Kontrola reportů s metrikami doby řešení zranitelností		
Integrace do procesů řízení incidentů a změn	Ověření funkčnosti v rámci řízení bezpečnostních incidentů a změn		

3. Specifikace služeb technické podpory dodavatele na 60 měsíců od 1. 6. 2026 do 31.5.2031.

Specifikace služeb technické podpory je uvedena v samostatném dokumentu:

- 01 – Technická specifikace – Společná definice technické podpory pro ID01 – ID09

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

Zadavatel tímto výslovně stanoví, že nepožaduje žádnou záruku nad rámec a mimo rozsah technické podpory vymezený v tomto dokumentu a dokumentu „01 – Technická specifikace – Společná definice technické podpory pro ID01 – ID09“ (dále jen „Společná definice“). Veškeré záruční povinnosti dodavatele, včetně úrovní služeb, reakčních dob, způsobu eskalace, podmínek dostupnosti, režimu aktualizací, EoL/EoS a výluk plnění, se řídí výlučně tímto dokumentem a Společnou definicí. Jakákoli plnění spočívající v rozvojových zásazích, změnových požadavcích, úpravách nad rámec specifikace či integracích nevyplývajících ze Společné definice nejsou součástí záruky, ledaže budou výslovně sjednána zvláštní smlouvou nebo dodatkem.

V případě rozporu nebo kolizního výkladu mezi touto technickou specifikací a Společnou definicí má přednost tato technická specifikace. Společná definice slouží jako doplňující a výkladový dokument a uplatní se pouze v rozsahu, v němž není v rozporu s touto Technickou specifikací.

3.a. Akceptační kritéria

Dodavatel se zavazuje poskytovat technickou podporu v rozsahu a za podmínek stanovených tímto dokumentem a Společnou definicí po dobu od 1. 6. 2026 do 31. 5. 2031 (60 měsíců). Dodavatel podpisem smlouvy stvrzuje, že po uvedené období bude plnit sjednané SLA a ostatní povinnosti dle tohoto dokumentu a Společné definice; nesplnění těchto povinností bude posuzováno jako porušení smlouvy se všemi z toho vyplývajícími právními následky podle smlouvy a příslušných právních předpisů.

8.2. Vlastní popis + Technické listy k nabízeným dodávkám

Veškerý nabízený hardware, software a další komponenty splňují technické požadavky a parametry, které stanovil Zadavatel a které jsou uvedeny v příloze č. 1 zadávací dokumentace.“

01 - Pokročilý síťový monitoring

GREYCORTEX Mendel - NDR - síťový monitoring

Data sheet

https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf

Podmínky podpory

https://partner.greycortex.com/userdocu/900d6aae6d7d4a1aa557fe5f9181823a/support.html

