Příloha zadávací dokumentace č. 2

Smlouva o dodávce, implementaci a technické podpoře řešení pro zvýšení kybernetické bezpečnosti informačních a komunikačních systémů

(dále jen „***Smlouva***“)

uzavřená ve smyslu § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“), za přiměřeného použití § 2358 a násl. občanského zákoníku, § 2586 a násl. ve spojení a § 2631 a násl. občanského zákoníku, a dle zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským (dále jen „autorský zákon“)

mezi těmito smluvními stranami:

Objednatel:	**Střední pedagogická škola Boskovice, příspěvková organizace**
se sídlem:	Komenského 343/5, 680 01 Boskovice
zastoupen:	Mgr. Leonou Valterovou, ředitelkou
IČO:	62073117
Bankovní spojení:	UniCredit Bank Czech Republic and Slovakia, a.s.
Číslo účtu:	[redacted]

(dále také jako „***Objednatel***“ či „***Nabyvatel***“)

Dodavatel:	**Aricoma Systems a.s.**
se sídlem:	Hornopolní 3322/34, 702 00 Ostrava
zastoupen:	Petr Konečný, ředitel RC, na základě plné moci
Zapsán OR:	Společnost je zapsána v Obchodním rejstříku vedeném Krajským soudem v Ostravě, oddíl B, vložka 11012
kontaktní osoba ve věcech smluvních:	Petr Konečný, ředitel RC, na základě plné moci
kontaktní osoba ve věcech technických:	Petr Polák
IČO:	04308697
DIČ:	CZ04308697
Bankovní spojení:	Československá obchodní banka, a.s.
Číslo účtu:	[redacted]

(dále také jako „***Dodavatel***“ či „***Poskytovatel***“)

(společně jako „***smluvní strany***“ či jednotlivě jako „***smluvní strana***“)

uzavřely tuto Smlouvu na základě výsledku zadávacího řízení na veřejnou zakázku s názvem „**Kybernetická bezpečnost – Střední pedagogická škola Boskovice“.**

I. ÚVODNÍ USTANOVENÍ

1. Objednatel zahájil veřejnou zakázku s názvem „Kybernetická bezpečnost – Střední pedagogická škola Boskovice“, přičemž nabídka Dodavatele byla vybrána jako nejvhodnější.

2. Na základě této Smlouvy má Dodavatel ve prospěch Objednatele dodat řešení pro zvýšení kybernetické bezpečnosti Objednatele, provést jeho implementaci do infrastruktury Objednatele, a zajistit technickou podporu tohoto řešení, a to za podmínek dále uvedených v této Smlouvě a jejích přílohách.

3. Závazek mezi smluvními stranami založený touto Smlouvou se řídí zákonem č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“), a zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „autorský zákon“).

4. Tato Smlouva je uzavřena na základě výsledku zadávacího řízení vedeného podle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „***ZZVZ***“). Jednotlivá ustanovení této Smlouvy musí být vykládána v souladu se zadávacími podmínkami uvedenými v zadávací dokumentaci veřejné zakázky, vč. jejich příloh, a v souladu s nabídkou Dodavatele podanou v rámci zadávacího řízení veřejné zakázky.

5. Účelem uzavření Smlouvy je dodávka komponent softwarové (SW) a hardwarové (HW) infrastruktury a jejich instalace, implementace a vzájemná integrace na stávající informační systémy Objednatele za účelem zvýšení kybernetické bezpečnosti Objednatele, a posílení schopnosti odolávat vnějším kybernetickým hrozbám.

6. Na realizaci projektu byla přislíbena finanční podpora Národního plánu obnovy. Dodavatel je povinen poskytnout objednateli veškerou součinnost tak, aby financování projektu nebylo ohroženo. Dodavatel je povinen uchovávat veškerou dokumentaci související s realizací projektu včetně účetních dokladů minimálně do konce roku 2036.

II. PROHLÁŠENÍ SMLUVNÍCH STRAN

1. Dodavatel prohlašuje, že je plně způsobilý k řádnému a včasnému provedení předmětu této Smlouvy, že se řádně seznámil s rozsahem a povahou předmětu Smlouvy, a to takovým způsobem, že jsou mu známy veškeré relevantní technické, kvalitativní a jiné podmínky nezbytné k jeho realizaci, a že disponuje takovými kapacitami a odbornými znalostmi, vlastním technickým vybavením a zázemím, které jsou nezbytné pro realizaci předmětu Smlouvy za dohodnuté smluvní ceny uvedené v této Smlouvě, a to rovněž ve vazbě na jím prokázanou kvalifikaci pro plnění veřejné zakázky.

2. Dodavatel je oprávněn plnit předmět této Smlouvy pouze prostřednictvím svých zaměstnanců nebo osob uvedených v seznamu poddodavatelů (příloha č. 3 této Smlouvy).

3. Dodavatel dále prohlašuje, že není v úpadku ani ve stavu hrozícího úpadku, a že mu není známo, že by vůči němu bylo zahájeno insolvenční řízení. Rovněž prohlašuje, že vůči němu není v právní moci žádné soudní rozhodnutí, případně rozhodnutí správního, daňového či jiného orgánu na plnění, které by mohlo být důvodem zahájení exekučního řízení na majetek Dodavatele a že takové exekuční řízení nebylo vůči němu zahájeno.

4. Smluvní strany prohlašují, že identifikační údaje smluvních stran uvedené v této Smlouvě odpovídají aktuálnímu stavu, a že osobami jednajícími při uzavření této Smlouvy jsou osoby oprávněné k jednání za smluvní strany. Jakékoliv změny předmětných údajů, jež nastanou v době po uzavření této Smlouvy, jsou smluvní strany povinny bez zbytečného odkladu písemně sdělit druhé smluvní straně.
5. V případě, že se kterékoliv prohlášení některé ze smluvních stran podle tohoto článku Smlouvy ukáže být nepravdivým, odpovídá tato smluvní strana za škodu a nemajetkovou újmu, která nepravdivostí prohlášení nebo v souvislosti s ní druhé smluvní straně vznikne.
6. Dodavatel a Objednatel se zavazují k vzájemné součinnosti za účelem plnění předmětu této Smlouvy.

III. PŘEDMĚT SMLOUVY

1. Předmětem této Smlouvy je závazek Dodavatele dodat komponenty softwarové (SW) a hardwarové (HW) infrastruktury, provést jejich instalaci, implementaci a vzájemnou integraci, zejména provést:
   1.1. pořízení a implementaci Next Generation Firewall (NGFW),
   1.2. pořízení a implementaci Endpoint protection řešení (EDR),
   1.3. pořízení a implementaci nástroje pro analýzu a monitoring síťového provozu – nástroje pro ochranu integrity komunikačních sítí,
   1.4. pořízení serverů a diskových úložišť, ostatního HW,
   1.5. pořízení a implementaci nástroje pro zajišťování úrovně dostupnosti informací,
   1.6. pořízení a implementaci nástroje pro multifaktorovou autentizaci a jednotné přihlašování,
   1.7. poskytnout Objednateli veškeré potřebné licence k dodanému řešení,
   1.8. provést zaškolení administrátorů a uživatelů na straně Objednatele,
   1.9. provést zkušební provoz a akceptační testy,
   1.10. zpracovat a předat Objednateli veškerou dokumentaci dodaného a implementovaného řešení do infrastruktury Objednatele,
   1.11. zajistit projektové vedení po celou dobu realizace plnění,
   1.12. poskytnout standardní záruku na dodané řešení,

   (dále společně jako „***předmět plnění***“).
2. Předmětem této Smlouvy je rovněž závazek Dodavatele:
   2.1. poskytnout Objednateli **nadstandardní (prodlouženou) záruku,**
   2.2. poskytnout Objednateli **technickou podporu (maintenance support + základní technická podpora)** dodaného a implementovaného řešení po dobu udržitelnosti projektu (min. 60 měsíců od jeho předání Objednateli), a

2.3. poskytnout Objednateli **rozšířenou servisní podporu** dodaného a implementovaného řešení na základě písemných požadavků Objednatele po dobu udržitelnosti projektu (min. 60 měsíců od jeho předání Objednateli).

3. Minimální technické, funkční a implementační/integrační požadavky na předmět plnění, a požadavky na poskytování dalších služeb, jak jsou vymezeny Objednatelem, a v rozsahu, v jakém se je zavázal naplňovat Dodavatel pro celou dobu plnění této Smlouvy, jsou závazně uvedeny v příloze č. 1 této Smlouvy.

4. Dodavatelem nabízený předmět plnění a zejména způsob jeho provedení musí splňovat požadavky stanovené vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).

5. Dodavatel poskytne Objednateli předmět plnění na základě písemného projektu, který bude obsahovat zejména:

   5.1. popis dodávaného řešení (specifikaci dodávaného HW a SW, funkční schéma řešení),

   5.2. popis způsobu a postupu implementace do infrastruktury Objednatele,

   5.3. popis zabezpečení dodávaného řešení včetně zabezpečení informačních a komunikačních systémů v průběhu provádění díla),

   5.4. popis plánu zálohování a obnovy síťové infrastruktury,

   5.5. plán zkušebního provozu a provedení akceptačních testů,

   5.6. plán zaškolení administrátorů a uživatelů,

   5.7. harmonogram postupu prací v členění minimálně na kalendářní týdny,

   5.8. požadavky na součinnost Objednatele a období pro poskytnutí takové součinnosti, aj.

   (dále jen „***prováděcí projekt***“).

6. Dodavatel prohlašuje, že je oprávněn k distribuci programů a služeb, jež tvoří předmět této Smlouvy vymezený v předchozím odst. 1. tohoto článku Smlouvy, a touto Smlouvou poskytuje Objednateli oprávnění k jeho využívání v rozsahu a za podmínek v této Smlouvě vymezených.

7. Dodavatel se zavazuje, že využije ke zhotovení předmětu plnění pro Objednatele takové hardwarové či softwarové produkty a technologie, o kterých na základě své odbornosti a dostupných roadmap výrobců ví či může předpokládat, že budou schopny plnit účel vyplývající z této Smlouvy a budou výrobcem podporovány nejméně po dobu 60 měsíců od okamžiku dokončení předmětu plnění dle předpokladů stanovených touto Smlouvou a jejími přílohami. Tato skutečnost bude posuzována k datu podání nabídky Dodavatele, která předcházela uzavření této Smlouvy. Dodavatel splní tento závazek zejména tehdy, využije-li takové hardwarové či softwarové produkty a technologie, o nichž bylo v době podání nabídky před uzavřením této Smlouvy známo, že pro ně není vyhlášeno datum ukončení prodeje (end of sale), ani datum ukončení podpory/servisu (end od support/service). Nesplnění podmínky dle předchozí věty se považuje za vadu plnění, pro kterou je Objednatel oprávněn plnění Dodavatele nepřevzít, a to až do okamžiku odstranění takové vady, zjistí-li tak před převzetím plnění; v ostatních případech bude Objednatel postupovat podle čl. XIII. odst. 3. této Smlouvy. Porušení uvedeného závazku a nezjednání nápravy dle této Smlouvy se považuje za podstatné porušení Smlouvy.

8. Předmětem této Smlouvy je závazek Objednatele zaplatit za Dodavatelem poskytnutý předmět plnění cenu sjednanou v čl. VI. této Smlouvy, v rozsahu Dodavatelem poskytnutého předmětu plnění dle přílohy č. 1 této Smlouvy a dle položkového ocenění podle přílohy č. 2 této Smlouvy.

IV. MÍSTO A DOBA PLNĚNÍ

1. Místem plnění je adresa sídla Objednatele: Komenského 343/5, 680 01 Boskovice. Smluvní strany předpokládají poskytování předmětu plnění rovněž prostřednictvím dálkové komunikace a vzdáleného přístupu.

2. Dodavatel se zavazuje zahájit provádění předmětu plnění bezodkladně po nabytí účinnosti této smlouvy.

3. Smluvní strany se dohodly, že provádění předmětu plnění a jeho harmonogram bude respektovat jako nejzazší níže uvedené uzlové body (milníky):

Označení milníku	Název milníku	Trvání (nejpozději do)
T0	Zahájení plnění	po nabytí účinnosti Smlouvy
T1	Předložení prováděcího projektu Objednateli k akceptaci *(akceptační protokol/prohlášení)*	T0 + 4 kalendářní týdny
T2	Dodávka a implementace řešení – kyberbezpečnostní opatření *(akceptační protokol/prohlášení)*	T0 + 24 kalendářních týdnů
T3	Zpracování a předání dokumentace dodaného a implementovaného řešení; Školení administrátorů *(akceptační protokol/prohlášení)*	T0 + 26 kalendářních týdnů
T4	Zkušební provoz a akceptační testy *(akceptační protokol/prohlášení)*	T0 + 28 kalendářních týdnů
T5	Předání a převzetí dokončeného řešení a zahájení ostrého provozu *(protokol o předání a převzetí předmětu plnění)*	T0 + 28 kalendářních týdnů
T6	Poskytování technické podpory	T5 + 60 měsíců

4. Smluvní strany se dohodly, že podmínkou pro zahájení dodávky a implementace řešení do infrastruktury Objednatele (T2) je písemná akceptace prováděcího projektu Objednatelem. Objednatel se zavazuje provést posouzení prováděcího projektu dle čl. III. odst. 5. této Smlouvy a sdělit výsledek tohoto posouzení bez zbytečného odkladu po jeho předložení Dodavatelem, nejpozději však do 3 pracovních dnů od jeho předložení Dodavatelem. Za účelem dosažení akceptace prováděcího projektu Objednatelem ve lhůtě dle milníku T1 je Dodavatel oprávněn průběžně seznamovat Objednatele se stavem a obsahem tohoto prováděcího projektu. Objednatel je oprávněn vyzvat Dodavatele k poskytnutí rozpracované verze prováděcího projektu.

   V případě, že prováděcí projekt nebude Dodavatelem zpracován v souladu s čl. III. odst. 5. této Smlouvy a/nebo bude vykazovat takové vady či nedostatky, v jejichž důsledku by bylo ohroženo naplnění účelu této Smlouvy vyjádřeného v čl. I. odst. 5. této Smlouvy, je Objednatel oprávněn odepřít akceptaci prováděcího projektu a sdělit důvody takového odepření akceptace. Nedojde-li k odstranění důvodů vedoucích k odepření akceptace prováděcího projektu ani v dodatečné lhůtě stanovené dohodou smluvních stran,

je Objednatel oprávněn od této Smlouvy odstoupit. V případě akceptace prováděcího projektu Objednatelem v dodatečné lhůtě stanovené dohodou smluvních stran není dotčena odpovědnost Dodavatele za případné prodlení se splněním milníků dle předchozího odst. 3. tohoto článku Smlouvy. Odstoupí-li Objednatel od Smlouvy z důvodu uvedeného v tomto odstavci Smlouvy, nevzniká Dodavateli jakýkoliv nárok na úhradu ceny plnění či její části.

5. Smluvní strany se dohodly, že řádná a včasná dodávka a implementace řešení do infrastruktury Objednatele, včetně úspěšného absolvování zkušebního provozu, bude Dodavatelem předána Objednateli tak, aby Objednatel akceptoval a převzal dokončené řešení nejpozději **do 28 kalendářních týdnů ode dne nabytí účinnosti této Smlouvy**.

6. Smluvní strany se dohodly, že technická podpora bude Dodavatelem poskytována po dobu 60 měsíců ode dne akceptace a převzetí dokončeného řešení Objednatelem, není-li dále v této Smlouvě uvedeno jinak. Po uvedené období bude zajištěna platnost a trvání veškerých poskytnutých licencí.

V. PŘEDÁNÍ (ČÁSTI) PŘEDMĚTU PLNĚNÍ, AKCEPTACE

1. Smluvní strany se dohodly na tom, že Objednatel není povinen předmět plnění či jeho část převzít (akceptovat), pokud vykazuje vady či nedodělky, nenaplňuje veškeré požadavky, k jejichž splnění se Dodavatel zavázal, zejména pak požadavky plynoucí z přílohy č. 1 této Smlouvy anebo z prováděcího projektu, který Dodavatel předložil; zejména pak Objednateli náleží právo nepřevzít (neakceptovat) předmět plnění nebo jeho dílčí část v případě, kdy taková vada, nedodělek či rozpor s výše uvedenými dokumenty brání řádnému užívání předmětu plnění, resp. při návaznosti jednotlivých milníků dle čl. IV. odst. 3. této Smlouvy brání taková vada, nedodělek či rozpor v zahájení navazujícího milníku. Zároveň Objednatel není povinen předmět plnění převzít, pokud není proveden včas.

2. Akceptací předmětu plnění Objednatelem se závazek Dodavatele považuje za splněný, a výsledek plnění Dodavatele za způsobilý k užívání Objednatelem.

3. Akceptaci předmětu plnění Objednatelem bude předcházet ověření, zda plnění poskytnuté Dodavatelem dle této Smlouvy vedlo k výsledku a naplnění účelu, ke kterému se smluvní strany zavázaly, a to porovnáním skutečných vlastností jednotlivých částí plnění poskytnutých Dodavatelem dle této Smlouvy s jednotlivými požadavky pro ně stanovenými v této Smlouvě.

4. Předmět plnění se považuje za akceptovaný okamžikem podpisu příslušného protokolu ze strany Objednatele. Formálními náležitostmi protokolu o předání a převzetí předmětu plnění je jeho označení, datum vystavení, celkový počet stran, označení Smlouvy, označení Dodavatele a Objednatele, název projektu, označení a popis plnění, které je předmětem akceptace, datum zahájení a ukončení plnění, jméno a podpis osob, které protokol podepsaly. Protokol bude vyhotoven ve dvou výtiscích, přičemž každý bude určen pro jednu smluvní stranu. V protokolu bude zřetelně označeno, zda byl předmět plnění (i) akceptován, (ii) akceptován s výhradami, nebo (iii) neakceptován. Pokud bude předmět plnění akceptován Objednatelem s výhradami, nebo nebude akceptován vůbec, bude k protokolu vyhotovena jeho příloha, ve které bude popis výhrad či vad, a bude zde zaznamenán také další dohodnutý postup a termíny odstranění těchto výhrad. Protokol bude podepsán oprávněnou osobou, která provedla na straně Objednatele akceptaci.

5. Před předáním předmětu plnění bude Dodavatel informovat Objednatele o termínu plánovaného předání plnění, a to písemně (alespoň prostřednictvím e-mailu) v dostatečném předstihu tak, aby vzhledem k charakteru předmětu plnění, jeho rozsahu a nárokům na kontrolu a ověření řádnosti a úplnosti jeho poskytnutí byly Objednateli vytvořeny podmínky k tomu, aby provedl kontrolu a ověření bez zbytečného odkladu po předání předmětu plnění Dodavatelem, a provedl akceptaci předmětu plnění ve lhůtě dle čl. IV. odst. 5 této Smlouvy.

6. V případě, že výsledek plnění Dodavatele neobsahuje dle Objednatele žádnou vadu či nedodělek a Objednatel nemá k plnění Dodavatele žádné výhrady ani připomínky, je předmět plnění akceptován bez výhrad, a tato skutečnost bude potvrzena v protokolu o předání a převzetí předmětu plnění.

7. V případě, že výsledek plnění Dodavatele obsahuje dle Objednatele drobné vady či nedodělky, které samostatně ani ve spojení s jinými nebrání užívání předmětu plnění k účelu stanovenému touto Smlouvou, nebo Objednatel má k výsledku plnění Dodavatele nepodstatné výhrady či připomínky, je předmět plnění akceptován s výhradami. Protokolu o předání a převzetí předmětu plnění tak bude obsahovat soupis vytknutých vad, nedodělků, výhrad či připomínek, a také způsoby a přiměřené lhůty pro jejich odstranění, na kterých se smluvní strany dohodly; nedohodnou-li se, budou odstraněny do 5-ti pracovních dnů. Smluvní strany považují v takovém případě výsledek plnění Dodavatele za Dodavatelem řádně předaný a Objednatelem řádně převzatý. Pakliže však nebudou Objednatelem vytknuté vady, nedodělky, výhrady či připomínky odstraněny v souladu se záznamem v protokolu a v termínech v něm uvedených, vzniká Objednateli nárok na smluvní pokutu dle sankčních ustanovení této Smlouvy. Dodavatel písemně informuje Objednatele o odstranění vad, nedodělků, výhrad či připomínek. Objednatel takto doplněný výsledek plnění bez zbytečného odkladu (nejpozději do 3 pracovních dnů od poskytnut informace Dodavatelem) posoudí, a odstranění vytknutých vad, nedodělků, výhrad či připomínek písemně potvrdí Dodavateli podepsáním přílohy protokolu.

8. V případě, že výsledek plnění Dodavatele trpí jinými než drobnými vadami či nedodělky, nebo Objednatel má k výsledku plnění Dodavatele podstatné výhrady či připomínky, pak předávaný předmět plnění neakceptuje. Smluvní strany nepovažují v takovém případě výsledek plnění Dodavatele za řádně předaný a Dodavatel je s předáním předmětu plnění v prodlení. Dodavatel je povinen bez zbytečného odkladu odstranit Objednatelem vytknuté vady, nedodělky, výhrady či připomínky, nebo poskytnout nové plnění. O této skutečnosti bude vyhotoven akceptační protokol, avšak v případě neakceptování předmětu plnění je Dodavatel po sjednání nápravy povinen znovu podstoupit celý proces akceptace podle této Smlouvy, aby mohl být předmět plnění Objednatelem akceptován. Tím není dotčena odpovědnost Dodavatele za prodlení s předáním předmětu plnění dle této Smlouvy, ani práva Objednatele z prodlení Dodavatele vyplývající z této Smlouvy.

9. Posouzení skutečnosti, zda vady či nedodělky zjištěné Objednatelem brání užívání předmětu plnění nebo jeho části, náleží výhradně Objednateli. Za vady či nedodělky je pro účely této Smlouvy považováno i dodání nesprávného druhu nebo množství částí předmětu plnění či nedodání jakýchkoliv dokladů či jiné dokumentace, které jsou k řádnému užívání předmětu plnění nezbytné.

10. Při předání předmětu plnění a podpisu protokolu si smluvní strany poskytnou vzájemnou součinnost. K účasti na akceptačním řízení a k podpisu protokolu o předání a převzetí předmětu plnění jsou vedle statutárních zástupců smluvních stran oprávněny tyto osoby:

    10.1. na straně Objednatele: Mgr. Leona Valterová, e-mail: reditel@spgs-bce.cz, tel.: +420 516 802 543,

10.2. na straně Dodavatele Petr Konečný, ředitel RC, na základě plné moci, e-mail: petr.konecny@aricoma.com, tel.: +420 602 448 917.

11. Den podpisu protokolu o předání a převzetí předmětu plnění je rozhodným dnem pro počátek běhu sjednané záruční doby a pro zahájení poskytování služeb technické podpory provozu dodaného řešení.

VI. CENA PLNĚNÍ A PLATEBNÍ PODMÍNKY

1. Ceny plnění dále uvedené v tomto článku Smlouvy jsou cenami úplnými v rozsahu stanoveném přílohou č. 2 této Smlouvy, a zahrnují veškeré náklady Dodavatele k poskytnutí předmětu plnění dle čl. III. odst. 1. a odst. 2. této Smlouvy. Celková cena plnění v uvedeném rozsahu činí:

12 619 000,00,- Kč bez DPH

výše DPH 21 % 2 649 990,00,- Kč

15 268 990,00,- Kč včetně DPH

(slovy: patnáct milionů dvě stě šedesát osm tisíc devět set devadesát korun českých)

2. Celková cena plnění dle předchozího odstavce se sestává z cen za dílčí části plnění, a to ve výši:

2.1. **Cena za dodávku a implementaci řešení v rozsahu čl. III. odst. 1. této smlouvy vč. standardní záruky** **11 642 200,00,- Kč Kč bez DPH,**

2.2. **Cena za poskytnutí nadstandardní (prodloužené) záruky pro 4. a 5. rok plnění** **46 800,00,- Kč bez DPH,**
2.2.1. tj. roční plnění (12 měsíců) činí 23 400,00,- Kč bez DPH,

2.3. **Cena za poskytnutí potřebné maintenance support a Základní technické podpory na 5 let (1. až 60. měsíc)** **750 000,00,- Kč bez DPH**,
2.3.1. tj. roční plnění maintenance support (12 měsíců) činí 106 800,00,- Kč bez DPH,
2.3.2. tj. roční plnění základní tech. podpory (12 měsíců) činí 43 200,00,- Kč bez DPH,

2.4. **Cena za poskytnutí rozšířené servisní podpory na 5 let (předpokládaná kalkulace 100 hodin)** **180 000,00,- Kč bez DPH,**
2.4.1. tj. cena za 1 hodinu služeb rozšířené servisní podpory činí 1 800,00,- Kč bez DPH,

3. Výše cen za jednotlivé položky plnění je uvedena v příloze č. 2 této Smlouvy. Za správnost stanovení sazby DPH a výše DPH odpovídá Dodavatel. Sazba DPH a výše DPH bude na faktuře Dodavatele stanovena vždy v aktuálně platné výši.

4. Cena plnění bude hrazena po částech, a to následovně:

4.1. Cena dílčí části plnění dle čl. VI. odst. 2.1. této Smlouvy bude uhrazena **jednorázově**, a to po předání a převzetí plnění a podpisu protokolu dle čl. V. odst. 10. této Smlouvy Objednatelem. Datem uskutečnění zdanitelného plnění je den podpisu protokolu o předání a převzetí předmětu plnění Objednatelem.

4.2. Cena dílčí části plnění dle čl. VI. odst. 2.2. této Smlouvy bude hrazena postupně **v pravidelných ročních paušálních platbách**, ve výši podílu připadajícího na roční plnění dle odst. 2.2.1. tohoto článku Smlouvy, a to pro každý nadcházející rok **předem**. Datem uskutečnění zdanitelného plnění je den zahájení poskytování nadstandardní (prodloužené) záruky dle této Smlouvy pro příslušný rok.

