Společnost: **T-Mobile Czech Republic a.s.**
IČO: 64949681
DIČ: CZ64949681
Se sídlem: Tomíčkova 2144/1, 148 00 Praha
Zastoupená: [redacted], na základě pověření
Bankovní spojení: Česká spořitelna, a.s., Budějovická 1912, Praha 4
Číslo účtu: [redacted]
Zapsaná v obchodním rejstříku Městského soudu v Praze, oddíl B, vložka 3787

dále jen **„poskytovatel"** na straně jedné,

a

Společnost: **Oblastní nemocnice Mladá Boleslav, a.s., nemocnice Středočeského kraje**
IČO: 272 56 456
DIČ: CZ27256456
Se sídlem: Mladá Boleslav, třída Václava Klementa 147, PSČ 293 01
Zastoupená: JUDr. Ladislav Řípa, předseda představenstva
Mgr. Daniel Marek, místopředseda představenstva
Bankovní spojení: Komerční banka, a.s.
Číslo účtu: [redacted]
Zapsaná v obchodním rejstříku Městského soudu v Praze, oddíl B, vložka 10019

dále jen **„objednatel"** na straně druhé,

se jako smluvní strany níže uvedeného dne, měsíce a roku dohodly, v souladu s ustanovením § 2079 a násl. zákona č. 89/2012 Sb., občanský zákoník, jak stanoví tato:

SMLOUVA O DODÁVCE A IMPLEMENTACI SOFTWARE

dále jen „smlouva"

1. Úvodní ustanovení

1.1. Objednatel má zájem na zajištění řešení zabezpečení koncových stanic a e-mailové komunikace ke zvýšení své kybernetické bezpečnosti, a to prostřednictvím dodávek software nástrojů.

1.2. Poskytovatel bere na vědomí, že objednatel je největším poskytovatelem zdravotních služeb v regionu Mladé Boleslavi, přičemž řádný chod jeho informačních systémů představuje klíčovou složku pro řízení jeho provozu, mající podstatný vliv na poskytování zdravotních služeb objednatelem.

1.3. Tato smlouva je uzavírána na základě výběru dodavatele veřejné zakázky zadávané v otevřeném řízení v nadlimitním režimu dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů s názvem **„Zabezpečení koncových stanic a e-mailové komunikace"** (dále jen **„veřejná zakázka").** Součástí smluvního ujednání je zadávací dokumentace veřejné zakázky, jakož i závazky, přísliby či prohlášení, které poskytovatel uvedl v podané nabídce. V případě

rozporu mezi ujednáním této smlouvy a obsahem nabídky poskytovatele, zadávací dokumentace nebo příloh této smlouvy, má vždy přednost ustanovení této smlouvy.

1.4. Poskytovatel prohlašuje, že měl před podáním své nabídky k dispozici požadavky objednatele na rozsah plnění dle této smlouvy, a to jako součást zadávací dokumentace. Poskytovatel tyto požadavky před podáním své nabídky s vynaložením odborné péče přezkoumal a na základě toho prohlašuje, že je schopen předmět plnění této smlouvy splnit. Poskytovatel potvrzuje, že měl v případě jakýchkoliv nejasností možnost požádat o vysvětlení zadávací dokumentace.

1.5. Poskytovatel dále prohlašuje, že předmět plnění této smlouvy odpovídá jeho podnikatelskému oprávnění a disponuje potřebným vybavením a kapacitami k řádnému a včasnému plnění předmětu této smlouvy.

1.6. Předmět plnění dle této smlouvy je realizován za finanční podpory IROP, název projektu „Rozvoj kybernetické bezpečnosti Klaudiánovy nemocnice", reg. číslo CZ.06.01.01/00/22_004/0000054 (dále také jen „projekt").

2. Předmět smlouvy

2.1. Předmětem této smlouvy je závazek poskytovatele dodat a implementovat objednateli e-mail protection, antivirové ochrany stanic - centralizovaný XDR systém a ochranu a správu mobilních zařízení - MDM (dále jen souhrnně **„Software"),** v prostředí Oblastní nemocnice v Mladé Boleslavi (Klaudiánova nemocnice), zajištění školení pro administrátory včetně příslušné produktové dokumentace, včetně dokumentace skutečného provedení zakázky, a zajištění technické podpory po dobu 5 let a závazek poskytovatele umožnit objednateli nabytí vlastnických, užívacích a jiných práv potřebných k řádnému a nerušenému provozu, správě a užívání Software objednatelem. Předmětem této smlouvy je dále závazek objednatele řádně dodaný a implementovaný Software převzít a zaplatit za něj poskytovateli sjednanou cenu a hradit cenu za poskytovanou podporu.

2.2. Podrobná specifikace Softwaru je uvedena v nabídce poskytovatele, která je přílohou č. 1 této smlouvy.

3. Dodávka a implementace Software

3.1. Poskytovatel v rámci implementace Software provede následující:

- dodávka a implementace (nasazení, nastavení) SW na místě určení
- Ekologická likvidace obalového materiálu
- Úvodní inicializace dodaných SW/VM appliance
- Integrace dodaných komponent do virtualizační vrstvy
- Zaškolení ICT administrátorů objednatele v trvání min. 16 hodin a v rozsahu nezbytném pro:
  - převzetí a správu předmětných zařízení
  - uplatňování nároků na poskytování služeb technické podpory služeb
  - možnost zadávat požadavky přes webové rozhraní, telefonicky nebo e-mailem
- dokumentace skutečného provedení zakázky, obsahující minimálně:
  - popis implementovaného řešení (včetně printscreenů potvrzujících nasazení)
  - časový harmonogram reálné implementace
  - provedená školení, včetně prezenčních listin

- produktová dokumentace (nebo alespoň výčet a samotná dokumentace jako příloha)
- popis splnění Požadavků na zajištění kybernetické bezpečnosti v realizační fázi
- shrnutí implementovaného řešení

- Integrace dodávaných technologií do monitoringu objednatele
- Reaktivní podpora v případě, že dojde k neplánovanému přerušení služeb.

3.2. Nedílnou součástí dodávky Software je dále:

- dodávka časově a místně neomezených licencí potřebných pro provozování, správu a užívání Software objednatelem,
- dodávka produktové dokumentace v rozsahu potřebném pro běžný provoz Software a pro běžnou správu Software.

3.3. Objednatel se zavazuje zajistit potřebnou součinnost svou a veškerých dodavatelů stávajících IT systémů v prostředí objednatele, a to v rozsahu nutném pro plnění této smlouvy poskytovatelem.

4. Zajištění technické podpory Software

4.1. Poskytovatel se zavazuje zajistit podporu pro každou nabízenou položku Software, a to po dobu 5 let od okamžiku převzetí Software objednatelem. Tato podpora musí pokrývat veškeré služby nutné pro zajištění plné funkčnosti instalovaných Software, jejich aktualizaci a předplatné pro všechny objednatelem požadované funkce. Podpora musí v plném rozsahu pokrytí garantovaná dodavatelem nabízené položky.

4.2. Pro hlášení požadavků je poskytovatel povinen zajistit provoz telefonické hotline a helpdeskové aplikace v režimu nejméně 8x7, s pracovní dobou nejméně od 8:00 hod do 16:00 hod., 7 dní v týdnu, součástí helpdeskové aplikace musí být reporting o průběhu řešení požadavků.

4.3. Poskytovatel musí ve svých vlastních prostorách a na svoje náklady zřídit a po dobu trvání smlouvy mít k dispozici (případně zajistit u VAD distributora pro ČR) testovací prostředí pro dodávané technologie. Testovací prostředí musí být dostupné pro řešení troubleshooting i koncepčních otázek. Za účelem ověření navrhovaného řešení poskytovatel poskytne na požádání pracovníka objednatele přístup k tomuto testovacímu prostředí pomocí vzdáleného šifrovaného přístupu. Jedná se o předcházení nežádoucího dopadu na produkční prostředí objednatele. Testovací prostředí musí zahrnovat:

- předinstalované a provozované navrhované řešení
- adresářovou strukturu s Active Directory
- MS Exchange

4.4. Poskytovatel objednateli garantuje, že:

- Dodaný Software bude od okamžiku jeho protokolárního předáním a převzetí do konce doby poskytování technické podpory bez vad a bude fungovat v souladu se specifikacemi uvedenými ve smlouvě a v zadávací dokumentaci veřejné zakázky.
- Software ve své poskytovatelem implementované podobě nebude obsahovat viry nebo jiné dysfunkce, které by bránily jeho řádnému provozu, správě a užívání.
- Software bude řádně fungovat v prostředí objednatele, zejména bude fungovat na jeho IT infrastruktuře, bude zajišťovat přebírání a předávání dat z/do stávajících informačních systémů objednatele.

4.5. Po dobu podpory je poskytovatel povinen nastoupit na odstraňování závady nejpozději do 4 hodin v pracovních dnech od jejího nahlášení a odstranit závadu nejpozději do 24 hodin od nástupu na opravu. Na odstraňování havarijní závady je poskytovatel povinen nastoupit bezodkladně, nejpozději do 2 hodin od jejího nahlášení a odstranit havarijní závadu nejpozději do 12 hodin od nástupu na opravu. Za závadu se považuje stav, kdy nefunguje jen některá část Software, ale Software je jinak plně funkční a použitelný ke svému účelu. Za havarijní závadu se považuje stav, kdy je Software nefunkční či je vyřazen z provozu.

5. Doba, místo a plnění

5.1. Poskytovatel se zavazuje uvést Software do provozu nejpozději do 6 týdnů od nabytí účinnosti této smlouvy. Podrobný harmonogram realizace jednotlivých kroků bude dohodnut a písemně potvrzen zástupci smluvních stran po podpisu této smlouvy. Podpora bude poskytována po dobu uvedenou v této smlouvě.