02 - Posílení primárního datového centra – redundance

8x server HPe DL360

Data sheet

https://www.hpe.com/psnow/doc/PSN1010007891USEN.pdf?utm_source=chatgpt.com

Podmínky podpory

https://www.hpe.com/us/en/collaterals/collateral.4aa3-8232enw.html

1x IBM FlashSystem 7300

Data sheet

https://www.ibm.com/products/flashsystem-7300

Podmínky podpory

https://www.ibm.com/docs/en/ssw_ibm_i_72/rzaji/rzajipdf.pdf

03 - Výměna a implementace aktivních síťových prvků

1x Aruba 6405 v2

Data sheet

https://www.hpe.com/psnow/doc/PSN1014613809AUEN.pdf

Podmínky podpory

https://www.hpe.com/us/en/collaterals/collateral.4aa3-8232enw.html

04 - Výměna a implementace WiFi infrastruktury

Komponenty Ubiquiti

Data sheet

1x USW-PRO-AGGREGATION

usw-pro-aggregation_ds.pdf

1x Ubiquiti Ethernet Security_Gateway

https://dl.ubnt.com/datasheets/unifi/UniFi_Security_Gateway_DS.pdf

10x Switch Enterprise 8 PoE

https://dl.ui.com/ds/usw-enterprise-8-poe_ds.pdf

60x WiFiAP U7 Pro Max

https://techspecs.ui.com/unifi/wifi/u7-pro-max

DAC kabel

https://dl.ubnt.com/ds/uacc-dac-sfp_ds.pdf

SFP moduly

https://dl.ubnt.com/datasheets/fiber/U_Fiber_Modules_FiberCable_DS.pdf

Podmínky podpory

https://ui.com/eu/en/ui-care

05 - Výměna a implementace zálohovací infrastruktury

1x server HPe DL320

Data sheet

https://www.hpe.com/psnow/doc/PSN1014696061DKEN

Podmínky podpory

https://www.hpe.com/us/en/collaterals/collateral.4aa3-8232enw.html

1x IBM FlashSystem 7300

Data sheet

https://www.ibm.com/products/flashsystem-7300

2x TS4300 Tape Base

Data sheet

https://www.flashsystemworks.com.au/datasheets/ibm_ts4300_tape_library.pdf

Podmínky podpory

https://www.ibm.com/docs/en/ssw_ibm_i_72/rzaji/rzajipdf.pdf

06 - Zavedení systému řízení kybernetické bezpečnosti včetně sledování a vyhodnocování rizik a atributů na úrovni podpůrných aktiv a výkon role manažera KB

OMIS Open Management for IT Security

Řízení kybernetické bezpečnosti jednoduše a pod kontrolou

Tým OMIS

Na vzniku aplikace se podíleli zkušení vývojáři, odborníci z oblasti kybernetické bezpečnosti, auditoři i specialisté v oblasti práva.

Jsme proaktivní a otevřený tým s více jak 20letou praxí, který najde řešení pro jakoukoli vaši situaci.

Najdeme správné řešení i pro Vás!

Řízení rizik dle standardu NIS2

Nová legislativní úprava promítající EU směrnici **NIS2** vstoupí v platnost **ke konci roku 2024** a nyní je v připomínkovém procesu NÚKIB. Přesto, že je ještě v přípravě, už nyní je jasné, že nová povinnost řídit rizika dopadne na daleko širší okruh subjektů než je tomu nyní. Pro ty je určen systém OMIS, který jednoduchou a přehlednou formou pomůže se zvládnutím této povinnosti a to nejen na startu, ale i během průběžné práce s řízením rizik.

Co je OMIS (Open Management for IT Security)?

Je to SaaS ISMS platforma pro řízení aktiv a rizik **bezpečnostni informací** založená na platných standardech včetně chystané **NIS2**. OMIS vám umožní za měsíční paušál vykonávat celou škálu činností v rámci výkonu **agendy řízení bezpečnosti**. Systém lze využívat v režimu SaaS jako službu nebo jej lze pořídit jako on-premise instalaci.

Proč využívat OMIS?

- **Vybrané procesy informační bezpečnosti budou v souladu s nařízením NIS2, TISAX, DORA i ISO 27001**
- **Efektivně řídíte bezpečností opatření**
- **Elektronické dokumenty pro bezpečnostní auditory na jeden klik**

Další výhody systému OMIS

- Interním zaměstnancům ušetří čas intuitivním naváděním v aplikaci
- Zajistí specialistům spolehlivý zdroj strukturovaných informací pro efektivní řízení SŘBI
- Implementuje bezpečnostní přehled pro management
- Má vaše rizika pod kontrolou
- Zná včas nutné investice
- Provozuje služby i aplikace vycházející z mezinárodně uznávaných standardů a certifikací **CRISC**, **CISA**, **CISM**, **ITIL** a **TOGAF**