4.3. Cena dílčí části plnění dle čl. VI. odst. 2.3. této Smlouvy bude hrazena postupně **v pravidelných ročních paušálních platbách**, ve výši podílu připadajícího na roční plnění dle odst. 2.3.1. a odst. 2.3.2. tohoto článku Smlouvy, a to pro každý nadcházející rok **předem**. Datem uskutečnění zdanitelného plnění je den výročí zahájení poskytování technické podpory dle této Smlouvy. Pro první rok poskytování technické podpory se za datum uskutečnění zdanitelného plnění považuje první den zahájení poskytování technické podpory následující po předání a převzetí předmětu plnění Objednatelem.

4.4. Cena dílčí části plnění dle čl. VI. odst. 2.4. této Smlouvy bude hrazena postupně dle míry skutečné spotřeby časových jednotek (1 hodina = 60 minut) násobených hodinovou sazbou dle odst. 2.4.1. tohoto článku Smlouvy, při poskytování služeb rozšířené servisní podpory realizované Dodavatelem na základě písemně zadaných požadavků Objednatele, a to po konci kalendářního měsíce, ve kterém byly takové služby Objednatelem od Dodavatele čerpány. Datem uskutečnění zdanitelného plnění je poslední den příslušného kalendářního měsíce.

5. Dodavatel vystaví Objednateli daňový doklad (fakturu) na plnění v souladu s odst. 4. tohoto článku Smlouvy. Minimální doba splatnosti faktury vystavené ze strany Dodavatele bude činit 30 dní od doručení faktury Objednateli. Faktura bude splňovat náležitosti účetního dokladu podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, a daňového dokladu podle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.

6. Dodavatel je povinen vystavit a předat veškeré faktury v elektronickém formátu PDF, a zaslat je datovou zprávou do Datové schránky Objednatele – IDS: hvixfpa.

7. Nezbytnou přílohou faktury bude zejména soupis skutečně dodaného plnění a provedených prací – zjišťovací protokol; v případě služeb rozšířené servisní podpory Objednatelem odsouhlasený soupis poskytnutých služeb s jejich časovým rozsahem. Přílohy budou připojeny v souboru ZIP nebo RAR v pořadí – 1. faktura jako hlavní dokument, 2. přílohy k faktuře jako příloha dokumentu. Plnění či práce, které provedl Dodavatel bez souhlasu Objednatele nad rámec předmětu této Smlouvy, nebudou do soupisu skutečně dodaného plnění a provedených prací zařazeny a považují se za součást celkové ceny, vyjma případů, kdy se smluvní strany písemně dohodnou jinak.

8. Faktura bude nad rámec zákonem požadovaných náležitostí (§ 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty) pro daňový doklad obsahovat také:

   a) číslo a datum vystavení faktury,
   b) číslo smlouvy a datum jejího uzavření,
   c) předmět plnění a jeho přesnou specifikaci ve slovním vyjádření,
   d) soupis provedených prací včetně zjišťovacího protokolu
   e) označení banky a číslo účtu, na který musí být zaplaceno (pokud je číslo účtu odlišné od čísla uvedeného v této Smlouvě, je Dodavatel povinen o této skutečnosti informovat Objednatele), číslo

a datum příslušných akceptačních protokolů podepsaných zástupcem Dodavatele a odsouhlasených zástupcem Objednatele,

f) lhůtu splatnosti faktury,
g) název, sídlo, IČO a DIČ Objednatele a Dodavatele,
h) název a registrační číslo projektu: Kybernetická bezpečnost – Střední pedagogická škola Boskovice, reg. č. projektu CZ.31.2.0/0.0/0.0/23_092/0008742,
i) jméno a podpis osoby Dodavatele, která fakturu vystavila, včetně kontaktního telefonu.

9. Nebude-li faktura obsahovat zákonem či touto Smlouvou stanovené náležitosti nebo bude chybně vyúčtována cena nebo DPH, je Objednatel oprávněn fakturu před uplynutím lhůty splatnosti vrátit Dodavateli k provedení opravy s vyznačením důvodu vrácení. Dodavatel provede opravu vystavením nové faktury. Dnem odeslání vadné faktury Objednatelem Dodavateli přestává běžet původní lhůta splatnosti a nová lhůta splatnosti počíná běžet znovu ode dne doručení nové a řádně vystavené faktury Objednateli.

10. V případě prodlení Objednatele se zaplacením řádně vystavené a doručené faktury se Objednatel zavazuje Dodavateli uhradit úrok z prodlení v zákonné výši.

11. Ceny plnění jsou uvedeny jako pevné a nejvýše přípustné ve vztahu k předmětu plnění v rozsahu stanoveném touto Smlouvou k okamžiku jejího uzavření, není-li v této Smlouvě výslovně uvedeno jinak. Smluvní strany sjednaly, že cena plnění zahrnuje rovněž náklady akceptačního řízení, zkušebního či testovacího provozu, technické podpory a servisu, a dalších služeb poskytovaných Dodavatelem Objednateli po dobu trvání této Smlouvy, a rovněž náklady na odstraňování vad a nedodělků plnění a vad plnění v průběhu záruky, včetně odměny za veškeré licence, které byly Objednateli poskytnuty na základě této Smlouvy, není-li dále ujednáno jinak. Dodavatel v souvislosti s ujednáním ceny předmětu plnění na sebe přebírá nebezpečí změny okolností ve smyslu § 2620 odst. 2 občanského zákoníku.

12. V případě, že dojde ke změně zákonné sazby DPH, je Dodavatel k ceně předmětu plnění bez DPH povinen účtovat DPH v platné výši. Tato situace představuje výjimku z nezměnitelnosti ceny předmětu plnění, přičemž smluvní strany výslovně uvádějí, že v případě změny ceny předmětu plnění v důsledku změny sazby DPH nebude ke Smlouvě uzavírán dodatek.

13. Smluvní strany si dále v souladu s § 100 odst. 1 ZZVZ, pro případ trvání a plnění této Smlouvy i po uplynutí prvních 60 měsíců poskytování technické podpory dle čl. III. odst. 2.2. a souvisejících této Smlouvy, vyhrazují právo stanovit pro 6. rok plnění a roky následující způsob stanovení ceny za poskytování technické podpory, a to dle dále uvedených pravidel:

    13.1. Výchozí hodnotou je vždy cena za poslední rok poskytování technické podpory (výchozí hodnotou pro stanovení ceny pro 6. rok plnění je tak cena za 5. rok plnění dle čl. VI. odst. 2.3.1. a odst. 2.3.2. této Smlouvy, resp. příslušné položky dle přílohy č. 2),

    13.2. Výchozí hodnota může být pro následující rok (12 měsíců) procentuálně zvýšena maximálně o míru inflace v ČR vyjádřenou přírůstkem průměrného ročního indexu spotřebitelských cen dle údajů publikovaných Českým statistickým úřadem za rok nejblíže předcházející. Ke stanovení hodnoty plnění pro následující rok dojde na základě jednání a souhlasu obou smluvních stran, při respektování maximálního limitu nárůstu dle předchozí věty. Faktické zvýšení hodnoty za poskytování technické podpory bude projeveno ve faktuře vystavené v souladu s odst. 4.3. tohoto článku Smlouvy; uzavření písemného dodatku k této Smlouvě se pro tento případ nevyžaduje.

13.3. Smluvní strany jsou povinny si vzájemně oznámit svůj zájem na pokračování poskytování technické podpory pro každý následující rok plnění nejpozději 6 měsíců před uplynutím aktuálního roku poskytované technické podpory, nebo v téže lhůtě závazek k poskytování technické podpory pro následující rok vypovědět. V případě výpovědi kterékoliv smluvní strany dle předchozí věty zaniknou závazky smluvních stran k poslednímu dni období aktuálního roku poskytované technické podpory.

14. Smluvní strany si dále v souladu s § 100 odst. 1 ZZVZ, pro případ trvání a plnění této Smlouvy i po uplynutí prvních 60 měsíců poskytování rozšířené servisní podpory dle čl. III. odst. 2.3. a souvisejících této Smlouvy, vyhrazují právo stanovit pro 6. rok plnění a roky následující způsob stanovení ceny za poskytování rozšířené servisní podpory, a to dle dále uvedených pravidel:

    14.1. Výchozí hodnotou je vždy cena za 1 hodinu (hodinová sazba) v posledním roce poskytování rozšířené servisní podpory (výchozí hodnotou pro stanovení hodinové sazby pro 6. rok plnění je tak hodinová sazba za 5. rok plnění dle čl. VI. odst. 2.4.1. této Smlouvy),

    14.2. Výchozí hodnota může být pro následující rok (12 měsíců) procentuálně zvýšena maximálně o míru inflace v ČR vyjádřenou přírůstkem průměrného ročního indexu spotřebitelských cen dle údajů publikovaných Českým statistickým úřadem za rok nejblíže předcházející. Ke stanovení hodinové sazby pro následující rok dojde na základě jednání a souhlasu obou smluvních stran, při respektování maximálního limitu nárůstu dle předchozí věty. Faktické zvýšení hodinové sazby za poskytování rozšířené servisní podpory bude projeveno ve faktuře vystavené v souladu s odst. 4.4. tohoto článku Smlouvy; uzavření písemného dodatku k této Smlouvě se pro tento případ nevyžaduje.

VII. PRÁVA A POVINNOSTI DODAVATELE, PRAVIDLA VZDÁLENÉHO PŘÍSTUPU DODAVATELE

1. Dodavatel je povinen provést předmět plnění v rozsahu a termínech specifikovaných touto Smlouvou, jejími přílohami, a prováděcím projektem. Zjistí-li Dodavatel překážky, které znemožňují provést předmět plnění dohodnutým způsobem či ve stanovených termínech, je povinen to neprodleně písemně oznámit Objednateli a navrhnout mu změnu v řešení. Jakékoliv změny v řešení, které by vedly ke změně podmínek sjednaných touto Smlouvou, podléhají písemnému schválení Objednatele. Ustanovení § 222 ZZVZ tímto není dotčeno.

2. Dodavatel je povinen provést předmět plnění v souladu s obecně závaznými právními předpisy a v souladu se závaznými interními předpisy Objednatele.

3. Dodavatel je povinen provést předmět plnění řádně a odborně, sám nebo prostřednictvím svých poddodavatelů, které Dodavatel vůči Objednateli identifikuje.

4. Dodavatel není oprávněn postoupit třetí straně jakákoliv práva, nároky či pohledávky plynoucí z této Smlouvy bez předchozího písemného souhlasu Objednatele.

5. Pokud bude při provádění předmětu plnění Dodavatelem využito i volně šiřitelné programové vybavení, je Dodavatel povinen zpracovat přehled licencí a předložit ho jako součást akceptačního protokolu. Dodavatel je povinen zajistit, že poskytnutím uvedených licencí nedojde k porušení práv třetích stran.

6. Dodavatel je povinen určit kontaktní osobu řídící evidenci osob Dodavatele oprávněných k přístupu do síťové infrastruktury Objednatele. V případě změny této kontaktní osoby je Dodavatel povinen bezodkladně oznámit Objednateli takovou změnu, včetně sdělení nové kontaktní osoby.

7. Přístup k síťové infrastruktuře Objednatele je možné povolit pouze po předchozím provedení evidence osoby zastupující Dodavatele v registru identit Objednatele nebo obdobném systému Objednatele, a to na základě požadavku Dodavatele na přístup. Přidělení oprávnění zaměstnancům Dodavatele bude řízeno principem nezbytného minima a není nárokové. Systém pro přístup do síťové infrastruktury Objednatele určí Objednatel.

8. Dodavatel se zavazuje, že neumožní, aby byl tentýž udělený přístup do síťové infrastruktury Objednatele sdílen více zaměstnanci Dodavatele, případně jeho poddodavateli či zaměstnanci poddodavatele.

9. Dodavatel se zavazuje zajistit, aby osoby podílející se na poskytování předmětu plnění této Smlouvy Objednateli, které přistupují do interní sítě, chránily autentizační prostředky a údaje. Dodavatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet zablokován a řešen jako kybernetická bezpečnostní událost ve smyslu příslušné řídící dokumentace, a mohou být uplatněny příslušné postupy zvládání kybernetické bezpečnostní události (např. okamžité zrušení přístupu k informačním aktivům fyzických osob externího subjektu). Dodavatel bere na vědomí, že postup zvládáním kybernetické bezpečnostní události či jiný důsledek porušení bezpečnostních opatření nebude posuzován jako okolnost vylučující odpovědnost Dodavatele za prodlení s řádným a včasným plněním předmětu této Smlouvy, a nebude důvodem k jakékoli náhradě případné újmy způsobené Dodavateli či jiné osobě na jeho straně.

10. Dodavatel se zavazuje, že neumožní připojit koncové zařízení do sítě Objednatele bez předchozího schválení připojení určenou osobu na straně Objednatele.

11. Dodavatel se zavazuje, že všechny jeho informační systémy, které se budou připojovat do síťové infrastruktury Objednatele, jsou a budou chráněny vhodným způsobem proti malware.

12. Dodavatel je povinen mít po celou dobu trvání této Smlouvy zajištěno **pojištění odpovědnosti za škodu** způsobenou třetí osobě, přičemž pojistná částka musí svou výší odpovídat minimálně 10.000.000 Kč. Dodavatel je povinen pojistnou smlouvu, nebo potvrzení o pojištění, předložit Objednateli bezodkladně po uzavření této Smlouvy, nejpozději však do předložení prováděcího projektu před zahájením dodávky a implementace řešení, a dále pak v průběhu provádění předmětu plnění kdykoliv na vyzvání Objednatele.

13. Dodavatel se zavazuje při provádění předmětu plnění dle této Smlouvy zajistit dodržování veškerých pracovněprávních předpisů (odměňování, pracovní doba, doba odpočinku mezi směnami, placené přesčasy, legální zaměstnávání pracovníků), 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., zákoník práce, ve znění pozdějších předpisů, a to vůči všem osobám, které se na plnění předmětu této smlouvy podílejí, bez ohledu na to, zda budou činnosti prováděné v rámci plnění předmětu této Smlouvy prováděny přímo Dodavatelem a jeho zaměstnanci, či poddodavatelem. Dodavatel se zavazuje, že provádění předmětu plnění dle této Smlouvy bude prováděno v souladu s úmluvami Mezinárodní organizace práce, jimiž je Česká republika vázána, zejména s úmluvami, které upravují stejné odměňování pracujících mužů a žen za práci stejné hodnoty, diskriminaci, bezpečnost a zdraví pracovníků, a pracovní prostředí.

14. Dodavatel se zavazuje zachovávat férové vztahy ke svým poddodavatelům. Jakýkoliv závazek uzavřený mezi Dodavatelem a jeho poddodavatelem v souvislosti s plněním (části) předmětu této smlouvy nesmí obsahovat splatnost faktury delší než 30 dnů.

15. Dodavatel se zavazuje při realizaci předmětu této Smlouvy k šetrnému využívání zdrojů a materiálů, k řádnému managementu nakládání s odpady a k omezení jejich nadbytečné produkce.

16. Objednatel je oprávněn průběžně kontrolovat dodržování povinností dodavatele dle odst. 13. až 15. tohoto článku Smlouvy, přičemž Dodavatel je povinen tuto kontrolu umožnit, strpět a poskytnout Objednateli veškerou nezbytnou součinnost k jejímu provedení. Zjistí-li Objednatel, že Dodavatel porušil některou z povinností dle odst. 13. až 15. tohoto článku Smlouvy, a nesjednal nápravu ani po předchozím písemném upozornění Objednatele, je Objednatel oprávněn od této smlouvy odstoupit pro podstatné porušení povinnosti Dodavatele.

VIII.PRÁVA A POVINNOSTI OBJEDNATELE

1. Objednatel se zavazuje poskytnout Dodavateli součinnost, která je nezbytná k řádnému poskytnutí předmětu plnění této Smlouvy, a lze ji po něm spravedlivě požadovat.

2. Objednatel je oprávněn průběžně vykonávat kontrolu provádění předmětu plnění. Dodavatel umožní provádění kontroly kdykoli během provádění předmětu plnění všem oprávněným osobám určeným Objednatelem. Dodavatel se též zavazuje předkládat Objednateli na jeho žádost ústní či písemné informace o průběhu a obsahu prováděného plnění, a to nejpozději do 2 (dvou) pracovních dnů od doručení žádosti Objednatele. Pro kontrolu provádění plnění platí:

   a) Objednatel alespoň 2 (dva) pracovní dny přede dnem plánované kontroly dle přechozího odstavce písemně sdělí Dodavateli termín kontroly. Dodavatel zajistí přítomnost osoby odpovědné za provádění příslušné části předmětu plnění po celou dobu konání kontroly.

   b) O výsledku kontroly smluvní strany provedou písemný zápis ve 2 (dvou) vyhotoveních, každá ze smluvních stran obdrží po 1 (jednom) vyhotovení zápisu.

   c) Objednatel je oprávněn na základě provedené kontroly požadovat, aby Dodavatel provedl nápravu zjištěného porušení povinnosti Dodavatele nebo odstranění zjištěné vady, a aby plnění poskytoval řádným způsobem.

   d) Dodavatel za účelem vykonání kontroly poskytne osobě pověřené Objednatelem výkonem kontroly veškerou nezbytnou součinnost potřebnou pro řádné plnění jejích povinností.

3. Objednatel se zavazuje uhradit Dodavateli řádně a včas veškeré finanční závazky vyplývající z této Smlouvy.

IX. TRVÁNÍ SMLOUVY A UKONČENÍ SMLOUVY

1. Smluvní strany se dohodly, že tato Smlouva se sjednává na dobu od okamžiku účinného uzavření této Smlouvy do ukončení technické podpory poskytnutého předmětu plnění.

2. Smluvní strany sjednávají poskytování technické podpory předmětu plnění na dobu neurčitou, nebo do doby jejího dřívějšího ukončení podle předchozích ustanovení této Smlouvy nebo podle následujících odstavců tohoto článku Smlouvy.

3. Smluvní strany sjednávají možnost předčasného ukončení této Smlouvy písemnou dohodou smluvních stran.

4. Smluvní strany se dohodly, že mohou od této Smlouvy odstoupit v případech, kdy to stanoví zákon nebo tato Smlouva. Odstoupení od Smlouvy musí být provedeno písemnou formou a je účinné okamžikem jeho doručení druhé smluvní straně. Odstoupením od Smlouvy nezanikají nároky na náhradu škody, smluvní ujednání týkající se volby práva, smluvních pokut, řešení sporů mezi smluvními stranami a jiná ujednání, která podle projevené vůle smluvních stran nebo vzhledem ke své povaze mají trvat i po ukončení Smlouvy. Zejména se jedná o práva a povinnosti související s odpovědností za škodu, smluvními pokutami, fakturací cen, s úroky z prodlení, odpovědností za vady, ochranou osobních údajů a důvěrných informací apod.

5. Objednatel je oprávněn odstoupit od této Smlouvy zejména, nikoli však výlučně, v případě, kdy:

   a) prodlení Dodavatele s předáním předmětu plnění k termínu stanoveném čl. IV. odst. 5. této Smlouvy trvá déle než 15 kalendářních dnů;

   b) prodlení Dodavatele se splněním povinnosti odstranit vady či nedodělky uvedené v protokolu o předání a převzetí předmětu plnění trvá déle než 7 kalendářních dnů od smluvními stranami sjednaného či Smlouvou stanoveného termínu;

   c) z průběžně prováděné kontroly vyvstanou důvodné pochybnosti o schopnosti Dodavatele splnit předmět plnění řádně a úplně, a Dodavatel nebude schopen na výzvu Objednatele tyto objektivní důvody vyvrátit;

   d) předmět plnění vykazuje vady či nedodělky, které neumožní jeho řádné užívání k účelu, který je sjednán touto Smlouvou,

   e) prokáže-li se kterékoliv prohlášení Dodavatele učiněné v této Smlouvě jako nepravdivé,

   f) Dodavatel neplní pokyny Objednatele při poskytování předmětu plnění, a nezjedná nápravu do 7 kalendářních dnů poté, co byl Objednatelem na tuto skutečnost písemně upozorněn,

   g) Dodavatel brání Objednateli v provádění kontrol či zkoušek předmětu plnění nebo jeho částí, či více než 7 kalendářních dnů neposkytuje součinnost, ke které se zavázal touto Smlouvou,

   h) pokud Dodavatel nevyhoví požadavku Objednatele na výměnu poddodavatele, pokud byly splněny podmínky podle této Smlouvy,

   i) poruší-li Dodavatel opakovaně (více než dvakrát) pravidla pro vzdálený přístup Dodavatele stanovená v čl. VII. této Smlouvy nebo nezajistí-li jejich dodržování,

   j) v případech vymezených § 223 odst. 1 až 3 ZZVZ,

   k) dostane-li se Dodavatel do stavu úpadku nebo hrozícího úpadku, dojde-li k zahájení likvidace Dodavatel, nebo dojde-li k postižení podstatné části majetku Dodavatel výkonem rozhodnutí nebo exekucí.

6. Dodavatel je oprávněn odstoupit od této Smlouvy v případě prodlení Objednatele se zaplacením jakékoliv splatné částky dle této Smlouvy po dobu delší než 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 15 kalendářních dnů od prokazatelného doručení takovéto výzvy Objednateli. Toto ustanovení se dle dohody smluvních stran nevztahuje na

případy, kdy bude prodlení Objednatele zapříčiněno opožděným uvolněním finančních prostředků z veřejných zdrojů.

7. V případě odstoupení od Smlouvy nemá Dodavatel nárok na zaplacení ceny předmětu plnění v plném rozsahu. Dodavatel je pouze oprávněn žádat po Objednateli to, o co se Objednatel poskytnutím předmětu plnění Dodavatelem obohatil, a to v rozsahu plnění, které je Objednatelem využitelné i po takovém odstoupení od Smlouvy.

8. Smluvní strany se dohodly, že v případě předčasného ukončení Smlouvy odstoupením od Smlouvy si poskytnou vzájemnou součinnost k převodu a nabytí licencí či oprávnění plynoucích z takových licencí již pořízených Dodavatelem pro Objednatele, kterými Objednatel nedisponuje, resp., které Objednatel případně dosud neuhradil Dodavateli podle čl. VI. této Smlouvy. Dodavatel je povinen takové licence převést na Objednatele, a Objednatel je povinen je nabýt a uhradit za ně Dodavateli cenu stanovenou podle této Smlouvy, celkově nejvýše však do částky odpovídající výši platby za 1 rok, nebrání-li takovému převodu objektivní překážky ležící vně vůle smluvních stran.

9. Při předčasném ukončení závazku z této Smlouvy se Dodavatel zavazuje provést na své náklady veškeré práce, které budou nezbytné k zabránění vzniku škody či jiné újmy na straně Objednatele či na straně třetích osob. Dodavatel bude v takovém případě rovněž povinen předat Objednateli bezplatně veškeré informace, které s dílem souvisí a jsou nezbytné k zabránění vzniku škody či jiné újmy na straně Objednatele či třetích osob.

X. REALIZAČNÍ TÝM

1. Dodavatel provede předmět plnění zejména prostřednictvím osob, které jsou uvedeny v příloze č. 3 této Smlouvy. Jedná se o osoby, kterými Dodavatel prokazoval splnění části technické kvalifikace v rámci své účasti v zadávacím řízení veřejné zakázky.

2. Dodavatel prohlašuje, že se všichni členové realizačního týmu, jimiž v rámci zadávacího řízení veřejné zakázky prokazoval splnění kvalifikace, budou aktivně podílet na provedení příslušné části předmětu plnění podle této Smlouvy a nabídky podané v rámci zadávacího řízení veřejné zakázky.

3. V případě, že kvalita předmětu plnění dle této Smlouvy prováděná některým z členů realizačního týmu neodpovídá požadavkům této Smlouvy, nebo člen realizačního týmu nevykonává pokyny Objednatele podle Smlouvy, nebo nastane jiný závažný důvod pro změnu realizačního týmu, pak je Objednatel oprávněn požadovat výměnu člena realizačního týmu. Dodavatel do 10 kalendářních dnů od doručení žádosti Objednatele navrhne nového člena realizačního týmu, přičemž nově navržený člen realizačního týmu musí disponovat stejnou nebo vyšší úrovní kvalifikace, jakou disponoval původní člen realizačního týmu, kterým byla prokazována kvalifikace v rámci zadávacího řízení veřejné zakázky, resp. v případě v zadávacím řízení veřejné zakázky hodnoceného člena realizační týmu stejnou nebo vyšší hodnocenou kvalitativní úrovní. Nový člen realizačního týmu následně musí být akceptován ze strany Objednatele. Akceptace nového člena realizačního týmu je podmíněna předložením dokladů, prokazujících dosažení minimálně shodné úrovně jeho zkušeností jako u původního člena.

4. Pokud jsou důvody pro změnu některého ze členů realizačního týmu dány na straně Dodavatele, Dodavatel může ke změně přistoupit pouze ze závažných důvodů s předchozím souhlasem Objednatele. Nově navržený člen realizačního týmu přitom musí disponovat stejnou nebo vyšší úrovní kvalifikace,

jakou disponoval člen realizačního týmu, kterým byla prokazována kvalifikace v rámci zadávacího řízení veřejné zakázky, resp. v případě v zadávacím řízení veřejné zakázky hodnoceného člena realizační týmu stejnou nebo vyšší hodnocenou kvalitativní úrovní Objednatel udělí písemný souhlas se změnou do 10 kalendářních dnů od doručení žádosti ze strany Dodavatele, jejíž přílohou budou doklady prokazující dosažení minimálně shodné úrovně zkušeností nového člena jako u původního člena.

5. Realizační tým Dodavatele může být tvořen i dalšími osobami nad rámec počtu stanoveného minimálními požadavky kvalifikace. Dodavatel se zavazuje, že při běžné pracovní komunikaci s Objednatelem či jeho zástupci bude užíváno českého nebo slovenského jazyka, nedohodnou-li se smluvní strany či jejich jednotlivý zástupci jinak.

