Kybernetická bezpečnost – Vyšší odborná škola a střední škola Boskovice

Smlouva o dílo

Evidenční číslo: xx

níže uvedeného dne, měsíce a roku uzavřeli

1.	**Název:**	**Vyšší odborná škola a střední škola Boskovice, příspěvková organizace**
	se sídlem:	Hybešova 982/53, 680 01 Boskovice
	IČ:	62073516
	DIČ:	CZ62073516
	Zástupce:	Mgr. Josef Sychra, ředitel
	dále jen "**Objednatel**"	

a

2.	**Název**	**Aricoma Systems a.s.**
	se sídlem:	Hornopolní 3322/34, Moravská Ostrava, 702 00 Ostrava
	IČ:	04308697
	DIČ:	CZ04308697
	Bankovní spojení:	Československá obchodní banka, a.s.
	Číslo účtu:	117878773/0300
	Zástupce:	Petr Konečný, ředitel RC, na základě plné moci
	Realizace:	
	dále jen "**Zhotovitel**"	

(**Objednatel** a **Zhotovitel** označováni společně dále též jako "**Smluvní strany**" nebo „Strany“)

podle § 2586 a násl. a § 2358 a § 2371 a násl. z. č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“), a zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), v platném znění (dále jen „autorský zákon“) tuto Smlouvu o dílo (dále jen „Smlouva“).

Úvodní ustanovení

(A) Definice.

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

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

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

„**Instalačním médiem**“ se rozumí flash paměť (flash disk), magnetické diskové paměťové jednotky (přenosné disky) a médium pro ukládání dat (cd-rom,dvd-rom);

„**Software**“ znamená veškeré systémové a aplikační programové vybavení, potřebné k řádnému, plně funkčnímu, nepřetržitému a bezporuchovému fungování předmětu plnění, které bude předmětem Dodávek. Software též zahrnuje Licencované programy Zhotovitele a Licencované programy třetích stran;

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

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

„Poddodavatel“ znamená jakoukoli právnickou nebo fyzickou osobu, s níž Zhotovitel uzavřel smlouvu, na jejímž základě bude taková osoba provádět plnění předmětu této Smlouvy nebo její části, nejedná-li se o osobu v základním pracovněprávním vztahu k Zhotoviteli;

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

„Zadávací řízení“ znamená řízení podle zákona č. 134/2016 Sb. o zadávání veřejných zakázek (dále jen „ZZVZ“), na zadání veřejné zakázky s názvem „Kybernetická bezpečnost – Vyšší odborná škola a střední škola Boskovice“ (dále jen „Veřejná zakázka“);

„Zadávací dokumentace“ znamená zadávací dokumentaci Veřejné zakázky ve znění dodatečných informací k této zadávací dokumentaci.

(B) Výklad

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

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

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

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

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

(C) Komunikace mezi stranami

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

Veškerá komunikace podle Smlouvy bude probíhat výlučně v českém jazyce.

(D) Licence

Zhotovitel prohlašuje, že je oprávněn poskytnout Objednateli uživatelskou licenci k Software dle této Smlouvy.

Zhotovitel dále prohlašuje, že poskytnutím licence Objednateli neporušuje práva duševního vlastnictví třetích osob a že nejsou třetí osoby, které by mohly oprávněně uplatňovat své nároky z těchto práv vůči Objednateli. V případě, že Zhotovitel nedodrží toto ustanovení, zavazuje se uhradit veškeré nároky třetích osob z důvodu porušení práv duševního vlastnictví třetích osob a dále náhradu škody způsobenou tím Objednateli.

Zhotovitel rovněž převádí Objednateli vlastnické právo k Instalačním médiím, na nichž je Software poskytován a k dalšímu příslušenství (návody v jakékoli podobě, hardwarové klíče apod.).

I. Předmět plnění smlouvy

1.1. Zhotovitel se touto Smlouvou zavazuje Objednateli řádně a včas, na svůj náklad a nebezpečí dodat a implementovat hardware a software specifikovaný v článku II. této Smlouvy včetně zajištění servisní podpory provozu hardware dle specifikace v čl. II (dále jen „dílo“) a Objednatel se zavazuje za provedené dílo zaplatit Zhotoviteli cenu ve výši a za podmínek sjednaných v této Smlouvě.

Součástí závazku Zhotovitele je rovněž poskytnutí oprávnění k užití hardware a software.

Součástí závazku Zhotovitele je dále také zaškolení obsluhy, jakož i dodání příslušné uživatelské dokumentace a koncepčních a systémových materiálů zajišťujících ve svém souhrnu zabezpečení podpory provozu díla minimálně v rozsahu požadovaném Přílohou č. 1 Smlouvy, a to v případě potřeby i třetí stranou.

1.2. Zhotovitel se touto Smlouvou zavazuje poskytnout Objednateli oprávnění k výkonu práva užít software (licenci) ve smyslu čl. XVI. Smlouvy. Cena za poskytnutí licence k software je již obsažena v ceně díla.

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

1.4. Předmětem díla jsou rovněž činnosti, práce a dodávky, které nejsou v uvedeny v tomto článku Smlouvy, ale o kterých Zhotovitel věděl nebo podle svých odborných znalostí vědět měl anebo mohl, že jsou k řádnému a kvalitnímu provedení díla dané povahy třeba, a dále, které jsou s řádným provedením předmětu díla nutně spojeny a vyplývají ze standardní praxe realizace děl analogického charakteru.

II. Specifikace díla

2.1. Hardware a software, který je předmětem Smlouvy, je podrobně specifikován v Příloze č. 1 této Smlouvy.

2.2. Požadavky na zajištění provozní podpory dodaných technologií, které jsou předmětem této Smlouvy, jsou podrobně specifikovány v Příloze č.1 této Smlouvy.

2.3. Musí být naplněny veškeré podmínky vyplývající ze skutečnosti, že předmět plnění veřejné zakázky je způsobilým výdajem ze strukturálních fondů EU včetně splnění podmínek publicity a podmínky umožňující kontrolu ze strany řídícího nebo zprostředkujícího orgánu IROP (CRR, MMR ČR), Platebního orgánu (MF ČR, příslušného finančního úřadu), Nejvyššího kontrolního úřadu a dalších oprávněných orgánů státní a veřejné správy, a EU (Evropské komise, Evropského soudního dvora, Evropského účetního dvora apod.). Zhotovitel je dále povinen poskytnout Objednateli veškeré doklady související s realizací Veřejné zakázky a plněním monitorovacích ukazatelů, které si vyžádají kontrolní orgány IROP.

2.4. Specifikace předmětu díla dle této Smlouvy vychází zejména z Přílohy č. 1 Zadávací dokumentace (Technická specifikace), která tvoří Přílohu č. 1 k této Smlouvě.

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

2.5.1. touto Smlouvou a jejími přílohami;

2.5.2. zadávacími podmínkami Veřejné zakázky;

2.5.3. nabídkou Zhotovitele;

2.5.4. písemnými pokyny Objednatele řádně podepsanými oprávněným zástupcem Objednatele;

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

2.6. Zadávací dokumentace je přitom závazná v plném rozsahu, v případě rozporu mezi zněním Zadávací dokumentace a této Smlouvy má Zadávací dokumentace přednost.

2.7. Nepředvídanými okolnostmi se rozumí:

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

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

2.8. Za nepředvídané okolnosti se nepovažují zejména:

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

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

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

2.9. Zhotovitel není nikdy v prodlení se závazkem či s termínem vyplývajícím z realizace této Smlouvy, je-li toto prodlení způsobeno z důvodu na straně Objednatele, vyšší mocí nebo na straně třetí osoby, která se přímo nepodílí na plnění na straně Zhotovitele. Stejně tak nejde o prodlení Zhotovitele, je-li nesplnění termínu či závazku Zhotovitele z této Smlouvy z důvodu realizace víceprací, které vylučují dokončení díla v původním rozsahu v řádném termínu, z důvodu obdržení zavádějících nebo nesprávných pokynů či informací od Objednatele, z důvodu prodlení Objednatele, z důvodu legislativních změn, které si vyžádají změny v provádění díla. Stejně tak nejde o prodlení Zhotovitele, je-li nesplnění termínu či závazku Zhotovitele z této Smlouvy z důvodu probíhajících správních či jiných řízení, z důvodu neudělení potřebného souhlasu/povolení ze strany správního orgánu, úřadu či soudu, pokud se nejedná o správní úkony, souhlasy/povolení či jiná řízení, která Zhotovitel měl zajistit v rámci realizace předmětu plnění.

2.10. Změny předmětu díla, včetně ceny a doby plnění, budou-li změnou ovlivněny, které splňují požadavky článku II. odst. 2.2 a 2.4. této Smlouvy, musí být specifikovány v písemném dodatku k této Smlouvě a pro Zhotovitele se stanou závaznými vždy ode dne účinnosti příslušného písemného dodatku Smlouvy.

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

2.11.1. Zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů,
2.11.2. Zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů,
2.11.3. Zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů,
2.11.4. Zákona č. 586/1992 Sb., o daních z příjmů, ve znění pozdějších předpisů,
2.11.5. Zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů.

III. Doba a místo plnění

3.1. Smluvní strany se dohodly, že předmět díla bude proveden dle následujícího harmonogramu, a to v následujících termínech:

Id	Činnosti	Termín
01	Podpis Smlouvy	*bude upřesněno dle ukončení zadávacího řízení*
02	Zahájení realizace projektu	do 1 týdne od nabytí účinnosti smlouvy
Instalace a implementace SYSTÉMU		
03	**Zpracování a akceptace Detailního realizačního konceptu** Výstupem bude dokument Detailní realizační koncept Předání dílčího plnění a Akceptace dílčího plnění	do 4 týdnů od zahájení realizace projektu
04	**Realizace předmětu plnění – implementace kyberbezpečnostních opatření**	do 22 týdnů od zahájení realizace projektu
05	**Školení administrátorů**	do 2 týdnů od ukončení fáze 04
06	**Zkušební a testovací provoz, migrace stávajících dat objednatele** Akceptace Testovacího provozu	do 2 týdnů od ukončení fáze 05
07	**Produkční provoz** Akceptace produkčního provozu	od ukončení fáze 06, celkem do 26 týdnů od zahájení realizace projektu
08	**Provozní podpora dodaných technologií**	60 měsíců po zahájení produkčního provozu

3.2. Požadované plnění díla jako celku bude zahájeno bezprostředně po nabytí účinnosti Smlouvy.

3.3. Provedením díla se rozumí úplné dodání a dokončení díla způsobilého sloužit svému účelu a prostého všech vad a současně řádné protokolární předání díla Objednateli formou dle článku X. této Smlouvy.

3.4. Smluvní strany se dohodly, že dílo bude provedeno v termínech uvedených v odst. 3.1. tohoto článku Smlouvy.

3.5. Smluvní strany se dohodly, že celková doba provedení díla stanovená touto Smlouvou je konečná a nelze ji prodlužovat vyjma případů popsaných v čl. II. odst. 2.10 a čl. III odst. 3.6 této Smlouvy.

3.6. Změna etap a termínů realizace předmětu díla stanovených v čl. III odst. 3.1., je možná pouze na základě předchozí písemné dohody Smluvních stran, není-li Smlouvou stanoveno jinak.

3.7. Zdrží-li se provádění předmětu díla z důvodů stanovených v čl. II. odst. 2.9. Smlouvy, má Zhotovitel právo na přiměřené prodloužení doby plnění předmětu díla či jeho části, a to o dobu, o kterou bylo plnění předmětu díla či jeho části takto zdrženo.

3.8. Před dobou sjednanou pro předání a převzetí řádně provedeného díla či jeho části dle článku III. odst. 3.1. Smlouvy není Objednatel povinen od Zhotovitele předmět díla či kteroukoli jeho část převzít.