5.2. Objednatel si vyhrazuje právo v nezbytném rozsahu prodloužit termín dodání Software v případě mimořádných provozních situací, nehod, havárií, stávek, výluk, nepříznivých klimatických podmínek, krizových stavů, nepříznivých zásahů ze strany orgánů veřejné moci či jiných nepříznivých a nepředvídatelných situací, nezávislých na vůli objednatele. V tomto případě nevzniká poskytovateli nárok na náhradu případných s tím souvisejících nákladů.

5.3. Poskytovatel je povinen průběžně informovat objednatele o stavu rozpracovanosti a předávat mu informace o plnění předmětu této smlouvy, a to na kontrolních dnech, jejichž termíny určí objednatel, zpravidla s nejméně týdenním předstihem. Objednatel je oprávněn předkládat ke zjištěným informacím své připomínky a návrhy řešení (dále jen **„připomínky").** Poskytovatel je povinen vynaložit maximální možné úsilí při zapracování těchto připomínek do řešení, případně objednateli řádně v písemné formě odůvodnit, proč nemohou být připomínky akceptovány.

5.4. Poskytovatel odpovídá za to, že implementace Software nebude narušovat chod ostatní IT infrastruktury objednatele, mimo v harmonogramu dojednané odstávky. Konfigurace jednotlivých částí Software bude probíhat vždy v časech předem dohodnutých s objednatelem.

5.5. Místem plnění je sídlo objednatele, konkrétně Oddělení výpočetní techniky.

5.6. Závazek poskytovatele dodat a implementovat Software bude splněn předáním a převzetím řádně dodaného Software v odpovídající kvalitě objednatelem. Předání a převzetí Software bude potvrzeno písemně podpisem akceptačního protokolu pověřenými zástupci smluvních stran. Součástí předávaného Software bude veškerá dokumentace a doklady ke všem částem Software, výrobkům a zařízením dodaných poskytovatelem a dále protokol o proškolení příslušných pracovníků objednatele.

5.7. Poskytovatel vyzve písemně objednatele k předání a převzetí Software nejméně 3 pracovní dny předem.

5.8. Vlastnické právo k Software přechází na objednatele okamžikem podpisu akceptačního protokolu zástupci smluvních stran. Právo užití těch částí Software, které podléhají ochraně podle zákonů upravujících práva duševního vlastnictví, přecházejí na objednatele okamžikem předání těchto částí Software.

5.9. Nebezpečí škody na Software nese poskytovatel do okamžiku protokolárního předání a převzetí Software objednatelem.

6. Cena, licenční poplatky a platební podmínky

6.1. Cena se skládá:

položka	Cena v Kč bez DPH	jednotka	Cena za požadované jednotky v Kč bez DPH
Cena za pořízení a implementaci software dle podrobné technické specifikace	= 8.900.000,-	**1**	= 8.900.000,- Kč
Cena za 1 rok provozu (podpory)	= 356.000,-	**5**	= 1.780.000,- Kč
Celková cena v Kč bez DPH			= 10.680.000,- Kč

Změna ceny je přípustná pouze v případě změny zákonných sazeb daně z přidané hodnoty. Poskytovatel odpovídá za uplatnění řádné sazby DPH.

6.2. Cena je stanovena dohodou jako cena konečná, maximální, nejvýše přípustná a zahrnuje veškeré náklady poskytovatele spojené s dodávkou a implementací Software dle této smlouvy, včetně licenčních poplatků za časově a místně neomezené licence, nákladů na dodání potřebných výrobků a zařízení, nákladů spojených s pracemi při realizaci dodávky, nákladů na dopravu, balné, pojištění, případné celní a daňové poplatky, zaškolení personálu apod., a dále za poskytování technické podpory.

6.3. Cena bude objednatelem uhrazena bezhotovostním převodem na účet poskytovatele uvedený v záhlaví této smlouvy, a to na základě daňového dokladu (faktury) vystavené poskytovatelem.

6.4. Poskytovatel je oprávněn vystavit fakturu za pořízení a implementaci software po předání a převzetí Software a po podpisu akceptačního protokolu. Splatnost faktury je do 30 dnů od data jejího doručení objednateli.

6.5. Poskytovatel je oprávněn vystavit fakturu za technickou podporu software vždy jednou ročně, a to vždy pro 1 rok provozu (podpory), a to vždy do konce prvního měsíce daného ročního období. Splatnost faktury je do 30 dnů od data jejího doručení objednateli.

6.6. Faktura vystavená poskytovatelem musí splňovat veškeré náležitosti řádného daňového a účetního dokladu ve smyslu zákona č. 563/1991 Sb., o účetnictví a zákona č. 235/2004 Sb., o dani z přidané hodnoty. Faktura musí být označena také názvem projektu *„Rozvoj kybernetické bezpečnosti Klaudiánovy nemocnice"*, a registračním číslem projektu CZ.06.01.01/00/22_004/0000054. Fakturu, která nebude splňovat touto smlouvou a zákonem stanovené náležitosti, je objednatel oprávněn kdykoliv ve lhůtě splatnosti vrátit. V takovém případě se lhůta splatnosti přerušuje a nová lhůta splatnosti začne běžet až ode dne doručení nové/opravené faktury objednateli.

6.7. V případě prodlení objednatele s úhradou ceny je poskytovatel oprávněn požadovat zaplacení úroku z prodlení v souladu s ustanovením § 1970 občanského zákoníku.

6.8. Objednatel neposkytuje zálohové platby.

6.9. Prevezme-li objednatel Software s vadami uvedenými v akceptačním protokolu, je objednatel oprávněn z fakturované částky pozdržet platbu ve výši 10% z ceny Software a tuto si ponechat jako zádržné. Objednatel uhradí poskytovateli částku odpovídající zádržnému do 15 dnů od odstranění všech vad zjištěných při předání Software. Pokud poskytovatel uvedené vady ve sjednané lhůtě neodstraní, je objednatel oprávněn použít zádržné k úhradě nákladů spojených s jejich odstraněním, nebo ze zádržného čerpat slevu z kupní ceny z titulu odpovědnosti za vady Software.

6.10. Zveřejní-li správce daně skutečnost, že poskytovatel je nespolehlivým plátcem ve smyslu zákona č. 235/2004 Sb., o dani z přidané hodnoty, je objednatel oprávněn z každé fakturované platby zadržet daň z přidané hodnoty a tuto, aniž by k tomu byl vyzván jako ručitel, uhradit za poskytovatele příslušnému správci daně. Co do částky takto objednatelem uhrazené není objednatel v prodlení s úhradou ceny dle této smlouvy.

7. Práva a povinnosti smluvních stran

7.1. Poskytovatel je povinen realizovat dodávku a implementaci Software kompletně a ve vysoké kvalitě, v rozsahu dle této smlouvy, zadávací dokumentace veřejné zakázky a nabídky poskytovatele ve veřejné zakázce. Totéž platí i pro činnosti a dodávky od všech poddodavatelů poskytovatele. Poskytovatel má právo vykonat veškeré práce způsobem, který považuje za nejvýhodnější k řádné realizaci předmětu smlouvy při respektování účelu této smlouvy, dohodnutého časového harmonogramu, smluvních termínů a dalších práv a povinností dle této smlouvy. Postup prací musí zohledňovat oprávněné zájmy objednatele.

7.2. Poskytovatel je povinen dodržovat při plnění předmětu této smlouvy veškeré platné právní předpisy, příslušné technické nomy, jejichž závaznost si smluvní strany tímto sjednávají, pravidla dobré praxe, standardy a certifikace, jakož i doporučení a pokyny výrobce příslušných částí Software, které se vztahující k činnosti poskytovatele.

7.3. Poskytovatel se zavazuje při činnostech prováděných v prostorách objednatele či jeho smluvních partnerů dodržovat veškeré vnitřní předpisy a pravidla objednatele či jeho smluvních partnerů, se kterými byl seznámen. Poskytovatel je povinen přizpůsobit realizaci předmětu smlouvy provozním podmínkám objednatele, zejména provozu zdravotnického zařízení objednatele. Poskytovatel nesmí zasahovat do obsahu dat zpracovávaných v rámci plnění, jakýchkoliv dat objednatele či jeho smluvních partnerů ani provést zásah, který by ovlivnil či mohl ovlivnit funkcionalitu hardware objednatele či jiného software provozovaného na hardware objednatele, včetně pracovních stanic, pokud nebude s objednatelem dohodnuto jinak.

7.4. Poskytovatel a objednatel se zavazují vzájemně se neprodleně informovat o všech skutečnostech, které znemožňují, resp. podstatně omezují, plnění jejich povinností z této smlouvy, a to bez zbytečného odkladu od vzniku takové skutečnosti.

7.5. Poskytovatel se zavazuje uchovávat všechny doklady, dokumenty a data po dobu a způsobem stanoveným platnými právními předpisy ČR, např. zákonem č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, a zákonem č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů. Poskytovatel je povinen uchovávat veškerou dokumentaci související s realizací projektu, včetně účetních dokladů, minimálně však do konce roku 2035.

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

7.7. Smluvní strany jsou povinny dodržovat právními předpisy stanovené povinnosti k ochraně práv průmyslového a jiného duševního vlastnictví, jakož i chránit práva spadající do autorského práva, ochrany obchodního tajemství a ochrany osobních údajů.

7.8. Poskytovatel je povinen zajistit, aby objednatel nabyl příslušná oprávnění z práv duševního vlastnictví, která se týkají předmětu této smlouvy a jsou nezbytná pro řádné plnění této smlouvy a pro řádný provoz, správu a užívání Software objednatelem.