Kontaktujte nás

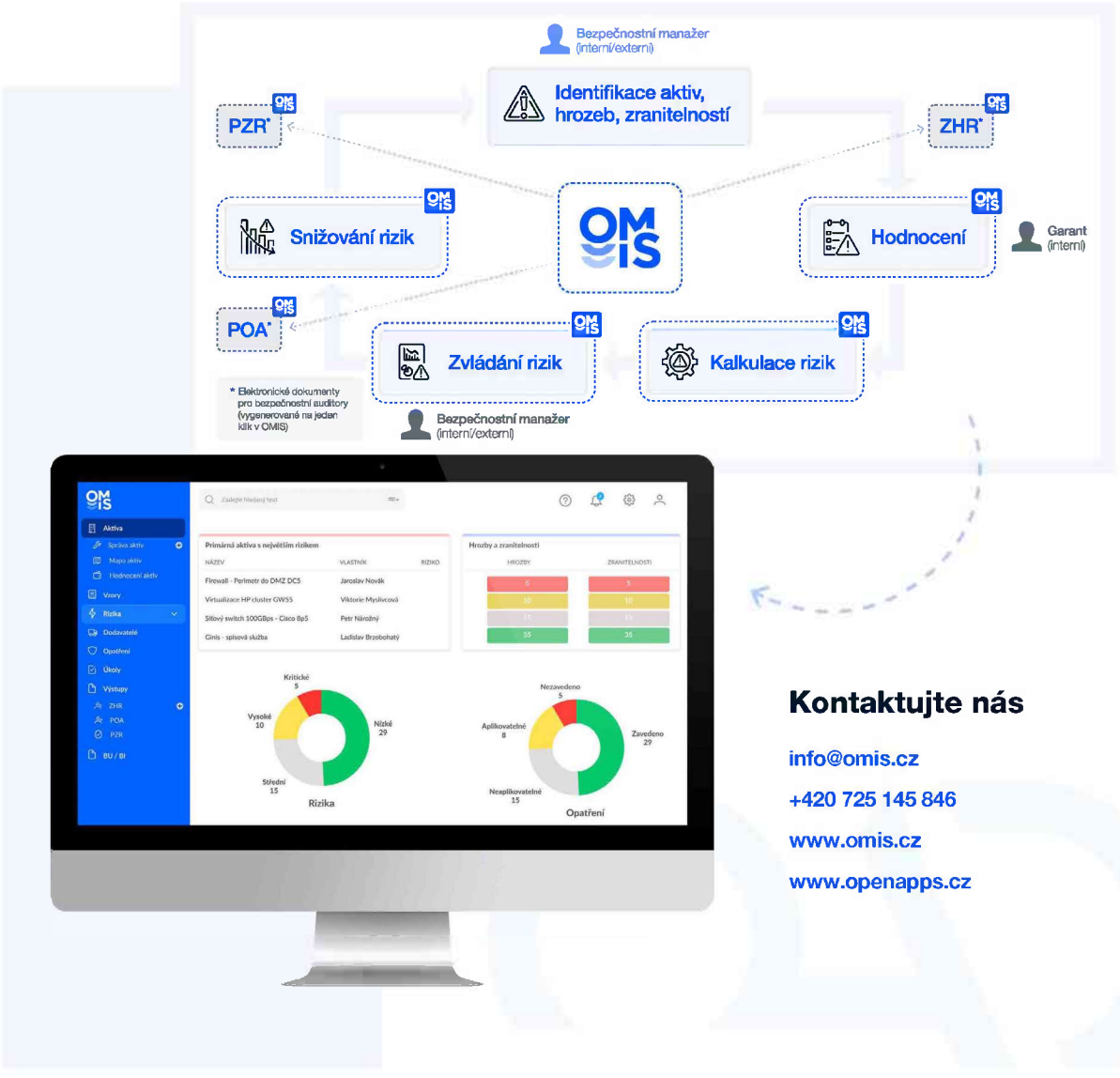
info@omis.cz | +420 725 145 846 | www.omis.cz | www.openapps.cz

OMIS Open Management for IT Security | Řízení kybernetické bezpečnosti jednoduše a pod kontrolou

Klíčové funkce systému OMIS

- Možnost spravovat více organizací
- Napojení na MS AD
- Fuil-Textové vyhledávání
- Auditní záznam změn v podobě transakčního protokolu
- Ukládání kompletní historie evidence včetně logů
- Možnost exportu veškerých záznamů
- Generování PDF dokumentů k evidovaným záznamům
- Vlastní atributy evidovaných objektů
- Generování dokumentů pro bezpečnostní auditory ZHR, POA, PZR*
- Evidence aktiv
- Šablony aktiv
- Mapy aktiv
- Správa dodavatelů
- Správa katalogu hrozeb zranitelností a opatření
- Správa lokalit
- Organizační struktura
- Správa a hodnocení rizik
- Správa a hodnocení opatření