3.9. Místem plnění je sídlo Objednatele a další budova objednatele na adrese Komenského 57/1, 680 01 Boskovice.

3.10. Místem předání a převzetí díla je sídlo Objednatele.

IV. Cena a platební podmínky

4.1. Sjednaná cena díla (včetně ceny zajištění provozní podpory) činí celkem 12.948.700,00,- Kč (slovy: dvanáct milionů devět set čtyřicet osm tisíc sedm set korun českých) korun českých) bez DPH (dále jen „Cena“).

4.2. K ceně sjednané v čl. 4.1 bude vyúčtována daň z přidané hodnoty dle aktuálně platných a účinných právních předpisů.

4.3. Podrobná specifikace cen je obsažena v Příloze č. 2 této Smlouvy. Cena zahrnuje veškeré náklady Zhotovitele nezbytné k řádnému splnění jeho závazku a je cenou konečnou.

4.4. Zhotovitel vystaví a předá Objednateli daňový doklad (fakturu) až poté, co je dílo provedeno ve smyslu čl. III. odst. 3.3. této Smlouvy. Servisní podpora je součástí cen sjednaných v Příloze č. 2 této Smlouvy a bude vyúčtována v tomto daňovém dokladu vystaveném po provedení díla.

4.5. Každý originální účetní doklad (faktura) musí být označen registračním číslem projektu CZ.31.2.0/0.0/0.0/23_092/0008750 a zkratkou NPO.

4.6. Faktura musí obsahovat náležitosti daňového a účetního dokladu dle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, a zákona č. 235/2004 Sb., o dani z přidané hodnoty, v znění pozdějších předpisů (dále jen „DPH“) a bude mít náležitosti obchodní listiny dle § 435 Občanského zákoníku. Smlouva bude označena Evidenčním číslem Objednatele (viz také záhlaví Smlouvy). V případě, že faktura nebude mít odpovídající náležitosti, je Objednatel oprávněn zaslat ji ve lhůtě splatnosti Zhotoviteli zpět k opravě či doplnění. Lhůta splatnosti počíná běžet znovu od opětovného doručení opravené či doplněné faktury Objednateli.

4.7. Faktura bude splatná do 30 dnů ode dne jejího doručení Objednateli. Za den úhrady se považuje den, kdy byla fakturovaná částka odepsána z účtu Objednatele ve prospěch účtu Zhotovitele.

4.8. Smluvní strany se dohodly, že nastane-li v souvislosti se Zhotovitelem jakákoliv skutečnost, v jejímž důsledku se může vůči Objednateli uplatnit ručení za daň odváděnou Zhotovitelem ve smyslu DPH, je Objednatel oprávněn nezaplatit Zhotoviteli vyúčtovanou DPH a odvést ji přímo správci daně a Objednatel je rovněž oprávněn odstoupit od této Smlouvy.

V. Součinnost smluvních stran

5.1. Smluvní strany sjednávají následující kontaktní osoby:

Za Objednatel 

Za Zhotovitele

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

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

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

5.5. Zhotovitel je podle ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, osobou povinnou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou zboží nebo služeb z veřejných výdajů. Zhotovitel je povinen při kontrole poskytnout na vyžádání kontrolnímu orgánu daňovou evidenci v plném rozsahu. Zhotovitel je rovněž povinen smluvně zajistit, aby totožným způsobem byli povinni spolupůsobit i všichni jeho Poddodavatelé.

5.6. Zhotovitel je povinen uchovávat veškerou dokumentaci související s realizací díla včetně účetních dokladů minimálně do konce roku 2035. Pokud je v českých právních předpisech stanovena lhůta delší, musí zhotovitel uvedenou dokumentaci uchovávat po dobu trvání takové lhůty.

Zhotovitel je povinen minimálně do konce roku 2035 poskytovat požadované informace a dokumentaci související s realizací díla zaměstnancům nebo zmocněncům pověřených orgánů (MF ČR, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout jim při provádění kontroly součinnost.

5.7. Zhotovitel je povinen všechny písemné zprávy, písemné výstupy a prezentace opatřit vizuální identitou projektů dle pravidel daných Výzvou, zejména dle Pravidel pro provádění informačních

a propagačních opatření. Zhotovitel prohlašuje, že ke dni nabytí účinnosti této Smlouvy je s těmito pravidly seznámen. V případě, že v průběhu plnění této Smlouvy dojde ke změně těchto pravidel, je Objednatel povinen o této skutečnosti Zhotovitele bezodkladně informovat.

VI. Prohlášení, práva a závazky Smluvních stran

6.1. Zhotovitel prohlašuje, že ke dni podpisu Smlouvy:

6.1.1. není jako právnická osoba v likvidaci;

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

6.1.3. uzavření/m této Smlouvy:

a. neporuší správní rozhodnutí orgánu státní správy České republiky;

b. neporuší ustanovení žádné dohody, smlouvy či jiného ujednání, které uzavřel se třetí osobou;

c. nebude mít za následek újmu nebo požadavek na splacení jakéhokoli správního poplatku, dotací nebo jiného závazku Zhotovitele;

d. neučinil nic, ať již sám anebo za spolupráce či prostřednictvím třetí osoby, co by omezilo či znemožnilo dosažení účelu této Smlouvy, a to v České republice, a pokud Zhotovitel má sídlo v jiné zemi než v České republice, tak i ve vztahu k zemi, v níž má sídlo.

6.2. Zhotovitel se zavazuje, že Objednateli bezodkladně po vzniku výše uvedené skutečnosti (viz odst. 6.1. této Smlouvy) písemně oznámí:

6.2.1. podání návrhu na prohlášení konkursu na majetek Zhotovitele dle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů; nebo

6.2.2. vstup Zhotovitele do likvidace; nebo

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

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

6.2.5. omezení či ukončení činnosti Zhotovitele, která bezprostředně souvisí s předmětem této Smlouvy; nebo

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

6.2.7. rozhodnutí o zrušení Zhotovitele.

Pokud Zhotovitel sídlí mimo ČR, bude postupovat podle právních předpisů země svého sídla přiměřeně.

6.3. Zhotovitel prohlašuje, že:

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

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

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

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

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

6.4. Zhotovitel se zavazuje:

6.4.1. při provádění předmětu díla postupovat s odbornou péčí a dodržovat právní předpisy a rozhodnutí orgánů veřejné správy,

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

6.5. Zhotovitel se zavazuje uhradit Objednateli do deseti dnů poté, kdy k tomu bude Objednatelem písemně vyzván, veškeré pokuty či další sankce, které byly Objednateli vyměřeny (pravomocným rozhodnutím) státními orgány v souvislosti s porušením povinností Zhotovitele stanovených touto Smlouvou či obecně závaznými právními předpisy při provádění předmětu díla. Úhrada bude provedena na účet Objednatele uvedený v záhlaví této Smlouvy.

6.6. Objednatel neudělil Zhotoviteli žádné oprávnění uzavírat pracovně právní či jiné vztahy jménem Objednatele nebo jednat jménem Objednatele. Současně smluvní strany dohodly, že každá osoba zaměstnaná nebo jinak využívaná Zhotovitelem při provádění předmětu díla bude placena výlučně Zhotovitelem.

Zhotovitel se zavazuje, že pokud pro plnění díla použije třetí osoby v jiném než pracovněprávním vztahu, tak s takovými osobami ošetří veškeré vztahy a zejména autorská práva tak, aby tyto třetí osoby nebyly oprávněny vznášet jakékoli nároky vůči Objednateli a aby nebyly oprávněny vystupovat samostatně vůči Objednateli. Zhotovitel je povinen na základě výzvy Objednatele předložit seznam osob, které se na plnění díla podílely, spolu se specifikací právního vztahu, na základě kterého tak činily, a současně prokázat splnění povinnosti podle předchozí věty. V případě, že Zhotovitel poruší povinnost stanovenou v první větě tohoto odstavce nebo tuto skutečnost na základě písemné výzvy Objednatele v přiměřené době nedoloží, zavazuje se zaplatit smluvní pokutu ve výši 10 000 Kč a uhradit veškeré škody, které v souvislosti s tímto porušením Objednateli vzniknou.

VII. Předání díla, přechod vlastnictví a nebezpečí škody

7.1. Zhotovitel se zavazuje realizovat předmět díla průběžně a předat výstupy z plnění předmětu díla v termínech definovaných harmonogramem v článku III. odst. 3.1. této Smlouvy.

7.2. O předání a převzetí bude sepsán písemný protokol dle čl. X. této Smlouvy podepsaný oprávněnými osobami obou Smluvních stran. V rámci předání díla je Zhotovitel povinen předvést, že dílo je způsobilé sloužit svému účelu a že je prosté jakýchkoliv vad.

7.3. Veškerá dokumentace (zejména uživatelská a technická dokumentace, koncepční materiály) bude Zhotovitelem Objednateli předávána v originálech, a to jak ve formě listinných dokumentů, tak v elektronické editovatelné podobě.

7.4. Objednatel nabývá právo užívat předmět plnění a přechází na něj nebezpečí škody k předmětu plnění okamžikem jeho předání Zhotovitelem, resp. převzetí na základě písemného protokolu podepsaného Objednatelem i Zhotovitelem

7.5. Po datu předání odpovídá Zhotovitel za ztrátu nebo škodu pouze v případě, že je tato ztráta nebo škoda způsobena zaviněním Zhotovitele nebo když má Zhotovitel předměty Dodávek v držení z důvodu poskytování záručního servisu.

VIII. Podmínky provádění předmětu díla

8.1. Zhotovitel se zavazuje:

8.1.1. zajistit provádění předmětu díla tak, aby provádění předmětu díla v co nejmenší míře omezovalo činnost Objednatele;

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

8.1.3. neprodleně, nejpozději však do tří (3) dnů, písemně oznámit Objednateli veškeré skutečnosti a okolnosti, které při poskytování Dodávek zjistil nebo se o nich dozvěděl a které mohou mít vliv na řádné poskytování Dodávek;

8.1.4. vyvstane-li v průběhu provádění předmětu díla nutnost upřesnění způsobu jeho provedení, neprodleně si vyžádat předchozí písemný souhlas či pokyn Objednatele;

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

8.1.6. vždy předkládat Objednateli návrhy veškerých písemných podkladů a dokumentů (např. protokolů, zápisů, Detailního cílového konceptu) souvisejících s plněním dle této Smlouvy, nestanovuje-li tato Smlouva či dohoda Smluvních stran jinak.

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

Zhotovitel prohlašuje, že zejména ve smyslu § 2914 NOZ odpovídá za veškeré škody, které způsobí osoby, které při plnění předmětu této smlouvy použije. Pro případ, že by Zhotovitel porušil svoji povinnost podle této Smlouvy, a pro plnění předmětu této Smlouvy použil pomocníka, jenž by jednal samostatně, přebírá ručení za jakoukoli škodu, kterou by tento pomocník způsobil.

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

Zhotovitel není oprávněn pověřit provedením předmětu díla ani jakékoli jeho části Subdodavatele bez předchozího písemného souhlasu Objednatele.

Zhotovitel je povinen:

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

b. v případě, že prokazoval splnění kvalifikačních předpokladů za pomoci Subdodavatelů, zajistit, aby příslušné plnění prováděli Subdodavatelé uvedeni v Nabídce,

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

d. předložit Objednateli doklady o odborné způsobilosti Poddodavatele před zahájením prací každým Poddodavatelem.

e. jednat se Poddodavateli v souladu se zásadami poctivého obchodního styku tzn. zejména uhradit Poddodavatelům sjednanou cenu za řádné a včasné poskytnutí příslušných částí Díla.

8.3. Zhotovitel se zavazuje ve lhůtách stanovených v Příloze č. 1 k této Smlouvě reagovat na nahlášené chyby funkčnosti či požadavky na servisní zásah a též zahajovat a ukončovat odstraňování uvedených chyb funkčnosti a uvedené servisní zásahy.