7.9. Poskytovatel bere na vědomí, že v rámci poskytování součinnosti nesmí docházet k nadměrnému zatěžování objednatele aktivitami, které by poskytovatel jakožto odborník na dodání a implementaci Software měl být schopen vyřešit vlastními silami. Objednatel poskytne poskytovateli nezbytnou součinnost, spočívající zejména v přípravě informací, dokumentů a dat, která je nezbytná k řádnému plnění předmětu smlouvy.

7.10. Poskytovatel prohlašuje a zavazuje se, že po celou dobu platnosti této smlouvy bude mít sjednáno pojištění pro případ odpovědnosti za škodu/újmu, přičemž toto pojištění se bude vztahovat i na škodu/újmu vzniklou v souvislosti s plněním předmětu této smlouvy objednateli či jakékoliv třetí osobě, s pojistným limitem odpovídajícím předmětu této smlouvy minimálně 10.000.000 Kč na jednu pojistnou událost. Poskytovatel je povinen předložit objednateli kopii pojistné smlouvy či jiný doklad o existenci pojištění, a to do 5 pracovních dnů od doručení výzvy objednatele.

7.11. Poskytovatel se zavazuje dodržovat požadavky objednatele stanovené v příloze č. 2 této smlouvy - Požadavky na zajištění kybernetické bezpečnosti. Strany sjednávají, že v případě rozporu má přednost ustanovení této smlouvy.

7.12. Instalace a implementace Software, jakož i technická podpora, budou ze strany poskytovatele poskytovány s odbornou péčí v souladu s touto smlouvou a prostřednictvím pracovníků disponujících dostatečným vzděláním a zkušenostmi s poskytováním daného plnění.

8. Odpovědnost za vady

8.1. Není-li uvedeno jinak, řídí se práva a povinnosti smluvních stran z vadného plnění příslušnými ustanoveními občanského zákoníku.

8.2. Poskytovatel se zavazuje, že Software bude mít vlastnosti stanovené zadávací dokumentací veřejné zakázky, obsahem nabídky poskytovatele a touto smlouvou, a to bez ohledu na skutečnost, zda se jedná o vadu skrytou nebo zjevnou, která mohla být ze strany objednatele identifikována před datem protokolárního předání Software.

8.3. Objednatel je oprávněn dle svého uvážení uplatnit vůči poskytovateli tato práva z odpovědnosti za vady:

a) právo na bezplatné odstranění vad,
b) právo na přiměřenou slevu z ceny,
c) právo na odstoupení od smlouvy, pokud vady či nedodělky jsou takového charakteru, že podstatně ztěžují či dokonce brání řádnému provozu, správě a užívání Software. Za takové vady se považují i vady, které jsou opakovaného charakteru.

9. Ochrana osobních údajů, důvěrné informace

9.1. V případě, že bude při plnění předmětu této smlouvy docházet ke zpracování osobních údajů, je tato smlouva zároveň smlouvou o zpracování osobních údajů ve smyslu článku 28, odst. 3 Nařízení Evropského parlamentu a Rady (EU) 201/679, ze dne 27.4.2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen **„GDPR").** Poskytovatel má v takovém případě pro účely ochrany osobních údajů postavení zpracovatele ve smyslu GDPR. Poskytovatel je povinen splnit všechny povinnosti z toho vyplývající.

9.2. Poskytovatel je oprávněn zpracovávat osobní údaje pouze v rozsahu nezbytně nutném pro plnění předmětu této smlouvy, za účelem plnění předmětu této smlouvy a na základě dalších písemných pokynů objednatele. Za tímto účelem je poskytovatel oprávněn osobní údaje zejména ukládat na nosiče informací, upravovat, uchovávat po dobu nezbytně nutnou k uplatnění práv poskytovatele vyplývajících z této smlouvy, předávat zpracované osobní údaje objednateli a nepotřebné osobní údaje likvidovat.

9.3. Poskytovatel učiní v souladu s platnými právními předpisy (zejména čl. 32 GDPR) dostatečná organizační a technická opatření zabraňující přístupu neoprávněných osob k osobním údajům a zabraňující jakémukoli úniku osobních údajů mimo sféru kontroly poskytovatele a porušení jejich integrity, dostupnosti a odolnosti systému zpracování.

9.4. Poskytovatel bude objednateli nápomocen při zajišťování jeho povinnosti ohlásit případné porušení zabezpečení osobních údajů dozorovému úřadu, oznámit případné porušení zabezpečení osobních údajů subjektu údajů, posoudit vliv zpracování na ochranu osobních údajů a případně konzultovat zpracování s dozorovým úřadem. Poskytovatel je dále povinen umožnit objednateli nebo jím pověřenému auditorovi či jiné objednatelem pověřené osobě kdykoli během plnění předmětu této smlouvy a 3 roky po skončení platnosti této smlouvy kontrolu opatření k ochraně osobních údajů a poskytnout v rámci této kontroly veškerou nezbytnou součinnost.

9.5. Po ukončení zpracování osobních údajů poskytovatel podle rozhodnutí objednatele všechny osobní údaje u něj uložené vymaže, včetně všech případných kopií a záloh, poskytne objednateli veškeré informace potřebné k doložení splnění povinností zpracovatele a umožní kontrolu objednatele nad jejich plněním.

9.6. Poskytovatel nezapojí do zpracování osobních údajů žádného jiného zpracovatele bez předchozího písemného souhlasu objednatele.

9.7. Poskytovatel zajistí, aby jeho zaměstnanci byli v souladu s platnými právními předpisy poučeni o povinnosti mlčenlivosti a o možných následcích pro případ porušení této povinnosti. Poskytovatel zajistí, aby písemnosti a jiné hmotné nosiče informací, které obsahují osobní údaje, byly uchovávány pouze v uzamykatelných místnostech. Poskytovatel dále zajistí, aby písemnosti a jiné hmotné nosiče informací, které obsahují citlivé údaje, byly uchovávány v uzamykatelných skříních umístěných v uzamykatelných místnostech.

9.8. Poskytovatel zajistí, aby elektronické datové soubory obsahující osobní údaje byly uchovávány v paměti počítače pouze:

a) je-li přístup k takovýmto souborům chráněn heslem nebo,

b) je-li přístup k užívání počítače, v jehož paměti jsou tyto soubory umístěny, chráněn heslem.

9.9. Veškeré skutečnosti obchodní, ekonomické a technické povahy související se smluvními stranami, které nejsou běžně dostupné v obchodních kruzích a se kterými se smluvní strany seznámí při realizaci předmětu smlouvy nebo v souvislosti s touto smlouvou, se považují za důvěrné informace.

9.10. Poskytovatel se zavazuje, že důvěrné informace týkající se objednatele jiným subjektům nesdělí, nezpřístupní, ani nevyužije pro sebe nebo pro jinou osobu. Zavazuje se zachovat je v přísné tajnosti a sdělit je výlučně těm svým zaměstnancům nebo poddodavatelům, kteří jsou pověřeni plněním předmětu této smlouvy a za tímto účelem jsou oprávněni se s těmito informacemi v nezbytném rozsahu seznámit. Poskytovatel se zavazuje zabezpečit, aby i tyto osoby považovaly uvedené informace za důvěrné a zachovávaly o nich přísnou mlčenlivost.

9.11. Povinnost ochrany důvěrných informací se nevztahuje na informace, které:

a) mohou být zveřejněny bez porušení této smlouvy,

b) byly písemným souhlasem dotčené smluvní strany zproštěny těchto omezení,

c) jsou známé nebo byly zveřejněny jinak, než následkem porušení povinnosti některé ze smluvních stran,

d) příjemce je zná dříve, než mu je předá druhá smluvní strana,

e) jsou vyžádány soudem, nebo příslušným orgánem veřejné moci, na základě zákona, popřípadě, jejichž uveřejnění je stanoveno zákonem,

f) smluvní strana sdělí osobě vázané zákonnou povinností mlčenlivosti (např. advokátovi nebo daňovému poradci) za účelem uplatňování svých práv.

9.12. Povinnost mlčenlivosti, ochrany osobních údajů a ochrany důvěrných informací trvá bez ohledu na ukončení platnosti této smlouvy.

9.13. Smluvní strany se zavazují, že obchodní a technické informace, které jim byly svěřeny druhou smluvní stranou, nezpřístupní třetím osobám bez písemného souhlasu druhé smluvní strany a nepoužijí tyto informace k jiným účelům, než k plnění předmětu této smlouvy.

10. Sankční ujednání

10.1. Za každý jednotlivý případ porušení povinnosti poskytovatele stanovené touto smlouvou, je poskytovatel povinen zaplatit objednateli smluvní pokutu stanovenou následovně:

a) při prodlení poskytovatele s dodáním a implementací Software oproti lhůtám uvedených v čl. 5 odst. 5.1 této smlouvy, smluvní pokutu ve výši 5.000,- Kč za každý i započatý den prodlení,

b) při porušení povinnosti poskytovatele uvedené v čl. 5 odst. 5.4. této smlouvy, smluvní pokutu ve výši 5.000,- Kč za každou i započatou hodinu přerušení provozu software objednatele,

c) při prodlení poskytovatele s odstraněním vad či nedodělků Software uvedených v akceptačním protokolu, smluvní pokutu ve výši 5.000,- Kč za každý i započatý den prodlení, to za každou vadu či nedodělek zvlášť,

d) při prodlení poskytovatele s odstraněním havarijních závad Software oproti lhůtám uvedených v čl. 4 odst. 4.5. této smlouvy, smluvní pokutu ve výši 2.000,- Kč za každou i započatou hodinu prodlení, a to za každou vadu zvlášť,

e) při prodlení poskytovatele s odstraněním jiných než havarijních závad Software oproti lhůtám uvedených v čl. 4 odst. 4.5 této smlouvy, smluvní pokutu ve výši 500,- Kč za každou i započatou hodinu prodlení, a to za každou vadu zvlášť,

f) při porušení povinnosti poskytovatele uvedené v čl. 9 odst. 9.1. až 9.8. této smlouvy, smluvní pokutu ve výši 100.000,- Kč za každý jednotlivý případ zvlášť, a to i opakovaně,

g) při porušení povinnosti poskytovatele uvedené v čl. 9 odst. 9.10. až 9.13. této smlouvy, smluvní pokutu ve výši 500.000,- Kč za každý jednotlivý případ zvlášť, a to i opakovaně.