XI. PODDODAVATELÉ

1. Dodavatel je oprávněn využít k provedení předmětu plnění jiné osoby pouze v případě, že tyto osoby jsou součástí seznamu poddodavatelů, který tvoří přílohu č. 4 této Smlouvy a který byl rovněž součástí nabídky Dodavatele do veřejné zakázky, není-li stanoveno jinak. Dodavatel se zavazuje, že poddodavatelé, kterými prokazoval splnění kvalifikace v zadávacím řízení veřejné zakázky, se budou podílet na plnění povinností Dodavatele vyplývajících ze Smlouvy v rozsahu podle nabídky Dodavatele podané do zadávacího řízení veřejné zakázky.

2. Dodavatel odpovídá za plnění poddodavatele tak, jako by plnil sám. Dodavatel je povinen vybrat takového poddodavatele, který neodporuje požadavkům, jaké má Objednatel na Dodavatele.

3. Dodavatel prohlašuje a zavazuje se, že ručí za uspokojení povinnosti poddodavatele nahradit újmu způsobenou poddodavatelem Objednateli při plnění nebo v souvislosti s plněním povinností ze Smlouvy, jestliže povinnost k náhradě újmy nesplnil poddodavatel sám.

4. V případě, že poddodavatel je s plněním svých závazků, které přímo souvisí s předmětem této smlouvy, v prodlení více než 10 kalendářních dnů, nebo byl poddodavateli uložen zákaz plnění veřejných zakázek, ocitnul se v úpadku nebo hrozícím úpadku, nebo byl pravomocně odsouzen za trestný čin uvedený v příloze č. 3 ZZVZ, nebo je zde jiný vážný důvod, pak je Objednatel oprávněn požadovat po Dodavateli výměnu poddodavatele. Za jiný vážný důvod dle předchozí věty se považuje rovněž stav nereflektování výhrad sdělených Objednatelem k činnosti poddodavatele, či řádnosti a kvality jím poskytovaného plnění apod., kdy uvedené nedostatky nebyly napraveny ani po předchozí písemné stížnosti adresované Objednatelem Dodavateli. Dodavatel je povinen navrhnout nového poddodavatele do 10 kalendářních dnů od doručení žádosti Objednatele. Nový poddodavatel se může podílet na poskytování předmětu plnění pouze na základě písemného souhlasu Objednatele, který Objednatel udělí po provedení kontroly dokladů předložených Dodavatelem k novému poddodavateli.

5. Pokud jsou důvody pro změnu či doplnění poddodavatele dány na straně Dodavatele, Dodavatel může ke změně či doplnění přistoupit pouze s předchozím souhlasem Objednatele. Jedná-li se o změnu poddodavatele, prostřednictvím něhož byla prokazována kvalifikace, nově navržený poddodavatel musí disponovat stejnou nebo vyšší úrovní kvalifikace, jakou disponoval poddodavatel, kterým byla prokazována kvalifikace v rámci zadávacího řízení veřejné zakázky. Objednatel udělí písemný souhlas se změnou poddodavatele po doručení žádosti ze strany Dodavatele, jejíž přílohou budou doklady prokazující kvalifikaci nového poddodavatele, a po provedení kontroly takto předložených dokladů.

XII. VLASTNICKÉ PRÁVO A UŽÍVACÍ PRÁVA, DUŠEVNÍ VLASTNICTVÍ

1. Objednatel nabývá vlastnické právo k poskytnutému předmětu plnění podpisem akceptačního protokolu, a to v rozsahu akceptace.

2. Dodavatel se zavazuje při poskytování předmětu plnění neporušit práva třetích osob, která těmto osobám mohou plynout z duševního vlastnictví, zejména z autorských práv a práv průmyslového vlastnictví. Dodavatel se zavazuje, že Objednateli uhradí veškeré náklady, výdaje, škody a majetkovou i nemajetkovou újmu, které Objednateli vzniknou v důsledku uplatnění práv třetích osob vůči Objednateli v souvislosti s porušením povinnosti Dodavatele dle předchozí věty. Uplatní-li třetí osoba své právo k předmětu plnění nebo jeho části, zavazuje se Dodavatel dále Objednateli bezplatně poskytnout, zabezpečit a/nebo uhradit náhradní řešení, které nebude dotčeno právem třetí osoby.

3. V případě, že je výsledkem činnosti Dodavatele dle této Smlouvy či jeho součástí dílo, které podléhá ochraně podle zákona č. 121/2000 Sb., o právu autorském, právech souvisejících s právem autorským a o změně dalších zákonů (autorský zákon), v platném znění (dále jen „autorský zákon“) a občanského zákoníku, získá Objednatel k takto vytvořenému dílu jako celku i k jeho jednotlivým částem licenci, přičemž odměna za poskytnutou licenci je již součástí ceny předmětu plnění.

4. Pro účely této Smlouvy rozlišují smluvní strany mezi „Individualizovaným dílem“ a „Standardizovaným dílem“, kdy:

   - Individualizovaným dílem se rozumí dílo dodávané Dodavatelem dle této Smlouvy, které bylo vytvořeno nebo upraveno pro účely této Smlouvy;
   - Standardizovaným dílem se rozumí dílo dodávané Dodavatelem dle této Smlouvy, které nebylo vytvořeno nebo upraveno pro účely této Smlouvy.

   V případě pochybností se na plnění hledí jako na Individualizované dílo, dokud Dodavatel neprokáže opak.

5. Dodavatel na základě této Smlouvy poskytuje Objednateli oprávnění k výkonu práv duševního vlastnictví k Individualizovanému dílu. Licence se týká veškerých autorských nebo jiných duševních práv k Individualizovanému dílu, jejichž povaha umožňuje licenci v dále uvedeném rozsahu poskytnout, a to:

   a) licence k veškerým známým způsobům užití takového díla, zejména, nikoliv však výlučně, k účelu stanovenému touto Smlouvou a v rozsahu minimálně nezbytném pro řádné užívání příslušného Individualizovaného díla Objednatelem v souladu s touto Smlouvou;
   b) licence neodvolatelná a nevypověditelná;
   c) licence neomezená územním rozsahem a rovněž tak neomezená způsobem nebo rozsahem užití;
   d) licence udělená na dobu určitou, a to po celou dobu trvání majetkových práv k dílu (účinnost licence však trvá i po skončení účinnosti této Smlouvy, nedohodnou-li se Smluvní strany výslovně jinak);
   e) licence vztahující se i na budoucí aktualizace dodaného předmětu plnění v rámci jeho podpory;
   f) licence převoditelná a postupitelná, tj. která je udělena s právem udělení podlicence či postoupení licence jakékoliv třetí osobě;
   g) licence, kterou není Objednatel povinen využít.

6. Licence je poskytnutá v maximálním rozsahu povoleném platnými právními předpisy. Dodavatel podpisem Smlouvy prohlašuje, že vlastní či oprávněně disponuje veškerými oprávněními k autorskému dílu, které bude součástí předmětu plnění dle této Smlouvy, zejména, nikoliv však výlučně, že získal veškerá oprávnění autorů či třetích osob k takovému dílu a je oprávněn je poskytnout Objednateli, a to zejména, nikoliv však výlučně, veškerá oprávnění uvedená v tomto článku Smlouvy.

7. Dodavatel uděluje Objednateli souhlas k tomu, aby Objednatel (či jím pověřená třetí osoba) dle své potřeby zasahoval do Individualizovaného díla, zejm. je oprávněn jej zveřejnit, upravovat, zpracovávat, překládat, měnit jeho název, spojit s dílem jiným a zařadit jej do díla souborného. Ustanovení tohoto odstavce neomezuje práva Objednatele plynoucí z § 66 zákona č. 121/2000 Sb., autorský zákon.

8. Dodavatel se zavazuje zajistit oprávnění k užití předmětu práv duševního vlastnictví jiných osob, který představuje Individualizované dílo, a souhlas se zásahy do takového předmětu práv duševního vlastnictví v takovém rozsahu, aby Objednateli mohl udělit licenci k Individualizovanému dílu v rozsahu této Smlouvy, souhlas k zásahům ve smyslu předchozího odst. 7. tohoto článku Smlouvy, a aby mohl Objednateli předat zdrojový kód a dokumentaci k takovému předmětu práv duševního vlastnictví.

9. Jedná-li se o oprávnění k výkonu práv duševního vlastnictví ke Standardizovanému dílu, je Dodavatel povinen Objednateli poskytnout:

    a) licenci ke Standardizovanému dílu, pokud je autorem Standardizovaného díla Dodavatel, nebo
    b) zajistit poskytnutí licence ke Standardizovanému dílu Objednateli třetí osobou, pokud je autorem Standardizovaného díla jiná třetí osoba,

    a to v rozsahu, který zajistí plnou využitelnost Standardizovaného díla při jeho vývoji, rozvoji, provozu a užívání bez nutnosti platit Dodavateli nebo třetí osobě odměnu nad rámec odměny dle této Smlouvy. Nabyvatelem licence ke Standardizovanému dílu podle tohoto odstavce musí být bezprostředně Objednatel.

10. Dodavatel je při plnění této Smlouvy oprávněn použít tzv. free and open-source software (dále jen „FOSS“) s tím, že užití FOSS a licence se k tomu vztahující nesmí být v rozporu s účelem této Smlouvy. Dodavatel společně s předáním svého výstupu, který obsahuje FOSS, sdělí Objednateli informace o tom, že byl FOSS použit a jaké licenční podmínky se na užití FOSS vztahují. Využije-li Dodavatel při plnění této Smlouvy FOSS, zavazuje se zajistit po dobu trvání Smlouvy jeho podporu tak, aby nedošlo k omezení jeho funkčnosti či bezpečnosti, zejména v situaci, kdy původní tvůrce příslušného FOSS ukončí poskytování podpory. Odměna za jakékoliv plnění Dodavatele související se zajištěním podpory FOSS dle předchozí věty, včetně případného nahrazení FOSS bez podpory jiným software, je zahrnuta v odměně za poskytování technické podpory dle čl. VI. této Smlouvy a Dodavateli nenáleží žádná další odměna či kompenzace.

11. Dodavatel je povinen současně s předáním předmětu plnění, resp. těch částí předmětu plnění, které jsou počítačovým programem, předat Objednateli zdrojový kód včetně administrátorského přístupu k němu (dále jen „zdrojový kód“); výjimku z této povinnosti tvoří odst. 14. tohoto článku Smlouvy.

12. Zdrojový kód musí být spustitelný v prostředí Objednatele a zaručující možnost ověření, že je kompletní a ve správné verzi, tzn. umožňující instalaci, spuštění a ověření funkcionality, a to včetně podrobné dokumentace zdrojového kódu, na základě které bude Objednatel schopen zjistit veškeré funkce a vnitřní vazby počítačového programu a zasahovat do něj. Zdrojový kód bude Objednateli Dodavatelem předán na nepřepisovatelném technickém nosiči dat s viditelně označeným názvem „Zdrojový kód“ a označením

jeho verze a dne předání zdrojového kódu, případně na základě dohody smluvních stran bude k předání využito sdíleného elektronického úložiště, které zřídí Dodavatel a poskytne do něj Objednateli přístup. O předání zdrojového kódu bude smluvními stranami sepsán písemný protokol.

13. Povinnost Dodavatele uvedená v předcházejícím odstavci se přiměřeně použije i pro jakékoliv opravy, změny, doplnění, upgrade nebo update zdrojového kódu, k nimž dojde při provádění předmětu plnění nebo v rámci jeho oprav (dále jen „změna zdrojového kódu“). Dokumentace změny zdrojového kódu musí obsahovat podrobný popis a komentář každého zásahu do zdrojového kódu.

14. Výjimkou z ujednání týkajících se předání zdrojového kódu je situace, kdy součástí plnění je Standardizované dílo a předání zdrojového kódu ke Standardizovanému dílu není možné s ohledem na práva třetích osob.

15. Práva získaná v rámci plnění poskytnutého podle tohoto článku 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.

XIII. ODPOVĚDNOST ZA VADY, ZÁRUKA A TECHNICKÁ PODPORA

1. Dodavatel poskytuje záruku za dodané řešení v délce, která je pro jednotlivé součásti řešení uvedena v příloze č. 1 této Smlouvy, minimálně však standardní záruku po dobu prvních 36 měsíců od převzetí dokončeného řešení Objednatelem, a dále nadstandardní (prodlouženou) záruku v délce 24 měsíců následujících po uplynutí standardní záruky, celkem tedy 60 měsíců.

2. Dodavatel odpovídá za vady, které má předmět plnění v době jeho převzetí a akceptace, a za vady, které se projeví v záruční době, popřípadě v důsledku škody, za kterou odpovídá Dodavatel.

3. Veškeré vady předmětu plnění je Objednatel oprávněn uplatnit u Dodavatele kdykoliv po zjištění vady během záruky, a to formou písemného oznámení, obsahujícího specifikaci zjištěné vady nebo popis, jak se vada projevuje. Objednatel je oprávněn uplatnit veškerá zákonná práva z vadného plnění. Volba práva z vadného plnění svědčí Objednateli. Neuvede-li Objednatel, jaké právo v souvislosti s vadou předmětu plnění uplatňuje, má se za to, že požaduje odstranění vady, tj. provedení opravy předmětu plnění nebo jeho části.

4. Dodavatel v rámci předmětu plnění této Smlouvy poskytuje Objednateli rovněž technickou podporu a rozšířenou servisní podporu dodaného řešení. Toto plnění zahrnuje zejména (nikoli výlučně):

   - odstraňování nebo spolupráci při odstraňování závad či nefunkčností,
   - kontrolu stavu jednotlivých komponent řešení a po vzájemné dohodě aplikaci nápravných opatření,
   - řešení vzniknuvších problémů a incidentů,
   - bezplatná výměna vadného zařízení/komponentu,
   - aktualizace firmware a software dodaných produktů,
   - aktualizaci dokumentace,
   - na vyžádání změnu nastavení, konfiguraci řešení,
   - podporu při implementaci upgradů,
   - poskytování informací,
   - poskytování odborných konzultací a podpory.

5. Za účelem poskytování služeb technické podpory, rozšířené servisní podpory a příjmu požadavků Objednatele je Dodavatel povinen zřídit a udržovat po celou dobu trvání této Smlouvy systém HelpDesk. Systém HelpDesk bude dostupný na adrese: Kounicova 67a, Brno, 602 00, E-mail: servishw@aricoma.com.

6. Příjem požadavků v systému HelpDesk musí být zajištěn v režimu 7x24. Samotná technická podpora Dodavatele bude poskytována v pracovní dny v pracovní době od 07:00 do 16:00 hodin (dále jen „*pracovní doba*“).

7. Garantovaná doba odezvy Dodavatele na Objednatelem nahlášený požadavek v systému HelpDesk činí v rámci pracovní doby 1 hodinu. Je-li požadavek nahlášen mimo pracovní dobu, je počátkem shora uvedené doby 07:00 hodin nejbližšího pracovního dne.

8. Dodavatel je povinen zahájit řešení **kritického incidentu** ohrožujícího provoz nejpozději do 4 pracovních hodin od nahlášení požadavku v systému HelpDesk, a v případě **nekritického incidentu** NBD (next business day) od nahlášení.

9. Dodavatel je povinen vyřešit požadavek za podmínek stanovených v příloze č. 1 této Smlouvy ve lhůtě dohodnuté zástupci Objednatele a Dodavatele, a nedohodnou-li se, pak v případě kritického incidentu ve lhůtě nejpozději do 1 pracovního dne od nahlášení, a v případě nekritického incidentu do 2 pracovních dnů od nahlášení požadavku v systému HelpDesk. V případě kritických incidentů způsobujících nefunkčnost řešení se Dodavatel zavazuje vyvinout maximální úsilí k odstranění závady způsobující takovou nefunkčnost a tuto odstranit bez zbytečného odkladu v co nejkratší technicky obhajitelné lhůtě.

10. Technická podpora bude Dodavatelem poskytována jak proaktivně (např. průběžné kontroly stavu komponent Dodavatelem), tak reaktivně (činnost Dodavatele vyvolaná na základě žádosti Objednatele). Kontaktními osobami v záležitostech poskytování technické podpory jsou:

    10.1. na straně Objednatele: Mgr. Leona Valterová, e-mail: reditel@spgs-bce.cz, tel.: +420 516 802 543,

    10.2. na straně Dodavatele: Petr Polák, e-mail: petr.polak@aricoma.com, tel.: +420 605 294 596.

11. Dodavatel je povinen vést evidenci poskytování technické podpory a předkládat ji Objednateli pravidelně 1 x za čtvrtletí, nebo na žádost Objednatele mimo uvedený interval (dále jen „***reporty***“). Z reportů bude zřejmé, v jakém rozsahu a v jaké oblasti byly služby technické podpory poskytnuty, a jaká je bilance čerpání hodin základní technické podpory a rozšířené servisní podpory. Nespotřebované hodiny základní technické podpory za jednotlivé měsíce jsou převoditelné v rámci jednoho roku. Dodavatel se zavazuje, že umožní Objednateli přístup k evidenci požadavků v HelpDesku Dodavatele a uchová takto přístupné záznamy po dobu trvání této Smlouvy, minimálně do ukončení poskytování technické podpory.

12. Další podmínky poskytování technické podpory jsou uvedeny v příloze č. 1 této Smlouvy.

XIV. NÁHRADA ŠKODY

1. Každá smluvní strana je povinna nahradit škodu jí způsobenou dle platných právních předpisů a této Smlouvy. Obě smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod.

2. V případě, že při činnosti prováděné Dodavatelem dojde ke způsobení škody Objednateli nebo třetím osobám, která nebude kryta pojištěním Dodavatele sjednaným dle této Smlouvy, bude Dodavatel povinen tuto škodu uhradit z vlastních prostředků.

3. Pokud v důsledku porušení povinností Dodavatele stanovených touto Smlouvou nebude Objednateli uhrazen finanční podíl nebo jeho část poskytovatelem dotace na projektu „Kybernetická bezpečnost – Střední pedagogická škola Boskovice, reg. č. projektu CZ.31.2.0/0.0/0.0/23_092/0008742, bude Dodavatel povinen uhradit Objednateli takto způsobenou škodu (celý finanční podíl, který nebude poskytovatelem dotace podle jeho rozhodnutí vyplacen, nebo který bude muset být Objednatelem vrácen).

XV. SANKCE

1. V případě prodlení Dodavatele s předáním předmětu plnění ve lhůtě dle čl. IV. odst. 5. této Smlouvy, sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 10.000 Kč za každý den prodlení Dodavatele.

2. V případě prodlení Dodavatele se splněním dílčího termínu dle čl. IV. odst. 3 této Smlouvy (T1, T2, T3, T4), sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 1.000 Kč za každý den prodlení Dodavatele.

3. V případě prodlení Dodavatele se splněním povinnosti odstranit vady uvedené v protokolu o předání a převzetí plnění v ujednané lhůtě, včetně drobných vad předmětu plnění, které byly Objednatelem vytknuty, sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 2.000 Kč za každý i započatý den a za každý případ prodlení (za každou vadu).

4. V případě prodlení Dodavatele s předáním zdrojového kódu, dokumentace nebo jiných souvisejících věcí dle čl. XII. odst. 11. a odst. 12. této Smlouvy, sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 5.000 Kč za každý i započatý den prodlení.

5. V případě prodlení Dodavatele se splněním povinnosti zahájit řešení požadavku nahlášeného Objednatelem ve lhůtě dle čl. XIII. odst. 8. této Smlouvy, sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 1.000 Kč za každou i započatou hodinu prodlení v rámci pracovní doby Dodavatele.

6. V případě prodlení Dodavatele se splněním povinnosti vyřešit Objednatelem nahlášený požadavek ve lhůtě stanovené dle čl. XIII. odst. 9. této Smlouvy, sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 5.000 Kč za každý i započatý pracovní den prodlení Dodavatele.

7. V případě nesplnění povinnosti Dodavatele vést evidenci poskytování technické podpory nebo v případě prodlení s jejím předložením Objednateli sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 2.000 Kč za každý jednotlivý případ.

8. V případě:

   a) porušení povinností Dodavatele v souvislosti s užívacími právy dle této Smlouvy sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 100.000 Kč, a to za každé jednotlivé porušení takovéto povinnosti, nestanoví-li Smlouva pro určité porušení jinou smluvní pokutu;

b) porušení povinností Dodavatele vztahujících se k ochraně osobních údajů vymezených v této Smlouvě, sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 100.000 Kč, a to za každé jednotlivé porušení takovéto povinnosti;

c) porušení povinnosti mlčenlivosti a ochrany důvěrných informací, či podmínek a požadavků na zajištění kybernetické bezpečnosti vymezených v této Smlouvě Dodavatelem, sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 200.000 Kč, a to za každé jednotlivé porušení takovéto povinnosti. Za porušení povinnosti mlčenlivosti ze strany Dodavatele jsou pro účely této Smlouvy považovány i případy, kdy k porušení mlčenlivosti dojde ze strany osob, které se podílely na poskytování předmětu plnění vůči Objednateli;

9. V případě, že Dodavatel poruší své povinnosti ve vztahu k pracovněprávní ochraně svých zaměstnanců nebo zaměstnanců poddodavatele, sjednávají smluvní strany povinnost Dodavatele zaplatit Objednateli smluvní pokutu ve výši 1.000 Kč za každý zjištěný případ.

10. V případě, že Dodavatel nedodrží svou povinnost ve vztahu k pravidlům pro vzdálený přístup Dodavatele stanoveným v čl. VII. odst. 6., odst. 7., odst. 8., odst. 10. a odst. 11. této Smlouvy, sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 3.000 Kč za každý jednotlivý zjištěný případ porušení této povinnosti.

11. V případě, že Dodavatel nedodrží svou povinnost předložit Objednateli kopii pojistné smlouvy nebo nebude udržovat své pojištění za podmínek stanovených v čl. VII. odst. 12. této Smlouvy, sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 5.000 Kč za každý i započatý den prodlení, ve kterém nebude uvedená povinnost Dodavatele splněna.

12. Smluvní pokuty a/nebo úroky z prodlení jsou splatné na bankovní účet oprávněné smluvní strany do 14 kalendářních dnů ode dne doručení písemné výzvy oprávněné smluvní strany k jejich úhradě povinnou smluvní stranou, není-li ve výzvě uvedena lhůta delší.

13. Úhrada jakékoliv smluvní pokuty nezbavuje Dodavatele povinnosti splnit své závazky ze Smlouvy, ani jí není dotčen nárok Objednatele na náhradu škody v plné výši, ani povinnost Dodavatele bezodkladně odstranit závadný stav.

XVI. OCHRANA OSOBNÍCH ÚDAJŮ

1. Dodavatel prohlašuje, že si je vědom, že Objednatel jako správce osobních údajů ve smyslu nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) zpracovává osobní údaje Dodavatele, jeho zaměstnanců či členů orgánů a osobní údaje poddodavatelů Dodavatele, jejich zaměstnanců a členů orgánů (vše společně dále jen „osobní údaje") pro účely plnění povinností vyplývajících ze zákona, plnění závazků podle této Smlouvy nebo oprávněných zájmů Objednatele.

2. Objednatel prohlašuje, že veškeré osobní údaje, které Dodavatel poskytne Objednateli nebo se kterými přijde Objednatel do styku v souvislosti s plněním závazku podle této Smlouvy, nebudou využívány k jiným účelům, než k jakým byly Dodavatelem Objednateli poskytnuty nebo Objednatelem pro účely plnění této Smlouvy shromážděny.

3. Dodavatel se zavazuje chránit veškeré osobní údaje, které mu budou poskytnuty, zpřístupněny či se kterými přijde do styku v souvislosti s plněním předmětu této Smlouvy.

XVII. OCHRANA INFORMACÍ, KYBERNETICKÁ BEZPEČNOST

1. Smluvní strany jsou si vědomy toho, že v rámci plnění závazků z této Smlouvy:
    a) si mohou vzájemně vědomě nebo opomenutím poskytnout informace, které budou považovány za důvěrné (dále jen „**důvěrné informace**“);
    b) mohou jejich zaměstnanci a osoby v obdobném postavení získat vědomou činností druhé smluvní strany nebo i jejím opomenutím přístup k důvěrným informacím a osobním údajům druhé smluvní strany.
2. Smluvní strany se zavazují, že žádná z nich bez písemného souhlasu druhé smluvní strany nezpřístupní třetí osobě důvěrné informace, které získala při plnění této Smlouvy, ani je nepoužije v rozporu s účelem této Smlouvy.
3. Veškeré informace, které Dodavatel při plnění této Smlouvy získá od Objednatele nebo o Objednateli či jeho zaměstnancích a spolupracovnících, se považují za důvěrné, není-li stanoveno jinak. Veškeré informace poskytnuté Dodavatelem Objednateli se považují za důvěrné, pouze pokud na jejich důvěrnost Dodavatel Objednateli předem písemně upozornil a Objednatel Dodavateli písemně potvrdil svůj závazek důvěrnost těchto informací zachovávat.
4. 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.
5. Bez ohledu na jiná ustanovení této Smlouvy je Objednatel povinen uveřejnit na příslušných webových stránkách v souladu se ZZVZ či zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů:
    a) tuto Smlouvu včetně všech jejích změn a dodatků;
    b) výši skutečně uhrazené ceny za plnění veřejné zakázky.
6. Dodavatel se zavazuje k zachování bezpečnosti informací a dat obsažených v informačních systémech spravovaných Objednatelem, včetně jiných informačních systémů, které budou plněním smlouvy dotčeny, a to zejm. z pohledu důvěrnosti, dostupnosti a integrity. Dodavatel je povinen při provádění díla jednat tak, aby důvěrnost, dostupnost a integrita informací a dat dle předchozí věty nebyla přerušena, ohrožena, ani omezena. Je-li k plnění dle smlouvy nezbytné důvěrnost, dostupnost či integritu dat omezit, ohrozit nebo přerušit, Dodavatel tak učiní pouze po předchozí dohodě s Objednatelem a jen v Objednatelem odsouhlaseném rozsahu.