8.4. V případě zjištění závad či nedostatků musí být o těchto zjištěných skutečnostech sepsán zápis a stanoveny termíny jejich odstranění.

8.5. Objednatel je oprávněn:

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

8.5.2. pokud Zhotovitel nesplní jakoukoliv povinnost podle této Smlouvy a nesplní ji ani v dodatečné lhůtě stanovené Objednatelem, jež však nebude delší než čtyři dny, je Objednatel, aniž by tím byla dotčena jakákoliv jiná práva a nároky Objednatele dle této Smlouvy, oprávněn, nikoliv však povinen, podle svého uvážení splnit povinnost Zhotovitele nebo pověřit splněním této povinnosti jiné osoby na náklady Zhotovitele,

8.5.3. po Zhotoviteli požadovat, aby pro splnění Veřejné zakázky nevyužíval člena týmu Zhotovitele, který prokazatelně:

a. plní své povinnosti nekompetentně nebo nedbale, nebo

b. opakovaně neplní nebo porušuje některá ustanovení této Smlouvy nebo právních předpisů, přičemž takový člen týmu Zhotovitele musí být po výzvě Objednatele bez zbytečného odkladu nahrazen jiným členem s odpovídající kvalifikací

c. to vše, aniž by tím byla dotčena jakákoliv jiná práva a nároky Objednatele dle této Smlouvy, zejména plnění termínů daných touto smlouvou a vymáhání sankcí z ní vyplývajících.

8.6. Všichni pracovníci Zhotovitele, kteří se budou podílet na plnění předmětu této Smlouvy musí být dostatečně zkušení a odborně zdatní a musí umět pracovat se všemi již zapojenými prvky, podstatnými pro plnění této veřejné zakázky, stejně tak jako s prvky nově dodávanými v rámci této veřejné zakázky, tj. plnění dle této Smlouvy.

8.7. Pokud si Objednatel jako zadavatel v Zadávací dokumentaci Veřejné zakázky stanovil požadavky na vzdělání a odbornou kvalifikaci ve vztahu k fyzickým osobám, které se mají na plnění předmětu Smlouvy podílet, je Zhotovitel tyto uvedené osoby, kterými splnění podmínek Zadávací dokumentace prokázal, pro plnění předmětu této smlouvy také použít. Tyto fyzické osoby je možné měnit pouze se souhlasem Objednatele, přičemž fyzické osoby, které se budou na plnění předmětu smlouvy nově podílet, musí splňovat stejné kvalifikační předpoklady jako nahrazované fyzické osoby. Objednatel nebude udělení souhlasu bezdůvodně odpírat.

IX. Záruka za jakost

9.1. Zhotovitel se zavazuje, že předaný předmět díla bude prostý jakýchkoli vad a bude mít vlastnosti dle obecně závazných právních předpisů, této Smlouvy a Zadávací dokumentace a bude proveden v souladu s ověřenou technickou praxí. Zhotovitel poskytuje Objednateli záruku za jakost díla, a to v délce pro jednotlivé součásti specifikované v Příloze č. 1 k této smlouvě.

9.2. Zhotovitelem bude Objednateli poskytován bezplatný záruční servis na Objednatelem reklamované vady předmětu díla vzniklé v době trvání záruční doby určené v článku IX. odst. 9.1. této Smlouvy.

9.3. Objednatel je oprávněn reklamovat v záruční době dle článku IX. odst. 9.1. této Smlouvy vady předmětu díla u Zhotovitele, a to písemnou formou. V reklamaci musí být popsána vada předmětu díla, určen nárok Objednatele z vady předmětu díla, případně požadavek na způsob odstranění vad, a to včetně termínu pro odstranění vad Zhotovitelem; tento termín nebude kratší než lhůty stanovené v Příloze č. 1 k této Smlouvě pro reakce na nahlášené chyby funkčnosti či požadavky na servisní zásah a na zahájení a ukončení odstraňování uvedených chyb funkčnosti a uvedených servisních zásahů. Objednatel má právo volby způsobu odstranění důsledku vadného plnění.

9.4. Zhotovitel se zavazuje zahájit odstraňování vady předmětu díla či jeho části i tehdy, neuznává-li svou odpovědnost za vady či příčiny, které ji vyvolaly, a vady odstranit v technicky co nejkratší době, a současně zahájit reklamační řízení. O reklamačním řízení budou Objednatelem pořizovány písemné zápisy ve dvojím vyhotovení, z nichž jeden stejnopis obdrží každá ze Smluvních stran. Reklamační řízení musí být ukončeno do čtyřiceti osmi hodin po jeho zahájení. Bude-li

v reklamačním řízení po vzájemném jednání Smluvních stran vada uznána jako reklamační vada, bude odstranění vady předmětu díla či jeho části provedeno bezúplatně. Nebude-li v reklamačním řízení vada uznána jako reklamační vada, bude odstranění vady předmětu díla či jeho části provedeno úplatně, pokud odstranění vady nespadá pod podporu provozu Software.

9.5. Práva a povinnosti ze Zhotovitelem poskytnuté záruky vznikají okamžikem provedení a předání díla Objednateli a nezanikají ani odstoupením kterékoli ze Smluvních stran od Smlouvy.

X. Protokol o předání a převzetí předmětu díla

10.1. Zhotovitel se zavazuje předmět díla řádně provést a protokolárně předat Objednateli. O předání předmětu díla Zhotovitelem Objednateli bude sepsán písemný protokol. Dílo a jeho jednotlivé části se považují za řádně předané, pokud je plněno řádně, včas, bez vad, pokud byla Zhotovitelem předvedena způsobilost díla sloužit svému účelu a tyto skutečnosti jsou vyznačeny v předávacím protokolu.

Osobou oprávněnou k podpisu předávacího protokolu za Objednatele je [redacted]

Osobou oprávněnou k podpisu předávacího protokolu za Zhotovitele je [redacted]

10.2. Nejpozději na poslední den provedení předmětu díla, resp. jeho části, Zhotovitel svolá do místa předání a převzetí díla předávací řízení. Na předávací řízení přizve Zhotovitel Objednatele, a to písemným oznámením, které musí být doručeno Objednateli alespoň pět pracovních dnů předem včetně návrhu předávacího protokolu a případně další příslušné dokumentace. Objednatel do dvou pracovních dnů buď potvrdí navržený termín, nebo požádá o stanovení nového termínu; posunutím předávacího řízení na žádost Objednatele se Zhotovitel nemůže dostat do prodlení s plněním předmětu této Smlouvy. V případě, že nebude Objednateli řádně a včas doručena výzva k účasti na předávacím řízení, může dojít k předávacímu řízení nejdříve po uplynutí pátého pracovního dne ode dne doručení písemné výzvy k zahájení předávacího řízení.

10.3. K předání předmětu díla, resp. jeho části Zhotovitelem Objednateli dojde na základě předávacího řízení, a to formou písemného předávacího protokolu (jehož součástí budou příslušné výstupy i příslušná dokumentace, pokud je to stanoveno touto Smlouvou či obvyklé), který bude podepsán oprávněnými zástupci obou smluvních stran.

Předávací protokol musí obsahovat alespoň předmět a charakteristiku předmětu díla, soupis zjištěných vad předmětu díla stanovených Zhotovitelem či Objednatelem, vyjádření Zhotovitele k vadám předmětu díla vytčeným Objednatelem, lhůty pro odstranění vad předmětu díla, zhodnocení jakosti předmětu díla, dohodu o lhůtách a opatřeních k odstranění vad díla či jeho části, záznam o nutných dodatečně požadovaných pracích, případnou dohodu o slevě z ceny za provedení předmětu díla, stanovisko Objednatele, zda předmět díla přejímá či nikoli a soupis příloh. Předávací protokol bude vyhotoven ve třech stejnopisech, z nichž jeden obdrží Zhotovitel a dva Objednatel. Každý stejnopis bude podepsán oběma stranami a má právní sílu originálu.

10.4. V případě, že je Objednatelem přebírán dokončený předmět díla, skutečnost, že předmět díla je dokončen co do množství, jakosti, kompletnosti a schopnosti trvalého užívání, prokazuje zásadně Zhotovitel a za tím účelem předkládá nezbytné písemné doklady Objednateli. V případě, že nedojde k předložení a předání Objednateli shora uvedených dokladů nejpozději při předávacím řízení, nepovažuje se předmět díla za řádně předaný.

10.5. V případě, že se při přejímání předmětu díla Objednatelem prokáže, že je Zhotovitelem předáván předmět díla, který nese vady nebo není schopen sloužit svému účelu, není Objednatel povinen předávaný předmět díla převzít. Tato skutečnost bude uvedena v předávacím protokolu. Po odstranění vad předmětu díla či jeho části, pro které Objednatel odmítl od Zhotovitele předmět díla převzít, se opakuje předávací řízení analogicky dle tohoto článku Smlouvy. V takovém případě bude k původnímu předávacímu protokolu sepsán dodatek, ve kterém bude uvedeno převzetí předmětu díla. Dodatek obsahuje veškeré náležitosti stanovené pro předávací protokol v tomto článku Smlouvy.

10.6. Objednatel má právo ve lhůtě 10 dnů od předání díla či části díla vznést výhrady nebo připomínky k předávanému dílu či části díla; v takovém případě se Strany zavazují zahájit společné jednání za účelem odstranění veškerých vzájemných rozporů a nalezení shody nad předávaným dílem či

částí díla, a to nejpozději do pěti (5) pracovních dnů od výzvy kterékoliv Strany. V takovém případě se dílo či část díla nepovažují za převzaté se všemi důsledky z toho vyplývajícími a předávací řízení se v takovém případě zopakuje analogicky dle tohoto článku Smlouvy.

10.7. Vadou se pro účely této Smlouvy rozumí odchylka v kvantitě, kvalitě, rozsahu, termínech nebo parametrech díla stanovených touto Smlouvou, Zadávací dokumentací a obecně závaznými předpisy bránící využití díla k jeho účelu.

10.8. Zhotovitel je povinen odstranit vady předmětu díla, i když se za ně necítí odpovědný. Náklady na odstranění těchto vad nese Zhotovitel, a to až do účinnosti dohody Smluvních stran o jejich úhradě nebo do právní moci rozhodnutí příslušného soudu ve věci úhrady těchto nákladů, pokud není Smlouvou stanoveno jinak.

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

11.1. Smluvní strany se dohodly na tom, že v případě porušení termínu předání a převzetí dodaného a implementovaného Software podle ustanovení článku III. odst. 3.1. a v případě porušení článku IX. odst. 9.4. Smlouvy Zhotovitelem je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 1 000 Kč, kterou je Objednatel podle této smlouvy povinen Zhotoviteli uhradit, a to za každý započatý den prodlení.

11.2. Smluvní strany se dohodly, že v případě nepravdivosti prohlášení v ustanovení článku VI. odst. 6.1. nebo porušení některé povinnosti sjednané v článku V. této Smlouvy Zhotovitelem je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 1 000 Kč, a to za každé porušení Smlouvy zvlášť.

11.3. Smluvní strany se dohodly na tom, že v případě porušení ustanovení článku VIII. odst. 8.3. této Smlouvy Zhotovitelem je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši stanovené v Příloze č. 1 této Smlouvy.

11.4. V případě, kdy nastane situace uvedená v čl. 12.4.5. je Zhotovitel povinen zaplatit smluvní pokutu ve výši 100.000,- Kč (slovy: jedno sto tisíc korun českých), a to za každý jednotlivý případ. Oprávnění požadovat smluvní pokutu není podmíněno přistoupením Objednatele k výpovědi či odstoupení od Smlouvy. Úhradou smluvní pokuty není dotčen nárok Objednatele na náhradu škody.