10.2. Smluvní pokuta je splatná do patnácti (15) dnů ode dne doručení písemné výzvy k jejímu uhrazení. Za účelem započtení smluvní pokuty proti pohledávce poskytovatele na zaplacení ceny je smluvní pokuta splatná ihned po zániku utvrzené povinnosti, případně okamžikem doručení písemné výzvy k jejímu uhrazení.

10.3. Zaplacením smluvní pokuty není dotčeno právo objednatele požadovat náhradu škody/újmy v plné výši.

11. Pověřené osoby

11.1. Pověřenou osobou ve věcech plnění této smlouvy na straně objednatele ve věcech smluvních je:

Jméno a příjmení: [redacted]
tel: [redacted]
fax: ---
email: [redacted]

Pověřenou osobou ve věcech plnění této smlouvy na straně objednatele ve věcech technických je:

Jméno a příjmení: [redacted]
tel: [redacted]
fax: ---
email: [redacted]

11.2. Pověřenou osobou ve věcech plnění této smlouvy na straně poskytovatele ve věcech smluvních / technických je:

Jméno a příjmení: [redacted]
tel: [redacted]
fax: ---
email: [redacted]

11.3. Ke změně údajů o pověřených osobách postačí písemné oznámení doručené druhé smluvní straně.

12. Samostatné ujednání - registr smluv

12.1. Vzhledem k tomu, že tato smlouva podléhá uveřejnění v registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování

těchto smluv a o registru smluv (zákon o registru smluv), uzavírají smluvní strany toto samostatné ujednání.

12.2. Smluvní strany se dohodly, že uveřejnění této smlouvy v registru smluv zajistí objednatel. Poskytovatel se zavazuje nejpozději při podpisu této smlouvy označit ty části smlouvy a ty údaje, které požaduje v souladu se zákonem o registru smluv vyloučit z uveřejnění (obchodní tajemství, osobní údaje apod.). Jinak platí, že souhlasí s uveřejněním v plném rozsahu.

12.3. Plnění poskytnuté přede dnem účinnosti této smlouvy se považuje za plnění dle této smlouvy.

12.4. Toto samostatné ujednání smluvních stran nabývá platnosti a účinnosti nezávisle na platnosti a účinnosti této smlouvy, a to podpisem této smlouvy oprávněnými zástupci smluvních stran.

13. Závěrečná ustanovení

13.1. Pokud některé z ustanovení této smlouvy je nebo se stane neplatným či neúčinným, nemá tato skutečnost vliv na platnost a účinnost ostatních ustanovení této smlouvy. Smluvní strany se zavazují takové ustanovení bez zbytečného odkladu nahradit novým platným a účinným ustanovením, které svým obsahem bude odpovídat účelu ustanovení předchozího.

13.2. Písemnosti ve věci této smlouvy se doručují na adresy uvedené v záhlaví, pokud některá ze smluvních stran neoznámí písemně druhé smluvní straně změnu své adresy pro doručování. Pro doručování platí vždy též adresy zveřejněné ve veřejném rejstříku. Má se za to, že písemnost byla doručena nejpozději pátý den po jejím odeslání, a to i tehdy, nepodaří-li sejí z jakéhokoliv důvodu doručit.

13.3. V případě zániku této smlouvy, nebo v případě, že bude tato smlouva shledána neplatnou nebo neúčinnou, zůstávají zachována ta práva a povinnosti, z jejichž povahy plyne, že mají trvat i po ukončení této smlouvy. To platí zejména pro právo požadovat smluvní pokutu, náhradu škody/újmy vzniklé porušením této smlouvy nebo závazek zachovávat mlčenlivost.

13.4. Smluvní strany se v souladu s ustanovením § 89a zákona č. 99/1963 Sb., občanský soudní řád, dohodly, že místní příslušnost soudu k projednání a rozhodnutí sporů a jiných právních věcí vyplývajících z právního vztahu založeného touto smlouvou, jakož i ze vztahů s tímto vztahem souvisejících, se řídí sídlem objednatele.

13.5. Práva a povinnosti smluvních stran touto smlouvou výslovně neupravená se řídí příslušnými ustanoveními zákona č. 89/2012 Sb., občanský zákoník.

13.6. Jakékoli změny a doplňky této smlouvy jsou možné pouze ve formě písemných vzestupně číslovaných dodatků, podepsaných oprávněnými zástupci obou smluvních stran. Totéž platí i pro vzdání se písemné formy.

13.7. Tato smlouva nabývá platnosti dnem podpisu a účinnosti dnem uveřejnění v registru smluv.

13.8. Objednatel předpokládá uzavření této smlouvy elektronickou formou. Bude-li smlouva uzavřena v listinné formě, bude vypracována ve dvou vyhotoveních, z nichž každá smluvní strana obdrží po jednom.

13.9. Nedílnou součástí této smlouvy jsou následující přílohy:

a) Příloha č. 1 - Nabídka poskytovatele (podrobná specifikace předmětu plnění)

b) Příloha č. 2 - Požadavky na zajištění kybernetické bezpečnosti

13.10. Smluvní strany si smlouvu přečetly, jejímu obsahu rozumí a na důkaz toho připojují vlastnoruční podpisy svých oprávněných zástupců.

V Praze dne dle el. podpisu

V Mladé Boleslavi dne _____

Zabezpečení koncových stanic a emailové komunikace	Splňuje ano/ne
bezpečnostní řešení centrální správa	
Správa všech poptávaných produktů (ochrana endpointů a serverů) z jednoho administračního rozhraní	ANO
Přístup do administračního rozhraní pomocí protokolu HTTPS	ANO
Centrální administrační rozhraní musí mít dokumentované API	ANO
Vícefaktorová autentifikace pro administrátory	ANO
Centrální administrace podporuje automatické odhlášení uživatele při nečinnosti	ANO
Umístění zabezpečeného datacentra je možné zvolit v rámci lokality EU (je zahrnuto v ceně nabízené licence)	ANO
Synchronizace uživatelů a skupin je zajištěna pomocí služby, jež vyčítá informace z Active Directory a šifrovaným tunelem je synchronizuje do centrální správy.	ANO
Synchronizace uživatelů a skupin z Azure Active Directory.	ANO
S Active Directory komunikuje synchronizační služba pomocí služeb LDAPS (port 636) případně LDAP (port 389)	ANO
Synchronizační služba synchronizuje minimálně tyto parametry: Username, Login, Email address, skupiny a členy každé skupiny	ANO
Synchronizační služba musí podporovat LDAP filtry pro užší výběr synchronizovaných položek	ANO
Synchronizační služba musí podporovat manuální a intervalovou synchronizaci v definovaných časových intervalech	ANO
Mimo synchronizaci uživatelů a skupin z Active Directory musí řešení nabízet vytváření lokálních uživatelů a skupin	ANO
Centrální administrační rozhraní musí umožnit vytvoření dvoustupňové hieararchické struktury (celá organizace - podřízené organizace)	ANO
Administrátor celé organizace musí mít právo vytvářet podřízené organizace a přidělovat jim potřebné licence z rozsahu přiděleného celé organizaci	ANO
Administrátoři podřízených organizací mohou administrovat pouze svoji organizaci a její uživatele	ANO
Centrální administrace podporuje řízení uživatelů dle rolí a to minimálně v rozsahu:	ANO
Administrátor celé organizace - Může vytvářet nové podřízené organizace a přidělovat jim administrátory	ANO
Hlavní administrátor podřízené organizace - Má plná práva pro správu a může přidělovat role dalším uživatelům	ANO
Běžný administrátor podřízené organizace - Má plná práva pro správu	ANO
Pracovník technické podpory - Má práva pro čtení pro správu, může číst logy, může vyvolat sken a update uživatelského zařízení, spravuje výstrahy	ANO
Uživatel s přístupem pro čtení - Má práva pro čtení pro správu, logy a výstrahy	ANO
Centrální administrace podporuje napojení na systémy SIEM a zasílání událostí typu Události a Výstrahy	ANO
Centrální administrace poskytuje vestavěné logování a reportování	ANO

Centrální adminsitrace podporuje zasílání alertů emailem na definované adresy	ANO
Centrální administrace disponuje souhrnným dashboardem, tedy místem, na kterém se zobrazují klíčové informace o celém prostře	ANO
Ochrana koncových bodů - 900 zařízení	
Licence na uživatele bez ohledu na počet použitých zařízení	ANO
Podpora OS Windows 8, Windows 10, Windows 11 a vyšší, MAC OS X 10.10 a vyšší	ANO
Blokování škodlivých webových stránek	ANO
Kontrola souborů dle reputace	ANO
Webová kontrola / Blokování URL na základě kategorie (nejméně 40 předdefinovaných kategorií)	ANO
Kontrola a blokování HW zařízení - USB disky, externí HDD/SSD, CD/DVD, Wi-Fi, Bluetooth, Infrared, Modemy	ANO
Kontrola a blokování aplikací, nejméně 40 předdefinovaných kategorií	ANO
Detekce malware pomocí strojového učení Deep Learning	ANO
Skenování souborů proti malware (lokální i vzdálené soubory)	ANO
Skenování archivů	ANO
Signatury AV dostupné v reálném čase v Cloudu, nezávislost na četnosti aktualizace databáze	ANO
Analýza chování před spuštěním souboru (HIPS)	ANO
Blokování potenciálně nechtěných aplikací (PUA)	ANO
DLP - blokování přenosu dat na základě pravidel, možnost úplné blokace nebo upozornění uživatele a vyžádání potvrzení	ANO
Detekce a prevence známých i neznámých exploitů, nezávislá na signaturách	ANO