7. Dodavatel je povinen v průběhu realizace plnění dle této Smlouvy průběžně poskytovat součinnost při identifikaci významných změn a jejich dopadů do oblasti kybernetické bezpečnosti Objednatele. V případě identifikace významných změn souvisejících s realizací plnění se Poskytovatel zavazuje spolupracovat s Objednatelem na identifikaci potencionálních rizik možných dopadů významných změn a v případě potřeby poskytne Objednateli informace o možných opatřeních pro snížení nepříznivých možných dopadů spojených s významnými změnami.

8. V případě výskytu kybernetického bezpečnostního incidentu, který souvisí s realizací plnění, je Dodavatel povinen o něm Objednatele neprodleně písemně informovat, a to nejpozději do následujícího dne po zjištění kybernetického bezpečnostního incidentu. Toto hlášení bude identifikovat konkrétní část předmětu plnění, kde ke kybernetickému bezpečnostnímu incidentu došlo, dále sdělení, kdy k němu došlo, a zejména popis tohoto incidentu. Smluvní strany následně budou spolupracovat na řešení incidentu a na nápravných opatřeních, tak aby byla minimalizována rizika z incidentu vyplývající.

9. Dodavatel se bude řídit bezpečnostní politikou a předpisy Objednatele, se kterými byl Objednatelem seznámen a které souvisí s plněním dle smlouvy.

XVIII. SOUČINNOST A EXTERNÍ KONTROLA

1. 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.

2. Dodavatel uchová veškerou dokumentaci a účetní doklady související s plněním podle této Smlouvy minimálně do 31.12.2036. Pokud je v českých právních předpisech stanovena lhůta delší než v evropských předpisech, musí být použita pro úschovu delší lhůta, a to i delší než lhůta ujednaná tímto odstavcem Smlouvy.

3. Dodavatel je povinen minimálně do 31. 12. 2036 poskytovat sám či prostřednictvím Objednatele požadované informace a dokumentaci (včetně účetních dokladů) související s realizací projektu zaměstnancům nebo zmocněncům pověřených orgánů (OLAF – Evropský úřad pro boj proti podvodům, Úřad evropského veřejného žalobce, Ministerstva financí ČR, Evropské komise, Evropského účetního dvora, Ministerstva vnitra ČR, Nejvyššího kontrolního úřadu a dalším příslušným vnitrostátním orgánům), a je povinen vytvořit výše uvedeným subjektům podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout jim při provádění kontroly součinnost. Náklady související s těmito kontrolami a poskytováním informací a součinnosti jsou zahrnuty do ceny díla.

XIX. ROZHODNÉ PRÁVO

1. Vztahy mezi smluvními stranami touto Smlouvou výslovně neupravené se budou řídit obecně závaznými právními předpisy České republiky, zejména občanským zákoníkem a příslušnými právními předpisy souvisejícími.

2. Veškeré spory mezi smluvními stranami vyplývající z této Smlouvy nebo z jejího porušení, ukončení nebo neplatnosti budou rozhodovány věcně a místně příslušnými soudy České republiky dle sídla Objednatele, pokud nebudou vyřešeny dohodou obou smluvních stran.

XX. ZÁVĚREČNÁ USTANOVENÍ

1. Tato Smlouva nabývá platnosti dnem podpisu obou smluvních stran, účinnosti nabývá okamžikem zveřejněním Smlouvy v registru smluv podle zákona č. 340/2015 Sb., o registru smluv. Uveřejnění Smlouvy v registru smluv zajistí Objednatel, o čemž bezodkladně vyrozumí Dodavatele.

2. Tato Smlouva představuje úplnou dohodu smluvních stran o předmětu této Smlouvy. Tuto Smlouvu je možné měnit pouze písemnou dohodou smluvních stran ve formě vzestupně číslovaných dodatků této Smlouvy uzavřených v souladu s příslušnými ustanoveními občanského zákoníku, popř. obdobných předpisů tyto předpisy nahrazujících, a podepsaných osobami oprávněnými jednat jménem smluvních stran.

3. Smluvní strany si nepřejí, aby nad rámec výslovných ustanovení této Smlouvy byla jakákoliv práva a povinnosti dovozována z dosavadní či budoucí praxe zavedené mezi smluvními stranami či zvyklostí zachovávaných obecně či v odvětví týkajícím se předmětu plnění této Smlouvy, ledaže je v této Smlouvě výslovně sjednáno jinak. Vedle shora uvedeného si smluvní strany potvrzují, že si nejsou vědomy žádných dosud mezi nimi zavedených obchodních zvyklostí či praxe.

4. Smluvní strany se podpisem této Smlouvy dohodly, že vylučují aplikaci ustanovení § 557 občanského zákoníku.

5. Pro vyloučení pochybností Dodavatel výslovně potvrzuje, že je podnikatelem, uzavírá tuto Smlouvu při svém podnikání, a na tuto Smlouvu se tudíž neuplatní ustanovení § 1793 občanského zákoníku.

6. Dodavatel na sebe v souladu s ustanovením § 1765 odst. 2 občanského zákoníku přebírá nebezpečí změny okolností. Tímto však nejsou nikterak dotčena práva smluvních stran upravená v této Smlouvě.

7. Je-li nebo stane-li se jakékoli ustanovení této Smlouvy neplatným, nezákonným nebo nevynutitelným, netýká se tato neplatnost a nevynutitelnost zbývajících ustanovení této Smlouvy. Smluvní strany se tímto zavazují nahradit do 10-ti pracovních dnů po doručení výzvy druhé smluvní strany jakékoli takové neplatné, nezákonné nebo nevynutitelné ustanovení ustanovením, které je platné, zákonné a vynutitelné a má stejný nebo alespoň podobný obchodní a právní význam.

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

9. Dodavatel není oprávněn započítat, zastavit ani postoupit žádné své peněžité nároky vůči Objednateli vzniklé na základě této Smlouvy na třetí osobu bez předchozího písemného souhlasu Objednatele.

10. Dodavatel se zavazuje, že bez předchozího výslovného písemného souhlasu Objednatele nepostoupí třetí straně tuto Smlouvu nebo jakoukoli její část nebo jakékoli právo či závazek z této Smlouvy vyplývající. Toto ustanovení se nevztahuje na případné právní nástupce smluvních stran.

11. Tato Smlouva je uzavřena elektronickou formou s využitím kvalifikovaných elektronických podpisů osob oprávněných právně jednat v zastoupení smluvních stran.

12. Smluvní strany prohlašují, že tato Smlouva je projevem jejich pravé a svobodné vůle a na důkaz dohody o všech článcích této Smlouvy připojují své podpisy.

13. Nedílnou součástí této Smlouvy jsou:

    Příloha č. 1 – Technická specifikace a popis nabízeného řešení

Příloha č. 2 – Cenová nabídka

Příloha č. 3 – Realizační tým

Příloha č. 4 – Seznam poddodavatelů

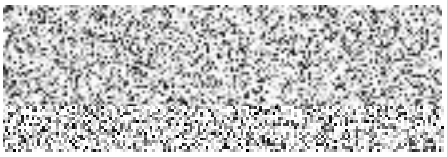
Za Objednatele

V Boskovicích

Mgr. Leona Valterová
ředitelka

Za Dodavatele

V Brně dne dle data el. podpisu



Petr Konečný, ředitel RC, na základě plné moci

Národní plán obnovy

Financováno Evropskou unií NextGenerationEU

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Střední pedagogická škola Boskovice, příspěvková organizace

TECHNICKÁ SPECIFIKACE

KYBERBEZPEČNOST

Veškeré produkty, které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky a dodavatel splnění těchto podmínek potvrdí samostatným čestným prohlášením:

(a) jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
(b) mají plnou záruku od výrobce,
(c) jsou podporovány výrobcem a jsou součástí servisního a podpůrného programu výrobce,
(d) obsahují všechny nezbytné licence na používání příslušného softwaru,
(e) jsou určeny pro provoz v České republice.

Tyto skutečnosti dodavatel doloží:

a) potvrzením výrobce daného zařízení, nebo
b) čestným prohlášením distributora, nelze-li prohlášení výrobce získat, nebo
c) jiným rovnocenným dokladem (doklady) v případě, že doklady dle předchozích písm. a) a b) není dodavatel z důvodů, které mu nelze přičítat, schopen předložit (takové důvody musí dodavatel doložit).

Zadavatel si vyhrazuje právo na ověření všech dodaných informací od výrobce daného zařízení a zjištění původu výrobků nejpozději při jejich předávání, a to dle příslušných sériových čísel a právo podpisu akceptačního protokolu, osvědčujícího převzetí dodávky, až po ověření původu výrobku.

Dodavatel doloží toto potvrzení dle předchozího odstavce ke všem nabídnutým technologiím v níže uvedeným kapitolám technické specifikace:

1) nástroj pro ochranu integrity komunikačních sítí
2) nástroj pro ochranu koncových stanic
3) nástroje pro ochranu integrity komunikačních sítí
4) nástroj pro zajišťování úrovně dostupnosti informací

- **Server 2 ks**
- **Server BACK UP - 1 ks**
- **SERVER BACKUP - časové zámky (Hardened Repository) – 1KS**
- **Diskové pole – 1KS**

5) nástroj pro ověřování identity uživatelů

1) nástroj pro ochranu integrity komunikačních sítí

FIREWALL – 1 KS

Parametr	Minimální požadavek
Výrobce a model	**FORTINET, FIREWALL FortiGate 120G + Licence, Unified Threat Protection + FortiCare Premium 36měsíců**
Provedení	Do racku 1U, včetně montážního kitu
Porty	min. 8x GE RJ45 a zároveň min. 2ks SFP+ port • Dedikovaný konzolový port – min 1x • USB port umožňující připojení USB flash paměti pro zálohování konfigurace, zároveň umožňující připojení USB modemu pro záložní připojení internetu – min 1x • Bluetooth Low Energy (BLE)
NGFW	Min. základní funkce Next-generation firewall - viz https://en.wikipedia.org/wiki/Next-generation_firewall - firewall, aplikační firewall s DPI, IPS. Administrace na bázi "objektů" (aplikace, uživatelů, lokality apod.) namísto IP adres, portů apod.
Počet současných spojení	min. 1,5 miliónu
Propustnost SSL VPN	min. 1,4 Gbps, při licenčním nebo technickém omezení počtu klientů požadujeme min. 25 klientů
Propustnost SSL inspekce	min. 2.6 Gbps
Propustnost firewallu	min. 27 Gbps pro pakety 512 bytů a větší
Propustnost NGFW	min. 2,5 Gbps
Propustnost IPS	min. 4.4 Gbps
Propustnost detekce škodlivého kódu	min. 2.1 Gbps
Logování	min. 7 dnů historie v zabezpečeném cloud prostředí
Zabezpečení VPN	Umožňuje dvoufaktorové ověřování pomocí mobilní aplikace
Virtualizace	min. 5 virtuálních kontextů
Vysoká dostupnost	Podporují režimy Active/Passive i Active/Active se společnou konfigurací v případě zapojení druhého firewallu
Dualstack	podpora současného běhu IPv4 a IPv6
Aplikační kontrola	detekce, monitoring, povolení či zakázání obvyklých síťových aplikací na základě signatury dané aplikace, nikoliv dle portu Kontrola komunikace v SSL šifrovaných protokolech (HTTPS, IMAPS, POP3S, …)
Antivir	Integrovaný antivirus, možnost volby různých databází signatur, podpora archivace škodlivého obsahu, podpora protokolu ICAP pro offload AV detekce, možnost detekce tzv. Grayware (rootkit, malware, spywave, keylogger, atd)
Kategorizace a blokace provozu	založená na kategorizaci webového obsahu, možnost monitorování navštívených kategorii na uživatele či skupinu, možnost kvóty – uživatel může navštěvovat určitou kategorii jen po určitou dobu během dne
Antispam	antispamová a antivirová inspekce elektronické pošty
Sandbox	Možnost integrovaného sandbox (ověření škodlivosti kódu spuštěním v reálných operačních systémech) v zařízení nebo

	integrované rozhraní pro napojení na externí službu výrobce zařízení (služba není součástí dodávky)
Aktualizace	automatická aktualizace bezpečnostních funkcí poskytovaná výrobcem zařízení
Ověřování uživatelů	LDAP, Active Directory, Single Sign On vůči Active Directory, Radius, Ověřování na základě certifikátu
Management a monitoring	HTTP/S, SSH, SNMP, syslog
Záruka	min. 36 měsíců v režimu 24x7 poskytovaná výrobcem zařízení. Doručení náhradního zařízení max. následující den po nahlášení závady, včetně nároku na bezpečnostní aktualizace firmware a bezpečnostních funkcí - URL filtrace, IPS, antimalvare, antispam, aplikační kontrola)
Další informace či odkazy dodavatele k nabízenému plnění *(nepovinné pole)*	

Systém pro ukládání a korelaci logů – 1 KS

Parametr	Minimální požadavek
Výrobce a model	**FORTINET , FortiAnalyzer VM Subscription, FortiAnalyzer-VM Záruka 5let. 5 GB/Day Central Logging & Analytics. Include FortiCare Premium support, IOC, SOC subscription, and FortiGuard Outbre – záruka 3roky**
Základní požadavky	• Je poptáván systém pro ukládání a korelaci logů z NGFW a síťových prvků poptávaných zadavatelem. Systém musí být plně kompatibilní s dodávanými zařízeními, musí podporovat analýzu logů nad provozem. Dále musí být schopné poskytovat reporty nad logy a informovat správce systému o hrozbách, které byly v síti odhaleny. • Celá dodávka musí obsahovat všechny HW komponenty a licence se zárukou 3 let. Žádné z nabízených řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány.
Hlavní parametry appliance	• Musí se jednat o virtuální appliance s podporou virtualizací minimálně VMware, KVM a Hyper-V • Minimální limit pro množství přijatých analyzovaných logů za jeden den 5GB • Podpora minimálně 4 virtuálních síťových rozhraní • Možnost škálovatelného navýšení denní kapacity analyzovaných dat na základě licence • Možnost provozovat appliance jako prostý Syslog pro nesíťová zařízení a možností vyhledávání v uložených datech
Multitenantnost	• Možnost rozdělení zařízení na oddělené administrativní sekce dle potřeby, virtuálního kontextu NGFW, účelu apod. • Každý administrativní celek musí mít možnost mít vlastního administrátora, který nebude mít přístup do jiných administrativních celků

Logovací funkce	• Musí se jedna o centrální logovací prvek pro všechny NGFW firewally a poptávané síťové prvky • Musí umět ukládat jakékoli Syslog zprávy • Zpětná korelace logů v rámci identifikace kompromitovaných stanic oproti pravidelně aktualizované databázi podezřelých IP adres, domén nebo webových URL adres. Zpětná kontrola probíhá alespoň 7 dní zpětně. • Možnost dostat se z vizuálního zobrazení proklikem na konkrétní logy • Realtime a historický náhled logů • Korelace logů • Samostatná sekce týkající se hrozeb v síti včetně vizualizace MITRA ATT&CK tabulky • Podpora prohlížení statistických údajů nad logy
Reporting	• Podpora reportů nad logy ve formátu HTML/CSV/XML/PDF • Možnost generování reportů v pravidelných intervalech • Předefinované vzory pro reporty na nejčastější použití • Možnost vytváření vlastních reportů na základě konkrétních SELECT dotazů do databáze • Možnost úpravy reportů do vlastního designu – vlastní loga, texty, úprava hlavičky
Další funkce	• Event Management – upozorňování na důležité informace z logů – emailem a SNMP trapy, syslog zprávou • Předvytvořený dashboard pro využití dohledovým centrem • Možnost customizace rozhraní pro NOC/SOC dle konkrétních požadavků na dohlížené informace • Incident Management – management incidentů vytvořených ze vzniklých eventů v SOC rozhraní • PlayBook Automatizace – automatizované odpovědi na incidenty dle vzorových scénářů • Outbreak služba – v případě rychle šířící se kybernetické hrozby vyhodnocené výrobcem systému může administrátor tohoto systému zobrazit varování a k tomu odpovídající event handlery a předdefinované reporty
Možnosti správy a komunikace	• Podpora SNMPv2, SNMPv3 • Podpora REST API • Správa přes webové rozhraní HTTPS • Administrátorské účty musí být možné konfigurovat lokálně nebo na vzdáleném serveru (LDAP, RADIUS) • Podpora statického směrování pro správu řešení pomocí více síťových rozhraní • Možnost zašifrování spojení mezi zařízením které odesílá logy a analyzačním nástrojem, který je předmětem této zadávací dokumentace
Další informace či odkazy dodavatele k nabízenému plnění *(nepovinné pole)*	

2) nástroj pro ochranu koncových stanic

Ochrana koncových stanic a SVR – 60 KS

Parametr	Minimální požadavek
Výrobce a model	**60x ESET PROTECT Elite**
ANTIVIROVÉ ŘEŠENÍ PRO KONCOVÉ BODY A SERVERY	• - Podporované klientské platformy - OS: Windows, Linux, MacOS, Android, vše v českém jazyce • - Antimalware, antiransomware, antispyware a anti-phishing pro aktivní ochranu před všemi typy hrozeb. • - Personální firewall pro zabránění neautorizovanému přístupu k zařízení se schopností automatického přebrání pravidel z brány Windows Firewall. • - Modul pro ochranu operačního systému a eliminaci aktivit ohrožující bezpečnost zařízení s možností definovat pravidla pro systémové registry, procesy, aplikace a soubory. • - Ochrana před neautorizovanou změnou nastavení / vyřazení z provozu / odinstalací antimalware řešení a kritických nastavení a souborů operačního systému • - Aktivní i pasivní heuristická analýza pro detekci dosud neznámých hrozeb. • - Systém pro blokaci exploitů zneužívajících zero-day zranitelností, jenž pokrývá nejpoužívanější vektory útoku: o síťové protokoly, o Flash Player, o Javu, o Microsoft Office, o webové prohlížeče, o e-mailové klienty, o PDF čtečky… • - Systém pro detekci malwaru již na síťové úrovni poskytující ochranu i před zneužitím zranitelností na síťové vrstvě. • - Kontrola šifrovaných spojení (SSL, TLS, HTTPS, IMAPS…). • - Anti-phishing se schopností detekce homoglyph útoků. • - Kontrola RAM paměti pro lepší detekci malwaru využívající silnou obfuskaci a šifrování. • - Cloud kontrola souborů pro urychlení skenování fungující na základě reputace souborů. • - Kontrola souborů v průběhu stahování pro snížení celkového času kontroly. • - Kontrola souborů při zapisování na disku a extrahování archivačních souborů • - Detekce s využitím strojového učení. • - Funkce ochrany proti zapojení do botnetu pracující s detekcí síťových signatur. • - Ochrana před síťovými útoky skenující síťovou komunikaci a blokující pokusy o zneužití zranitelností na síťové úrovni. • - Kontrola s podporou cloudu pro odesílání a online vyhodnocování neznámých a potenciálně škodlivých aplikací. • - Lokální sandbox • - Modul behaviorální analýzy pro detekce chování nových typů ransomwaru • - Systém reputace pro získání informací o závadnosti souborů a URL adres.

	• - Cloudový systém pro detekci nového malwaru ještě nezaneseného v aktualizacích signatur. • - Technologie pro detekci rootktitů obvykle se maskujících za součásti operačního systému. • - Skenr firmwaru BIOSu a UEFI. • - Skenování souborů v cloudu OneDrive. • - Podpora odečítače obrazovky pro zrakově postižené • - Funkcionalita pro klienty MS Windows – Antimalware, Antispyware, Personal Firewall, Personal IPS, Application control, Device control, Security Memory (zabraňuje útokům na běžící aplikace), kontrola integrity systémových komponent • - Funkcionalita pro klienty MacOS – Personal Firewall, Device control, autoupgrade • - Možnost aplikování bezpečnostních politik i v offline režimu na základě definovaných podmínek • - Ochrana proti pokročilým hrozbám (APT) a 0-day zranitelnostem • - Podpora automatického vytváření dump souborů na stanici na základě nálezů • - Okamžité blokování/mazání napadených souborů na stanici (s možností stažení administrátorem k další analýze) • - Duální aktualizační profil pro možnost stahování aktualizací z mirroru v lokální síti a zároveň vzdálených serverů při nedostupnosti lokálního mirroru (pro cestující uživatele s notebooky). • Možnost definovat webové stránky, které se spustí v chráněném režimu prohlížeče, pro bezpečnou práci s kritickými systémy nebo internetovým bankovnictví • Aktivní ochrany před útoky hrubou silou na protokol SMB a RDP • Možnost zablokování konkrétní IP adresy po sérii neúspěšných pokusů o přihlášení pro protokoly SMB a RDP s možností výjimek ve vnitřních sítích
INTEGROVANÁ CLOUDOVÁ ANALÝZA NEZNÁMÝCH VZORKŮ	• Funkce cloudového sandboxu je integrována do produktu pro koncové a serverové zařízení, tzn. Cloudový sandbox nemá vlastního agenta, nevyžaduje instalaci další komponenty ať už v rámci produktu nebo implementace HW prvku do sítě • Sandbox umožňující spuštění vzorků malwaru pro: Windows, Linux • Možnost využití na koncových bodech a serverech pro aktivní detekci škodlivých souborů • Analýza neznámých vzorků v řádu jednotek minut. • Reporty poskytují i nízkoúrovňové informace o vzorku - informace o konkrétním problematickém chování, detailní informace o procesech, API • Optimalizace pro znemožnění obejití anti-sandbox mechanismy. • Schopnost analýzy rootkitů a ransomwaru. • Schopnost detekce a zastavení zneužití nebo pokusu o zneužití zero day zranitelnosti. • Řešení pracuje s behaviorální analýzou. • Kompletní výsledek o zanalyzovaném souboru včetně informace o nalezeném i nenalezeném škodlivém chování daného souboru • Manuální odeslání vzorku do sandboxu. • Možnost proaktivní ochrany, kdy je potenciální hrozba blokována, dokud není znám výsledek analýzy ze sandboxu. • Neomezené množství odesílaných souborů.

	• Veškerá komunikace probíhá šifrovaným kanálem. • Okamžité odstranění souboru po dokončení analýzy v cloudovém sandboxu • Možnost volby, jaké kategorie souborů do cloudového sandboxu budou odcházet (spustitelné soubory, archivy, skripty, pravděpodobný spam, dokumenty atp.) • Velikost odeslaných souborů do cloudového sandboxu může dosahovat až 64MB.
ŠIFROVÁNÍ CELÝCH DISKŮ	• Podpora platforem Windows a MacOS • Správa skrze centrální management • Unikátní technologie pro platformu Windows (nevyužívá se BitLocker) • Podpora Pre-Boot autentizace • Podpora TMP modulu • Podpora Opal samošifrovacích disků • Možnost definovat počet chybně zadaných pokusů • Možnost definovat složitost a délku autentizačního hesla • Možnost omezit platnost autentizačního hesla • Podpora okamžitého smazání šifrovacího klíče a následné uzamčení počítače • Recovery z centrální konzole
EDR ŘEŠENÍ	• - Možnost provozu centrálního serveru on-premise na platformě Windows Server Možnost provozu s databázemi: - MS SQL - MySQL. • - Možnost provozu v offline prostředí. • - Možnost logování činností administrátora • - Podpora EDR agenta pro prostředí Windows, Windows server, macOS a linuxové distribuce • - Možnost autentizace do managementu EDR pomocí 2FA Možnost řízení managementu EDR a EDR agentů prostřednictvím API, a to jak pro: - Přijímání informací z EDR serverů/agentů - Zasílání příkazů na EDR servery/agenty EDR řešení podporuje vzdálené pouštění příkazů přímo z EDR konzole. U jednotlivých OS požadujeme plnou podporu funkcionalit: - Powershell u OS Windows Vzdálené spouštění příkazů umožňuje vynucení 2FA ověření daného uživatele. • - Možnost izolace zařízení od sítě prostřednictvím EDR agenta přímo z konzole. • - Možnost tvorby vlastních IoC. • - Možnost škálování množství historických dat vyhodnocených v EDR, až 3 měsíce pro raw-data, 3 roky pro detekované incidenty • - Možnost aktivovat „učící režim" pro automatizované vytváření výjimek k detekčním pravidlům • Indikátory útoku pracující s behaviorální detekcí. • Indikátory útoku pracující s reputací. • Řešení umožnuje analýzu vektorů útoku. Schopnost detekce: - škodlivých spustitelných souborů - skriptů, - exploitů, - rootkitů, - síťových útoků,

	- zneužití WMI nástrojů, - bezsouborového malwaru. - Pokusů o dumpování přihlašovacích údajů uživatele • Schopnost detekovat laterální pohyb útočníka. • Schopnost ukončit infikovaný proces. • Možnost ruční analýzy procesů veškerých spustitelných souborů a DLL knihoven. • Možnost náhledu na spuštěné skripty použitých v daném incidentu • Možnost zabezpečeného vzdáleného spojení přes servery výrobce do konzole EDR • Možnost vytváření automatizovaného response úkonu v podobě izolace stanice, blokace konkrétní hash, odhlášení uživatele, restartování počítače pro jednotlivá detekční pravidla. • Možnost automatického vyřešení incidentu definovaných administrátorem • - Schopnost prioritizace vzniklých incidentů. • - Schopnost stažení problémového souboru. • - Schopnost zobrazení detekcí provedených antimalware produktem. • - Řešení je schopno generovat tzv. forest / full execution tree model. • - Možnost vyhledávání pomocí nově vytvořených IoC nad historickými daty. • - Provázání s technikami popsanými v knowledge base MITRE ATT&CK. • - řešení umožňuje fungovat v offline režimu, a to konkrétně jeho detekční pravidla + předem definované komplexnější incidenty/set detekčních pravidel po sobě jdoucích. • - Průběžně aktualizovaná detekční pravidla EDR systému bez nutnosti aktualizace centrální správy/klienta • - Možnost definice vlastních komplexních „incidentů" spojující v chronologickém pořadí detekci vybraných událostí • - pokročilý detekční mechanismy pro detekci útoku i při nedostupnosti cloudového/centrálního detekčního mozku výrobce • - možnost exportu raw dat (veškerých dat) na externí úložiště, např. Azure Blob • - Možnost definice kontrolního součtu ve formátu SHA256 • - možnost filtrování určitého typu dat zpracovávaného a odesílaného z klientské stanice/server do centrální správy. • - u detekčních pravidel možnost definovat jako automatickou součást pravidla/remediace odeslat soubor na analýzu do cloudového sandboxu výrobce
MANAGEMENT KONZOLE PRO SPRÁVU VŠECH ŘEŠENÍ V RÁMCI NABÍZENÉHO BALÍKU	• - Webová konzole. • - Možnost instalace na Windows i Linux. • - Předpřipravená virtual appliance pro virtuální prostředí VMware, Microsoft Hyper-V a Microsoft Azure, Oracle Virtual Box. • - Server/proxy architektura pro síťovou pružnost – snížení zátěže při stahování aktualizací detekčních modulů výrobce. • - Možnost probuzení klientů pomocí Wake On Lan. • - Možnost konfigurace virtual appliance přes uživatelsky přívětivé webové rozhraní Webmin. • - Nezávislý agent (pracuje i offline) vzdálené správy pro zajištění komunikace a ovládání operačního systému klienta • - Offline uplatňování politik a spouštění úloh při výskytu definované události (například: odpojení od sítě při nalezení škodlivého kódu).