11.5. Smluvní strany se dohodly na tom, že v případě prodlení s úhradou ceny dle ustanovení čl. IV této Smlouvy je Objednatel povinen uhradit Zhotoviteli úrok z prodlení ve 0,01 % (slovy: jedna setina procenta) z nezaplacené částky za každý započatý den prodlení.

11.6. Smluvní pokuta a úrok z prodlení jsou splatné do 21 dní ode dne, kdy byla povinné straně doručena písemná výzva k jejich zaplacení ze strany oprávněné strany, a to na účet oprávněné strany uvedený v písemné výzvě. Ustanovením o smluvní pokutě není dotčeno právo oprávněné strany na náhradu škody v plné výši s tím, že zaplacená smluvní pokuta se na úhradu škody nezapočítává. Případným odstoupení od Smlouvy nárok na úhradu smluvní pokuty a úroku z prodlení nezaniká.

11.7. V případě, že porušením povinnosti Zhotovitele podle této Smlouvy vznikne Objednateli škoda, jejímž důsledkem bude odejmutí dotace nebo její části poskytovatelem dotačního titulu, odpovídá dodavatel objednateli za škodu až do výše finančního postihu ze strany poskytovatele dotačního titulu uplatněného vůči objednateli.

11.8. Pro případ porušení povinností podle odst. 14.1. této smlouvy si Smluvní strany sjednávají smluvní pokutu ve výši 1.000,- Kč za každé jednotlivé porušení.

XII. Ukončení smlouvy

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

12.2. Odstoupení od smlouvy musí být provedeno písemnou formou a je účinné okamžikem jeho doručení druhé straně smluvního vztahu. Odstoupením od smlouvy se tato Smlouva od okamžiku doručení projevu vůle směřujícího k odstoupení od Smlouvy druhé smluvní straně ruší od počátku

s tím, že Objednatel má právo od smlouvy odstoupit ve smyslu § 2004 odst. 2 občanského zákoníku i částečně.

12.3. Výpovědí či odstoupením nejsou dotčena práva a povinnosti stran vzniklé před účinností ukončení Smlouvy.

12.4. Odstoupení od Smlouvy ze strany Objednatele – Objednatel je oprávněn odstoupit od této Smlouvy v těchto případech:

12.4.1. Zhotovitel poruší povinnost z této Smlouvy zvlášť závažným způsobem ve smyslu § 2002 odst. 1 OZ, a to zejména pro opakovaná neplnění parametrů servisních služeb podle Přílohy č. 1 Smlouvy v rámci podpory provozu, čímž se rozumí alespoň třikrát opakované neplnění parametrů servisních služeb v období 3 po sobě jdoucích měsíců,

12.4.2. jestliže se Zhotovitel dostane do prodlení s prováděním předmětu díla, ať již jako celku či jeho jednotlivých částí, ve vztahu k termínům provádění předmětu díla dle článku III. odst. 3.1. této Smlouvy, které bude delší než čtrnáct kalendářních dnů,

12.4.3. Zhotovitel porušil některou ze svých povinností uvedených v článku VIII. Smlouvy;

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

12.4.5. Zhotovitel poruší povinnost mlčenlivosti dle čl. XVII odst. 17.6. této Smlouvy,

12.4.6. Zhotovitel přestane být subjektem oprávněným poskytovat Dodávky dle této Smlouvy.

12.5. V případě částečného odstoupení od Smlouvy ze strany Objednatele ve smyslu § 2004 odst. 2 občanského zákoníku vzniká Objednateli vůči Zhotoviteli nárok na úhradu prokázaných vícenákladů (tj. nákladů vynaložených Objednatelem nad cenu za provedení předmětu díla) vynaložených na dokončení předmětu díla třetí osobou a na úhradu škod vzniklých prodlením se splněním předmětu díla. Povinnost Zhotovitele zaplatit smluvní pokuty, k jejichž úhradě vznikla povinnost před odstoupením, nezaniká.

12.6. Pokud Objednatel odstoupí od Smlouvy jen částečně, pak odstoupením od Smlouvy nebudou dotčena plnění Zhotovitele podle této Smlouvy převzatá Objednatelem před účinností odstoupení, na které odstoupení nedopadá, ani povinnost Objednatele uhradit Zhotoviteli část ceny připadající na taková plnění. Objednatel si ponechá taková plnění Zhotovitele a Zhotovitel si ponechá část ceny připadající na tato plnění.

12.7. Výpověď Smlouvy ze strany Objednatele – jestliže Zhotovitel poruší některou povinnost podle Smlouvy, může Objednatel oznámením vyzvat Zhotovitele, aby toto porušení napravil v přiměřené lhůtě stanovené jednoznačně Objednatelem s tím, že taková lhůta nesmí být kratší než patnáct (15) dnů. Objednatel je oprávněn Smlouvu vypovědět s výpovědní lhůtou šest měsíců, jež počíná běžet prvního dne měsíce následujícího po měsíci, ve kterém byla výpověď doručena Zhotoviteli, pokud Zhotovitel poruší povinnost z této Smlouvy jiným než zvlášť závažným způsobem definovaným v odstavci 12.4 písm. a) a neprovede nápravu takového porušení povinností ani v dodatečné lhůtě stanovené Objednatelem, která nebude kratší než 15 dnů.

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

12.9. Výpověď Smlouvy ze strany Zhotovitele – Zhotovitel je oprávněn tuto Smlouvu vypovědět s výpovědní lhůtou šesti (6) měsíců, jež počíná běžet prvního dne měsíce následujícího po měsíci, ve kterém byla výpověď doručena Objednateli, pokud je Objednatel v prodlení s platbou Zhotoviteli podle čl. IV této Smlouvy po dobu delší než šedesát (60) dnů od data splatnosti.

XIII. Adresy pro doručování

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

13.1.1. adresa pro doručování Objednateli je: Hybešova 982/53, 680 01 Boskovice.

13.1.2. adresa pro doručování Zhotoviteli je: Sochorova 23, 616 00 Brno.

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

XIV. Doručování

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

14.2. Aniž by tím byly dotčeny další prostředky, kterými lze prokázat doručení, má se za to, že písemnost byla řádně doručená:

14.2.1. při doručování do datové schránky:

a. okamžikem přihlášení oprávněné osoby do datové schránky,

b. pro případ, že se do datové schránky oprávněná osoba nepřihlásí ani čtvrtý pracovní den od dodání zprávy do datové schránky, platí, že zásilka je doručena pátým pracovním dnem od odeslání analogicky podle § 570 odst. 1 občanského zákoníku (zmaření doručení).

14.2.2. při doručování prostřednictvím držitele poštovní licence:

a. se má za to, že došlá zásilka odeslaná s využitím provozovatele poštovních služeb došla třetí pracovní den po odeslání, byla-li však odeslána na adresu v jiném státu, pak patnáctý pracovní den po odeslání, a to doručování na adresy pro doručování dle článku XIII. odst. 13.1., resp. 13.2. této Smlouvy.

14.2.3. při doručování osobně:

a. dnem faktického přijetí písemnosti příjemcem; nebo

b. dnem, v němž bylo doručeno osobě na příjemcově adrese určené k přebírání listovních zásilek; nebo

c. dnem, kdy bylo doručováno osobě na příjemcově adrese určené k přebírání listovních zásilek, a tato osoba odmítla listovní zásilku převzít; nebo

d. dnem, kdy příjemce při prvním pokusu o doručení zásilku z jakýchkoli důvodů nepřevzal či odmítl zásilku převzít, a to i přesto, že se v místě doručení nezdržuje, pokud byla na zásilce uvedena adresa pro doručování dle článku XIII. odst. 13.1., resp. 13.2. této Smlouvy.

XV. Společná ustanovení

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

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

15.2. Smluvní strany se zavazují:

15.2.1. vzájemně se včas a řádně informovat o všech podstatných skutečnostech, které mohou mít vliv na plnění dle této Smlouvy,

15.2.2. vyvinout potřebnou součinnost k plnění této Smlouvy.

15.3. Pokud kterékoliv ustanovení této Smlouvy nebo jeho část bude neplatné či nevynutitelné anebo se stane neplatným či nevynutitelným nebo bude shledáno neplatným či nevynutitelným soudem

či jiným příslušným orgánem, pak tato neplatnost či nevynutitelnost nebude mít vliv na platnost či vynutitelnost ostatních ustanovení Smlouvy nebo jejich částí.

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

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

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

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

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

XVI. Autorské právo a ochrana duševního vlastnictví

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

16.2. Zhotovitel se touto Smlouvou zavazuje poskytnout Objednateli oprávnění (licenci) k výkonu práva užít Software jedním z následujících způsobů dle písm. a) nebo dle písm. b) (v souladu s požadavky Přílohy 1 Zadávací dokumentace.

Zhotovitel poskytuje dle této Smlouvy Objednateli uživatelskou licenci k Software jako nevýhradní, nepřenositelné právo užívání Software s množstevním rozsahem uživatelských licencí dle Přílohy č.1 k této Smlouvě.

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

16.4. Objednatel nabývá práva užívat předmět licence okamžikem předání té části díla, jejíž součástí příslušné programové produkty jsou. Objednatel není povinen licenci k software využít.

16.5. Pokud Zhotovitel v průběhu plnění předmětu Smlouvy nahradí programové produkty podle odst. 16.2 novějšími, zavazuje se poskytnout Objednateli oprávnění k výkonu práva užít tyto nové programové produkty za stejných nebo výhodnějších podmínek ve vztahu k původnímu oprávnění.

16.6. V případě, že třetí strana uplatní nárok z důvodu porušení patentu nebo autorského práva produktem, jenž Zhotovitel dodal Objednateli, bude Zhotovitel hájit Objednatele před takovým nárokem na své náklady. Zhotovitel uhradí veškeré náklady, škody nebo poplatky uložené soudem nebo vynaložené Objednatelem na základě uzavřeného smíru nebo dohody o narovnání. Toto ustanovení se uplatní pouze za předpokladu, že Objednatel neporušil licenční podmínky stanovené touto Smlouvou.

XVII. Ochrana informací

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

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

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

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

17.3. Za třetí osoby se nepovažují:

17.3.1. zaměstnanci Stran a osoby v obdobném postavení,

17.3.2. orgány Stran a jejich členové a

17.3.3. Poddodavatelé Zhotovitele,

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

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

17.5. Smluvní strany se výslovně dohodly, že za důvěrné informace nejsou považovány informace poskytnuté v rámci veřejné zakázky tzn., Zadávací dokumentace, Nabídka Zhotovitele, smluvní dokumentace jakož i informace a dokumentace předané Zhotovitelem v rámci realizace předmětu plnění. Smluvní strany prohlašují, že skutečnosti uvedené v této Smlouvě nepovažují za obchodní tajemství ve smyslu § 504 zákona 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů a tímto výslovně souhlasí se zveřejněním veškerých náležitostí a podmínek této smlouvy a/nebo souvisejících dokumentů a informací, včetně zveřejnění této smlouvy jako celku, v rámci informací zpřístupňovaných veřejnosti bez stanovení jakýchkoli dalších podmínek, a to i prostřednictvím dálkového přístupu, zejména na webových stránkách Objednatele. V případě utajovaných příloh (například podléhající obchodnímu tajemství) Zhotovitel při podpisu Smlouvy předal Objednateli verzi strany nebo přílohy, která zůstane neveřejná – z této listiny musí být patrný alespoň obsah tohoto dokumentu.

17.6. Strany se zavazují v plném rozsahu zachovávat povinnost mlčenlivosti a povinnost chránit Důvěrné informace způsobem vyplývajícím ze Smlouvy a též z příslušných právních předpisů, zejména povinností vyplývajících z 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). Strany se v této souvislosti zavazují poučit veškeré osoby, které se budou podílet na plnění Smlouvy, o výše uvedených povinnostech mlčenlivosti a ochrany Důvěrných informací a dále se zavazují vhodným způsobem zajistit dodržování těchto povinností všemi osobami podílejícími se na plnění Smlouvy.