* ZHR – Zpráva z hodnocení rizik, POA – Prohlášení o aplikovatelnosti, PZR – Plán zvládání rizik



Kontaktujte nás

info@omis.cz

+420 725 145 846

www.omis.cz

www.openapps.cz

07 - Firewally pro detašovaná pracoviště

Fortinet

Data sheets

FG 50G:

https://www.fortinet.com/resources/data-sheets/fortigate-fortiwifi-50g-series

FG 70G:

https://www.fortinet.com/resources/data-sheets/fortigate-fortiwifi-70g-series

Forti Manager:

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf

Podmínky podpory

https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-forticare-services.pdf

08 - Kompletní správa životního cyklu logů

TeskaLabs

Data sheet

https://logman.io/en/home/

Podmínky podpory

https://docs.teskalabs.com

09 - Automatická, periodická kontrola stavu bezpečnosti IT systémů a aplikací

Nessus pro

Data sheet

https://www.tenable.com/data-sheets/nessus-professional

Podmínky podpory

https://www.tenable.com/data-sheets/tenable-technical-support-guide

06 - Zavedení systému řízení kybernetické bezpečnosti včetně sledování a vyhodnocování rizik a atributů na úrovni podpůrných aktiv a výkon role manažera KB

OMIS Open Management for IT Security

Řízení kybernetické bezpečnosti jednoduše a pod kontrolou

Tým OMIS

Na vzniku aplikace se podíleli zkušení vývojáři, odborníci z oblasti kybernetické bezpečnosti, auditoři i specialisté v oblasti práva.

Jsme proaktivní a otevřený tým s více jak 20letou praxí, který najde řešení pro jakoukoli vaši situaci.

Najdeme správné řešení i pro Vás!

Řízení rizik dle standardu NIS2

Nová legislativní úprava promítající EU směrnici **NIS2** vstoupí v platnost **ke konci roku 2024** a nyní je v připomínkovém procesu NÚKIB. Přesto, že je ještě v přípravě, už nyní je jasné, že nová povinnost řídit rizika dopadne na daleko širší okruh subjektů než je tomu nyní. Pro ty je určen systém OMIS, který jednoduchou a přehlednou formou pomůže se zvládnutím této povinnosti a to nejen na startu, ale i během průběžné práce s řízením rizik.

Co je OMIS (Open Management for IT Security)?

Je to SaaS ISMS platforma pro řízení aktiv a rizik **bezpečnostni informací** založená na platných standardech včetně chystané **NIS2**. OMIS vám umožní za měsíční paušál vykonávat celou škálu činností v rámci výkonu **agendy řízení bezpečnosti**. Systém lze využívat v režimu SaaS jako službu nebo jej lze pořídit jako on-premise instalaci.

Proč využívat OMIS?

- **Vybrané procesy informační bezpečnosti budou v souladu s nařízením NIS2, TISAX, DORA i ISO 27001**
- **Efektivně řídíte bezpečností opatření**
- **Elektronické dokumenty pro bezpečnostní auditory na jeden klik**

Další výhody systému OMIS

- Interním zaměstnancům ušetří čas intuitivním naváděním v aplikaci
- Zajistí specialistům spolehlivý zdroj strukturovaných informací pro efektivní řízení SŘBI
- Implementuje bezpečnostní přehled pro management
- Má vaše rizika pod kontrolou
- Zná včas nutné investice
- Provozuje služby i aplikace vycházející z mezinárodně uznávaných standardů a certifikací **CRISC**, **CISA**, **CISM**, **ITIL** a **TOGAF**