	• - Administrace v nejpoužívanějších jazycích včetně češtiny • - Široké možnosti konfigurace oprávnění administrátorů (například možnost správy pouze části infrastruktury, které konkrétnímu administrátorovi podléhá). • - Zabezpečení přístupu administrátorů do vzdálené správy pomocí 2FA. • - Informace o aktuálně přihlášených uživatelích na daném zařízení • - Podpora štítků/tagování pro snazší správu a vyhledávání • - Správa karantény s možností vzdáleného vymazání / obnovení / obnovení a vyloučení objektu z detekce. • - Vzdálené získání zachyceného škodlivého souboru z klienta. • - Detekce nespravovaných (rizikových) počítačů komunikujících na síti. • - Instalace a odinstalace aplikací 3. stran. • - Vyčítání informací o verzích softwaru 3. stran. • - Možnost vyčítat informace o hardwaru na spravovaných zařízeních (CPU, RAM, diskové jednotky, grafické karty…). • - Odeslání zprávy na počítač / mobilní zařízení, které se následně zobrazí uživateli na obrazovce. • - Vzdálená odinstalace antivirového řešení 3. strany. • - Vzdálené spuštění jakéhokoli příkazu na cílové stanici pomocí Příkazového řádku. • - Dynamické skupiny pro možnost definování podmínek, za kterých dojde k automatickému zařazení klienta do požadované skupiny a automatickému uplatnění klientské úlohy • - Dynamické skupiny musí umět fungovat i v konkrétních časových slotech a uplatňovat podporované klientské úlohy • - Automatické zasílání upozornění při dosažení definovaného počtu nebo procent ovlivněných klientů (například: 5 % všech počítačů / 50 klientů hlásí problémy). • - Podpora SNMP Trap, Syslogu a qRadar SIEM. • - Podpora instalace skriptem - *.bat, *.sh, *.ini (GPO, SSCM…). • - Rychlé připojení na klienta pomocí RDP z konzole pro vzdálenou správu. • - Reportování stavu klientů chráněných jinými bezpečnostními programy. • - Schopnost zaslat reporty a upozornění na e-mail. • - řešení umožňuje odesílat notifikace o vybraných událostech prostřednictvím tzv. webhooků • - Možnost integrace s řešením třetích stran podporující MDM funkcionalitu (např. MS intune, Workspace One) • - Možnost definice kontrolního součtu ve formátu SHA256 • Možnost řízení managementu konzole a jeho komponent prostřednictvím API, a to jak pro: • Centrální správu samotnou • Komponenty antimalware řešení, jeho správy, politik a nastavení • EDR řešení, - Možnost exportu informací o detekcích, incidentech - Možnost úpravy detekčních pravidel EDR • správy zařízení a jeho nastavení, instalačních balíčků, včetně možnosti automatizace jednotlivých úkonů Přidání zařízení do vzdálené správy pomocí: • o synchronizace s Active Directory (jedné nebo více Active Directory), včetně možnosti synchronizace počítačů a uživatelů • o ruční přidání pomocí dle IP adresy nebo názvu zařízení, • o pomocí síťového skenu nechráněných zařízení v síti.

Další informace či odkazy dodavatele k nabízenému plnění *(nepovinné pole)*	

3) nástroje pro ochranu integrity komunikačních sítí

INFRASTRUKTURA – core SWITCH – 2 KS + MINIGBIC 30 KS

Parametr	Minimální požadavek
Výrobce a model	**FORTINET - FortiSwitch-1024E, záruka 5let + 30KS 10GE SFP+ transceiver module (FN-TRAN-SFP+LR)**
Základní vlastnosti	• Záruka výrobce na výměnu vadného HW platná po celou dobu životnosti zařízení, minimálně 5 let od ukončení prodeje daného zařízení • Podpora výrobce pro řešení technických problému platná po celou dobu životnosti zařízení, minimálně 5 let od ukončení prodeje daného zařízení s dostupností 24/7 v případě zaplacené podpory výrobce. • Pravidelné a automaticky instalované bezpečnostní a funkční aktualizace sítových prvku po celou dobu platnosti zaplacené podpory výrobce. • Veškerá konfigurace a monitoring všech síťových prvků, které jsou předmětem poptávky, musí probíhat jak centralizovaně, a to buďto pomocí samostatného centralizovaného switch kontroléru od stejného výrobce, nebo prostřednictvím cloudové webové aplikace nebo případně lokálně na daném zařízení přes příkazovou řádku/webové rozhraní daného přepínače. • Centrální administrativní rozhraní je kompatibilní pro přepínače i firewall • Automatická karanténa připojených koncových zařízení na základě detekce bezpečnostní hrozby řídícím NGFW
Technické požadavky na agregační přepínače LAN	• L2/L3 přepínač • Rackmount provedení pro 19'' rozvaděč • Rozměr 1 RU • 24x 10GE SPF+ porty • 2x 40GE / 100GE QSPP+ / QSPF28 porty • 1x RJ45 Sériový port pro připojení konzole • 1x RJ45 Management port • Minimální kapacita přepínání 850 Gbps • Minimální paketový výkon přepínače 1200 Mpps • Minimální počet záznamů MAC tabulky 64 000 • Minimální počet MST Spanning tree instancí 15 • Minimální počet záznamů v routovací tabulce 24 000 • Packet buffer minimálně 8MB • Maximální hloubka přepínače: 46 cm • Duální napájecí zdroje s možností výměny za chodu přepínače • Airflow – Front to back
Funkční požadavky	• L2/L3 přepínač • Podpora IEEE 802.3ad • Podpora IEEE 802.1q

	• Podpora IEEE 802.1ab • Podpora IEEE 802.1s • Podpora IEEE 802.1w • Podpora IEEE 802.1p • Podpora ACL (IPv4 a IPv6) až 4000 záznamů • Podpora L2 ACL • Podpora ECMP • Podpora 802.1x • Podpora MAB • Podpora Radius CoA • Podpora Radius Accounting • Podpora ARP inspekce • Podpora IGMP, DHCP a MLD snooping • Podpora protokolů RIPv2, BGP, OSPFv2, IS-IS, VRRP • Podpora multicast PIM-SM protokolu • Podpora Jumbo Frame o velikosti alespoň 9000B • Podpora SPAN, RSPAN a ERSPAN • Podpora Multi-Chassis Link Aggregeation protokolu • Podpora administrátorského přístupu pomocí Telnet, SSH a HTTPS • Podpora REST API pro konfiguraci a monitoring prvku • Podpora duálního firmwaru • Podpora SNMP v1/v2c/v3, sFlow, Syslog (včetně možnosti komunikace pomocí TCP), Radius a TACACS+ protokolu • Podpora centrální správy z NGFW zařízení stejného výrobce s možností vynutit L2 inspekci provozu přes NGFW per VLAN Integrovaný nástroj pro packet capture
MINIGBIC – 30KS	• 10G SFP+ Transceiver SM
Certifikace dodavatele, původ zboží	• Jsou splněny „Požadavky na certifikaci dodavatele HW a původ zboží“
Další informace či odkazy dodavatele k nabízenému plnění *(nepovinné pole)*	

Aktivní prvky – POE – 14 KS

Parametr	Minimální požadavek
Výrobce a model	**FORTINET - FortiSwitch-148F-FPOE záruka 5let**
Základní vlastnosti	• Záruka výrobce na výměnu vadného HW platná po celou dobu životnosti zařízení, minimálně 5 let od ukončení prodeje daného zařízení • Podpora výrobce pro řešení technických problému platná po celou dobu životnosti zařízení, minimálně 5 let od ukončení prodeje daného zařízení s dostupností 24/7 v případě zaplacené podpory výrobce. • Pravidelné a automaticky instalované bezpečnostní a funkční aktualizace sítových prvku po celou dobu platnosti placené podpory výrobce. • Veškerá konfigurace a monitoring všech síťových prvků, které jsou předmětem poptávky, musí probíhat jak centralizovaně, a to buďto pomocí samostatného centralizovaného switch kontroléru od stejného výrobce, nebo prostřednictvím cloudové webové aplikace nebo případně lokálně na daném

	zařízení přes příkazovou řádku/webové rozhraní daného přepínače. • Centrální administrativní rozhraní je kompatibilní pro přepínače i firewall • Automatická karanténa připojených koncových zařízení na základě detekce bezpečnostní hrozby řídícím NGFW.
Technické požadavky na agregační přepínače LAN	• L2 přepínač • Rackmount provedení pro 19'' rozvaděč • Rozměr 1 RU • 48x GE RJ45 portů celkem z toho všech 48 portů podporující PoE/PoE+ (802.3af/at) • 4x 10GE SFP+ porty • 1x RJ45 Sériový port pro připojení konzole • Minimální výkon PoE/PoE+ 740W • Minimální kapacita přepínání 170 Gbps • Minimální paketový výkon přepínače 250 Mpps • Minimální počet záznamů MAC tabulky 32 000 • Minimální počet MST Spanning tree instancí 15 • Packet buffer minimálně 2MB • Maximální hloubka přepínače: 33 cm • Zdroj napájení integrovaný v těle přepínače • Airflow – Side to back
Funkční požadavky	• Podpora IEEE 802.3ad • Podpora IEEE 802.1q • Podpora IEEE 802.1ab • Možnost propojení s prvkem podporující IEEE 802.1s • Podpora IEEE 802.1w • Podpora ACL IPv4 • Podpora QoS pro IPv4 včetně 802.1p • Podpora 802.1x • Podpora MAB • Podpora Radius CoA • Podpora Radius Accounting • Podpora ARP inspekce • Podpora IGMP a DHCP snooping • Podpora Jumbo Frame o velikosti alespoň 9000B • Podpora SPAN • Podpora administrátorského přístupu pomocí Telnet, SSH a HTTPS • Podpora REST API pro konfiguraci a monitoring prvku • Podpora SNMP v1/v2c/v3, Syslog (včetně možnosti komunikace pomocí TCP), Radius a TACACS+ protokolu pro autentizaci administrátorů • Podpora centrální správy z NGFW zařízení stejného výrobce s možností vynutit L2 inspekci provozu přes NGFW per VLAN
Certifikace dodavatele, původ zboží	• Jsou splněny „Požadavky na certifikaci dodavatele HW a původ zboží"
Další informace či odkazy dodavatele k nabízenému plnění *(nepovinné pole)*	

WIFI – 40 KS

Parametr	Minimální požadavek
Výrobce a model	**FORTINET - FortiAP 231G, záruka 5let + držák**
Základní vlastnosti	• Formát AP: indoor s interními anténami v katefgorii WiFi 6E • WiFi s 3 rádii a 2 spatial streams • Příslušenství k montázi na zeď/strop/T-Rail • Počet rádií: minimálně 3 pro přenos v pásmech 2,4 a 5GHz a 5 GHz/ 6 GHz/skenovací rádio • Minimálně 2x2 MIMO • Dedikované rádio pro analýzu okolního provozu • Dedikované Bleutooth/ZigBee rádio pro lokalizační služby • Současná podpora 2,4 GHz, 5GHz a 6GHz pásma • Podpora standardů 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, • 802.11j, 802.11k, 802.11n, 802.11r, 802.11u, 802.11v, 802.11w, • 802.11ac, 802.11ax, 802.1Q, 802.1X, 802.3ad, 802.3af, • 802.3at, 802.3az, 802.3bz • 2x 10/100/1000 Base-T RJ45 uplink porty s možností sestavení LAG, min. jeden z portů podporuje i 2.5 GbE • 1x USB 3.0 • 1x seriový port • Počet SSID: min. 8 per rádio • Cellular Co-existence • Podpora BSS Coloring • Podpora TWT (Target Wake Time) • Spektrální analýza přímo na AP • Možnost zachytávání paketů na AP pro jejich analýzu • Provoz min. dvou rádií při napájení pomocí 802.3af • Obousměrná a výrobcem podporovaná integrace s wireless kontrolérem • Podpora výrobce na 60 měsíců • Kensigton lock • AP umožňují centrální správu jak z cloudu výrobce, tak z centralizovaného nástroje, který umožňuje současnou správu ostatních nabízených prvků stejného výrobce (přepínače, NGFW)
Záruka, servis	• HW záruka na 5 let
Certifikace dodavatele, původ zboží	• Jsou splněny „Požadavky na certifikaci dodavatele HW a původ zboží“
Další informace či odkazy dodavatele k nabízenému plnění *(nepovinné pole)*	

NAC – 1 KS

Parametr	Minimální požadavek
Výrobce a model	**FORTINET, FortiNAC, FortiNAC Control and Application Extended-VM – záruka 3roky + FortiNAC PLUS License for 500 concurrent endpoint devices – záruka 3roky**

OBECNÉ POŽADAVKY NA PLATFORMU	• Virtuální appliance pro platformu VMWARE ESX, Microsoft Hyper-V, KVM (HW alternativa není poptávána) • Možnost instalace VM v prostředí AWS a Azure s podporou HA režimu, který kombinuje cloud a on-prem instance • Podpora distribuované architektury s centrálním správním prvkem a distribuovanými autentizačními branami • Autentizační brány musí být nasazené mimo samotný datový tok (tzv. inline řešení není akceptovatelné) • Podpora HA v režimu active-passive se sdílením licencí mezi aktivním a pasivním prvkem • Možnost nasazení v režimu L2 nebo L3 jak pro HA, tak i pro komunikaci se síťovými prvky • Schopnost NAC řešení komunikovat se síťovými prvky, drátovými i bezdrátovými, jiných výrobců pomocí SNMP a CLI a vymáhat na nich definované bezpečnostní politiky bez nutnosti využití 802.1x nebo MAB • Možnost instalace samostatného NAC řešení v podobě pouze enforcement brány bez nutnosti nákupu dalších prvků, jako například centrální management. Pokud je další prvek nutný, musí být součástí nabídky. • Autentizační brána je schopna poskytnout DHCP a DNS služby pro zařízení, která je třeba registrovat do systému před jejich vpuštěním do produkční sítě • Autentizační brána funguje sama o sobě jako Radius server pro autentizaci i accounting • Všechny požadované funkce pokrývá jeden typ licence a je možné doatenčně zvýšit počet licencí v systému • Správa řešení pomocí zabezpečeného webového rozhraní, pomocí CLI protokolem SSH a možnost granulárního nastavení administrátorských oprávnění do úrovně spravovaných síťových zařízení a portů
POŽADAVKY NA KONTROLU PŘÍSTUPU DO SÍTĚ	• Autentizace a bezpečnostní kontrola endpointu před jeho připojením do sítě (nezávisle na způsobu připojení jako wired, wireless, VPN) • Možnost detailní profilace připojeného zařízení a klienta a to buď manuálně vytvořeným pravidlem nebo na základě jeho otisku, který je získán skenem sítě nebo komunikací s externím systémy a to bez nutnosti dodatečného licencování této funkcionality • Podpora politik pro automatickou profilaci zařízení (minimálně na základě: SNMP, RADIUS, SYSLOG, DHCP, API, SSH, NMAP, DHCP fingerprinting, HTTP(s), IP range, telnet, expect scripty, vyhodnocení TCP/UDP portů, VENDOR OUI/MAC, WMI profil, pollování firewallu a vyhodnocování síťové komunikace, perl skripty) a to bez nutnosti dodatečného licencování této funkcionality • Periodická kontrola připojeného zařízení, zda odpovídá profilu, na základě kterého bylo zařízeno vpuštěno do sítě a možnost odpojit zařízení v případě, kdy nesplňuje podmínky původního profilu • Podporované autentizační protokoly: min. MS-CHAP v2, PAP, EAP-PEAP, EAP-TLS, EAP-FAST, EAP-TEAP • Po úspěšné autentizaci je možné definovat parametry konfigurace síťového portu nebo SSID, kde je autentizovaná entita připojená, pomocí stadarttních Radius atributů • Po úspěšné autentizaci je možné na síťové zařízení, kde je klient připojen, instalovat z NAC brány konfiguraci, jako například ACL • Podpora 802.1x • Podpora MAB autentizace

	• Podpora tvorby lokálních účtů a lokální autentizace • Podpora registrace koncových zařízení v NAC řešení před jejich fyzickým připojením do sítě • Podpora funkce RADIUS proxy • Podpora agentů pro operační systémy: Windows, MacOS, Linux (agent dodává detailní informace o počítači, informace o login/logout, umožňuji spouštění skriptů a zajišťuje notifikace pro uživatele) a licence pro tyto agenty je součástí dodané licence • Podpora Integrace se stávajícím AD serverem pro autentizaci uživatelů pomocí LDAP • Podpora captive portálů v rámci autentizační brány s plně editovatelným prostředí • Podpora tzv. sponozorovaného přístupu pro autentizaci hostů a BYOD zařízení s možností zaslání přístupových údajů pomocí SMS a Email • NAC řešení je schopné zablokovat konektivitu připojeného zařízení nebo změnit síťový segment na úrovní přístupové vrstvy v případě zjištění bezpečnostního incidentu • Podpora integrace s MDM nástroji jako Microsoft In-Tune a dále s OT/ioT nástroji Nozomi, Claroty • Podpora integraace s poptávaným NGFW a analytickým nástrojem nad provozem poptávaného NGFW • Podpora alespoň RSSO komunikace s NGFW • Administrátor má možnost manuálně, volbou v GUI, registrovat, zablokovat, smazat nebo i definovat nové zařízení a uživatele
POŽADAVKY NA ENDPOINT COMPLIANCE	• Endpoint compliance se provádí před povolením přístupu do sítě na základě definovaného profilu nebo agenta na koncové stanici • Endpoint compliance je možné provádět periodicky (v době, kdy je počítač připojen do sítě) • Kontrola stavu AV na stanici • Kontrola stavu registrů • Kontrola existence konkrétních souborů v lokálním filesystému • Ověření domény • Ověření certifikátu a jeho částí jako je vydavatel, expirace, common-name, • Ověření verze a patch levelu operačního systému • Podpora sběru informací o instalovaných aplikacích na endpointech • Notifikace uživatele v případě nesplnění bezpečnostní kontroly, s využitím funkce captive portál • Možnost kontaktovat koncovou stanice v reálném čase textovou správu v případě nasazení endpoint agenta pro compliance
AUTOMATIZACE	• Možnost definovat playbook, nativně v GUI, který bude vykonávat automatické akce na základě definované události a následné akce dle aktuálního stavu (minimálně v podobě blokace portu, změny L2 segmentu, aplikace skriptu) • Řešení je možné obsluhovat pomcí výrobcem popsaných API volání • Možnost automatické tvorby tiketů v systému ServiceNow na základě definované události
REPORTING	• Možnost tvorby reportů o stavu platformy a stavu připojených zařízení v reálném čase a alespoň zpětně o jeden týden. Reporting je nativní funkce dostupná v GUI bez nutnosti dodatečného licencování

NOTIFIKACE ADMINISTRÁTORŮ A UŽIVATELŮ	• Možnost napojení autetntizační brány na SMS nebo email bránu promocí konektoru přímo z GUI
POŽADAVKY NA LICENCE A PODPORU VÝROBCE	• záruka 3 roky v režimu 24x7 od výrobce řešení • Licence pro min. **500** endpointů
Certifikace dodavatele, původ zboží	• Jsou splněny „Požadavky na certifikaci dodavatele HW a původ zboží"
Další informace či odkazy dodavatele k nabízenému plnění *(nepovinné pole)*	

Analýza síťového provozu – 1 KS

Parametr	Minimální požadavek
Výrobce a model	**GREYCORTEX Mendel All-in-one - senzor + kolektor MA-SC-500**
Základní vlastnosti	**Systém pro analýzu síťového provozu** • Systém složený z hardwarových zařízení musí monitorovat síťovou aktivitu v reálném čase a identifikovat potenciální kybernetické hrozby, bezpečnostní rizika a anomální chování a musí o nich v reálném čase vytvářet upozornění. • 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. • 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. • Dodaný systém musí být schopen analyzovat síť také na základě zpracování statistických protokolů typu NetFlow, IPFIX, NetStream, Cisco NSEL a případně dalších. • 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. • Aktualizace systému musí být možné provádět uživatelsky v off-line režimu. **Zpracování a ukládání síťových toků** • Systém ukládá síťové toky ve formátu, který umožní analýzu síťové komunikace na úrovni jednotlivých toků, včetně dohledání informací o aplikačních transakcích a jejich metadatech z L2 až L7, obsažených v daném síťovém toku. • 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. • Je požadováno vysokorychlostní úložiště pro uchování historie datových toků na dobu minimálně 6 měsíců složené z SSD nebo NVMe disků. • 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. **Uživatelské rozhraní** • Systém musí poskytovat jednotné grafické uživatelské rozhraní pro veškerou práci uživatelů, včetně všech detekcí, analýzy síťových statistik, nastavení systému, konfiguraci alertů, reportů a dashboardů. • 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), • granulárního nastavení přístupu k datům z různých segmentů sítě organizace s definovanými úrovněmi přístupu (alespoň read, write, execute), • vytváření vlastních filtrů veškerých dat a jejich sdílení mezi uživateli a skupinami uživatelů, • vytváření vlastních uživatelských pohledů, reportů, dashboardů apod. **Automatické hlášení (alerty) a reporting** • Systém musí být schopen upozorňovat uživatele prostřednictvím minimálně emailu a logu o všech identifikovaných událostech a dále o událostech filtrovaných minimálně dle IP a MAC adresy, podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu. • 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. • 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.). • Je požadováno vytváření automatizovaných reportů v českém jazyce. **Integrace systému** • 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) • přímé url odkazy na libovolnou obrazovku grafického uživatelského rozhraní a filtrovaná zobrazení v grafickém uživatelském rozhraní • export informací o toku ve formátu IPFIX nebo podobném formátu včetně plné podpory filtrů (exportovat lze pouze požadovaná data) včetně aplikačních metadat alespoň pro protokoly HTTP, HTTPS a SMTP • integrace se službami identity uživatelů bez nutnosti konfigurace zasílání logů do systému Microsoft Active Directory • integrace s firewallem pro automatické a manuální reakce vyvolané systémem **Podpora EDR**

	• Systém musí poskytovat nástroje umožňující přímou integraci se softwarem EDR třetích stran pro získání informací a zkvalitnění detekce. •
Dodavatel stručně popíše způsob naplnění jednotlivých požadavků základních vlastností	Splňuje Nabízené řešení je HW appliance se SW. Monitoruje síťovou aktivitu v reálném čase a identifikuje kybernetické hrozby, bezpečnostní rizika a anomální chování. V reálném čase o těchto nálezech vytváří upozornění. Řešení analyzuje síť na základě zrcadleného síťového provozu ze SPAN portů / TAPů a nevyžaduje agenty na koncových stanicích ani další zařízení v síti. Řešení analyzuje obsah datových paketů v reálném čase a detekuje protokol/ aplikaci na základě obsahu provozu prostřednictvím DPI, ne jen čísla portu. Nabízené řešení umí analyzovat síť také na základě zpracování statistických protokolů typu NetFlow, IPFIX, NetStream, Cisco NSEL a dalších. Řešení je plně funkční v offline prostředí zadavatele bez využití cloudu pro sběr, ukládání a zpracování dat. Kkonfigurace a reporty jsou k dispozici přímo v systému. Aktualizace systému lze provádět také uživatelsky v off-line režimu. Řešení ukládá síťové toky ve formátu, který umožňuje analýzu síťové komunikace na úrovni jednotlivých toků, včetně dohledání informací o aplikačních transakcích a jejich metadatech z L2 až L7, obsažených v daném síťovém toku. Nabízí zpracování uvedených protokolů pro ukládání aplikačních metadat z transakcí: DHCP, DNS, SMB, HTTP, HTTPS, SMTP, SMTPS, POP3, IMAP, SSH, LDAP, LDAPS, KERBEROS, SNMP, CIFS, MSSQL, RDP, SIP, TELNET, FTP, FTP-DATA, TFTP, TFTP-DATA, NFS, ARP, SSL/TLS zapouzdření. Nabízené řešení je osazeno vysokorychlostním úložištěm pro uchování historie datových toků na dobu minimálně 6 měsíců, složeným z SSD disků. Řešení sbírá a analyzuje aplikační a systémové logy ve formátu syslog z dohledovaných zařízení a identifikuje nebezpečné nebo potenciálně škodlivé aktivity. Řešení poskytuje jednotné GUI pro veškerou práci uživatelů, včetně detekcí, analýzy síťových statistik, nastavení, konfiguraci alertů, reportů a dashboardů. Řešení poskytuje intuitivní nástroj pro vytváření profilů a skupin uživatelů pro omezení funkcionality a viditelnosti dat s podporou: granulárního nastavení přístupu k analytickým i konfiguračním komponentám s definovanými úrovněmi přístupu R/W/E, granulárního nastavení přístupu k datům z různých segmentů sítě s definovanými úrovněmi přístupu R/W/E, vytváření vlastních filtrů

	veškerých dat a jejich sdílení mezi uživateli a skupinami uživatelů, vytváření vlastních uživatelských pohledů, reportů, dashboardů. Nabízené řešení upozorňuje uživatele prostřednictvím např. emailu a logu o všech identifikovaných událostech a o událostech filtrovaných dle IP a MAC adresy, podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu. Alerty dodává i ve strojově čitelném formátu pro vyžití v nástrojích typu SIEM, obsahuje kompletní informace o detekované události včetně URL odkazu v reportovaném období do grafického rozhraní. Nabízené řešení umožňuje vytvářet automatizované manažerské reporty v českém jazyce o stavu kyberbezpečnosti z pohledu zprávy kybernetických incidentů dle oblastí jejich vzniků (např.: doména, web, email apod.). Nabízené řešení poskytuje hotové nástroje pro integraci se softwarem třetích stran bez použití API systému: syslog, CEF a LEEF pro export událostí včetně plné podpory filtrů, přímé url odkazy na libovolnou obrazovku GUI a filtrovaná zobrazení v GUI, export informací o toku ve formátu IPFIX včetně plné podpory filtrů, včetně aplikačních metadat pro protokoly HTTP, HTTPS a SMTP, integraci se službami identity uživatelů bez nutnosti konfigurace zasílání logů do systému Microsoft AD, integraci s FW pro automatické a manuální reakce vyvolané systémem . Nabízené řešení poskytuje nástroje umožňující přímou integraci se softwarem EDR třetích stran pro získání informací a zkvalitnění detekce.
Požadavky na architekturu nasazení	• Pro všechny HW komponenty senzor a kolektor je požadován formát 1U nebo 2U server o velikosti 19". • Pro všechny HW komponenty senzor a kolektor je požadován duální zdroj napájení se schopností hot-swap. • Pro všechny HW komponenty senzor a kolektor je požadováno samostatné síťové rozhraní pro vzdálenou správu serveru v případě výpadku systému typu IPMI, IDRAC, ILO apod. • Požadavky pro pokrytí IT prostředí • Je požadován 1x HW datový kolektor/sensor umožňující trvalý průtok 500Mbps pro alespoň 1500 monitorovaných IP adres s monitorovacím rozhraním 4x 1GbE. • Na zařízení je požadována dostupná historie dat minimálně 6 měsíců.
Dodavatel stručně popíše způsob naplnění jednotlivých požadavků na architekturu nasazení	Nabízené řešení je postaveno na HW kombinace senzor a kolektor ve formátu 1U nebo 2U server o velikosti 19", s duálním zdrojem napájení se schopností hot-swap, samostatným síťovým rozhraním pro vzdálenou správu serveru v případě výpadku systému typu IPMI, IDRAC, ILO apod. Nabízené řešení HW kolektor a sensor v jednom umožňuje trvalý průtok 500Mbps pro minimálně 1500 monitorovaných IP adres s monitorovacím rozhraním 4x 1GbE.