17.7. Budou-li informace poskytnuté Objednatelem či třetími stranami, které jsou nezbytné pro plnění Smlouvy, obsahovat data podléhající režimu zvláštní ochrany podle 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), zavazuje se Zhotovitel zabezpečit splnění všech povinností, které citované nařízení vyžaduje po zpracovateli osobních údajů, a v případě, že v rámci plnění povinností dle této Smlouvy je Zhotovitel povinen údaje od subjektů údajů též získat, pak je povinen obstarat platný právní titul ke zpracování osobních údajů předaných ke zpracování.

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

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

17.9.1. se staly veřejně známými, aniž by to zavinila záměrně či opominutím přijímající strana,

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

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

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

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

17.11. Zhotovitel bere na vědomí, že Objednatel v software dodaném na základě této Smlouvy bude zpracovávat osobní údaje. Software musí respektovat Nařízení EU a právní předpisy České republiky s ochranou osobních údajů související, zejména

17.11.1. Nařízení (EU) 2016/679 Obecné nařízení na ochranu osobních údajů neboli GDPR (General Data Protection Regulation) a

17.11.2. Nařízení Evropské unie č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu EIDAS

a prohlašuje, že dodaný software odpovídá těmto a dalším předpisům týkajících se ochrany osobních údajů.

XVIII. Závěrečná ustanovení

18.1. Práva a povinnosti z této Smlouvy vyplývající a ve Smlouvě neupravené se řídí příslušnými ustanoveními zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, a s obsahem smlouvy souvisejícími předpisy. Pokud by bylo jedno z výše uvedených ustanovení zcela nebo zčásti právně neúčinné, zůstává tím nedotčena právní účinnost ostatních ustanovení. Totéž platí i pro případ smluvní mezery.

18.2. Pokud jakýkoliv závazek vyplývající z této Smlouvy, avšak netvořící její podstatnou náležitost a současně plně oddělitelný od ostatních ustanovení této Smlouvy, je nebo se stane neplatným nebo nevymahatelným jako celek nebo jeho část, taková neplatnost nebo nevymahatelnost nebude mít žádný vliv na platnost a vymahatelnost jakýchkoliv ostatních závazků z této Smlouvy. Strany se zavazují v rámci této Smlouvy nahradit formou dodatku k této Smlouvě tento neplatný nebo nevymahatelný oddělený závazek takovým novým platným a vymahatelným závazkem, jehož předmět bude v nejvyšší možné míře odpovídat předmětu původního odděleného závazku. Pokud však jakýkoliv závazek vyplývající z této Smlouvy a tvořící její podstatnou náležitost je nebo kdykoliv se stane neplatným nebo nevymahatelným jako celek nebo jeho část, Strany nahradí neplatný nebo nevymahatelný závazek formou dodatku k této Smlouvě takovým novým platným a vymahatelným závazkem, jehož předmět bude v nejvyšší možné míře odpovídat předmětu původního závazku obsaženému v této Smlouvě. Totéž platí i pro případ smluvní mezery.

18.3. Strany tímto prohlašují, že si nejsou vědomy, že by kterákoliv Strana při sjednávání této Smlouvy zneužila svou kvalitu odborníka či své hospodářské postavení, přičemž Strany prohlašují, že vzájemná práva a povinnosti sjednané v této Smlouvě považují za rovnovážná.

18.4. Zhotovitel je povinen umožnit Řídícímu orgánu z dotačního titulu přístup i k těm částem nabídek, smluv a souvisejících dokumentů, které podléhají ochraně podle zvláštních právních předpisů (např. jako obchodní tajemství, utajované skutečnosti).

18.5. Zhotovitel se dále zavazuje, že po splnění Dodávek dle této Smlouvy poskytne Objednateli součinnost, aby Objednatel mohl dostát svým povinnostem dle zákona 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, zejména mu na jeho žádost poskytne seznam poddodavatelů (subdodavatelů) podílejících se na plnění.

18.6. Práva vzniklá z této Smlouvy nesmí být postoupena bez předchozího písemného souhlasu druhé Smluvní strany.

18.7. Tato Smlouva může být měněna nebo doplňována pouze písemnými oboustranně odsouhlasenými, a průběžně číslovanými dodatky, podepsanými oprávněnými zástupci obou Smluvních stran, které musí být obsaženy na jedné listině. Žádné úkony či jednání ze strany jedné Smluvní strany nelze považovat za příslib uzavření smlouvy nebo dodatku k této Smlouvě. V souladu s ustanovením § 1740 odstavce 3 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, Smluvní strany nepřipouští přijetí návrhu na uzavření smlouvy s dodatkem nebo odchylkou. Smluvní strany se dále dohodly, že možnost zhojení nedostatku písemné formy právního jednání se vylučuje, a že neplatnost právního jednání, pro nějž si Smluvní strany sjednaly písemnou formu, lze namítnout kdykoliv, tedy že mezi Smluvními stranami neplatí ustanovení § 582 odstavce 1 první věta a odstavce 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

18.8. Smluvní strany berou na vědomí, že text Smlouvy je veřejně přístupnou listinou ve smyslu zákona č. 106/1999 Sb. o svobodném přístupu k informacím, ve znění pozdějších předpisů, a že Objednatel jako povinný subjekt má povinnost na žádost poskytnout informace o tomto smluvním vztahu včetně poskytnutí kopie Smlouvy. Při poskytnutí informace bude postupováno v souladu s Nařízením 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) a výše uvedeným zákonem o svobodném přístupu k informacím.

18.9. Nedílnou a neoddělitelnou součástí této smlouvy jsou její přílohy:

Příloha č. 1: Specifikace předmětu smlouvy

Příloha č. 2: Položkový rozpočet

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

- Zadávací dokumentace
- Nabídka Zhotovitele
- očíslované články této Smlouvy
- ostatní přílohy Smlouvy.

18.10. Tato Smlouva obsahuje úplné ujednání o předmětu Smlouvy a všech náležitostech, které Strany měly a chtěly ve Smlouvě ujednat, a které považují za důležité pro závaznost této Smlouvy. Žádný projev Stran učiněný při jednání o této Smlouvě ani projev učiněný po uzavření této Smlouvy nesmí být vykládán v rozporu s výslovnými ustanoveními této Smlouvy a nezakládá žádný závazek žádné ze Stran.

18.11. Tato Smlouva je vyhotovena v jednom elektronickém originálu, přičemž každá smluvní strana obdrží elektronický originál.

18.12. Tato smlouva nabývá platnosti dnem podpisu oběma smluvní stranami a účinnosti dnem uveřejnění v Registru smluv. Osobou povinnou k uveřejnění v Registru smluv je objednatel.

18.13. Strany po přečtení této Smlouvy prohlašují, že souhlasí s jejím obsahem, což potvrzují svými podpisy.

V Boskovicích dne dle elektronického podpisu

Za Objednatele

Mgr. Josef Sychra, ředitel

V Brně dne dle elektronického podpisu

Za Zhotovitele

Petr Konečný, ředitel RC, na základě plné moci

Kybernetická bezpečnost
– Vyšší odborná škola a střední škola Boskovice, příspěvková organizace

TECHNICKÁ SPECIFIKACE

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 v databázi výrobce uvedeny jako prodaná kupujícímu,
(f) jsou určeny pro provoz v České republice.

Tyto skutečnosti dodavatel doloží potvrzením výrobce daného zařízení, nebo čestným prohlášením distributora, popř. dodavatelovým samotným, nelze-li prohlášení distributora získat.

Zadavatel si vyhrazuje právo na ověření všech dodaných informací od výrobce daného zařízení a zjištění původu výrobků před podpisem smlouvy a 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 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**
    - **BACK UP - časové zámky**
    - **Diskové pole**
5) **nástroj pro ověřování identity uživatelů**

1) nástroj pro ochranu integrity komunikačních sítí

FIREWALL – 1KS

Parametr	Minimální požadavek
Výrobce a model	**FORTINET, FIREWALL FortiGate 120G + Licence, Unified Threat Protection + FortiCare Premium - záruka 36měsíců 24x7**
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)

Systém pro ukládání a korelaci logů – 1KS

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

2) nástroj pro ochranu koncových stanic

Ochrana koncových stanic a SVR – 150KS

Parametr	Minimální požadavek
Výrobce a model	**150x 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 kservice • ledge 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.

3) nástroje pro ochranu integrity komunikačních sítí

INFRASTRUKTURA – core SWITCH – 1KS

Parametr	Minimální požadavek
Výrobce a model	**Aruba 6300M 24SFP+ 4SFP56 Swch + 2x Aruba X371 12VDC 250W PS – záruka 5let**
Základní vlastnosti	• Třída zařízení: L3 switch • Formát zařízení do racku • Velikost zařízení: 1U • Počet 1/10 GE portů s volitelným fyzickým rozhraním: • Počet optických 10/25/50GE portů s volitelným fyzickým rozhraním: 4 • 2x Interní AC hot-swap napájecí zdroje • Redundatní vyměnitelné ventilátory – hot swap • Celková přepínací propustnost přepínače 880 Gbit/s • Celkový paketový výkon přepínače 600 Mpps • Minimální paketový buffer: 8MB • Maximální hloubka přepínače: 39 cm
Vlastnosti stohování	• Podporovaný počet přepínačů ve stohu: 10 • Kapacita stohovacího propojení: 200 Gbps • Stoh podporuje distribuované přepínaní paketů • Redundance řídícího prvku v rámci stohu • Jednotná konfigurace stohu (IP adresa, správa, konfigurační soubor) • Seskupení portů IEEE 802.3ad mezi různými prvky stohu (Multichassis LAG) • Stoh funguje jako jedno L3 zařízení (router, gateway, peer) včetně podpory dynamických směrovacích protokolů jako je OSPF • Součástí každého přepínače je stohovací 50GE kabel s minimání délkou 1m
Základní funkce a protokoly	• Podpora "jumbo rámců" včetně velikosti 9198 Byte • Podpora linkové agregace IEEE 802.1AX • Konfigurovatelné rozkládání LACP zátěže podle L2,L3 • Počet LACP skupin/linek ve skupině: 256/8 • Minimální počet záznamů v tabulce MAC adres: 32 000 • Minimální počet záznamů v tabulce ARP: 45 000 • Protokol pro definici šířených VLAN: MVRP • Podpora VLAN podle IEEE 802.1Q, minimálně 4000 aktivních VLAN • VLAN translace - swap 802.1Q tagů na trunk portu • Podpora zařazování do VLAN podle standardu 802.1v • IEEE 802.1s - Multiple Spanning Tree • STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+) • Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED • Detekce jednosměrnosti optické linky (např. UDLD) • DHCP server • DHCP relay pro IPv4 a IPv6 • Podpora NTPv4 pro IPv4 a IPv6 včetně VRF a MD5 autentizace • Statické směrování IPv4 a IPv6 • Minimální počet záznamů ve směrovací tabulce: 61 000 • Dynamické směrování OSPFv2, OSPFv3 a BGP včetně podpory BFD • Podpora BGP a MP-BGP včetně podpory BFD • Podpora směrovacího protokolu RIP a RIPng • Podpora Layer-3 routed port • IGMP v2 a v3 • MLD v1 a v2 • Podpora protokolu ERPS • Hardware podpora IPv4 a IPv6 ACL • ACL definice na základě skupiny fyzických portů • ACL aplikovatelný na interface, LAG, VLAN