Kontaktujte nás

info@omis.cz | +420 725 145 846 | www.omis.cz | www.openapps.cz

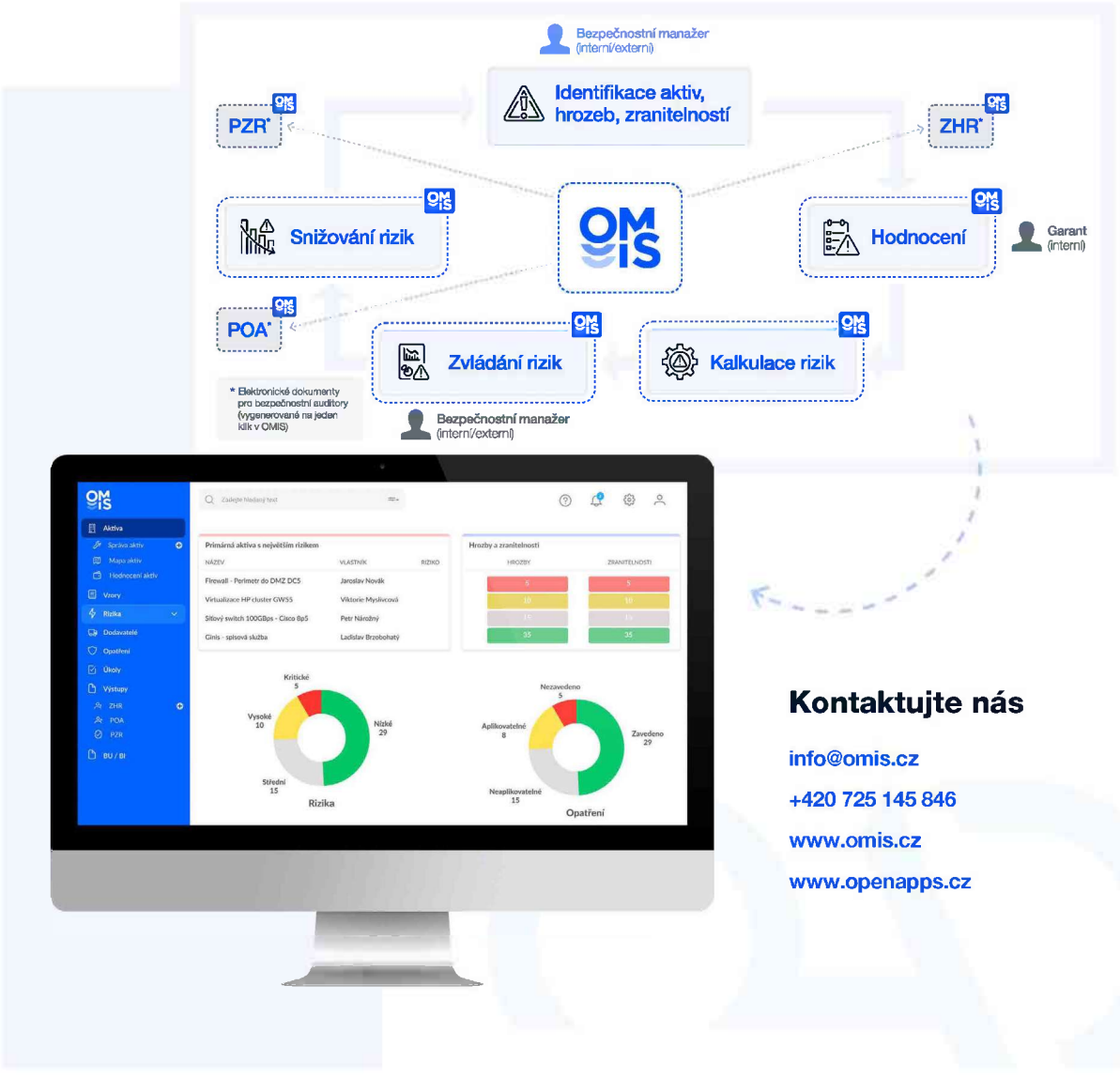
Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

OMIS Open Management for IT Security | Řízení kybernetické bezpečnosti jednoduše a pod kontrolou

Klíčové funkce systému OMIS

- Možnost spravovat více organizací
- Napojení na MS AD
- Fuil-Textové vyhledávání
- Auditní záznam změn v podobě transakčního protokolu
- Ukládání kompletní historie evidence včetně logů
- Možnost exportu veškerých záznamů
- Generování PDF dokumentů k evidovaným záznamům
- Vlastní atributy evidovaných objektů
- Generování dokumentů pro bezpečnostní auditory ZHR, POA, PZR*
- Evidence aktiv
- Šablony aktiv
- Mapy aktiv
- Správa dodavatelů
- Správa katalogu hrozeb zranitelností a opatření
- Správa lokalit
- Organizační struktura
- Správa a hodnocení rizik
- Správa a hodnocení opatření