	Zařízení je vybaveno diskovou kapacitou pro uložení dostupné historie dat minimálně 6 měsíců.
Požadavky na schopnost detekce bezpečnostních událostí	**Monitorování zařízení, segmentů sítě a využívaných síťových služeb** • Dodaný systém musí identifikovat všechna zařízení připojená do sítě včetně koncových zařízení, serverů, IoT zařízení apod. Zároveň musí být systém schopen identifikovat změny v síti – minimálně: 1. změna IP/MAC adresy hosta, 2. duplicitní IP/MAC adresa, 3. změna VLAN, 4. vytvoření nové podsítě, 5. připojení nového zařízení, 6. použití nebo vznik nové služby, 7. nedostupnost dříve dostupné a komunikující služby nebo dříve dostupného komunikujícího zařízení, 8. přístup nového zařízení ke službě či zařízení 9. ověřování platnosti interních certifikátu pro validní TLS šifrování u HTTPS a upozornění před datem jejich vypršení. • Systém musí uživateli umožnit pomocí těchto detekčních metod nastavovat bezpečnostní politiky pro různé segmenty sítě a pro různá zařízení a na porušení těchto politik reagovat upozorněním. **Samostatné učení behaviorálních aktivit a detekce anomálií** • Systém musí používat matematické metody samostatného učení pro analýzu síťové aktivity, vytvářet a v čase automaticky modifikovat modely chování na základě běžného chování jednotlivých zařízení a na nich provozovaných služeb v rámci celé organizace. • 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: 1. odchylku od modelu pro přenos dat, toků a paketů, 2. odchylku od modelu pro počet komunikačních partnerů, 3. odchylku od modelu entropie na komunikačních portech, 4. odchylku od modelu pro počet síťových toků a využitých síťových služeb, 5. odchylku od modelu výkonnosti sítě (rychlost přenosu) a aplikací (doba odezvy). • Samostatné učení je požadováno na všech síťových zařízeních a na nich provozovaných službách (port číslo 0 až 65535 u TCP i UDP) na IPv4 a IPv6 a dalších protokolech L3 a L4 síťové vrstvy. **Identifikace neznámých hrozeb a podezřelých chování** • Systém musí být schopen detekovat neznámé hrozby, které nelze identifikovat prostřednictvím detekčních signatur, jako jsou trojské koně, botnety apod. Zejména musí být identifikovány tyto příznaky potenciálně škodlivého chování: 1. průzkumné aktivity v síti, 2. detekce podezřelého strojového chování, které nevytvářejí lidští uživatelé sítě, 3. detekce repetitivních vzorců chování na síti, 4. detekce botnetů a ovládání kompromitované stanice, 5. detekce příznaků těžení kryptoměn, 6. útoky hrubou silou a enumerace dat,

	7. rozpoznání tunelovaného síťového provozu – alespoň IPv4 prostřednictvím IPv6 a DNS tunely. **Detekce na základě databáze známých hrozeb** • Systém musí být schopen identifikovat hrozby a reportovat události na základě 1. 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, 2. reputační databáze známých škodlivých IP adres, TLS certifikátů, záznamů DNS a hostname, URL adres a hashů souborů. • Tyto databáze musí být aktualizované minimálně na hodinové bázi. Nesmí se jednat pouze o volně dostupné/open-source databáze, ale musí se jednat o komerční databázi renomovaného vendora nebo poskytovatele těchto služeb. • Uživatel musí být schopen importovat vlastní záznamy. • Systém musí využívat tuto detekci pro veškerý monitorovaný provoz (na perimetru i v interní síti mezi všemi segmenty), nikoliv pouze pro omezený segment nebo podmnožinu celkové komunikace. • 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). • Uživatel musí být schopen prostřednictvím webové aplikace přidávat vlastní detekční pravidla v praktickém a obecně využívaném formátu bez nutnosti znalosti syntaxe a sémantiky pravidel. • Příklad možné syntaxe detekčního pravidla: • alert tcp $HOME_NET any -> any any (msg:"Command Shell Access"; content:"C:\\Users\\Administrator\\Desktop\\hfs2.3b";) **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. **Asistované učení** • Je požadován uživatelsky přívětivý proces vytváření pravidel pro zpřesnění detekce a eliminaci falešně pozitivní detekce, a to na základě minimálně následujících parametrů: 1. IP adresa, 2. MAC adresa, 3. hostname, 4. segment sítě / podsíť, 5. lokalita – ASN, země apod. 6. směr komunikace – určení klienta, nebo serveru, 7. detekovaná událost – kategorie, název apod. 8. použité služby, protokolu, portu, 9. libovolné kombinaci výše popsaných. Systém musí být schopen eliminovat falešné alarmy i pro události detekované v historii.
Dodavatel stručně popíše způsob naplnění jednotlivých požadavků na schopnost detekce bezpečnostních událostí	Nabízené řešení identifikuje všechna zařízení připojená do sítě včetně koncových zařízení, serverů, IoT zařízení apod. Identifikuje změny v síti jako: změna IP/MAC adresy hosta, duplicitní IP/MAC adresa, změna VLAN, vytvoření nové podsítě, připojení nového zařízení, použití nebo vznik nové služby, nedostupnost dříve dostupné a komunikující služby

	nebo dříve dostupného komunikujícího zařízení, přístup nového zařízení ke službě či zařízení, ověřování platnosti interních certifikátu pro validní TLS šifrování u HTTPS a upozornění před datem jejich vypršení. Nabízený systém umožňuje uživateli pomocí těchto detekčních metod nastavovat bezpečnostní politiky pro různé segmenty sítě a pro různá zařízení a na jejich porušení reaguje upozorněním. Nabízené řešení používá matematické metody samostatného učení pro analýzu síťové aktivity, vytváří a v čase automaticky modifikuje modely chování na základě běžného chování jednotlivých zařízení a na nich provozovaných služeb v rámci celé organizace. Na základě matematického modelu daného zařízení a jeho služeb systém identifikuje nestandardní síťové chování, a to zejména odchylky od modelu normálního chování pro: odchylku od modelu pro přenos dat, toků a paketů, odchylku od modelu pro počet komunikačních partnerů, odchylku od modelu entropie na komunikačních portech, odchylku od modelu pro počet síťových toků a využitých síťových služeb, odchylku od modelu výkonnosti sítě (rychlost přenosu) a aplikací (doba odezvy). Samostatné učení je aplikováno na všech síťových zařízeních a na nich provozovaných službách (port číslo 0 až 65535 u TCP i UDP) na IPv4 a IPv6 a dalších protokolech L3 a L4 síťové vrstvy. Nabízené řešení detekuje neznámé hrozby, které nelze identifikovat prostřednictvím detekčních signatur, jako jsou trojské koně, botnety apod. Identifikuje příznaky potenciálně škodlivého chování jako jsou: průzkumné aktivity v síti, detekce podezřelého strojového chování, které nevytvářejí lidští uživatelé sítě, detekce repetitivních vzorců chování na síti, detekce botnetů a ovládání kompromitované stanice, detekce příznaků těžení kryptoměn, útoky hrubou silou a enumerace dat, rozpoznání tunelovaného síťového provozu – alespoň IPv4 prostřednictvím IPv6 a DNS tunely. Nabízené řešení identifikuje hrozby a reportuje události na základě detekční databáze známých hrozeb, tj. malware (trojské koně, viry, červy, rootkity, apod.), známých útoků (exploity) a zranitelností, porušení bezpečnostních pravidel a „best practices" a dalších rizik, reputační databáze známých škodlivých IP adres, TLS certifikátů, záznamů DNS a hostname, URL adres a hashů souborů. Tyto databáze jsou aktualizované na hodinové bázi, jedná se o komerční databázi ProofPoint. Uživatel má možnost importovat vlastní záznamy. Řešení využívá tuto detekci pro veškerý monitorovaný provoz (na perimetru i v interní síti mezi všemi segmenty). Databáze detekčních pravidel (signatur) je založena na pokročilých regulárních výrazech pro zpracování řetězců, které dokáží provádět

	inspekci veškeré síťové komunikace od L2 (Ethernet apod.) po L7. Řešení detekuje události na základě vyšších desítek tisíc signaturních pravidel . Uživatel má možnost prostřednictvím webové aplikace přidávat vlastní detekční pravidla v praktickém a obecně využívaném formátu bez nutnosti znalosti syntaxe a sémantiky pravidel. (Typický příklad syntaxe pravidla: alert tcp $HOME_NET any -> any any (msg:"Command Shell Access"; content:"C:\\Users\\Administrator\\Desktop\\hfs2.3b";) Nabízené řešení používá také další metody pro analýzu šifrované komunikace, jako TLS fingerprinting a s ní spojenou detekci známých hrozeb. Nabízené řešení poskytuje uživatelsky přívětivý proces vytváření pravidel pro zpřesnění detekce a eliminaci falešně pozitivní detekce na základě parametrů: IP adresa, MAC adresa, hostname, segment sítě / podsíť, lokalita – ASN, země apod. směr komunikace – určení klienta, nebo serveru, detekovaná událost – kategorie, název apod., použité služby, protokolu, portu, libovolné kombinaci předchozích. Nabízené řešení umožňuje eliminaci falešných alarmů i pro události detekované v historii.
Požadavky na zajištění síťové viditelnosti	**Vyhledávání, filtrování a vizualizace dat** • Systém musí být schopen okamžitého (v řádu vteřin) vyhledávání a vizualizace pro forenzní analýzu a podporu threat hunting bez zvláštního dotazovacího jazyka. • 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: 1. 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, 2. prostřednictvím full-textového vyhledávání v datech a vyhledávání na základě definice směru (zdroj, cíl) a logických výrazů and, or, not. • Systém musí pro vyhledávání poskytovat již předpočítané hodnoty výkonnostních a behaviorálních charakteristik pro každé zařízení v síti a pro všechny na něm provozované služby, bez nutnosti zpracování surových dat ze síťových logů. • Systém musí být schopen filtrovat a vizualizovat výsledky v grafech, výčtových tabulkách s možností řazení a TOP N statistikách. • Systém musí být schopen ukládat a následně vyhledávat aplikační metadata (vždy dotaz i odpověď všech transakcí v

	toku) minimálně z následujících protokolů, které jsou nebo mohou být využívány ve vnitřní síti organizace: FTP, FTP-DATA, TFTP, TFTP-DATA, SSH, Telnet, SMTP, SMTPS, DNS, DHCP, 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. • Systém musí umožnit uživatelsky jednoduché a okamžité vizualizace síťových prostupů mezi zařízeními a podsítěmi; využitím uživatelského datového filtru modifikovat vizualizační pohledy. **Kontextuální informace** • Systém musí být schopen pro každé zařízení získávat, vizualizovat a v jednom grafickém pohledu zobrazovat kontextuální informace: 1. jméno uživatele a další jeho parametry z doménového řadiče (MS Active Directory), včetně její historie 2. hostname zařízení a jeho historie na základě zpracování relevantních dat z DNS a DHCP provozu 3. IP geolokace 4. IP reputace, vč. údaje, jestli je IP adresa na blacklistu nebo podezřelá 5. historie použitých MAC adresa a výrobce zařízení 6. operační systém a jeho historie na zařízení 7. uživatelem zadané poznámky a informace k zařízení 8. automaticky přiřazené značky/tagy zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy. 9. seznam provozovaných a využívaných služeb (klient a server) u daného zařízení a množství na nich přenesených dat. 10. seznam detekovaných bezpečnostních a provozních událostí daného zařízení. **Zaznamenávání, ukládání a zpětná analýza 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. • Je požadována schopnost importu vlastního PCAP souboru prostřednictvím webového rozhraní a jeho zpětná analýza všemi detekčními a analytickými prostředky kolektoru. • Je požadována schopnost zobrazení plného obsahu PCAP souboru v prostředí webového rozhraní aplikace a dále pak automatizovaná analýza surových dat za účelem identifikace provozních nedostatků zachycených pouze v datovém PCAP souboru.
Dodavatel stručně popíše způsob naplnění jednotlivých požadavků na zajištění síťové viditelnosti	Nabízené řešení umožňuje okamžité (v řádu vteřin) vyhledávání a vizualizaci pro forenzní analýzu a podporu threat hunting bez zvláštního dotazovacího jazyka.

	Umožňuje okamžitě filtrovat a vyhledávat v plné historii všech uložených dat, tj. bezpečnostních událostí, síťových toků a agregovaných síťových statistikách 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, prostřednictvím full-textového vyhledávání v datech a vyhledávání na základě definice směru (zdroj, cíl) a logických výrazů and, or, not. Nabízené řešení pro vyhledávání poskytuje 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. Umožňuje filtrovat a vizualizovat výsledky v grafech, výčtových tabulkách s možností řazení a TOP N statistikách. Dále ukládá a následně vyhledává aplikační metadata 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 návratový kód a další http parametry. Systém umožňuje uživatelsky jednoduché a okamžité vizualizace síťových prostupů mezi zařízeními a podsítěmi; využitím uživatelského datového filtru modifikovat vizualizační pohledy. Systém umožňuje pro každé zařízení získávat, vizualizovat a v jednom grafickém pohledu zobrazovat kontextuální informace: jméno uživatele a další jeho parametry z doménového řadiče (MS Active Directory), včetně její historie, hostname zařízení a jeho historie na základě zpracování relevantních dat z DNS a DHCP provozu, IP geolokace, IP reputace, vč. údaje, jestli je IP adresa na blacklistu nebo podezřelá historie použitých MAC adresa a výrobce zařízení, operační systém a jeho historie na zařízení, uživatelem zadané poznámky a informace k zařízení, automaticky přiřazené značky/tagy zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy, seznam provozovaných a využívaných služeb (klient a server) u daného zařízení a množství na nich přenesených dat, seznam detekovaných bezpečnostních a provozních událostí daného zařízení. Nabízené řešení umožňuje volitelné nahrávání plného síťového provozu (full packet capture) ve formátu PCAP na všech dodaných zařízeních na základě parametrů: cílová a zdrojová IP/MAC adresa, podsíť, využitý protokol, IPv4 nebo IPv6. Zaznamenávání lze zapínat automaticky dle detekovaných událostí nebo uživatelskou aktivací.

	Systém umožňuje import vlastního PCAP souboru prostřednictvím webového rozhraní a jeho zpětnou analýzu všemi detekčními a analytickými prostředky kolektoru. Dále umožňuje zobrazit plný obsah PCAP souboru v prostředí webového rozhraní aplikace a automatizovanou analýzu surových dat za účelem identifikace provozních nedostatků zachycených pouze v datovém PCAP souboru.
Další požadované oblasti využití	**Monitorování politik kybernetické bezpečnosti** • Systém musí umožňovat vytváření komplexních komunikačních a bezpečnostních politik, a to minimálně: 1. 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. 2. detekce změn v síti – přinejmenším nové komunikační vektory, nová nebo změněná zařízení a podsítě, obcházení perimetru. 3. Pro účely monitorování politik kybernetické bezpečnosti musí systém poskytovat uživatelský rámec pro definování pravidel pomocí: 4. uživatelem definované podsítě na základě rozsahů IP adres 5. uživatelsky libovolně definovaných skupin zařízení 6. 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. **Management bezpečnostních událostí a incidentů** • Systém musí poskytovat funkcionalitu pro reporting bezpečnostních incidentů (prohlášení identifikované události za bezpečnostní incident), včetně: 1. 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, 2. jednoduché sdílení informací o bezpečnostních incidentech, včetně uživatelem zadaných komentářů, 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.), 4. možnost exportování dat do emailu, csv, pdf, syslogu a podobně, 5. možnost exportu bezpečnostních událostí a incidentů do systémů typu ticket management třetích stran. **Detekce úniku dat** • Systém musí být schopen detekovat přenosy citlivých souborů a dat definovaných pomocí jejich názvů, hashů, specifického binárního obsahu (vodoznaku) nebo regulárních výrazů (např. rodné číslo). • Systém musí být schopen detekovat přenosy citlivých souborů a dat alespoň u následujících protokolů: HTTP, FTP, SMTP, SMB, NFS. • V rámci historických metadat u HTTP, FTP, SMTP, SMB a NFS je požadováno ukládání informací o všech po síti přenášených souborech alespoň v rozsahu: 1. název souboru, 2. velikost souboru,

	3. HASH souboru. **Monitoring výkonu aplikací a sítě** • Systém v celé monitorované síti, mezi všemi zařízeními a na všech službách měří a vytváří automaticky (bez nutnosti nastavovat manuálně limitní hodnoty) model normálního chování pro výkonnostní parametry minimálně: 1. přenosová rychlost sítě, 2. rychlost odezvy aplikace, 3. odezva systému z pohledu uživatele. • Výpočet uvedených výkonnostních parametrů a automatické detekce anomálií na základě odchylky od modelu normálního chování musí být prováděna pro: 1. všechny porty a služby TCP, 2. pro všechny kombinace služeb a zařízení. • Systém musí v celé monitorované síti, mezi všemi zařízeními a na všech službách měřit informace o retransmission paketech, out of order paketech, TTL, QoS a komunikaci blokované firewally. **Monitoring cloudových služeb** • Systém musí být schopen monitorovat přístupy zařízení a uživatelů ke cloudovým službám, a to minimálně Google Workspace a Microsoft Office 365, vč. monitoringu operací se soubory, změn oprávnění a nastavení a neúspěšných přístupů. • Systém musí být schopen tyto informace autonomně a průběžně získávat z aplikačních rozhraní těchto cloudových služeb bez nutnosti využití řešení třetích stran. **Inventarizace sítě a grafická vizualizace topologie** • Systém musí být schopen zobrazit celý inventář monitorované sítě s počtem zařízení v jednotlivých lokalitách, segmentech, nebo podsítích. Včetně detailního přehledu zařízení. • Systém musí být schopen graficky vykreslit celou topologii sítě, dle zaznamenané komunikace. • Systém musí být schopen zobrazit inventář jednotlivých lokalit, přehledy zařízení, přehledy výrobců, tagy zřízení, uživatele. • Systém umožňuje všechny inventarizační informace řadit dle různých parametrů.
Dodavatel stručně popíše způsob naplnění jednotlivých požadavků pro další požadované oblasti využití	Systém umožňuje vytvářet komplexní komunikační a bezpečnostní politiky: 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, detekovat změny v sít, jako nové komunikační vektory, nová nebo změněná zařízení a podsítě, obcházení perimetru. Pro účely monitorování politik kybernetické bezpečnosti poskytuje uživatelský rámec pro definování pravidel pomocí uživatelem definované podsítě na základě rozsahů IP adres, uživatelsky libovolně definovaných skupin zařízení, automaticky přiřazené značky/tagu zařízení, které popisují jejich účel a chování – 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. Systém poskytuje nástroj pro reportování bezpečnostních incidentů, včetně spolupráce 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, jednoduché sdílení informací o bezpečnostních incidentech, včetně uživatelem zadaných komentářů, umožňuje vyhledávat a z pohledu workflow bezpečnostního incidentů filtrovat nad všemi událostmi (reportovaná událost, událost v řešení, vyřešená událost, události v řešení daného uživatele apod.). Umožňuje exportovat data do emailu, csv, pdf, syslogu; exportovat bezpečnostní události a incidenty do systémů typu ticket management třetích stran. Systém detekuje přenosy citlivých souborů a dat definovaných pomocí jejich názvů, hashů, specifického binárního obsahu (vodoznaku) nebo regulárních výrazů (např. rodné číslo). Dále detekuje přenosy citlivých souborů a dat u protokolů: HTTP, FTP, SMTP, SMB, NFS. V rámci historických metadat u HTTP, FTP, SMTP, SMB a NFS jsou ukládány informace o všech po síti přenášených souborech v rozsahu: název souboru, velikost souboru a HASH souboru. Systém v celé monitorované síti, mezi všemi zařízeními a na všech službách měří a vytváří automaticky model normálního chování pro výkonnostní parametry: přenosová rychlost sítě, rychlost odezvy aplikace, odezva systému z pohledu uživatele. Uvedené výkonnostní parametry a automatické detekce anomálií na základě odchylky od modelu normálního chování jsou přepočítávány pro všechny porty a služby TCP a pro všechny kombinace služeb a zařízení. Systém v celé monitorované síti, mezi všemi zařízeními a na všech službách měří informace o retransmission paketech, out of order paketech, TTL, QoS a komunikaci blokované firewally. Nabízené řešení monitoruje přístupy zařízení a uživatelů ke cloudovým službám, jako Google Workspace nebo Microsoft Office 365, vč. monitoringu operací se soubory, změn oprávnění a nastavení a neúspěšných přístupů. Tyto informace autonomně a průběžně získává z aplikačních rozhraní těchto cloudových služeb bez nutnosti využití řešení třetích stran Systém umožňuje zobrazit celý inventář monitorované sítě s počtem zařízení v jednotlivých lokalitách, segmentech a podsítích včetně detailního přehledu zařízení. Graficky vykresluje celou topologii sítě dle zaznamenané komunikace, zobrazuje inventář jednotlivých lokalit, přehledy zařízení, přehledy výrobců, tagy zřízení, uživatele. Všechny inventarizační informace řadí dle různých parametrů.