	• BPDU a Root guard • Podpora uživatelských rolí definovaných lokálně v přepínači, jejich aplikace na základě výsledku autorizace • Podpora uživatelských rolí dynamicky stahovatelných z RADIUS serveru, jejich aplikace na základě výsledku autorizace • Podpora IPv6 RA Guard • IP source guard / dynamic IP lockdown • Podpora Dynamic ARP protection • Port security • Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU • Podpora IPv4 a IPv6 QoS • IEEE 802.1p - minimální počet front: 8 • DHCP snooping pro IPv4 a IPv6 • HW ochrana proti zahlcení portu (broadcast/multicast/icmp) nastavitelná na kbps a pps • 802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port • Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou) • Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675 • Podpora Critical VLAN • Podpora uživatelských rolí definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely.
SDN funkce	• Podpora service insertion včetně technologie VXLAN • Podpora BGP EVPN s využitím VXLAN • Podpora tunelování uživatelského provozu pomocí L2 GRE tunelů - schopnost izololovat více koncových zařízení na jednom portu do unikátních tunelů • Přiřazení koncového zařízení do tunelu na základě výsledku autorizace
Analytické a automatizační nástroje	• Podpora REST API pro automatizaci nastavení sítě. • Podpora skriptování v jazyce Python – lokální interpret jazyka v přepínači • Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní) • Interpretace uživatelských skriptů monitorujících definované parametry síťového provozu s možností automatické reakce na události • Grafické rozhraní pro vynášení výsledků monitorování a analytických skriptů. Možnost vynášení stavu monitorovaných metrik do grafů atp. • Root cause analysis v grafickém rozhraní – možnost vrácení se ke konkrétní funkční konfiguraci a stavu protokolů v čase. • Interní uložiště dat pro sběr provozních dat a pokročilou dignostiku zařízení • Kapacita interního úložiště dat pro analytické účely minimálně 30 GB
Management	• USB-C konzolový port • 1xRJ45 OoB management port s podporou ethernetu • Podpora minimálně 64 virtuálních směrovacích instancí (VRF) • Konfigurace zařízení v člověku čitelné textové formě • Podpora automatických i manuálních snapshotů konfigurace systému • USB port pro diagnostiku, přenos konfigurace a firmware • Přímé bezdrátové připojení ke konzoli zařízení skrze bluetooth • Podpora managementu přes IPv4 i IPv6 • SSHv2 a HTTPS pro IPv4 a IPv6 • Podpora SNMPv2c a SNMPv3 • RMON • Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL • Lokálně vynucené RBAC na úrovni přepínače • Dualní flash image • Podpora UDP, TCP a TLS SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů • Podpora RADIUS včetně RADIUS CoA (RFC3576) • Podpora Secure RADIUS (RadSec) • Podpora standardního Linux Shellu (BASH) pro debugging a skriptování • Podpora TACACS+

	• Analýza síťového provozu sFlow podle RFC 3176 • Ochrana proti nahrání modifikovaného SW do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu OS zařízení prostřednictvím TPM chipu • Port mirroring, alespoň 4 různé obousměrné session: SPAN, ERSPAN • Podpora IP SLA pro měření zpoždění provozu VoIP • Podpora Zero Touch Provisioning (ZTP)
Ostatní podmínky:	• Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství). • Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů. • Je požadována záruka na hardware s výměnou NBD v délce 60 měsíců. Tato záruka musí být garantovaná výrobcem zařízení.

aktivní prvky – POE 48port – 11KS

Parametr	Minimální požadavek
Výrobce a model	**Aruba 6100 48G CL4 4SFP+ Swch PN: JL675A/ záruka 5let**
Základní vlastnosti	• Třída zařízení: L3 switch • Formát zařízení do racku • Velikost zařízení: 1U • Počet 10/100/1000Mbit metalických portů : 48×RJ 45 • Počet 10Gbit/s SFP+ nezávislých optických portů s volitelným fyzickým rozhraním : 4×SFP+ • 10GE interface zpětně kompatibilní s 1Gbit/s transceivery • Všechny ethernet porty jsou dostupné zepředu • Interní napájecí zdroj • Podpora PoE+ dle standardu 802.3at • Dostupný výkon pro PoE+ napájení : 370 W • Podpora Energy Efficient Ethernet (802.3az) • Celková propustnost přepínače 176 Gb/s • Celkový paketový výkon přepínače 95 mpps • Minimálně 12MB paketový buffer • Maximální přípustná hloubka přepínače max. 31cm
Základní funkce a protokoly	• Podpora "jumbo rámců" včetně velikosti 9100 Byte • Podpora linkové agregace IEEE 802.3ad • Konfigurovatelné rozkládání LACP zátěže podle L3 a L4 • Minimální počet LACP skupin/linek ve skupině: 8/8 • Protokol pro definici šířených VLAN: MVRP • Podpora VLAN podle IEEE 802.1Q, minimálně 512 aktivních VLAN • IEEE 802.1s - Multiple Spanning Tree • STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+) • Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED • Detekce jednosměrnosti optické linky (např. UDLD) • NTP pro IPv4 a IPv6 včetně MD5 autentizace • Statické směrování IPv4 a IPv6 • IGMP v2 a v3 • MLD v1 a v2 • Hardware podpora IPv4 a IPv6 ACL • ACL definice na základě skupiny fyzických portů • ACL aplikovatelný na rozhraní IN včetně virtuálních VLAN • BPDU guard a Root guard

	• HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na množství paketů za vteřinu • ICMPv4 a ICMPv6 rate-limiting per port • Ověřování 802.1X včetně více uživatelů na port, minimálně 32 uživatelů/port • Konfiguovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou) • 802.1X s podporou odlišných Preauth VLAN, Fail VLAN a Critical VLAN • Dynamické zařazování do VLAN • 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení) • Port security - omezení počtu MAC adres na port, statické MAC • Ochrana proti opakovaným výpadkům linek (flapování) s možností konfigurace citlivosti a akce při překročení • Ochrana control plane (CPU) před útoky typu DoS • Podpora IPv4 a IPv6 QoS • Minimálně 8 front pro IEEE 802.1p
Management	• CLI formou 1x USB-C Console Port • Konfigurace zařízení v člověku čitelné textové formě • Podpora automatických i manuálních snapshotů konfigurace systému • USB port pro diagnostiku, přenos konfigurace a firmware • Podpora managementu přes IPv4 i IPv6 • SSHv2 a a SFTP • Podpora SNMPv2c a SNMPv3 • RMON • Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL • Lokálně vynucené RBAC na úrovni přepínače • Dualní flash image • TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů • Podpora Syslog over TLS • Podpora RADIUS včetně RADIUS CoA (RFC3576) • Podpora RADIUS IPSEC • Aktivní monitoring dostupnosti RADIUS přednastaveným jménem a heslem • Podpora TACACS+ • Analýza síťového provozu sFlow podle RFC 3176 • Port mirroring (SPAN), alespoň 4 různé obousměrné session • Podpora Zero Touch Provisioning (ZTP) • REST API pro automatizaci nastavení • Automatická konfigurace portu podle připojeného zařízení • Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů
Ostatní podmínky:	• Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství). • Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů. • Je požadována záruka na hardware s výměnou NBD v délce 60 měsíců. Tato záruka musí být garantovaná výrobcem zařízení.

aktivní prvky – POE 24port – 8KS + 28KS MINIGBIC

Parametr	Minimální požadavek
Výrobce a model	**Aruba 6100 24G CL4 4SFP+ Swch PN: JL677A/ záruka 5let + X132 10G SFP+ LC LR Transceiver**
Základní vlastnosti	• Třída zařízení: L3 switch • Formát zařízení do racku • Velikost zařízení: 1U • Počet 10/100/1000Mbit metalických portů : 24×RJ 45 • Počet 10Gbit/s SFP+ nezávislých optických portů s volitelným fyzickým rozhraním : 4×SFP+ • 10GE interface zpětně kompatibilní s 1Gbit/s transceivery • Všechny ethernet porty jsou dostupné zepředu • Interní napájecí zdroj • Podpora PoE+ dle standardu 802.3at • Dostupný výkon pro PoE+ napájení : 370 W • Podpora Energy Efficient Ethernet (802.3az) • Celková propustnost přepínače 120 Gb/s • Celkový paketový výkon přepínače 95 mpps • Maximální přípustná hloubka přepínače max. 31cm
Základní funkce a protokoly	• Podpora "jumbo rámců" včetně velikosti 9220 Byte • Podpora linkové agregace IEEE 802.3ad • Konfigurovatelné rozkládání LACP zátěže podle L3 a L4 • Minimální počet LACP skupin/linek ve skupině: 8/8 • Protokol pro definici šířených VLAN: MVRP • Podpora VLAN podle IEEE 802.1Q, minimálně 512 aktivních VLAN • IEEE 802.1s - Multiple Spanning Tree • STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+) • Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED • Detekce jednosměrnosti optické linky (např. UDLD) • NTP pro IPv4 a IPv6 včetně MD5 autentizace • Statické směrování IPv4 a IPv6 • IGMP v2 a v3 • MLD v1 a v2 • Hardware podpora IPv4 a IPv6 ACL • ACL definice na základě skupiny fyzických portů • ACL aplikovatelný na rozhraní IN včetně virtuálních VLAN • BPDU guard a Root guard • HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na množství paketů za vteřinu • ICMPv4 a ICMPv6 rate-limiting per port • Ověřování 802.1X včetně více uživatelů na port, minimálně 32 uživatelů/port • Konfiguovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou) • 802.1X s podporou odlišných Preauth VLAN, Fail VLAN a Critical VLAN • Dynamické zařazování do VLAN • 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení) • Port security - omezení počtu MAC adres na port, statické MAC • Ochrana proti opakovaným výpadkům linek (flapování) s možností konfigurace citlivosti a akce při překročení • Ochrana control plane (CPU) před útoky typu DoS • Podpora IPv4 a IPv6 QoS • Minimálně 8 front pro IEEE 802.1p
Management	• CLI formou 1x USB-C Console Port • Konfigurace zařízení v člověku čitelné textové formě • Podpora automatických i manuálních snapshotů konfigurace systému • USB port pro diagnostiku, přenos konfigurace a firmware • Podpora managementu přes IPv4 i IPv6 • SSHv2 a a SFTP

	• Podpora SNMPv2c a SNMPv3 • RMON • Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL • Lokálně vynucené RBAC na úrovni přepínače • Dualní flash image • TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů • Podpora Syslog over TLS • Podpora RADIUS včetně RADIUS CoA (RFC3576) • Podpora RADIUS IPSEC • Aktivní monitoring dostupnosti RADIUS přednastaveným jménem a heslem • Podpora TACACS+ • Analýza síťového provozu sFlow podle RFC 3176 • Port mirroring (SPAN), alespoň 4 různé obousměrné session • Podpora Zero Touch Provisioning (ZTP) • REST API pro automatizaci nastavení • Automatická konfigurace portu podle připojeného zařízení • Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů
MINIGBIC – 28KS	• 10G SFP+ Transceiver SM
Ostatní podmínky:	• Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství). • Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů. • Je požadována záruka na hardware s výměnou NBD v délce 60 měsíců. Tato záruka musí být garantovaná výrobcem zařízení.