Ochrana před následujícími exploitními technikami: - Enforce Data Execution Prevention (DEP) - Mandatory Address Space Layout Randomization (ASLR) - Bottom Up ASLR - Null Page (Null Dereference Protection) - Heap Spray Allocation - Dynamic Heap Spray - Stack Pivot - Stack Exec (MemProt) - Stack-based ROP Mitigations (Caller) - Branch-based ROP Mitigations - Structured Exception Handler Overwrite Protection (SEHOP) - Import Address Table Filtering (IAF) - Load Library - Reflective DLL Injection - VBScript God Mode - WoW64 - Syscall - Hollow Process - DLL Hijacking - Shellcode a Dynamic Shellcode - APC Protection (Double Pulsar / AtomBombing) - Squiblydoo AppLocker Bypass - Process Privilege Escalation	ANO
Detekce a odstranění rootkitů	ANO
Detekce škodlivého provozu typu Command and Control (botnet)	ANO
Analýza chování při běhu procesů	ANO
Aktivní zamezení negativních dopadů zneužití zranitelností	ANO
Blokování neautorizovaného šifrování (kryprovirus) dat	ANO
Automatická obnova souborů do původního stavu před zašifrováním	ANO
Ochrana Master Boot Record před zašifrováním	ANO
Ochrana prohlížeče před injektáží kódu	ANO
Automatické odstranění malware	ANO

Automatické odstranění zbytkových souborů (čištění registrů) po zablokování malware	ANO
Určení zdroje a příčiny útoku, grafická reprezentace děje útoku	ANO
Ochrana proti zásahu uživatele s lokálními admin. právy do nastavení klienta	ANO
Detekce pomocí strojového učení bez nutnosti připojení k internetu	ANO
Zjednodušený náhled na nákazu minimálně v rozsahu, vstupní bod malware do systému (aplikace), malware, přijaté opatření Grafické znázornění průběhu nákazy minimálně v rozsahu, vstupní bod malware do systému (aplikace), zápisy do systému a do registrů OS, komunikace na internet včetně zobrazí IP a URL adres	ANO
Možnost globálního vyčištění a blokování nalezeného malware na všech systémech najednou (pomocí jedné akce).	ANO
Vytvoření „hash" pro soubor na úrovni lokálního agenta	ANO
Vyhledání infikovaných počítačů na základě „hash" malware	ANO
Automatické vyhodnocení incidentů	ANO
Zobrazení obecných informací o proběhnutých útocích (alespoň z poslední doby)minimálně v rozsahu jméno malware, počet postižených systémů a hodnocení nebezpečnosti malware výrobcem.	ANO
Možnost dešifrace a kontroly HTTPS provozu	ANO
Application lockdown (Web Browser, Java, Media, Office)	ANO
Součástí řešení je lehký klient na koncové stanice	ANO
Řešení poskytuje zázemí pro threat hunting	ANO
Možnost terminálového připojení na endpoint z centální správy na úrovni systému	ANO
Možnost spouštění SQL dotazů vůči endpointům pro aktivní vyhledávaní hrozeb (minimálně 290 před definovaných dotazů)	ANO
Automatická nebo manuální izolace koncového zařízení (např. při napadení malwarem)	ANO
Správa Windows Firewall	ANO
Ochrana serverů - 120 serverů	
Licence na chráněný serverový OS	ANO
Podpora OS Windows Server 2012 a vyšší, Amazon Linux 2, CentOS 7/Minimal/Stream, Red Hat Enterprise Linux 7/8, Ubuntu 18.04/20.04/Minimal	ANO
Podpora Windows Remote Desktop Services	ANO
Podpora MS Azure a Amazon Web Services	ANO
Blokování škodlivých webových stránek	ANO
Kontrola souborů dle reputace	ANO

Webová kontrola / Blokování URL na základě kategorie (nejméně 10 předdefinovaných kategorií)	ANO
Kontrola a blokování HW zařízení - USB disky, externí HDD/SSD, CD/DVD, Wi-Fi, Bluetooth, Infrared, Modemy	ANO
Kontrola a blokování aplikací, nejméně 40 předdefinovaných kategorií	ANO
Whitelisting aplikací	ANO
Správa Windows Firewall	ANO
Možnost bezagentového skenování virtuálních prostředí VMware a Hyper-V	ANO
Detekce malware pomocí strojového učení Deep Learning	ANO
Automatické výjimky ze skenování	ANO
Skenování souborů proti malware	ANO
Skenování archivů	ANO
Signatury AV dostupné v reálném čase v Cloudu, nezávislost na četnosti aktualizace databáze	ANO
Analýza chování před spuštěním souboru (HIPS)	ANO
Blokování potenciálně nechtěných aplikací (PUA)	ANO
DLP - blokování přenosu dat na základě pravidel, možnost úplné blokace nebo upozornění uživatele a vyžádání potvrzení	ANO
Detekce a prevence známých i neznámých exploitů, nezávislá na signaturách	ANO

Ochrana před následujícími exploitními technikami: - Enforce Data Execution Prevention (DEP) - Mandatory Address Space Layout Randomization (ASLR) - Bottom Up ASLR - Null Page (Null Dereference Protection) - Heap Spray Allocation - Dynamic Heap Spray - Stack Pivot - Stack Exec (MemProt) - Stack-based ROP Mitigations (Caller) - Branch-based ROP Mitigations - Structured Exception Handler Overwrite Protection (SEHOP) - Import Address Table Filtering (IAF) - Load Library - Reflective DLL Injection - VBScript God Mode - WoW64 - Syscall - Hollow Process - DLL Hijacking - Shellcode a Dynamic Shellcode - APC Protection (Double Pulsar / AtomBombing) - Squiblydoo AppLocker Bypass - Process Privilege Escalation	ANO
Detekce a odstranění rootkitů	ANO
Detekce škodlivého provozu typu Command and Control (botnet)	ANO
Analýza chování při běhu procesů	ANO
Aktivní zamezení negativních dopadů zneužití zranitelností	ANO
Blokování neautorizovaného šifrování (kryprovirus) dat	ANO
Automatická obnova souborů do původního stavu před zašifrováním	ANO
Ochrana Master Boot Record před zašifrováním	ANO
Ochrana prohlížeče před injektáží kódu	ANO
Automatické odstranění malware	ANO

Automatické odstranění zbytkových souborů (čištění registrů) po zablokování malware	ANO
Určení zdroje a příčiny útoku, grafická reprezentace děje útoku	ANO
Ochrana proti zásahu uživatele s lokálními admin. právy do nastavení klienta	ANO
Uzamčení stavu serveru z pohledu aplikací a služeb	ANO
Zjednodušený náhled na nákazu minimálně v rozsahu, vstupní bod malware do systému (aplikace), malware, přijaté opatření Grafické znázornění průběhu nákazy minimálně v rozsahu, vstupní bod malware do systému (aplikace), zápisy do systému a do registrů OS, komunikace na internet včetně zobrazí IP a URL adres	ANO
Možnost globálního vyčištění a blokování nalezeného malware na všech systémech najednou (pomocí jedné akce).	ANO
Vytvoření „hash" pro soubor na úrovni lokálního agenta	ANO
Vyhledání infikovaných počítačů na základě „hash" malware	ANO
Automatické vyhodnocení incidentů	ANO
Zobrazení obecných informací o proběhnutých útocích (alespoň z poslední doby)minimálně v rozsahu jméno malware, počet postižených systémů a hodnocení nebezpečnosti malware výrobcem.	ANO
Možnost tzv. Lockdownu zařízení, následně není možná instalace aplikací	ANO
Aktivní rozeznávání běžících aplikací	ANO
Možnost spouštění SQL dotazů vůči endpointům pro aktivní vyhledávaní hrozeb (minimálně 290 před definovaných dotazů)	ANO
Řešení poskytuje zázemí pro threat hunting	ANO
Řešení disponuje před-definovanými politikami dle best practices	ANO
Anti-Virus pro Linux servery (Amazon Linux/Amazon Linux 2, CentOS 7/8, Debian 9/10, Oracle Linux 7/8, RHEL 7/8, SUSE Linux Enterprise Server 12/15, Ubuntu 18LTS/20.04 LTS)	ANO
Ochrana mobilních zařízení - tablety 200 ks	
Licence na uživatele bez ohledu na počet použitých zařízení	ANO
Podpora Android, iOS, iPadOS	ANO
Možnost oddělených konfiguračních profilů pro zařízení organizace / BYOD	ANO
Možnost hromadného enrollmentu zařízení / hromadné instalace zabezpečených kontejnerů na BYOD zařízeních	ANO
Enrollment pomocí emailu / on-line registrací	ANO
Podpora Apple Configurator, Apple DEP, Android Zero-Touch a Samsung Knox Enrollment,	ANO
Konfigurovatelný samoobslužný portál pro uživatele umožňující minimálně:	ANO
- Regsitraci nového zařízení	ANO