Implementační služby	• Všechna dodavatelem instalovaná zařízení budou zabezpečena a nebudou obsahovat zjevná rizika a zranitelnosti, a to po celou dobu provozu služby. Dodavatel zajistí vyladění a nastavení detekce všech dodávaných systémů tak, aby nebyly detekované nežádoucí a falešně pozitivní události. Tato činnost bude provedena ve spolupráci s kompetentními osobami zadavatele.
Záruka	• Záruka 36měsíců.
Akceptační podmínky	• Veškeré komponenty systému jsou řádně licencované • Bylo dodáno fyzické zařízení dle požadované technické specifikace. • Všechny HW i SW komponenty systému jsou nainstalovány a napojeny na infrastrukturu zadavatele. • Dochází k záznamu flow a zrcadleného provozu, informace jsou dostupné k zobrazení a dalšímu zpracování. • V systému jsou zavedeny všechny zadavatelem dodané podsítě. • Pro všechna zařízení v síti jsou okamžitě dostupné informace o zařízeních (název, mac adresy, IP adresa, uživatele, klientské služby, serverové služby, detekované události, …) • Systém zobrazuje inventarizovanou grafickou topologii celé sítě, včetně počtu zařízení v jednotlivých segmentech sítě a jejich bezpečnostním rizikem. • Systém graficky znázorňuje skutečně přenesená data (In/Out) filtrovaná podle jednotlivých zdrojů flow nebo fyzických/logických interface. • Byla vytvořena a dodána provozní dokumentace. • Bylo provedeno školení v požadovaném rozsahu •
Potvrzení	**Produkty které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky** • jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce, • mají plnou záruku od výrobce, • mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce, • obsahují všechny nezbytné licence na používání příslušného softwaru, • jsou v databázi výrobce uvedeny jako prodaná kupujícímu a určeny pro tento konkrétní projekt • jsou určeny pro provoz v České republice. • Tyto skutečnosti dodavatel doloží potvrzením výrobce nebo oficiálního distributora tohoto zařízení
Další informace či odkazy dodavatele k nabízenému plnění *(nepovinné pole)*	

4) Nástroj pro zajišťování úrovně dostupnosti informací

Server 2 ks

Parametr	Minimální požadavek
Výrobce a model	**HPE DL320 Gen11 4LFF CTO Server/ INT Xeon-Gold 6530 CPU for HPE/768 GB RAM/BCM 57504 10/25GbE 4p SFP28 Adptr/HPE SN1610E 32Gb 2p FC HBA/2x480GB NVMe/HPE DL320 Gen11 NBD support – 5let**
Provedení, příslušenství	• Rackové provedení, max 2U
CPU	• Min. 1x procesor o výkonu minimálně 62000 bodů dle http://cpubenchmark.net/, min počet jader 32
RAM + HDD	• minimálně 768 GB RAM v provedení min. DDR5, min. 5600 MHz • Server musí disponovat alespoň 4x diskovou hotswap šachtou pro disky přístupnou zpředu. Požadujeme osazení min. dvěma SSD 2x 480GB NVMe Hot Plug disky s HW ochranou proti výpadku min. RAID 1
Vlastnosti	• Řadič min. 4GB cache s ochranou proti výpadku napájení • podpora hot-plug disků SAS, SSD i SATA • podpora min. RAID - 0, 1, 5, 6, 10, 50, 60 • 4 x 10/25GbE SFP28 • 1x Dual Port 32GB Fibre Channel karta • Zásuvné ližiny pro rack Podpora systémů: • Microsoft Windows Server • Red Hat® Enterprise Linux • SUSE Linux Enterprise Server
Záruka, servis	• Záruka na 5 let typu NBD, oprava v místě instalace serveru, servis je poskytován výrobcem serveru.
Kompatibilita	• Všechny servery budou od jednoho výrobce z důvodu zajištění maximální kompatibility a jednotného servisního místa a managementu
Další informace či odkazy dodavatele k nabízenému plnění *(nepovinné pole)*	

Server BACK UP - 1 ks

Backup server

Parametr	Minimální požadavek
Výrobce a model	**HPE DL320 Gen11 4LFF CTO Server/ INT Xeon-Gold 6530 CPU for HPE/768 GB RAM/BCM 57504 10/25GbE 4p SFP28 Adptr/HPE SN1610E 32Gb 2p FC HBA/2x480GB NVMe + 4x 6TB HDD/HPE DL320 Gen11 NBD support – 5let**
Provedení, příslušenství	• Rackové provedení, max 2U
CPU	• Min. 1x procesor o výkonu minimálně 62000 bodů dle http://cpubenchmark.net/, min počet jader 32
RAM + HDD	• minimálně 768 GB RAM v provedení min. DDR5, min. 5600 MHz • Server musí disponovat alespoň 4x diskovou hotswap šachtou pro disky přístupnou zpředu. Požadujeme osazení min. dvěma SSD 2x 480GB NVMe Hot Plug disky s HW ochranou proti výpadku min. RAID 1 a diskovou skupinou o hrubé kapacitě min **20T**
Vlastnosti	• Řadič min. 4GB cache s ochranou proti výpadku napájení • podpora hot-plug disků SAS, SSD i SATA • podpora min. RAID - 0, 1, 5, 6, 10, 50, 60 • 4 x 10/25GbE SFP28 • 1x Dual Port 32GB Fibre Channel karta • Zásuvné ližiny pro rack Podpora systémů: • Microsoft Windows Server • Red Hat® Enterprise Linux • SUSE Linux Enterprise Server
Záruka, servis	• Záruka na 5 let typu NBD, oprava v místě instalace serveru, servis je poskytován výrobcem serveru.
Kompatibilita	• Všechny servery budou od jednoho výrobce z důvodu zajištění maximální kompatibility a jednotného servisního místa a managementu
Další informace či odkazy dodavatele k nabízenému plnění *(nepovinné pole)*	

BACK UP - časové zámky

Parametr	Minimální požadavek
Výrobce a model	**ExaGRID PN: EX27-SEC, Disk Capacity: Raw: 72 TB, Useable: 54 TB. 27 TB Full Backup. Disks are encrypted / 10 Gigabit Ethernet Dual Port SFP+ Optical Option for all ExaGrid models. Includes two qualified SFP+ short-range Modules/5let záruka 8x5 NBD**
Výkon a škálovatelnost:	• Řešení musí mít minimálně 54 TB využitelné (usable) lokální kapacity bez redukce dat včetně všech potřebných licencí pro tuto kapacitu.

	• Řešení musí umožňovat rozšíření alespoň do úrovně 1,5 PB využitelné lokální kapacity bez redukce dat a bez nutnosti výměny jakékoliv dodávané součásti, cloudové uložiště jako rozšíření není uznatelné • Propustnost při zálohování dodávaného řešení (skutečný počet disků a dalších komponent) alespoň 6TB/hodinu, • Zařízení musí při ukládání dat využívat princip deduplikace, • Úložiště nesmí vytvářet deduplikační pooly – musí disponovat globální deduplikací bez ohledu na typ dat, přenosový protokol a množství zálohovacích serverů/aplikací, které na něj data ukládají, • Řešení musí být postaveno na fyzické instalaci operačního systému bez další virtualizace.
Integrace a interoperabilita	• Zařízení musí podporovat minimálně následující protokoly: CIFS, NFS, S3 a musí umožnit jejich současné použití, • Zálohovací řešení musí být univerzální z hlediska podpory datových typů zálohovaných dat, musí podporovat všechny datové typy používané v produkčním prostředí • Řešení musí umožnit komprimaci ukládaných deduplikovaných dat • Nabízený diskový úložný systém musí být plně podporován stávajícím zálohovacím SW - VEEAM. Nabízené řešení bude uvedeno na webu výrobce zálohovacího SW VEEAM mezi kompatibilními deduplikačními appliance.
Replikace	• Zařízení musí obsahovat potřebné licence pro nativní funkcionalitu replikace dat do dalšího zařízení stejného výrobce, • Řešení musí posílat pouze deduplikovaná zkomprimovaná data • Řešení musí podporovat alespoň následující scénáře pro replikaci: 1:1, M:1 a kaskádovou replikaci • Řešení musí umožnit funkcionalitu šifrování replikačního toku data-in-flight • Řešení musí umožnit kontrolu a správu využití pásma pro přenos dat (QoS) **Spolehlivost, ochrana a obnova** • Zařízení musí disponovat redundantními hot-swap napájecími zdroji a ventilátory • Zařízení musí zajišťovat ochranu dat alespoň na úrovni duální diskové parity • Zařízení musí umožňovat šifrování úložného prostoru a to bez omezení výkonu - dodání včetně potřebných licencí pro výše požadovanou kapacitu • Zařízení musí zajišťovat výměnu všech disků za chodu – hot-swap, • Zařízení musí obsahovat HotSpare disk pro všechny RAID skupiny v rámci zařízení, • Zařízení musí obsahovat algoritmy pro kontrolu a verifikaci konzistence a čitelnosti uložených dat, • Zařízení musí umožňovat nastavit ochranu dat proti nechtěnému smazání či modifikaci dat pomocí časových zámků. Po nastavenou dobu lze data číst, ale nelze je přepisovat. Tato funkce nesmí být závislá na zálohovacím software, přenosovém protokolu (CIFS, NFS, S3) či typu dat. To znamená, že tato funkce musí být plně funkční nejenom s nabízeným

	zálohovacím SW, ale také jakýmkoliv jiným. Časové zámky se musí aplikovat uvnitř zařízení, nikoliv pomocí externích nástrojů a zálohovacích SW. • Zařízení musí mít integrovanou ochranu časové integrity. • Zařízení musí disponovat síťovými kartami 2x1GbE a 2x10Gb SFP+ včetně GBIC. • Zařízení musí být v provedení RACK (šíře 19"), výška maximálně 2U, výsuvné kolejnice pro instalaci do racku.
Správa	• Řešení musí umožnit centrální správu pro všechna dodávaná zařízení prostřednictvím webového rozhraní • Řešení musí poskytovat funkcionalitu automatického reportingu, automatický call-home, • Řešení musí umožnit správu na principu rolí s různými typy oprávnění (Role-based Access Control). • Řešení musí umožnit vynucení přihlášení minimálně dvou typů účtů (administrátorský, bezpečnostní) pro změny spojené se změnou nastavení ochrany dat – časových zámků. • Řešení musí umožňovat zasílat strukturovaná data provozních a bezpečnostních událostí přes Syslog a SNMP. • Řešení musí umožnit dvoufaktorové ověřování účtů pro správu díky jednorázovým heslům (Time-based One-Time Password). Pokud je potřeba externí nástroj, musí být součástí nabídky všechny potřebné licence až pro 20 uživatelů včetně potřebného hardware pro zajištění vysoké dostupnosti. Licence musí být perpetuální a instalace v místě zadavatele.
Podpora	• Podpora na hardware a software musí být od jednoho výrobce, • Součástí nabízeného řešení musí být služba ponechání si vadných disků. • V rámci povýšení verze softwaru dochází zároveň ke změně verze firmware na kompatibilní úroveň pro důležité komponenty – minimálně pro diskový řadič. • Požadovaná podpora celé nabídky je s reakcí 8x5 NBD po dobu 5 let.
Požadavky na certifikaci dodavatele HW a původ zboží	• Dodavatel doloží certifikace od **výrobce konkrétně** nabízeného řešení jež bude zcela jasně definovat, že je dodavatel dostatečně erudován k instalaci a správě tohoto řešení včetně potvrzení, že nabízené zboží je určené pro EU trh, je nové, nepoužité a pochází z oficiálního distribučního kanálu v ČR a je určeno pro tento konkrétní obchodní případ.
Další informace či odkazy dodavatele k nabízenému plnění *(nepovinné pole)*	

SERVER - virtualizační platforma

Parametr	Minimální požadavek
Výrobce a model	**MICROSOFT H-V 2025 (obsaženo v MICROSOFT SERVER 2025 DATACENTER)**

Parametry	• Funckionalita umožňující bezvýpadkovou migraci virtuálních strojů mezi jednotlivými fyzickými serverovými hostiteli za provozu zajišťující tak plynulou správu a údržbu IT • Funkcionalita, která automaticky nastartuje virtuální stroje při výpadku fyzického serveru na jiném produkčním serveru ze společného diskového prostoru nebo opětovně restartuje dotčený virtuální stroj např. při pádu OS • Funkcionalita, která bude umožňovat za běhu přidávat CPU a paměť virtuálním strojům bez jakéhokoliv přerušení provozu • Rozhraní umožňující zálohovacímu SW třetí strany provádět konzistentní plné, rozdílové a přírůstkové zálohy • Podpora operačních systémů Windows 2016 a novější, Linux • Licence musí pokrývat minimálně 64CORE (dva fyzické servery) s možností dalšího rozšíření
Další informace či odkazy dodavatele k nabízenému plnění *(nepovinné pole)*	

SERVER OS + CAL

Parametr	Minimální požadavek
Výrobce a model	**3x MICROSOFT Windows Server 2025 DATACENTER 32CORE + 200x Windows Server 2025 DATACENTER DEVICE CAL (EDU)**
Parametry	3 ks licencí 64-bitového serverového operačního systému v aktuální verzi • Podpora min. 64 procesorových socketů • Podpora běhu v on-premise, hybrid a cloudovém prostředí • Podpora TPM 2.0 čipů • Podpora ochrany firmware před neoprávněným přepsáním • Podpora replikace úložišť • Vestavěná technologie serverové i desktopové virtualizace • Nativní podpora virtualizace sítí • Neomezený počet virtuálních serverů • Počet licencí bude určen počtem jader procesorů ve všech navržených serverech – min 3x32CORE • Operační systém musí být kompatibilní s již provozovanými aplikacemi. Aktuálně zadavatel provozuje operační systémy od společnosti MICROSOFT. • licence pro nabízené operační systémy umožňující využívat těchto systémů minimálně pro **200** zařízení
Další informace či odkazy dodavatele k nabízenému plnění *(nepovinné pole)*	

Diskové pole

Parametr	Minimální požadavek
Výrobce a model	**IBM STORAGE FLASHSYSTEM 5045 SFF CONTROL ENCLOSURE, PN: 4680-3P4 / 17x 1.92TB 12 GB SAS 2.5 INCH FLASH DRIVE / 16 GB FC 4 PORT ADAPTER CARDS (PAIR) / 5 YEAR ADVANCED EXPERT CARE**
Parametry	• modulární, minimálně dvou řadičové hybridní diskové pole, řešení je koncipováno jako HW a SW od jednoho výrobce • škálování výkonnosti je možné nativním přidáváním dalších řadičů minimálně do čtyř 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 • celková velikost cache/RAM v jednom řadiči je minimálně 32GB • celková nativní rozšiřitelnost je minimálně 400 disků, v případě nasazení více řadičů až dvakrát tolik 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: • enterprise úrovně tzn. minimálně eMLC, 3D TLC, SLC nebo eSLC nebo enterprise flash modulů s hodnotou DWPD 1 a vyšší • rotační disky minimálně na SAS 3.0 architektuře • podpora minimálně následujících režimů RAID - 1, 5, 6 nebo DRAID 1, 5 a 6 • minimálně **32TB hrubé kapacity na SSD**, maximální velikost jednoho disku 2TB • Nabízené řešení nesmí přesáhnout 2U • diskové pole obsahuje připojení diskového pole blokovým přístupem minimálně pomocí 16Gbit FC a 10Gbit iSCSI • jsou požadovány min. 4 porty 16Gb FC a 2 porty 10Gb iSCSI na řadič, tzn. minimálně 8x 16Gbit FC portů a 4x 10Gbit iSCSI portů na jedno dvouřadičové diskové pole • 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 • deduplikace dat v reálném čase bez nutnosti dedikování dodatečného diskového prostoru pro post-processing pro celou požadovanou kapacitu včetně SW licence • možnost budoucího šifrování dat pro jakýkoliv typ disků a nabízenou kapacitu (licence nemusí být součástí dodávky) • možnosti budoucího nasazení inteligentní správy výkonnostních charakteristik (pro minimálně 3) virtualizovaných diskových prostorů (automatická migrace více utilizovaných dat na rychlejší disky nebo SSD), licence nemusí být součástí dodávky • 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 • 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 • blokový, standard FCP a iSCSI • ochrana proti ransomware útokům nativní funkcionalitou nabízeného pole v rámci jeho funkcionalit – řešení z aplikační vrstvy pomocí aplikací třetích stran 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 • řešení musí umožňovat detekci ransomware v reálném čase na blokové úrovni • 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 • 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 • 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 • řešení obsahuje licence na neomezený počet připojení hostitelských serverů • 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.
Záruka, servis	• Minimálně 5 let; v online režimu 24x7 s odezvou tentýž pracovní den včetně SW podpory, která umožňuje např. přístup k novým verzím FW, opravným patchům apod a s garancí opravy do 24hod od nahlášení
Certifikace dodavatele, původ zboží	• Jsou splněny „Požadavky na certifikaci dodavatele HW a původ zboží“
Další informace či odkazy dodavatele k nabízenému plnění *(nepovinné pole)*	

NAS – 1 KS + 4 KS HDD

Parametr	Minimální požadavek
Výrobce a model	**Synology RS1221RP+ Rack Station + 2x Synology D4ES01-8G + Synology 2x10GbE SFP+ síťový adaptér (E10G30-F2) + Sada ližin Synology, RKS-02 + Synology Hardware NBD replacement RS1221RP+ service - 60 měsíců** **+ 4x Synology HAT5300/ 12TB/ HDD/ 3.5"/ SATA/ 7200 RPM/ 5R**

Parametry	• Čtyřjádorový procesor v architektuře x86 64 bit s výkonem min: 4500 bodů v https://www.cpubenchmark.net/cpu_list.php
	• Systémová paměť 16 GB DDR4 2666 MHz
	• Pozice pro diskové jednotky
	  ○ 8 x 3,5" nebo 2,5" SATA HDD/SSD
	• Kompatibilita diskových jednotek
	  ○ 3,5" SATA jednotky pevných disků
	  ○ 2,5" SATA jednotky pevných disků
	  ○ 2,5" SATA SSD
	• Diskové jednotky vyměnitelné za provozu
	• Min.2x Gigabitový Ethernet port (RJ45)
	• 2x 10GbE SFP+
	• USB port
	  ○ 2x USB 3.0
	• Indikátory LED
	• Napájení/stav, LAN, HDD 1-8
	• Systémové varování
	• Disky:
	  ○ 4x12T HDD stejný výrobce jako NAS a určen pro provoz v NAS
	  ○ rychlost přenosu dat 200 MB/s,
	  ○ vyrovnávací paměť 256 MB,
	  ○ rozhraní SATA III (6 Gb/s),
	  ○ rychlost 7 200 ot./min.
	• Záruka 5LET NBD

Další informace či odkazy dodavatele k nabízenému plnění	

(nepovinné pole)	

UPS – 2 KS

Parametr	Minimální požadavek
Výrobce a model	**APC Smart-UPS 3000VA LCD RM 2U 230V with SmartConnect + UPS Network Management Card 3 + NMC3 for Smart-UPS & 1-Ph Symmetra – záruka 5let**
Parametry	• Min. kapacita výstupního výkonu [W]: 2 700 • Jmenovité výstupní napětí [V]: 230 • 8x IEC 320 C13 (Záložní provoz na baterie) • Topologie: Line interaktivní • Zvukové upozornění: Upozornění na stav, kdy je systém napájen z baterie • Zřetelné upozornění na nízkou kapacitu baterie (dobu musí jít nastavit) • Port rozhraní: RJ-45 10/100 Base-T, RJ-45 Serial, rozšiřující slot, USB • Záruka 5LET
Další informace či odkazy dodavatele k nabízenému plnění *(nepovinné pole)*	

Databázový SW

Parametr	Minimální požadavek
Výrobce, název, verze a licenční program databázového SW	**MICROSOFT SQL Server Standard Core SLng LSA 4CORE + SA 3Y**
Verze	• Databázový systém v nejnovější verzi
Vlastnosti	• Databázový SW systému v aktuální verzi pro EDU. Licence musí umožnit provoz neomezeného počtu uživatelů. Databázový SW bude provozován ve virtuálním prostředí a licenčně mu budou přiřazena 4CORE. • Min. 64 GB paměti pro buffer pool • Velikost databáze: min 10TB
Další informace či odkazy dodavatele k nabízenému plnění *(nepovinné pole)*	

Zálohovací SW – pro 15VM

Parametr	Minimální požadavek

Výrobce, název, verze a licenční program	**Veeam Data Platform Essentials Universal Perpetual License. Includes Enterprise Plus Edition features. Production (24/7/365) Support is included. Education sector – 15VM**
Verze	• Zálohovací software v nejnovější verzi
Vlastnosti	• Trvala licence - PERPETUAL • Podporované platformy: VMware vSphere, Microsoft Hyper-V, Nutanix AHV, Red Hat Virtualization, Microsoft Windows, Linux, macOS, IBM AIX, Oracle Solaris. • Podpora cloudových služeb: AWS, Azure, Google Cloud, Microsoft Entra ID, Amazon EC2, RDS, EFS, VPC, Azure VMs, SQL, Files, Google Cloud VMs, Cloud SQL. Podpora databází a aplikací: Microsoft, Oracle, SAP HANA, PostgreSQL, MySQL, • Podpora fyzických serverů: Windows, Linux, macOS, IBM AIX, Oracle Solaris. • Podpora nestrukturovaných dat: Objektové úložiště, NAS, souborové sdílené. • Podpora: 24/7/365 produkční podpora během celého období
Další informace či odkazy dodavatele k nabízenému plnění *(nepovinné pole)*	

Implementace

Implementace analýzy síťového provozu:

- Instalace a konfigurace sondy a agentů pro dohled nad celý prostředím
- Instalace a konfigurace systému pro sběr dat a vyhodnocení
- Konfigurace monitorovacích politik na základě doporučení dané technologie a schválené projektové dokumentace
- Ověření monitorovacích pravidel, testovací provoz

Implementace serverového HW:

- Fyzická instalace serverového HW, aktualizace firmware, zahoření, provedení HW testů
- Konfigurace konzole pro vzdálenou správu a management
- Nasazení a konfigurace virtualizace
- Nasazení a konfigurace SW pro replikaci datového úložiště
- Instalace a konfigurace UPS
- Instalace prostředí a virtuálních systémů
- Migrace stávajícího prostředí virtuálních serverů na nový HW

Implementace síťových prvků a FW

- Instalace a fyzické rozmístění switchů a FW v definovaných lokalitách
- Konfigurace bezpečnostních politik na FW
- Konfigurace sítě a jednotlivých segmentů
- Fyzické propojení síťových prvků včetně přepojení celé sítě a klientských zařízení do nové sítě
- Kompletní konfigurace a nastavení NAC

Implementace zálohování a archivace:

- Instalace a konfigurace zálohovacího serveru
- Konfigurace zálohovacích politik pro zálohování serverové infrastruktury
- Konfigurace a implementace HARDENED REPOSITORY dle BP
- Ověření zálohovacích pravidel

Provedení závěrečných akceptačních testů, zpracování dokumentace a zaškolení

- Provedení testu výpadku jednoho fyzického nodu
- Provedení testu výpadku napájení
- Provedení testu obnovy libovolného serveru či dat ze zálohy
- Zpracování komplexní dokumentace popisující konfiguraci celého prostředí
- Zpracování komplexní bezpečnostní dokumentace dle požadavků bezpečnostních norem
- Zaškolení interní obsluhy správy sítě, zaškolení obsluhy dohledového centra podpory pro vyhodnocení bezpečnostních událostí.

5) nástroj pro ověřování identity uživatelů

Pořízení a implementace nástroje pro multifaktorovou autentizaci a SSO

Parametr	Minimální požadavek
Výrobce, název, verze a licenční program serverového OS	**50x Licence IMPRIVATA SUB-SSO/AM-NON-CLINICAL-S License: OneSign Single Sign-On/Authentication Management for Non-Clinical Users + 50x HDW-IMP-MFR75A Hardware: Imprivata Reader MFR75A (replacement for MFR75)+ 50x Čipová klíčenka DUAL MIFARE S50/EM4200 - (FOB)+2x SUB-VIR-APP-G4 Imprivata Virtual Appliance (4th Generation) – záruka 3roky**
Funkční specifikace	Klientská část řešení musí podporovat Windows Desktop OS (Windows 10 a novější), Linuxové OS tenkých klientů a v případě mobilních klientských zařízení minimálně operační systémy rodiny Windows pro minimálně **50 uživatelů** Řešení bude ve výchozím stavu navrženo a dodáno jako vysoce dostupné, s odolností vůči výpadku jednoho serverového prvku, s minimálně dvěma vzájemně zastupitelnými prvky. Při výpadku jednoho prvku zůstává řešení plně funkční, zbylý funkční prvek/prvky nadále poskytují plnou funkčnost. K překlopení na funkční prvek/prvky musí dojít automaticky, bez nutnosti ručního zásahu, maximálně v jednotkách sekund. Všechny prvky si vzájemně replikují nastavení a data, v případě výpadku prvku tedy nedojde ke ztrátě nastavení či dat. Všechny prvky řešení musí být spravovány jako jeden celek, jednotnou správou z webové konzoly, napříč datovými centry, případně cloudy. Serverová část řešení bude nasazena ve formě virtuálních strojů (podpora minimálně VMware vSphere, Microsoft Hyper-V). Virtuální stroje musí být možné, a ze strany výrobce podporované, provozovat v cloudu (podpora minimálně Microsoft Azure). Řešení musí být možné nasadit také v hybridním režimu, kdy jeden nebo více virtuálních strojů je provozováno v místním datovém centru a další virtuální stroj nebo stroje v cloudu, formou SaaS. Minimálně jeden virtuální stroj však musí být provozován v místním datovém centru organizace zadavatele.