aktivní prvky – 24port – 11KS

Parametr	Minimální požadavek
Výrobce a model	**Aruba 6100 24G 4SFP+ Swch PN: JL678A / záruka 5let + X132 10G SFP+ LC LR Transceiver**
Základní vlastnosti	• Třída zařízení: L3 switch • Formát zařízení do racku • Velikost zařízení: 1U • Počet 10/100/1000Mbit metalických portů : 24×RJ 45 • Počet 10Gbit/s SFP+ nezávislých optických portů s volitelným fyzickým rozhraním : 4×SFP+ • 10GE interface zpětně kompatibilní s 1Gbit/s transceivery • Všechny ethernet porty jsou dostupné zepředu • Interní napájecí zdroj • Celková propustnost přepínače 120 Gb/s • Celkový paketový výkon přepínače 95 mpps • Maximální přípustná hloubka přepínače max. 22cm
Základní funkce a protokoly	• Podpora "jumbo rámců" včetně velikosti 9220 Byte • Podpora linkové agregace IEEE 802.3ad • Konfigurovatelné rozkládání LACP zátěže podle L3 a L4 • Minimální počet LACP skupin/linek ve skupině: 8/8 • Protokol pro definici šířených VLAN: MVRP • Podpora VLAN podle IEEE 802.1Q, minimálně 512 aktivních VLAN • IEEE 802.1s - Multiple Spanning Tree • STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+) • Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED • Detekce jednosměrnosti optické linky (např. UDLD) • NTP pro IPv4 a IPv6 včetně MD5 autentizace • Statické směrování IPv4 a IPv6 • IGMP v2 a v3 • MLD v1 a v2

	• Hardware podpora IPv4 a IPv6 ACL • ACL definice na základě skupiny fyzických portů • ACL aplikovatelný na rozhraní IN včetně virtuálních VLAN • BPDU guard a Root guard • HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na množství paketů za vteřinu • ICMPv4 a ICMPv6 rate-limiting per port • Ověřování 802.1X včetně více uživatelů na port, minimálně 32 uživatelů/port • Konfiguovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou) • 802.1X s podporou odlišných Preauth VLAN, Fail VLAN a Critical VLAN • Dynamické zařazování do VLAN • 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení) • Port security - omezení počtu MAC adres na port, statické MAC • Ochrana proti opakovaným výpadkům linek (flapování) s možností konfigurace citlivosti a akce při překročení • Ochrana control plane (CPU) před útoky typu DoS • Podpora IPv4 a IPv6 QoS • Minimálně 8 front pro IEEE 802.1p
Management	• CLI formou 1x USB-C Console Port • Konfigurace zařízení v člověku čitelné textové formě • Podpora automatických i manuálních snapshotů konfigurace systému • USB port pro diagnostiku, přenos konfigurace a firmware • Podpora managementu přes IPv4 i IPv6 • SSHv2 a a SFTP • Podpora SNMPv2c a SNMPv3 • RMON • Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL • Lokálně vynucené RBAC na úrovni přepínače • Dualní flash image • TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů • Podpora Syslog over TLS • Podpora RADIUS včetně RADIUS CoA (RFC3576) • Podpora RADIUS IPSEC • Aktivní monitoring dostupnosti RADIUS přednastaveným jménem a heslem • Podpora TACACS+ • Analýza síťového provozu sFlow podle RFC 3176 • Port mirroring (SPAN), alespoň 4 různé obousměrné session • Podpora Zero Touch Provisioning (ZTP) • REST API pro automatizaci nastavení • Automatická konfigurace portu podle připojeného zařízení • Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů
Ostatní podmínky:	• Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství). • Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů. • Je požadována záruka na hardware s výměnou NBD v délce 60 měsíců. Tato záruka musí být garantovaná výrobcem zařízení.

WIFI – 39KS

Parametr	Minimální požadavek
Výrobce a model	**Aruba AP-505 (RW) Unified AP, PN: R2H28A + AP-MNT-D AP mount bracket individual D/ záruka 5let**
Základní vlastnosti	• Třída zařízení: indoor přístupový bod • Uzavřená konstrukce bez ventilátorů • Podpora bezdrátových standardů: 802.11a/b/g/n, 802.11ac wave2, 802.11ax • Plnohodnotná certifikace Wi-Fi Aliance: IEEE 802.11a/b/g/n/ac • Plnohodnotná certifikace Wi-Fi Aliance: WPA3-CNSA, WPA3-SAE, WPA3-OWE • Pracovní režim AP bez kontroléru (autonomní) • Pracovní režim AP řízené kontrolérem (lightweight) • Pracovní režim AP v roli kontroléru s možností správy až 120 AP • Minimální počet portů ethernet LAN: 1x 100/1000 Mbit/s RJ45 • Podpora standardů IEEE 802.3af (PoE), IEEE 802.3at (PoE+) • Podpora standardního PoE IEEE 802.3af 15W bez nutnosti redukce výkonu libovolného rádia • Podpora napájení z AC napájecího zdroje • Vestavěná interní anténa MIMO, omni down-tilt • Radiová část: dual band, současná podpora pásem 2,4GHz a 5GHz • MIMO a počet nezávislých streamů na 2,4GHz rádio: 2x2:2 • MIMO a počet nezávislých streamů na 5GHz rádio: 2x2:2 • Podpora šířky kanálu 80 MHz • HW podpora DL-OFDMA, UL-OFDMA a DL-MU-MIMO • Automatické ladění kanálu a síly signálu v koordinaci s ostatními AP • Možnost nastavení vysílacího výkonu s krokem 0.5 dBm • Minimální komunikační rychlost na fyzické vrstvě (Max data rate) pro 5GHz: 1200 Mbps • Minimální komunikační rychlost na fyzické vrstvě (Max data rate) pro 2.4GHz: 570 Mbps • Integrovaný TPM pro bezpečné uložení certifikátů a klíčů • Podpora 802.11ac explicitního beamformingu • Podpora airtime fairness • Prioritizace jednotlivých SSID na základě vysílacího času • USB port s podporou 3G/4G USB modemu jako WAN uplink • Vypínatelné indikační LED diody informující o stavu zařízení • Band Steering či obdobné (prioritizace 5GHz pásma v případě je-li podporováno) • Detekce Rogue AP • Minimální počet inzerovaných SSID (BSSID) na radio: 16 • Nastavitelný DTIM interval pro jednotlivé SSID • Mapování SSID do různých VLAN podle IEEE 802.1Q • VLAN Pooling • HW Podpora wireless MESH funkcionality s protokolem pro optimální výběr cesty v rámci MESH stromu • Podpora Layer-2 izolace bezdrátových klientů • HW Podpora spektrální analýzy v pásmech 2,4GHz a 5GHz • Hardware filtry pro filtraci intermodulačního rušením pocházejícím z mobilních sítí (Advanced Cellular Coexistence nebo obdobné) • Detekce a monitorování problémů WLAN odchytáváním provozu na AP ve formátu PCAP a jeho zasíláním do Ethernetového analyzátoru, schopnost zachytávat rámce včetně 802.11 hlaviček • DHCP server, směrování a NAT pro bezdrátové klienty • AP v režimu IPSec VPN klient s možností tvorby L2 či L3 VPN • Automatická identifikace připojeného zařízení a jeho operačního systému • Předávání konektivity mezi AP při pohybu bez výpadku spojení – roaming • Dynamické vyvažování zátěže klientů mezi AP se zohledněním zátěže, počtu klientů, síly signálu v koordinaci s ostatními AP • Optimalizace provozu: multicast-to-unicast konverze

	• Možnost řízení QoS (šířky pásma) na základě aplikací (Office 365, Dropbox, Facebook, P2P sdílení, VoIP, video aplikace) • Filtrování přístupu na web • Podpora RadSec (RADIUS over TLS) • 802.11w ochrana management rámců • Podpora Kensington lock • Podpora MAC ověřování a 802.1X ověřování s využitím lokální DB v AP • Podpora 802.1X suplicant, AP se ověřuje před připojením do LAN • Volitelně možnost spravovat AP cloud management nástrojem • CLI formou serial konsole port a serial over bluetooth • SSHv2, SNMPv2c a SNMPv3 • AP podporuje zero touch provisioning pomocí externího management SW jehož IP adresu získá z cloud aktivační služby poskytované výrobcem • Integrované Bluetooth 5.0 Low Energy (BLE) rádio • Integrované Zigbee 802.15.4 rádio • Podpora režimu SLEEP s max. spotřebou energie do 4W • Součástí AP je příslušenství pro montáž na zeď nebo strop
Ostatní podmínky:	• Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství). • Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů. • Je požadována záruka na hardware s výměnou NBD v délce 60 měsíců. Tato záruka musí být garantovaná výrobcem zařízení.

NAC – 1KS

Parametr	Minimální požadavek
Výrobce a model	**2x Aruba ClearPass Cx000V VM Appl E-LTU + 1x Aruba ClearPass NL AC 500 CE E-LTU**
POŽADAVKY NA KONTROLU PŘÍSTUPU DO SÍTĚ	• Autentizační platforma (AAA) pro řízení přístupu uživatelů a zařízení do LAN a Wi-Fi. • On-premise appliance, nepřipouští se cloud řešení. • Virtuální appliance bez nutnosti dodatečných licencí např. pro OS nebo database. • Režimu vysoké dostupnosti – minimálně 2 autentizační node s jednotnou správou • Podporované hypervisory: VMware (.OVA formát), Hyper-V, KVM. • Plná kompatibilita s infrastrukturou Objednatele, na které bude probíhat ověřování (stávající prvky jsou HPE ARUBA). • Podpora 802.1X autentizace pro bezdrátové sítě, Ethernet LAN sítě a VPN. • Požadovaný počet licencí pro současně autentizovaná zařízení (pomocí 802.1X): 500 • Požadovaný počet licencí pro současně profilovaná zařízení: 500 • Možnost vytváření active-active clusterů. Cluster musí poskytovat vysokou dostupnost pro všechny funkcionality a umožňovat navýšení počtu podporovaných uživatelů přidáním další instance. • Režim vysoké dostupnosti umožňuje v jednom clusteru kombinovat specializovanou HW a virtuální appliance • Podpora minimálně následujících autentizačních metod: PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, Tunnel Extensible Authentication Protocol (TEAP), MAC autentizace. • Platforma musí umožňovat úplné oddělení autentizace a autorizace, např. autentizace proti službě Active Directory, ale autorizace proti externí SQL databázi. • Autorizace zařízení a uživatelů na základě kontextových informací jako čas, místo připojení, typ zařízení, osobní profil či členství ve skupině v Active Directory.