- Odstranění a smazání původního zařízení	ANO
- Lokalizaci, uzamčení i smazání zařízení	ANO
- Reset hesla zbezpečenho kontejneru	ANO
Podrobné logování aktivity administrátorů řešení	ANO
Reporting zaměřený na:	ANO
- Výskyt malware	ANO
- Stav zařízení	ANO
- Soulad zařízení s organizačními standady	ANO
- Provozované aplikace	ANO
- Certifikáty	ANO
Možnost vzdálené lokalizace / uzamčení / smazání zařízení	ANO
Možnost vzdálené instalace certifikáů	ANO
Možnost vzdálené konfigurace proxy	ANO
Možnost vzdálené konfigurace opávnění aplikací	ANO
Detekce Jailbreaku či Rootu	ANO
Šifrování zařízení / zabezpečeného aplikačního prostředí (kontejneru)	ANO
Kontrola a vynucení zabezepečení zařízení (heslo / biometrika)	ANO
Možnost vymazání zařízení / kontejneru po definovaném počtu neplatných pokusů o přihlášení	ANO
Kontrola verze OS (minimální / maximální verze)	ANO
Možnost inventarizace a instalace aplikací - Povinně instalované aplikace / whitelising / blacklisting	ANO
Detekce / zamezení instalace aplikací z neověřených zdrojů (prevence sideloadingu)	ANO
Možnost vzdálené centrální konfigurace aplikací (Minimálně MS Office 365 aplikace)	ANO
Možnost vzdálené instalace / odstranění aplikací z centrální správy	ANO
Možnost zamezení využití Google Play / Apple AppStore	ANO
Detekce MitM útků	ANO
Ochrana před malware - Signaturová (Android)	ANO
Ochrana před malware - Machine learning (Android)	ANO
Možnost zamezení přístupu ke klíčovým aplikacím (minimálně email) při nesouladu s požadavky a politikami (verze OS, přítomnost neautorizovaných aplikací, přítomnpst jailbreak / root a další)	ANO
Ochrana před škodlivými webovými stránkami (web filtering)	ANO
Možnost webové filtrace dle kategorií stránek - Alespoň 10 předdefinovaných kategorií	ANO
Zamezení přístupu na nevhodné / nežádoucí typy stránek, možnost definice vlastních pravidel.	ANO
Šifrovaný správce uživatelských hesel	ANO

Blokace bluetooth / airdrop / NFC přenosu dat	ANO
Možnost blokace copy / paste	ANO
Blokace externích paměťových médií (USB / SS / MicroSD)	ANO
Možnost vynucení provozu v režimu "Kiosk" pro účelová zařízení - Zamezení opuštění aplikace	ANO
Možnost zamezit odesílání dat o pádu aplikací / systému	ANO
Možnost zamezení manuálního nastavení WiFi (připojit / odpojit / nové sítě)	ANO
Možnost zamezení využití webových prohlížečů	ANO
Možnost zakázání asistentů (Siri / Google)	ANO
Možnost správy nastavení zobrazování notifikací notifkací na zamykací obrazovce / v notifikačním centru (při uzamčeném zařízení)	ANO
Zamezení neautorizovaného unenrollmentu zařízení ze správy	ANO
Možnost ovládání mobilního tarifu při roamingu (deaktivace data / volání)	ANO
Zabezpečení emailové komunikace - 1300 e-mailových stránek	
Zařízení ve formě Virtual appliance s podporou virtualizační platformy Vmware	ANO
Zařízení musí umožňovat využít prostředky virtualizační platformy a to až do výše 4TB systémového úložiště (karanténa, logy, reporty atd.) a 6 síťových rozhraní	ANO
podpora IPv4 i IPv6	ANO
možnost nasazení v režimu gateway/MTA a v transparentním režimu - pokud jsou tyto funkce licencovány, požadujeme dodání licence pro oba režimy	ANO
licenční model nezávislý na počtu chráněných emailových schránek/IP adres/uživatel. Pokud jsou tyto parametry licencované, potom požadujeme dodání licence pro neomezený počet emailových schránek/IP adres/uživatel	ANO
architektura MTA musí umožnit provést kontrolu emailu ještě před uložením do emailové fronty. Výkonnostní požadavky (viz níže) musí odpovídat výkonnosti bez využívání emailové fronty	ANO
Management rozhraní musí být provozované přímo na daném zařízení (externí management není akceptovatelný)	ANO
plnohodnotná správa pomocí web gui (HTTPs) a CLI (SSH)	ANO
podpora protokolů SNMP (v2c, v3) a syslog pro možnost začlenění do monitorovacího systému	ANO
součástí dodávky musí být i specifický MIB soubor výrobce	ANO
podpora archivace (např. přístup do archivu pomocí protokolu IMAP)	ANO
podpora systémové karantény	ANO
podpora uživatelské karantény přes webové rozhraní	ANO
možnost uvolnění zpráv z karantény pomocí odkazu v emailu	ANO
podpora ověřování pres SAML 2.0 a ADFS pro přihlášení do uživatelské karantény	ANO

podpora opakované kontroly emailu ve chvíli vyzvednutí emailu z karantény	ANO
podpora externího úložiště (šifrovaná komunikace, např. SFTP)	ANO
podpora DKIM, DMARC a DANE	ANO
výrobcem spravovaná proprietární AS funkcionalita s možností kategorizace v emailu nalezených URL	ANO
ochrana typu spam-outbreak (tj opakované dotázání se signaturového server po předdefinované prodlevě)	ANO
IP reputační databáze výrobce, graylisting, reputace odesílatelů, behaviorální analýza, analýza hlaviček mailů, heuristická analýza mailů	ANO
podpora systémů třetích stran (blacklisty)	ANO
kontrola založená na Bayesian přístupu, white a black listing, analýza obrázků s možností detekce a selekce newsletter emailů	ANO
podpra funkce tzv. bounce verification, podpora greylistingu	ANO
podpora DNSBL a SURBL	ANO
možnost vytvoření lokálního slovníku zakázaných slov (email obsahující některé z těchto slov bude vyhodnocen jako spam)	ANO
reakce na detekovaný spam minimálně: přidání tágu přidání hlavičky přeposlání emailu na jiný SMTP server přidání BCC archivace odmítnutí (reject) zahození (discard) uložení do karantény přepsání adresy příjemce	ANO
Možnost limitace v rámci SMTP navázané relace: počet zpráv od jednoho klienta za určitou dobu, maximální počet spojení od jednoho klienta za určitou dobu, podpora endpoint reputace, napojení na LDAP za účelem verifikace uživatelů; možnost omezení počtu HELO/EHLO v rámci jedné SMTP relace, možnost omezit počet emailových zpráv v rámci SMTP relace, možnost omezit počet příjemců v rámci adresátů emailu, možnost manipulace s hlavičkou mailu (odstratení Received hlavičky)	ANO
Antivirová ochrana aktualizovaná výrobcem s možností nastvení následně prováděné akce	ANO
Požadujeme integraci s platformou sandbox	ANO
Možnost rozšíření řešení o on-premise sandbox plně funkčně integrovaný s emailovou branou (pokud se jedná o sandbox jiného výrobce, musí být tato funkční integrace garantována a podporována ze strany obou výrobců)	ANO

Ochrana před únikem citlivých informací, filtrování příchozích a odchozích typů souboru (minimálně podpora regulárních výrazů a typů souborů v příloze)	ANO
Podpora funkce ochrany před útoky typu DoS, Antispoofing, rate limiting	ANO
Lokálně udržované hodnocení odesílatelů (vyhodnocování lokálního skóre odesílatelů na základě nedávné aktivity s možností nastavení omezení pro různé úrovně skóre)	ANO
Podpora tzv. "click protection" (URL obsažená v přijímaných emailech jsou přepsána tak, aby byl uživatel po kliknutí přesměrován na emailovou bránu. Ta provede kontrolu přístupu proti aktuální databázi kategorizovaných URL a přístup povolí/zakáže na základě své konfigurace)	ANO
Podpora ochrany před cílenými phising útoky - možnost definovat seznam emailových adres klíčových osob organizace	ANO
Integrované logování a reporting, monitoring	ANO
Podpora REST API pro možnost integrace management funkcí do stávající řídící infrastruktury	ANO
Podpora funkce šifrování přenosu mailové komunikace end-to-end bez nutnosti instalovat sw na pracovní stanice (např. uložení šifrované zprávy lokálně s možností vyzvednout zprávu bezpečným způsobem přes web rozhraní)	ANO
Podpora tzv. neutralizace dokumentů v příloze (odstranění potenciálně nebezpečných prvků v dokumentu (makra, URL,...) v dokumentech MS Office a PDF, při zachování původního typu dokumentu	ANO
Automatická dekrypce šifrovaných dokumentů za pomoci administrátorem předdefinovaného slovníku hesel a výrobcem udržovaným slovníkem často používaných hesel	ANO
Možnost rozšíření o integrace s platformou Exchange online (Office365) a to přes nativní Office365 Graph API	ANO
Podpora antivirové antispamové kontroly pro tuto službu v reálném čase	ANO
Podpora REST API pro konfiguraci a management - Pokud tato funkce vyžaduje licenci, tak tato musí být součástí dodávky a to na minimálně 5 let	ANO
Minimální požadovaná výkonnost pro email routing: 300.000 emailů/hod	ANO
Minimální požadovaná výkonnost pro AS+ AV kontrolu: 200.000 emailů/hod	ANO
Součástí dodávky musí být podpora v režimu nejméně 8x7, s pracovní dobou nejméně od 8:00 hod do 16:00 hod., 7 dní v týdnu, a to na minimálně 5 let	ANO
Zařízení nesmí být licencováno na počet chráněných emailových schránek/uživateL V opačném případě požadujeme licenci pro neomezený počet.	ANO
Řešení nesmí být omezeno na počet chráněných domén. V opačném případě musí být součástí dodávky podpora pro minimálně 10 emailových domén	ANO

Požadavky na zajištění kybernetické bezpečnosti

Za účelem povinností stanovených Objednateli jakožto povinné osobě vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), je Poskytovatel povinen nad rámec povinností stanovených smlouvou plnit níže uvedené povinnosti zejm. součinnostního a bezpečnostního charakteru.