* ZHR – Zpráva z hodnocení rizik, POA – Prohlášení o aplikovatelnosti, PZR – Plán zvládání rizik



Kontaktujte nás

info@omis.cz

+420 725 145 846

www.omis.cz

www.openapps.cz

Open Apps Development

Licenční podmínky

Nástroj na sběr a vyhodnocování logů z FW, Dohledový systém

1. Úvodní ustanovení

1.1 Tyto Licenční podmínky upravují práva a povinnosti mezi poskytovatelem licence k softwarové aplikaci OMIS/ODP/KYBON (dále jen „Aplikace") (dále jen „Poskytovatel") a jejím uživatelem/objednatelem (dále jen „Zákazník").
1.2 Poskytovatel je oprávněným vlastníkem Aplikace jakožto autorského díla dle zákona č. 121/2000 Sb. Aplikace je chráněna právními předpisy na ochranu autorských práv a mezinárodními dohodami.
1.3 Zákazník prohlašuje, že má zájem o poskytnutí licence k Aplikaci v rozsahu dle těchto Licenčních podmínek a za odměnu podle Ceníku (příloha).

2. Zpřístupnění a instalace Aplikace

2.1 Poskytovatel nainstaluje a implementuje Aplikaci na infrastrukturu Zákazníka bez zbytečného odkladu po úhradě odměny za licenci a první platby předplatného; přesný termín bude dohodnut.
2.2 V rámci implementace Poskytovatel aktivuje uživatelský účet a předá Zákazníkovi přístupové údaje. Zákazník si po prvním přihlášení zvolí vlastní heslo a je povinen chránit své přístupové údaje.
2.3 Pro řádné fungování Aplikace je nutné, aby Zákazník do Aplikace vkládal svá data a používal ji prostřednictvím přihlášeného uživatelského účtu. Poskytovatel neodpovídá za správnost ani úplnost vkládaných dat.
2.4 Zákazník uchovává data na své infrastruktuře; instalace Aplikace probíhá na zařízeních Zákazníka. Zálohování, šifrování a zabezpečení zajišťuje Zákazník. Poskytovatel nezajišťuje archivaci dat.

3. Podmínky používání Aplikace

3.1 Zákazník je povinen užívat Aplikaci v dobré víře, v souladu s účelem Aplikace, s těmito Licenčními podmínkami a pokyny Poskytovatele, a způsobem, který neomezuje ostatní uživatele.
3.2 Zákazník je povinen chránit data a dodržovat bezpečnostní pravidla (volba silného hesla, nesdělování přístupových údajů třetím osobám apod.).
3.3 Zákazník není oprávněn užívat Aplikaci k protiprávnímu jednání ani ji používat tak, aby z užívání měla prospěch třetí osoba; není oprávněn vytvářet další instalace bez vědomí Poskytovatele.
3.4 Poskytovatel bez výslovného souhlasu Zákazníka nenahlíží do dat; vyžaduje-li to povaha

plnění a Zákazník trvá na plnění, má se za to, že souhlas udělil.
3.5 Poskytovatel neodpovídá za správnost výsledků získaných používáním Aplikace ani za soulad funkcí s očekáváními Zákazníka, která Poskytovatel nevyvolal.
3.6 Poskytovatel neodpovídá za újmu způsobenou výpadky připojení Zákazníka, nesprávným či protiprávním použitím Aplikace, vlivy mimo přiměřenou kontrolu, jednáním nebo nečinností Zákazníka či třetích osob, únikem informací nebo ztrátou či poškozením dat nezaviněnou Poskytovatelem, ani za nepřímé následky (např. ušlý zisk).