	• Podpora dalších způsobů autentizace a autorizace. Minimálně: LDAP, MS AD, Token, MAC auth, generická SQL databáze, Kerberos, HTTPS web autentizace, Single Sign-On (minimálně SAML 2+ IdP a SP, OAuth, Shibboleth a Okta). • Podpora změny autorizačního stavu zařízení bez nutnosti změny definice autorizační politiky, např. pro odpojení nebo karanténu koncových zařízení. • Podpora autorizace pomocí externího Cloud zdroje identity: Azure Active Directory. • Podpora RADIUS CoA podle RFC3576 pro změnu autorizace ověřeného zařízení • Podpora RadSec (RADIUS over TLS) a RadSec proxy pro IPv4 a IPv6 • Možnost autorizace uživatelů na základě jejich vlastních accounting informací z předchozích připojení – např. za účelem omezení celkového času online či objemu přenesených dat za delší časové období. • Sběr dodatečných informací o připojených zařízeních (profilování) jako jsou DHCP volby klienta, HTTP uživatelský agent či předvolba MAC adresy. Tyto informace lze využít pro doplňkové ověření přístupu zařízení do sítě. • Sběr dodatečných informací o připojených IoT zařízeních (profilování), pomocí aktivních metod jako jsou: SNMP, WMI a NMAP scan. Tyto informace lze využít pro doplňkové ověření přístupu zařízení do sítě. • Automatická identifikace a označení privátních (randomizovaných) MAC adres koncových zařízení. • Platforma obsahuje funkci otestovani autentizační politiky, včetne flexibilní volby typu autentizace, atributů klienta, atd. • Podpora REST API pro většinu základních úkonů AAA platformy. Podpora REST volání vyvolaného autentizační či autorizační událostí (pro předání informací o klientovi jinému systému, automatického založení support ticketu atp.). • Zpracovávání SYSLOG hlášení z externích zdrojů, vyhledávání klíčových událostí a automatizovaná reakce na ně. Minimálně v rozsahu přijmutí bezpečnostního hlášení z firewallu a izolace konkrétního klienta na základě tohoto hlášení. • Možnost vlastní tvorby parseru/integrace SYSLOG hlášení pro možnost uživatelské integrace s libovolnými systémy třetích stran. • Podpora SYSLOG podle RFC 5424. • Možnost registrace zařízení pomocí MAC adresy pro non-IT uživatele - omezená funkce administračního rozhraní, se zařazením zařízení do skupiny s definovanou politikou přístupu. • Podpora TACACS+ autentizace správců síťových zařízení. • Možnost integrace s MDM (Mobile Device Management) platformami třetích stran (minimálně AirWatch, Citrix, MobileIron, JAMF). • Funkce pro řízení přístupu hostů – LAN a WiFi Guest Captive portál • Podpora HTTP a HTTPS web autentizace (Captive portál). • Podpora CAPPORT - RFC 8908 • Podpora autentizace hostů pomocí účtů sociálních sítí: Google, Google Plus, Facebook, Facebook WIFI, Twitter, LinkedIn, Microsoft. • Podpora autentizace lokálními účty v rámci portálu, ověření pomocí jméno+heslo, autentizační kód. • Možnost samoobslužné registrace hosta do sítě se SMS a email ověřením. • Přístup zdarma pouze s akceptací podmínek užití. • Tarify lze omezit časově, z hlediska rychlosti připojení či objemu přenesených dat. • Vynucení odpojení zařízení ihned po naplnění jakéhokoliv z limitů. • Perzistence autentizace/registrace s využitím MAC cache a zobrazení jen uvítacích stránek s osobním oslovením hosta při opakovaných návštěvách. Konfigurovatelné hodnoty trvání MAC cache pro různé hosty v rámci jedné služby (např. jedno SSID). • Možnost vytváření účtů samoobslužnou registrací. • Možnost provozovat více graficky i obsahově unikátních portálů v rámci jedné instalace.

	• Redakční systém pro plnou grafickou a obsahovou úpravu jednotlivých captive portálů umožňuje: • Uprava barev, fontů, pozadí a loga. • Úprava registračních formulářů – přidávání a odebírání polí pro vstupní data formuláře včetně validace vkládaného obsahu. • Možnost vkládání animací, videí a dalšího dynamického obsahu. • Vytváření specifických stránek pro různé typy zařízení a operačních systémů (např. pro efektivní navedení do specifického app store).

Analýza síťového provozu – 1KS

Parametr	Minimální požadavek	
Výrobce a model	**GREYCORTEX Mendel All-in-one - senzor + kolektor MA-SC-500, záruka 36měsíců (FYZICKÝ HW SERVER plnící všechny technické požadavky)**	
Základní vlastnosti	Požadované funkcionality/vlastnosti Nabízené řešení splňuje/nesplňuje, **vč. vysvětlení**, jak je zadání splněno	Splňuje Nabízené řešení
	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.	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.
	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.	Řešení analyzuje síť na základě zrcadleného síťového provozu ze SPAN portů / TAPů a nevyžaduje agenty na koncových stanicích ani 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.	Řešení analyzuje obsah datových paketů v reálném čase a detekuje protokol/ aplikaci na základě obsahu provozu prostřednictvím DPI, ne jen čísla portu.
	Dodaný systém musí být schopen analyzovat síť také na základě zpracování statistických protokolů typu NetFlow, IPFIX, NetStream, Cisco NSEL a případně dalších.	Nabízené řešení umí analyzovat síť také na základě zpracování statistických protokolů typu NetFlow, IPFIX, NetStream, Cisco NSEL a 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.	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 musí být možné provádět uživatelsky v off-line režimu.	Aktualizace systému lze provádět také 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.	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.

	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.	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“.	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 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.	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	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.

	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.	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.
	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.	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.
	Detekce na základě databáze známých hrozeb Systém musí být schopen identifikovat hrozby a reportovat události na základě	Nabízené řešení identifikuje hrozby a reportuje události na základě detekční databáze známých hrozeb, tj. malware (trojské koně, viry, červy, rootkity, apod.), známých útoků (exploity) a zranitelností, porušení bezpečnostních pravidel a „best practices" a dalších rizik, reputační databáze známých škodlivých IP adres, TLS certifikátů,

	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,	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,

	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.	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,	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

	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**	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.

	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.	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	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.

	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.	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.
	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,	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.

	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.	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.	Ve spolupráci s kompetentními a vyškolenými osobami zadavatele bude dodavatel průběžně zajišťoval ladění a nastavení detekce k eliminaci nežádoucích falešně pozitivních nálezů.
Záruka	Záruka 36měsíců.	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,	**Viz potvrzení**

	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	

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

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.

SERVER - virtulizační 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

SERVER OS + CAL

Parametr	Minimální požadavek
Výrobce a model	**2x MICROSOFT Windows Server 2025 DATACENTER 32CORE + 300x Windows Server 2025 DATACENTER DEVICE CAL (EDU)**
Parametry	2 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 virtualizačních serverech – min 2x32CORE • 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 **300** zařízení

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“

NAS – 1KS + 4KS 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/ 5LET záruka**

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

UPS – 2KS

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

Databázový SW

Parametr	Minimální požadavek
Výrobce, název, verze a licenční program databázového SW	**MICROSOFT SQL Server Standard Core SLng LSA 4CORE + SA**
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

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

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	**125x Licence IMPRIVATA SUB-SSO/AM-NON-CLINICAL-S License: OneSign Single Sign-On/Authentication Management for Non-Clinical Users + 125x HDW-IMP-MFR75A Hardware: Imprivata Reader MFR75A (replacement for MFR75)+ 125x 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 **125uživatelů** 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 – **125KS**	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 – **125KS**	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

Společné požadavky pro části 1 – 5

Požadavek
Uchazeč bere na vědomí, že součástí akceptace plnění jsou výsledky auditu, který bude prověřovat, zda jím implementovaná bezpečnostní opatření jsou funkční. Uchazeč 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

Vyšší odborná škola a Střední škola Boskovice, příspěvková organizace
KYBERBEZPEČNOST 1.0

1) nástroj pro ochranu integrity komunikačních sítí

				Cena za jednotku v Kč bez DPH	Cena za požadované množství v Kč bez DPH	Cena za požadované množství v Kč včetně DPH
FIREWALL						
FIREWALL	Firewaal/8x GE RJ45 a zároveň min. 2ks SFP+ port/propustnost min. 2,5 Gbps /IPS, Malware ochrana,aplikační kontrolal, URL, DNS, Antispam - záruka 5 LET	KS	1			
Centralizované logování analýza a report	Centralizované logování + analýza a report min. 5 GB logů/den	KS	1			
MAINTENENCE support	Potřebná maintenance nutná pro provoz systémů	ROK	5			
IMPLEMENTACE	IMPLEMENTACE + ŠKOLENÍ + dokumentace projektu	MD	10			

2) nástroj pro ochranu koncových stanic

Ochrana koncových stanic a SVR						
Endpoint NGA + EDR	Ochrana koncových stanic Endpoint + EDR, záruka 5 LET	KS	150			
MAINTENENCE support	Potřebná maintenance nutná pro provoz systémů	ROK	5			
IMPLEMENTACE	IMPLEMENTACE / zaškolení	MD	20			

3) nástroje pro ochranu integrity komunikačních sítí

INFRASTRUKTURA - core						
Aktivní prvky core switch	CORE SWITCH /24 x 10Gb SFP+ - 5let záruka	KS	1			
INFRASTRUKTURA - aktivní prvky - POE						
Aktivní prvky PoE - 48port	PoE SWITCH /48x GE RJ45 PoE - 5let záruka	KS	11			
Aktivní prvky PoE - 24port	PoE SWITCH /24x GE RJ45 PoE - 5let záruka	KS	8			
Aktivní prvky minigbic	10G SFP+ Transceiver - 5let záruka	KS	28			
INFRASTRUKTURA - aktivní prvky						
Aktivní prvky - 24port	SWITCH /24x GE RJ45 - 5let záruka	KS	11			
INFRASTRUKTURA - WIFI						
WIFI interní	WIFI AP - indoor s interními anténami v katefgorii WiFi 6E - 5let záruka	KS	39			
NAC	NAC - Virtuální appliance/NAC pro min 500endpointů - 5 let záruka	KS	1			
MAINTENENCE support	Potřebná maintenance nutná pro provoz systémů	ROK	5			
IMPLEMENTACE	IMPLEMENTACE / zaškolení	KS	10			

Analýza šiťového provozu						
SONDA a COLEKTOR - SW	SW licence: senzor + kolektor /500Mbps pro alespoň 1500 monitorovaných IP adres	KS	1			
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. 5 let záruka	KS	1			
MAINTENENCE support	Potřebná maintenance nutná pro provoz systémů	ROK	5			
IMPLEMENTACE	IMPLEMENTACE / zaškolení	KS	15			

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, 5 let záruka	KS	2			
BACK UP - časové zámky	BACK UP - vrstvené zálohovací úložiště s diskovou mezipamětí / 54T, dlouhodobé a bezpečné uložiště pro uchovávání záloh - záruka 5Y	KS	1			
SERVER - virtulizační platforma	Virtualizační platforma - Licence musí pokrývat minimálně 64CORE (dva fyzické servery) s možností dalšího rozšíření, 5 let záruka	KS	1			
SERVER OS	Serverové operační systémy - pokrývající 32core/SERVER - EDU	KS	2			
SERVER CAL	Serverové operační systémy - CAL - EDU	KS	300			
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			
NAS	NAS Rack /Minimálně 8šachtové NAS zařízení /Čtyřjádorový 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			
HDD pro NAS	HDD pro NAS/12TB/HDD/3.5"/SATA/7200 RPM/ záruka 5let	KS	4			
UPS - páteřní prvky	UPS min 2700W/8x IEC 320 C13 / LAN management - 5Y záruka	KS	2			
DATABÁZE - pro neomezený počet uživatelů	DATABÁZOVÝ SW pro celkem 4 CORE pro neomezený počet uživatelů	KS	1			
BACKUP SW pro 15VM	BACKUP SW pro min. 15VM - PERPETUAL	KS	1			
MAINTENENCE support	Potřebná maintenance nutná pro provoz systémů	ROK	5			
IMPLEMENTACE a MIGRACE	IMPLEMENTACE a MIGRACE/zaškolení	MD	20			

5) nástroj pro ověřování identity uživatelů

MFA + SSO přihlašování						
K4a - MFA + SSO - licence USER	MFA + SSO - licence USER	KS	125			
K4b - MFA + SSO - licence SERVER	MFA + SSO - licence SERVER	KS	2			
K4c - HW - čtečky karet	Čtečky bezkontaktních čipů, 5 let záruka	KS	125			
K4d - HW - bezkontaktní karty	Bezkontaktní čip, 5 let záruka	KS	125			
MAINTENENCE support	Potřebná maintenance nutná pro provoz systémů	ROK	5			
IMPLEMENTACE	IMPLEMENTACE / zaškolení	MD	15			

nce je již součástí OS (MS WIN 2025 DATACENTER a ty jsou součástí dodávky)

Celková cena KYBERBEZPEČNOST, maintenance	bez DPH	s DPH
	12.948.700,00 Kč	**15.667.927,00 Kč**

HARMONOGRAM

Aktivita	Začátek	Termín
Předání místa plnění	D	D
Zahájení projektu – úvodní projektová schůzka - detailní harmonogram včetně návaznosti implementačních prací	D	D+4
Realizace předmětu plnění - implementace kyberbezpečnostních opatření	D+4	D+22
Školení administrátorů	D+22	D+24
Akceptační testy	D+24	D+26
Zahájení ostrého provozu	D+26	-

jednotka = 1týden