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

1) Systém řízení bezpečnosti informací

Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 3 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) (dále jen „VKB"), které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění na své straně:

a) Prosadit bezpečnostní zásady a procesy, které budou pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně Poskytovatele při poskytování předmětu plnění.

b) Na základě bezpečnostních potřeb a výsledků hodnocení rizik zavést příslušná bezpečnostní opatření v rozsahu poskytovaného předmětu plnění, monitorovat je, vyhodnocovat jejich účinnost.

c) Vést záznamy o vytváření a zpracování dat a informací v rozsahu poskytovaného předmětu plnění, zaznamenávat veškeré podstatné okolnosti související se zajištěním bezpečnosti těchto dat a informací a na vyžádání tyto záznamy Objednateli zpřístupnit.

d) Stanovit a udržovat aktuální bezpečnostní politiku, která bude pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně Poskytovatele při poskytování předmětu plnění. Bezpečnostní politika musí obsahovat hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací.

e) Stanovit a udržovat aktuální opatření bezpečnosti ve formě procesů a technologií, které zajišťují naplnění bezpečnostní politiky.

2) Řízení aktiv

Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 4 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění na své straně:

a) Stanovit a udržovat rozsah a seznam aktiv využívaných pro plnění této smlouvy (aktivy se rozumí např. data a informace k předmětu plnění dle této smlouvy, systémy ICT, moduly, HW prvky - infrastruktura hlasové a datové komunikace, aplikace, databáze, servery, úložiště, koncová zařízení - pracovní stanice typu osobní počítač nebo notebook, mobilní koncová zařízení - přenosná zařízení typu telefon, tablet, notebook, netbook, PDA, apod.), a tato aktiva

strukturovaně popsat a Objednateli předložit do 30 dnů od podpisu této smlouvy a následně na vyžádání, a to po celou dobu trvání smlouvy a do 2 let po jejím ukončení.

3) Řízení rizik

Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 5 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění na své straně:

a) Řídit vlastní rizika, která mohou ovlivnit poskytování předmětu plnění.

b) V minimálním intervalu 1x ročně vytvořit a předložit Zprávu o řízení kybernetických rizik, která bude minimálně pokrývat:

i. Vyhodnocení stavu kybernetické bezpečnosti za hodnocený rok

ii. Identifikaci a hodnocení rizik s vazbou na předmět plnění

iii. Realizovaná bezpečnostní opatření

iv. Nepokrytá bezpečnostní rizika a návrh opatření

v. Vyhodnocení bezpečnostních událostí a incidentů

vi. Aktuální stav souladu Poskytovatele s těmito Kybernetickými požadavky

4) Organizační bezpečnost

Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 6 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:

a) Jmenovat nejpozději do 5 dnů po uzavření této smlouvy odpovědnou kontaktní osobu pro potřeby zajištění plnění těchto Kybernetických požadavků a související komunikaci mezi Smluvními stranami (dále také jen **„Kontaktní osoba").** Kontaktní osobu sdělí Poskytovatel písemně Objednateli v téže lhůtě. Objednatel stanovuje, že určení Kontaktní osoby pro bezpečnost na straně Poskytovatele nemá dopad na ustanovení smlouvy týkající se odpovědných osob ve věcech smluvních a technických.

b) Využívat pro poskytování předmětu plnění pouze oprávněných osob, které byly řádně seznámeny příslušnými ustanoveními interních řídících aktů Objednatele a mají ověřenou kvalifikaci, znalosti a zkušenosti k řádnému poskytování předmětu plnění.

5) Řízení dodavatelů

Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 8 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění na své straně:

a) Využívá-li při poskytování předmětu plnění poddodavatele, zajistit adekvátní dodržování Kybernetických požadavků rovněž ve smluvních vztazích se svými poddodavateli, přičemž tuto skutečnost se Poskytovatel zavazuje doložit Objednateli do 10 dnů od Potvrzení objednávky, na jejímž plnění se budou poddodavatelé podílet v případě Služeb specialistů nebo do 10 dnů od počátku poskytování jiných služeb, písemným prohlášením o dodržování Kybernetických požadavků u svých poddodavatelů.

b) Pokud při poskytování předmětu plnění dochází ke zpracování osobních údajů, zajistit nad rámec smlouvy uzavření samostatných smluv (tj. smluv se svými poddodavateli, zaměstnanci a případnými dalšími osobami podílejícími se na poskytování plnění z této smlouvy) ve smyslu

příslušných ustanovení Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

6) Bezpečnost lidských zdrojů

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 9 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění na své straně:

    a) Zajistit, aby Kontaktní osoba nejpozději do 30 dnů od uzavření smlouvy potvrdila písemně Objednateli, že všechny osoby podílející se na poskytování předmětu plnění za stranu Poskytovatel byly prokazatelně seznámeny s těmito Kybernetickými požadavky a příslušnými ustanoveními interních řídících aktů Objednatele.

    b) Dodržovat příslušná ustanovení interních řídících aktů Objednatele v rozsahu, v jakém byl s těmito akty seznámen. Za prokazatelné seznámení se považuje školení pracovníků Poskytovatel zajištěné Objednatelem, protokolární či elektronické předání příslušné dokumentace nebo Objednatelem zajištěný přístup na sdílené úložiště obsahující příslušné interní akty řízení.

    c) V případě, že je součástí předmětu plnění služba dohledu nad předmětem plnění, definovat a naplnit role a odpovědnosti pro monitoring sítě a zařízení v rozsahu předmětu plnění.

    d) Zajistit, aby osoby podílející se na poskytování plnění Objednateli v prostředí nebo s prostředky Objednatele, a to i tehdy, pokud jsou prostředky Objednatele používány mimo jeho prostředí:

        i. Pro uložení a sdíleni dat a informací Objednatele využívaly pouze k tomu schválené prostředky (aktiva);

        ii. Neukládaly ani nesdílely data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno Objednatele;

        iii. Nestahovaly, nesdílely, neukládaly, nearchivovaly ani neinstalovaly datové a spustitelné soubory v rozporu s licenčními podmínkami nebo autorským zákonem;

        iv. Nenavštěvovaly internetové stránky s eticky nevhodným obsahem;

        v. Nerealizovaly pokusy o neautorizovaný přístup ke zdrojům Objednatele ani ke zdrojům jiných subjektů;

        vi. Nerealizovaly pokusy o neoprávněnou modifikaci ani jiné neoprávněné zásahy do prostředků Objednatele, a to ani v případě, kdy jim byl prostředek Objednatele svěřen do správy;

        vii. Nepodílely se s prostředky Objednatele na šíření spárnu ani škodlivého softwaru.

2. Dodavatel si je vědom, že součástí podmínek pro získání přístupu ke zdrojům a aktivům Objednatele je na straně Objednatele zpracování osobních údajů pracovníků Poskytovatele, kteří se podílejí na zajištění předmětu plnění. Pokud nebude Objednateli umožněno osobní údaje dotčených pracovníků Poskytovatele v rámci plnění smlouvy zpracovat, nebude těmto pracovníkům umožněn žádný přístup ke zdrojům Objednatele.

7) Řízení provozu a komunikací

Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 10 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění na své straně:

a) Zajistit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování předmětu plnění.

b) Na vyžádání poskytnout Objednateli přehled, report, či jinou adekvátní informaci o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře.

c) Zajistit, že pro poskytování předmětu plnění budou využívány pouze aplikace a technologie, které jsou v souladu splatnou českou a evropskou legislativou, především s ohledem na licenční podmínky a autorský zákon.

8) Řízení změn

Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 11 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění na své straně:

a) Přiměřeně reagovat na změny na straně Objednatele a upravit na své straně technická a organizační opatření tak, aby odpovídala novému stavu po provedení změny.

b) Aktivně spolupracovat při testování významné změny.

9) Řízení přístupu

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 12 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění na své straně:

   a) Přidělovat oprávnění svým jednotlivým pracovníkům ve smyslu oprávnění k výkonu činností tak, aby byla minimalizována rizika nežádoucího přístupu k aktivům Objednatele.

   b) Zajistit, aby udělený přístup nebyl sdílen více osobami za stranu Poskytovatele, pokud sdílený přístup nevyžaduje využívaná technologie. V takovém případě musí Poskytovatel vést evidenci využívání sdílených přístupů a tuto na vyžádání předložit Objednateli kdykoli v průběhu trvání účinnosti této smlouvy a 2 roky po ukončení její platnosti.

   c) Stanovit v požadavku na přístup rozsah dat/informací, služby, účelu, pro které je přístup k systému ICT Objednatele požadován a časový údaj o délce platnosti přístupu (např.: na dobu neurčitou / 1 rok / 1 měsíc / 1 den).

   d) Zajistit, aby osoby podílející se na poskytování předmětu plnění a mající přístup k informačním aktivům Objednatele chránily autentizační prostředky a údaje a nikdy neposkytovaly neautorizovaný přístup dalším osobám.

   e) Průběžně kontrolovat a vyhodnocovat oprávněnost a potřebu přístupu, jak fyzického, tak i logického, u všech osob na straně Poskytovatele, které přistupují do prostředí Objednatele.

2. Poskytovatel bere na vědomí, že přístup k systému ICT je možné povolit pouze fyzické identitě zaměstnance Poskytovatele / poddodavatele Poskytovatele, a to na základě požadavku Poskytovatele na přístup.

3. Poskytovatel bere na vědomí, že přidělení oprávnění zaměstnanci Poskytovatele musí být řízeno principem nezbytného minima a není nárokové.

4. Poskytovatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele (osoby za stranu Poskytovatele) může být příslušný účet zablokován a řešen jako bezpečnostní incident a mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu (např. okamžité zrušení přístupu k informačním aktivům Objednatele).

10) Akvizice, vývoj a údržba

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 13 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění na své straně:
    a) Zajistit bezpečnou implementaci, inovaci, aktualizaci a testování technologií, které jsou předmětem plnění.
    b) Předat Objednateli dokumentaci předmětu plnění minimálně v následujícím rozsahu:
        i. dokumentaci všech bezpečnostních nastavení, funkcí a mechanismů,
        ii. dokumentaci obsahující popis autorizačního konceptu a oprávnění,
        iii. dokumentaci obsahující instalační a konfigurační postupy.
2. V případě, že předmět plnění zahrnuje vývoj softwaru, zavazuje se Poskytovatel:
    a) Dodržovat a implementovat nejlepší praktiky pro bezpečný vývoj softwaru definované na základě smluvního vztahu.
    b) Na vyžádání umožnit Objednateli provedení auditu prováděného nebo provedeného plnění, předložit objednateli vyvíjený kód SW a výstupy z provedeného code-review (automatizovaně prostřednictvím bezpečnostního nástroje i manuálně), po jeho dokončení, pokud není v této smlouvě stanoveno jinak, a to zejména za účelem ověření skutečnosti, zda Poskytovatel postupuje či postupoval při poskytování plnění v souladu se smlouvou a těmito Kybernetickými požadavky.
    c) Poskytovat Objednateli v termínech stanovených Objednatelem, resp. bez zbytečného odkladu požadovanou součinnost na provedení bezpečnostního testování v průběhu vývoje softwaru či kdykoli po jeho předání.
    d) Zajistit, že plnění bude obsahovat jen ty součásti, které jsou objektivně potřebné pro řádné provozování softwaru a/nebo které jsou specifikovány výslovně ve smlouvě (zejména, že software nebude obsahovat žádné nepotřebné komponenty, žádné programové vzorky apod.).
    e) Pokud je součástí plnění i instalace operačního systému případně softwaru třetích stran, zajistit v průběhu jeho instalace, že budou použity předepsané verze těchto produktů kompatibilní a funkční v prostředí Objednatele.
    f) Zajistit bezpečnost testovacího prostředí u Poskytovatele a ochranu poskytnutých testovacích dat Objednatelem.
    g) Zajistit, že do produkčního prostředí Objednatele bude dodán jen předmětem smlouvy specifikovaný kompilovaný, respektive spustitelný kód a další nezbytná data pro provozování předmětu plnění.
    h) Zajistit, že v rámci poskytovaného plnění bude dodávaný software
        i) v souladu s bezpečnostními politikami a standardy Objednatele
        ii. otestován na soulad s bezpečnostními politikami Objednatele (platí pro Poskytovatele, pokud byl s takovými bezpečnostními politikami seznámen)
    i. Instalovat software pouze na základě Objednatelem předem schválených migračních postupů.
    j) Nevyvíjet, nekompilovat a nešířit v prostředí Objednatele programový kód, který má za cíl nelegální ovládnutí, narušení dostupnosti, důvěrnosti nebo integrity nebo neautorizované či nelegální získání dat a informací.

11) Zvládání kybernetických bezpečnostních událostí a incidentů

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 14 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění na své straně:
    a) Stanovit a popsat na své straně činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání bezpečnostních incidentů.
    b) Bez zbytečného odkladu hlásit Objednateli všechny bezpečnostní události a incidenty s potenciálním negativním dopadem na Objednatele, a to stanoveným komunikačním kanálem nebo prostřednictvím Kontaktní osoby.
    c) Vyhodnocovat informace o bezpečnostních incidentech a uchovávat je pro budoucí použití s ohledem na požadavky platné české a evropské legislativy.
    d) V případě vzniku bezpečnostní události a následného zvládání a vyhodnocování bezpečnostního incidentu a/nebo v případě podezření na bezpečnostní incident poskytnout Objednateli aktivní součinnost a relevantní informace o podezřelém zařízení či osobě na straně Poskytovatele.
    e) Bez zbytečného odkladu a po dohodě s Objednatelem realizovat opatření požadovaná Objednatelem v dohodnutých termínech ke snížení dopadu bezpečnostního incidentu nebo zamezení pokračování incidentu.
    f) Spolupracovat při analýze příčin bezpečnostního incidentu a navrhnout opatření s cílem zamezit jeho opakování v případě, že Poskytovatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.
2. Poskytovatel bere na vědomí, že postup zvládání bezpečnostního incidentu či jiný důsledek porušení Kybernetických požadavků, jehož příčina je na straně Poskytovatele, nebude posuzován jako okolnost vylučující odpovědnost Poskytovatele za prodlení s řádným a včasným plněním předmětu smlouvy a nebude důvodem k jakékoli náhradě případné újmy Poskytovateli či jiné osobě ze strany Objednatele. Ostatní ustanovení ohledně odpovědnosti Poskytovatele za prodlení obsažená ve smlouvě nejsou tímto ustanovením dotčena.

12) Řízení kontinuity činností

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 15 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění na své straně:
    a. Zajistit adekvátní kontinuitu svých aktiv, které jsou potřebné k poskytování předmětu plnění.
    b. Pravidelně kontrolovat a testovat, že je schopen kontinuitu aktiv zajistit dle sjednané úrovně služeb.

13) Kontrola a audit

Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 8 a § 16 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění poskytnout adekvátní součinnost při výkonu kontroly Objednatele ze strany Úřadu dle § 23 ZKB.

14) Fyzická bezpečnost

Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 17 VKB,

které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění na své straně:

a) Dodržovat provozní řády budov (režimová opatření) a využívaných prostor, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěny aktiva systémů ICT, anebo datové nosiče.

b) V rozsahu předmětu plnění zajistit fyzické zabezpečení, zejména označení, uchování a likvidaci, instalačních, záložních nebo archivních médií a dokumentace v souladu s klasifikací aktiv Objednatele, pokud s ní byl Poskytovatel seznámen.

15) Bezpečnostní nástroje

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 18 až § 27 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění na své straně:

a) Realizovat bezpečnostní opatření pro odstranění nebo blokování síťového spojení/síťových spojení, které/která neodpovídají požadavkům na ochranu integrity komunikační sítě.

b) Realizovat přístup z mobilního zařízení do prostředí Objednatele pouze prostřednictvím zabezpečeného připojení virtuální privátní sítě (VPN) nebo zvolit adekvátní technické opatření.

c) Připojovat do prostředí Objednatele pouze ta síťová zařízení (switch, přístupový bod wifi, router, hub apod.), která prošla schvalovacím procesem a jejich připojení bylo schváleno oprávněnou osobu ve věcech technických na straně Objednatele určenou v této smlouvě.

d) Bez zbytečného odkladu deaktivovat všechna nevyužívaná zakončení sítě anebo nepoužívané porty aktivního síťového prvku, který je v rozsahu předmětu plnění a je ve správě Poskytovatele.

e) Na aktiva Objednatele neinstalovat a nepoužívat v prostředí Objednatele tyto typy nástrojů, pokud nejsou součástí předmětu plnění:

i. Keylogger - software nebo hardware, který neautorizované zaznamenává stisky kláves s cílem narušit důvěrnost zadávaných dat a informací.

ii. Sniffer - software nebo hardware umožňující odposlouchávání síťového provozu.

iii. Analyzátor zranitelností (scanner zranitelností) - softwarový nebo hardwarový nástroj umožňující vyhledávání zranitelností systémů ICT, detekování dostupných síťových služeb a portů, běžících procesů, běžících aplikací a jejich verzí apod.

iv. Backdoor - skrytý softwarový nebo hardwarový nástroj, který umožňuje obejití schválených autentizačních procedur, instalovaný s cílem budoucího snadnějšího a neautorizovaného přístupu do systému ICT.

v. Malware a jiný škodlivý software, který narušuje, obchází či jinak omezuje bezpečnostní opatření v prostředí Objednatele.

f) Připojovat do prostředí Objednatele pouze zařízení ICT, která jsou chráněna proti malware a jinému škodlivému softwaru, pokud to jejich technologie umožňuje.

g) Průběžně zaznamenávat a uchovávat data o provozu zařízení ICT (provozní a lokalizační údaje) v rozsahu předmětu plnění a v souladu s požadavky platné české a evropské legislativy.

h) Na vyžádání poskytnout Objednateli report obsahující výsledky monitorování veškerých uživatelských a administrátorských aktivit a jiných událostí v rozsahu předmětu plnění, a to po celou dobu trvání smlouvy a do 2 let po jejím ukončení.

i) Zajistit sběr informací o provozních a bezpečnostních činnostech v rozsahu předmětu plnění a

ochranu získaných informací před jejich neoprávněným čtením nebo změnou.

j) Pro on-line transakce realizované prostřednictvím webových technologií implementovat TLS/SSL certifikáty s cílem zajistit jejich důvěrnost, integritu a identitu komunikujících protistran.

k) Veškeré neveřejné informace poskytnuté Objednatelem chránit vhodným šifrováním a proti neautorizovanému přístupu, a to zejména na mobilních zařízeních.

2. Poskytovatel bere na vědomí, že v případě, kdy technické spojení Objednatele s Poskytovatelem narušuje chod služeb Objednatele, může být toto spojení ihned ukončeno bez předchozího upozornění, pokud tato smlouva nestanoví jinak.

3. Poskytovatel bere na vědomí, že veškeré aktivity Poskytovatele a jeho plnění realizované v prostředí Objednatele jsou monitorovány a vyhodnocovány v rozsahu předměty plnění a v souladu s interními dokumenty Objednatele, se kterými byl Poskytovatel seznámen.