	Řešení musí umožnovat definovat práva na činnosti ve správcovských nástrojích na základě členství v Active Directory skupinách. Řešení musí být schopno definovat různé úrovně administrátorských přístupů – delegování administrativních oprávnění – vytvořením kombinací (sad) oprávnění. Řešení musí být integrováno na jednu nebo více instancí adresářových služeb Microsoft Active Directory Directory Services (AD DS). Identita – uživatelský účet – uživatele dodaného řešení musí odpovídat identitě v AD DS. Změny v AD DS (změny stavu účtu, atributů, členství ve skupinách) musí být automaticky synchronizovány s dodaným řešením. Dodané řešení musí být možné integrovat na více samostatných AD DS bez nutnosti jejich propojení pomocí vztahů důvěryhodnosti (trustu), a dále musí být možné řešení integrovat na další adresářové (LDAP) služby jiných výrobců. Komunikace mezi jednotlivými komponenty řešení v rámci HTTPS komunikace musí být šifrována TLS protokolem minimálně verze 1.2, uložená citlivá data – zejména přihlašovací údaje uživatelů – musí být chráněna FIPS 140-2 validovaným šifrováním AES 256.
Více-faktorová autentizace	Řešení musí umožňovat používání různých autentizačních předmětů pro více-faktorovou autentizaci, minimálně: kontaktní čipové karty (smart karty), bezkontaktní karty a předměty včetně karet NXP Mifare DesFire, bezkontaktní FIDO2 bezpečnostní karty a kontaktní FIDO2 USB klíče, USB tokeny, bezkontaktní RFID předměty, biometrické prvky (otisk prstu), login/heslo (s vazbou i bez vazby na adresářovou službu), a jejich vzájemné kombinace. Vyžádání druhého faktoru musí být možné definovat dynamicky, na základě splnění podmínky (např. uplynutí časového intervalu).
	Řešení musí umožnit volbu parametrů autentizačního PIN kódu pro více-faktorové ověřování (podobně, jako u hesla např. v Active Directory). Délku PINu v rozmezí alespoň od 4 do alespoň 16 znaků, musí umožnit exspiraci PIN kódu po definovaném časovém intervalu, musí umožnit použití jak čistě numerického PINu, tak PINu obsahujícího čísla a písmena a speciální znaky. Řešení dále musí umožnit vynucení historie PINu a zamezit uživateli, aby si při obnově PINu zvolil dříve jím použitý PIN kód (je požadováno, aby si systém pamatoval alespoň 8 posledních PINů). Řešení musí volitelně umožnit vynutit nastavení, které uživateli zamezí nastavit si snadno uhodnutelný PIN (minimálně nedovolit opakování stejných po sobě jdoucích znaků, jako např. „1111" a jednoduchou číselnou řadu, jako např. „1234").
	Řešení musí obsahovat technologii pro automatizaci přihlašovacího procesu, která uživateli umožní přihlášení do vzdálené plochy s využitím již zadaných přihlašovacích pověření, bez nutnosti opakovaně zadávat přihlašovací údaje, potvrzovat připojovací dialogy, znovu použít autentizační předmět, znovu zadávat PIN kód. Tato technologie musí podporovat nejběžnější produkty pro virtualizaci aplikací a desktopů (Microsoft Remote Desktop Services, Citrix Virtual Apps and Desktops, Omnissa Horizon).
	Řešení musí umožňovat režim redukovaného uživatelského rozhraní, tzv. "appliance mode", na tenkých klientech. V tomto režimu je běžné uživatelské rozhraní tenkého klienta nahrazeno přihlašovací obrazovkou pro více-faktorovou autentizaci.
	Řešení musí umožnit nastavení různých kombinací přihlašovacích faktorů pomocí politik, a tyto politiky aplikovat na skupiny uživatelů, skupiny koncových zařízení, typy koncových zařízení s

	rozlišením minimálně: 1. koncová stanice s OS Windows, 2. mobilní zařízení s OS Android
	Řešení musí zajistit funkčnost více-faktorové autentizace pomocí bezkontaktních předmětů i v případě, kdy klientské zařízení není připojeno k síti (je offline) nebo není dostupná serverová strana řešení.
	Řešení musí poskytnout funkce více-faktorové autentizace na koncových (klientských) zařízeních používaných jedním uživatelem, používaných více uživateli, a dále na sdílených koncových stanicích s častým střídáním uživatelů během pracovní doby. Řešení musí poskytnout funkce více-faktorové autentizace na koncovém (klientském) zařízení přihlášeném pomocí jmenného účtu, pomocí obecného (skupinového) Active Directory účtu a pomocí obecného (skupinového) lokálního účtu. Ve všech případech musí být více-faktorové ověření provedeno jménem konkrétního uživatele, tedy přihlašování musí být prováděno uživatelským Active Directory účtem reprezentujícím konkrétní přihlašovanou osobu. Výše uvedené funkce musí být dostupné také na koncových stanicích, které nejsou členy Active Directory domény.
Single Sign-On (SSO)	Řešení musí poskytovat funkci automatického přihlášení SSO (Single Sign-On) alespoň do následujících aplikací: • INFORMAČNÍ SYSTÉM ŠKOLY (Bakaláři/EDUPAGE) • IS pro provoz školy (stravování, účetnictví, docházka, ACS atd) • O365 V případě webových aplikací musí být pro funkci SSO podporovány minimálně tyto prohlížeče: Microsoft Edge Chromium verze 120 a vyšší, Google Chrome verze 120 a vyšší. Dále musí být pro webové aplikace podporována autentizace pomocí protokolu SAML a pomocí protokolu OpenID Connect.
	Řešení musí poskytovat funkci Single Sign-On do aplikací (popsaných v předchozím bodu) z koncových (klientských) zařízení používaných jedním uživatelem, používaných více uživateli, a dále na sdílených koncových stanicích s častým střídáním uživatelů v průběhu pracovní doby. Řešení musí poskytnout funkce SSO do aplikací (popsaných v předchozím bodu) na koncovém zařízení přihlášeném pomocí jmenného účtu, pomocí obecného (skupinového) Active Directory účtu a pomocí obecného (skupinového) lokálního účtu. Ve všech případech musí být funkce SSO poskytovány jménem konkrétního uživatele, tedy přihlašování do aplikací musí být prováděno uživatelským účtem reprezentujícím konkrétní přihlašovanou osobu. Výše uvedené funkce musí být dostupné také na koncových stanicích, které nejsou členy Active Directory domény.
	Řešení musí zajišťovat funkčnost SSO pro aplikace, jejichž klientská strana běží jak na fyzických stanicích, tak ve virtuální ploše – VDI, dále pro virtualizované aplikace a server vzdálené plochy. Řešení musí poskytnout plnou funkčnost SSO pro nejběžnější technologie virtualizace aplikací a desktopů na trhu (Microsoft Remote Desktop Services, Citrix Virtual Apps and Desktops, Omnissa Horizon).
	Přihlašovací údaje do jednotlivých aplikací musí být dostupné jen příslušnému uživateli. Přihlašovací údaje do jednotlivých aplikací a systémů musí být šifrovány, a musí být ukládány na serverovou stranu řešení, aby byly dostupné na každé koncové stanici, ke které se uživatel přihlašuje. Systém musí umožnit, aby pro kritické

	aplikace bylo přihlášení pomocí SSO vynucováno.
	Řešení musí umožnit funkci SSO přihlašování do aplikací jak identitou (účtem) z Active Directory, tak účtem spravovaným danou aplikací. Řešení musí dále poskytovat funkcionalitu Identity Provider (IdP).
	Řešení musí obsahovat integrovaný správce hesel (Password Manager) pro všechny uživatele, s možností uživatelské správy. IT správce musí mít možnost nastavit, zda uživatel může přihlašovací údaje editovat nebo jen zobrazit, a dále, zda může zobrazit heslo v čitelné podobě. Funkce zobrazení hesla v čitelné podobě musí být možné dodatečně zabezpečit (např. vyžádáním hesla, PINu apod.).
	Řešení musí obsahovat grafické uživatelské rozhraní pro vytváření, editaci a správu Single Sign-On napojení (konektorů/profilů). Toto prostředí musí být intuitivní a uživatelsky přívětivé, bez nutnosti psát kód, programovat, používat řádkové příkazy a umožnit zadavateli vytvářet vlastní napojení (konektory/profily) na další aplikace uživatelsky, vlastními silami, bez nutnosti objednávání nových napojení u dodavatele a bez nutnosti úprav kódu těchto aplikací.
Čtečky karet – **50 KS**	Požadované parametry stacionárních čteček bezkontaktních předmětů: • Pracovní frekvence: 13,56 MHz • Podpora bezkontaktních karet/předmětů: rodina NXP Mifare® • Rozhraní: připojitelná přes USB • Typ: externí • Napájení: přes USB rozhraní • Formát: stolní • Přenos dat: zabezpečený, přes API (nesmí simulovat klávesnici) Kompatibilita OS: Windows 10 a vyšší
Autentizační předměty – **50 KS**	Požadované parametry bezkontaktních předmětů: • Pracovní frekvence: 125 kHz a 13,56 MHz • Standardy bezkontaktních předmětů: EM4102/EM4200 a NXP Mifare® minimálně S50, 1kb • Formát: přívěšek (fob) Provedení: plastový, mechanicky odolný, možnost potisku nebo gravírování
Implementace	Instalace a konfigurace SW pro dvoufaktorovou autentizaci a SSO Konfigurace přístupu uživatelů Pilotní ověření a ostré nasazení
Záruky a podpora	Záruka 36měsíců
Další informace či odkazy dodavatele k nabízenému plnění *(nepovinné pole)*	

Společné požadavky pro kapitoly 1 – 5

Požadavek
Dodavatel bere na vědomí, že součástí akceptace plnění jsou výsledky auditu, který bude prověřovat, zda jím implementovaná bezpečnostní opatření jsou funkční. Dodavatel pak poskytne součinnost nebo napraví nalezené chyby vysoké závažnosti v implementaci technických opatření.
Součástí je zajištění instalace a konfigurace veškerých komponent v návaznosti na stávající infrastrukturu školy (tj. včetně dopravy, montáže, instalace a implementace do stávající IT infrastruktury) v sídle zadavatele.
Součástí instalace musí být i zaškolení IT administrátorů minimálně v rozsahu nutném pro samostatnou administraci všech komponent zakázky. Administrací se rozumí zejména: konfigurace, monitoring činnosti, aktualizace, řešení problémů, zálohování konfigurace.
Zákaznická dokumentace bude zahrnovat: • popis všech prvků/zařízení, • popis způsobu zálohy a obnovy konfigurace všech prvků/zařízení • veškeré požadavky na zachování záruky/podpory (např. environmentální, kompatibilita, …) • informaci o způsobu řešení servisních požadavků
Dodavatel do své nabídky zahrne veškerý instalační materiál a kabeláž nutnou k plnohodnotnému zprovoznění dodané technologie jako logického a funkčního celku.
Dodavatel zajistí instalaci a konfiguraci dodaných HW a SW komponent v návaznosti na stávající infrastrukturu organizace, a to včetně instalace a implementace do stávající IT infrastruktury v sídle zadavatele: • instalace zařízení do standardní RACK skříně 19" 42U • implementace Best Practice scénářů pro dané konfigurace • kontroly kompatibility verzí ovladačů a firmware jednotlivých zařízení a jejich aktualizace • registrace záruk u výrobců • umístění do racku a zapojení kabeláže vč. jejího označení, • inicializace a konfigurace všech dodaných zařízení • nastavení IP adres • nastavení vysoké dostupnosti • konfiguraci datových prostor polí, integrace s hypervizorem, nastavení dohledu a instalace SW pro monitoring výkonu • zapojení do stávající LAN

Maintenance

MAINTENANCE - (software maintenance) je proces pravidelného udržování, vylepšování a opravování softwarových aplikací po jejich prvotním vývoji a nasazení. Zadavatel v rámci stanovení nabídkové ceny nacení veškerou potřebnou maintenance k řádnému provozovaní dodaného řešení. Potřebnou maintenence dodavatel nacení po dobu udržitelnosti projektu 5let. Maintenance bude dle povahy dodaného řešení pokrývat níže uvedené scénáře:

Korekční údržba: Oprava chyb a problémů, které se objeví po nasazení softwaru. To může zahrnovat opravy bezpečnostních zranitelností, chyb v kódu nebo jiné problémy, které ovlivňují funkčnost softwaru.
Adaptivní údržba: Úpravy a změny softwaru, aby zůstal kompatibilní s měnícím se prostředím. To může zahrnovat aktualizace pro nové operační systémy, hardware nebo jiné softwarové závislosti.
Perfekcionistická údržba: Vylepšení softwaru za účelem zvýšení jeho výkonu nebo použitelnosti. To může zahrnovat optimalizaci kódu, zlepšení uživatelského rozhraní nebo zavádění nových funkcí. Údržba softwaru je klíčová pro zajištění, že software zůstane funkční, bezpečný a relevantní i po dlouhou dobu po jeho původním nasazení.

Provozní podpora

Požadavek
Podpora a servis pro dodaný HW a SW budou poskytovány po dobu udržitelnosti projektu (tj. 60 měsíců od předání díla), nebude-li dohodnuto smluvními stranami jinak – dodavatel bude kalkulovat pro základní technickou podporu **2 hodiny/měsíc.**
Bude zajištěna udržitelnost HW a SW včetně třetích stran, dodaných v rámci veřejné zakázky.
Technická podpora a servis zařízení HW a SW budou realizovány dodavatelem, případně prostřednictvím odpovídajícího servisního kanálu výrobce.
Technická podpora a servis budou realizovány v místě zadavatele. Výjimku tvoří činnosti realizovatelné vzdáleným připojením.
Technická podpora bude zajišťována těmito způsoby: • Telefonicky prostřednictvím přiděleného tel. kontaktu. • Prostřednictvím servisního e-mailu. • Prostřednictvím elektronické oznamovací služby (tzv. helpdesku). • Prostřednictvím vzdáleného připojení na PC uživatele / server.
Telefonická, e-mailová podpora a podpora prostřednictvím vzdáleného připojení bude k dispozici minimálně v pracovních dnech od 7 do 16 hod.
Služba HelpDesk umožní příjem požadavku na servisní zásah v českém jazyce prostřednictvím webového rozhraní v režimu 7x24 hod (s výjimkou předem nahlášených servisních zásahů při správě systému HelpDesk).
Postup při řešení incidentů – SLA Zadavatel bude incident oznamovat dodavateli bez zbytečného odkladu jedním ze způsobů a na kontaktních místech, kam budou mít zajištěny přístup pověřené osoby Zadavatele (HelpDesk). Součástí nahlášení požadavku Zadavatelem musí být: • popis Incidentu nebo Požadavku, • jiné relevantní upřesňující informace, včetně případných textových či obrazových příloh nezbytných pro replikaci incidentu, • kontaktní osoba. Dodavatelem používaný systém pro HelpDesk musí pokrýt uvedené informace pro nahlášení požadavku. **<u>Dodavatel zahájí řešení kritického incidentu ohrožující provoz organizace do 4 pracovních hodin od nahlášení, za pracovní hodiny se považuje období mezi 7:00 a 16:00 v pracovní dny.</u>** **<u>Dodavatel zahájí řešení nekritického incidentu NBD od nahlášení.</u>** Dodavatel neprodleně potvrdí obdržení požadavku v systému HelpDesk a poskytne Zadavateli informace o předpokládaném způsobu řešení požadavku, požadavcích na součinnost Zadavatele a předpokládaný termín vyřešení požadavku. Dodavatel v průběhu řešení požadavku, pokud mu to charakter požadavku a způsob řešení umožňuje, průběžně informuje Zadavatele o aktuálním stavu a případných změnách v předpokládaném způsobu, požadované součinnosti a termínů vyřešení. V případě že dodavatel v průběhu řešení požadavku zjistí, že se jedná o Incident, jehož zdroj je prvek třetích stran, informuje Zadavatele o této skutečnosti, předpokládaném způsobu, požadované součinnosti a termínů vyřešení a pokračuje v řešení v režimu BE (Best Effort) tzn. dodavatel vyvine maximální možné úsilí na provedení požadavku a zejména na zajištění požadovaných parametrů předmětu plnění v nejkratší možné době.

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

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

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

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

- v případě Incidentu specifikuje příčinu (pokud je známa),
- vyzve iniciátora k ověření funkčnosti služby.

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

Po vyřešení požadavku dodavatel požadavek uzavře v systému HelpDesk a informuje Zadavatele.

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

Záruky na servisní služby

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

Střední pedagogická škola Boskovice, příspěvková organizace
KYBERBEZPEČNOST 1.0

Položka	Popis položky	Jednotka	Počet Jednotek	Jednotková cena v Kč bez DPH	Celková cena v Kč bez DPH	Celková cena v Kč vč. DPH	
1) nástroj pro ochranu integrity komunikačních sítí							
FIREWALL							
FIREWALL	Firewall/8x GE RJ45 a zároveň min. 2ks SFP+ port/propustnost min. 2,5 Gbps /IPS, Malware ochrana,aplikační kontrolar, URL, DNS, Antispam - záruka 3ROKY	KS	1	[redacted]	[redacted]	[redacted]	
Centralizované logování analýza a report	Centralizované logování + analýza a report min. 5 GB logů/den	KS	1	[redacted]	[redacted]	[redacted]	
Nadstandardní záruky a podpory výrobců	Záruky/ (4.ROK projektu)	KS	1	[redacted]	[redacted]	[redacted]	
Nadstandardní záruky a podpory výrobců	Záruky/ (5.ROK projektu)	KS	1	[redacted]	[redacted]	[redacted]	
MAINTENANCE support	Potřebná maintenance nutná pro provoz systémů	ROK	5	[redacted]	[redacted]	[redacted]	
IMPLEMENTACE	IMPLEMENTACE + ŠKOLENÍ + dokumentace projektu	MD	10	[redacted]	[redacted]	[redacted]	
					[redacted]	[redacted]	
2) nástroj pro ochranu koncových stanic							
Ochrana koncových stanic a SVR							
Endpoint NGA + EDR	Ochrana koncových stanic Endpoint + EDR	KS	60	[redacted]	[redacted]	[redacted]	
Nadstandardní záruky a podpory výrobců	Záruky/ (4.ROK projektu)	KS	1	[redacted]	[redacted]	[redacted]	záruka na SW je v tomto případě irelevantní/vyrobce neuplatnuje
Nadstandardní záruky a podpory výrobců	Záruky/ (5.ROK projektu)	KS	1	[redacted]	[redacted]	[redacted]	záruka na SW je v tomto případě irelevantní/vyrobce neuplatnuje
MAINTENANCE support	Potřebná maintenance nutná pro provoz systémů	ROK	5	[redacted]	[redacted]	[redacted]	
IMPLEMENTACE	IMPLEMENTACE / zaškolení	MD	30	[redacted]	[redacted]	[redacted]	
					[redacted]	[redacted]	
3) nástroje pro ochranu integrity komunikačních sítí							
INFRASTRUKTURA - core							
Aktivní prvky core switch	CORE SWITCH /24 x 10Gb SFP+ - 5let záruka	KS	2	[redacted]	[redacted]	[redacted]	
Aktivní prvky minigbic	10G SFP+ Transceiver - 5let záruka	KS	30	[redacted]	[redacted]	[redacted]	
INFRASTRUKTURA - aktivní prvky - POE							
Aktivní prvky PoE - 48port	PoE SWITCH /48x GE RJ45 PoE - 5let záruka	KS	14	[redacted]	[redacted]	[redacted]	
INFRASTRUKTURA - WIFI							
WIFI interní	WIFI AP - indoor s interními anténami v katefgorii WiFi 6E - 5let záruka	KS	40	[redacted]	[redacted]	[redacted]	
NAC	NAC - Virtuální appliance/NAC pro min 500endpointů	KS	1	[redacted]	[redacted]	[redacted]	
Nadstandardní záruky a podpory výrobců	Záruky/ (4.ROK projektu)	KS	1	[redacted]	[redacted]	[redacted]	HW již se zárukou 5let dle požadavku TS
Nadstandardní záruky a podpory výrobců	Záruky/ (5.ROK projektu)	KS	1	[redacted]	[redacted]	[redacted]	HW již se zárukou 5let dle požadavku TS
MAINTENANCE support	Potřebná maintenance nutná pro provoz systémů	ROK	5	[redacted]	[redacted]	[redacted]	
IMPLEMENTACE	IMPLEMENTACE / zaškolení	KS	10	[redacted]	[redacted]	[redacted]	
					[redacted]	[redacted]	
Analýza šíťového provozu							
SONDA a COLEKTOR - SW	SW licence: senzor + kolektor /500Mbps pro alespoň 1500 monitorovaných IP adres	KS	1	[redacted]	[redacted]	[redacted]	
SONDA a COLEKTOR - HW	HW datový kolektor/sensor umožňující trvalý průtok 500Mbps pro alespoň 1500 monitorovaných IP adres s monitorovacím rozhraním min 4x 1GbE. Na zařízení je požadována dostupná historie dat minimálně 6 měsíců.	KS	1	[redacted]	[redacted]	[redacted]	
Nadstandardní záruky a podpory výrobců	Záruky/ (4.ROK projektu)	KS	1	[redacted]	[redacted]	[redacted]	
Nadstandardní záruky a podpory výrobců	Záruky/ (5.ROK projektu)	KS	1	[redacted]	[redacted]	[redacted]	
MAINTENANCE support	Potřebná maintenance nutná pro provoz systémů	ROK	5	[redacted]	[redacted]	[redacted]	
IMPLEMENTACE	IMPLEMENTACE / zaškolení	KS	15	[redacted]	[redacted]	[redacted]	
					[redacted]	[redacted]	
4) nástroj pro zajišťování úrovně dostupnosti informací							
INFRASTRUKTURA							
SERVER	SERVER min.1x procesor o výkonu minimálně 62000 bodů dle http://cpubenchmark.net/, min počet jader 32 /RAM 768GB, 5600MT/s/2x480GB SSD/2x32Gb Fibre CARD/4x25GbE /5Y NBD	KS	2	[redacted]	[redacted]	[redacted]	
SERVER BACKUP	SERVER min.1x procesor o výkonu minimálně 62000 bodů dle http://cpubenchmark.net/, min počet jader 32 /RAM 768GB, 5600MT/s/2x480GB SSD +20T SAS/2x32Gb Fibre CARD/4x25GbE /5Y NBD	KS	1	[redacted]	[redacted]	[redacted]	
BACK UP - časové zámky	BACK UP - vrstvené zálohovací úložiště s diskovou mezipamětí / 54T, dlouhodobé a bezpečné uložiště pro uchovávání záloh - záruka 5Y	KS	1	[redacted]	[redacted]	[redacted]	
SERVER - virtulizační platforma	Virtualizační platforma - Licence musí pokrývat minimálně 64CORE (dva fyzické servery) s možností dalšího rozšíření	KS	1	[redacted]	[redacted]	[redacted]	licence je již součástí OS (MS WIN 2025 DATACENTER)
SERVER OS	Serverové operační systémy - pokrývající 32core/SERVER - EDU	KS	3	[redacted]	[redacted]	[redacted]	
SERVER CAL	Serverové operační systémy - CAL - EDU	KS	200	[redacted]	[redacted]	[redacted]	
DISKOVÉ POLE	Diskové pole/min. 32TB hrubé kapacity na SSD, maximální velikost jednoho disku 2TB/16 GB FC 4 PORT ADAPTER CARDS (PAIR)/záruka 5let s garancí opravy do 24hod	KS	1	[redacted]	[redacted]	[redacted]	
NAS	NAS Rack /Minimálně 8šachtové NAS zařízení /Ctyřjádorový procesor v architektuře x86 64 bit s výkonem min: 4500 bodů v https://www.cpubenchmark.net/cpu_list.php/16GB RAM /ližiny/ záruka 5let	KS	1	[redacted]	[redacted]	[redacted]	
HDD pro NAS	HDD pro NAS/12TB/HDD/3.5"/SATA/7200 RPM/ záruka 5let	KS	4	[redacted]	[redacted]	[redacted]	
UPS - páteřní prvky	UPS min 2700W/8x IEC 320 C13 / LAN management - 5Y záruka	KS	2	[redacted]	[redacted]	[redacted]	
DATABÁZE - pro neomezený počet uživatelů	DATABÁZOVÝ SW pro celkem 4 CORE pro neomezený počet uživatelů	KS	1	[redacted]	[redacted]	[redacted]	
BACKUP SW pro 15VM	BACKUP SW pro min. 15VM - PERPETUAL	KS	1	[redacted]	[redacted]	[redacted]	
Nadstandardní záruky a podpory výrobců	Záruky/ (4.ROK projektu)	KS	1	[redacted]	[redacted]	[redacted]	
Nadstandardní záruky a podpory výrobců	Záruky/ (5.ROK projektu)	KS	1	[redacted]	[redacted]	[redacted]	
MAINTENANCE support	Potřebná maintenance nutná pro provoz systémů	ROK	5	[redacted]	[redacted]	[redacted]	
IMPLEMENTACE a MIGRACE	IMPLEMENTACE a MIGRACE/zaškolení	MD	20	[redacted]	[redacted]	[redacted]	
					[redacted]	[redacted]	
5) nástroj pro ověřování identity uživatelů							
MFA + SSO přihlašování							
K4a - MFA + SSO - licence USER	MFA + SSO - licence USER	KS	50	[redacted]	[redacted]	[redacted]	
K4b - MFA + SSO - licence SERVER	MFA + SSO - licence SERVER	KS	2	[redacted]	[redacted]	[redacted]	

K4c - HW - čtečky karet	Čtečky bezkontaktních čipů	KS	**50**			
K4d - HW - bezkontaktní karty	Bezkontaktní čip	KS	**50**			
Nadstandardní záruky a podpory výrobců	Záruky/ (4.ROK projektu)	KS	**1**			
Nadstandardní záruky a podpory výrobců	Záruky/ (5.ROK projektu)	KS	**1**			
MAINTENANCE support	Potřebná maintenance nutná pro provoz systémů	ROK	**5**			
IMPLEMENTACE	IMPLEMENTACE / zaškolení	MD	**15**			

Technická podpora						
Základní technická podpora (ZTP)	**Základní technická podpora (ZTP)** - Dodavatel nacení Základní technickou podporu poskytovanou formou servisních služeb v časové dotaci: **2 hodiny/měsíc x 12 měsíců**. Dodavatel do jednotkové ceny uvede **cenu za roční základní technickou podporu**	ROK	**5**			
Rozšířená servisní podpora (RTP)	Rozšířená servisní podpora (RTP) - Dodavatel nacení Rozšířenou servisní podporu poskytovanou formou servisních služeb v časové dotaci: **100 hodin/rok**. Tato hodinová sazba bude fixní po dobu prvních 5-ti let poskytování RSP. Pro potřeby hodnocení bude kalkulován indikativní počet hodin rozšířené servisní podpory. Dodavatel do jednotkové ceny uvede nabízenou HODINOVOU SAZBU.	HOD	**100**			

Cena za dodávku a implementaci řešení KYBERBEZPEČNOST včetně standardní záruky *(k doplnění do čl. VI. odst. 2.1. Smlouvy)*	
Cena za poskytnutí nadstandardní (prodloužené) záruky pro 4. a 5. rok plnění *(k doplnění do čl. VI. odst. 2.2. Smlouvy)*	
Cena za poskytování potřebné maintenance support a Základní technické podpory na 5 let *(k doplnění do čl. VI. odst. 2.3. Smlouvy)*	
Cena za poskytování Rozšířené servisní podpory na 5 let *(k doplnění do čl. VI. odst. 2.4. Smlouvy)*	
CELKOVÁ CENA - kritérium hodnocení *(k doplnění do čl. VI. odst. 1. Smlouvy)*	

Pozn.: Pokud dodavatel nabídne pro některou položku nulovou hodnotu, uveden ve sloupci H důvod takového (ne)ocenění.
Pozn.: Účastník odpovídá za cenovou kalkulaci; před podáním cenové kalkulace zkontroluje správnost nastavení vzorců.

Příloha č. 3 smlouvy

Realizační tým

Projektový manažer – Filip Junga

Technický specialista – Mrkvica Stanislav

Specialista/konzultant – kybernetická bezpečnost – Chalota Jiří

Doklady realizačního týmu jsou součástí nabídky.

Příloha č. 4 smlouvy

Seznam poddodavatelů

K plnění veřejné zakázky nebudou využití žádní poddodavatelé – Dodavatel bude zakázku realizovat výhradně vlastními silami.