4. Licence

4.1 Aplikace (včetně grafického rozhraní a obsahu) je autorským dílem.
4.2 Poskytovatel uděluje Zákazníkovi nevýhradní, celosvětovou licenci k užívání Aplikace po dobu trvání těchto Licenčních podmínek, bez množstevního omezení počtu uživatelů, koncových zařízení či zaznamenaných událostí.
4.3 Zákazník není povinen Aplikaci užívat; za zpřístupnění se považuje i pouhá možnost užití.
4.4 Bez předchozího souhlasu Poskytovatele Zákazník nesmí Aplikaci ani její části kopírovat, rozmnožovat, pozměňovat, překládat, distribuovat, prodávat, pronajímat, půjčovat, poskytovat třetím osobám, ani udělovat podlicence či postoupit práva z licence třetí osobě.
4.5 Zákazník není oprávněn provádět zpětnou analýzu zdrojového kódu, spojovat Aplikaci s jiným dílem za účelem vytvoření odvozeného díla ani ji užívat k vývoji zaměnitelného díla.
4.6 Poskytovatel nepostupuje na Zákazníka majetková práva k Aplikaci. Účelem licence je zabezpečení činností Zákazníka pro řízení kybernetické bezpečnosti.
4.7 Licence je poskytována od okamžiku úhrady předplatného za příslušné fakturační období.

5. Dostupnost, omezení a podpora (SLA)

5.1 Aplikace je přístupná nepřetržitě; Poskytovatel zajišťuje minimální dostupnost v rozsahu 99% času v kalendářním měsíci (dostupnost se vyhodnocuje ročně).
5.2 Poskytovatel je oprávněn dočasně omezit dostupnost z důvodů aktualizací, oprav, údržby, eliminace bezpečnostních rizik, vyšší moci, krizových stavů či na základě rozhodnutí orgánů veřejné moci; pokud je to možné, informuje Zákazníka předem.
5.3 V případě prodlení Zákazníka s úhradou odměny, zneužití Aplikace nebo porušení těchto podmínek je Poskytovatel oprávněn omezit přístupnost Aplikace.
5.4 Servisní podpora (Helpdesk) je dostupná v pracovních dnech (Po–Pá) od 8:00 do 17:00. Vady budou odstraňovány ve sjednaných lhůtách podle závažnosti (kritické/střední/nezávažné).

6. Údržba a aktualizace (Maintenance)

6.1 Poskytovatel zajišťuje průběžné aktualizace technologií, vylepšení, zvýšení bezpečnosti (update/upgrade), pravidelné legislativní aktualizace a technickou podporu.
6.2 Maintenance zahrnuje poskytnutí oprávnění užít aktualizované verze Aplikace a jejich instalaci a implementaci u Zákazníka.

9. Zpracování osobních údajů a mlčenlivost

9.1 Poskytovatel je povinen zachovávat mlčenlivost o osobních údajích a zpracovávat je bezpečně; bude-li působit jako zpracovatel dle GDPR, uzavřou strany smlouvu o zpracování osobních údajů.
9.2 Smluvní strany se zavazují zachovávat mlčenlivost o veškerých důvěrných informacích, používat je pouze k plnění povinností a chránit dobré jméno druhé strany.
9.3 Porušení povinnosti mlčenlivosti zakládá povinnost uhradit smluvní pokutu 50 000 Kč za každé porušení; tím není dotčeno právo na náhradu škody.

10. Práva a povinnosti stran

10.1 Poskytovatel poskytne licenci a Služby v dohodnutém rozsahu a kvalitě, zajistí odbornou péči a kapacity, může změnit přístupové údaje z naléhavých technických důvodů a změnit technické řešení; k plnění může využít třetí osoby, za něž odpovídá.
10.2 Zákazník je povinen řádně a včas hradit odměnu, ohlašovat vady bez zbytečného odkladu, zajišťovat bezpečnost, zálohování a šifrování dat, chránit přístupové údaje a informovat o změnách identifikačních údajů.
10.3 Zákazník odpovídá za správnost, legálnost a použitelnost dat vložených do Aplikace a nahradí Poskytovateli újmu či vydá bezdůvodné obohacení vzniklé jejich použitím, pokud právo neumožňuje odpovědnost vyloučit.

11. Komunikace

11.1 Komunikace probíhá primárně prostřednictvím uživatelského účtu a e-mailem. Písemnosti doručené e-mailem se považují za doručené okamžikem doručení na server adresáta.

12. Závěrečná ustanovení

12.1 Tyto Licenční podmínky se řídí právem České republiky; spory rozhodují obecné soudy ČR místně příslušné podle sídla Poskytovatele.