Společnost: **Next Generation Security Solutions s.r.o.**

IČO: 062 91 031

DIČ: CZ06291031

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

Zastoupená: Mgr. Ondřejem Dedkem, jednatelem

Bankovní spojení: ČSOB, a.s.

Číslo účtu: 301 607 295/0300

Zapsaná v obchodním rejstříku Městského soudu v Praze, oddíl C, vložka 279627

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: 35-3525450227/0100

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, implementaci a podpoře software**

dále jen „smlouva“

# Úvodní ustanovení

## Objednatel má zájem na zvýšení své kybernetické bezpečnosti, a to prostřednictvím dodávek software nástrojů.

## 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.

## 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 *„***Rozvoj kybernetické bezpečnosti Klaudiánovy nemocnice – SIEM*“*** (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.

## 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.

## 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.

## 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“).

# Předmět smlouvy

## Předmětem této smlouvy je závazek poskytovatele dodat a implementovat objednateli komplexní řešení systému Security Information and Event Management (SIEM) včetně veškerých činností a komponent potřebných pro jeho implementaci a provoz v prostředí Oblastní nemocnice v Mladé Boleslavi (Klaudiánova nemocnice) (dále jen souhrnně „**Software**“), zajištění školení pro administrátory včetně příslušné produktové dokumentace, včetně dokumentace skutečného provedení zakázky, a zajištění základní 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.

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

# Dodávka a implementace Software

## Poskytovatel v rámci dodávky a implementace Software provede následující:

## analýza aktuálního stavu

## doprava a implementace (instalace a konfigurace) SW/appliance na místě určení v rámci jednoho datového centra včetně integrace se zdroji

## ekologická likvidace obalového materiálu

## úvodní inicializace dodaných SW/appliance

## Zaškolení ICT administrátorů objednatele 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

## pilotní provoz o délce 1 měsíc (zajištění vzdáleného dohledu a spolupráce na řešení jednotlivých událostí a incidentů v rozsahu 5x8 v pracovní době od 8:00 do 16:00)

## 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.

## 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.

## 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.

# Zajištění základní podpory Software

## Poskytovatel se zavazuje zajistit základní podporu Software, a to po dobu 5 let od okamžiku převzetí řádně implementovaného (po splnění všech podmínek dodávky a implementace vč. pilotního provozu) 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 být v plném rozsahu pokrytí garantovaná dodavatelem nabízené položky. Minimální rozsah základní podpory je specifikován takto:

## přístup k opravným balíčkům,

## pravidelná profylaxe SW (prevence havárií a dalších mimořádných událostí),

## kontrola funkcí SW,

## úprava IS dle legislativních změn,

## aktualizace a upgrade SW,

## optimalizace, identifikace výkonnostních problémů apod.,

## další preventivní činnosti,

## provoz hotline,

## aktualizace dodané provozní dokumentace.

## Pro hlášení požadavků je poskytovatel povinen zajistit provoz telefonické hotline a helpdeskové aplikace v režimu nejméně 5x8, s pracovní dobou nejméně od 8:00 hod do 16:00 hod., 5 dní v týdnu, součástí helpdeskové aplikace musí být reporting o průběhu řešení požadavků.

## 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.

# Doba, místo a plnění

## Poskytovatel se zavazuje dodat a implementovat Software nejpozději do 3 měsíců od nabytí účinnosti této smlouvy. Podrobný harmonogram realizace jednotlivých kroků bude dohodnut zástupci smluvních stran po podpisu této smlouvy. Podpora bude poskytována po dobu uvedenou v této smlouvě.

## 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.

## 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.

## 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.

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

## 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.

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

## 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.

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

# Cena, licenční poplatky a platební podmínky

## 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** | xxx,00 | 1 | xxx,00 Kč |
| **Cena za 1 rok základní podpory** | xxx,00 | 5 | xxx,00 Kč |
| **Celková cena v Kč bez DPH** | | | **3 219 000,00 Kč** |

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

## 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.

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

## 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.

## Poskytovatel je oprávněn vystavit fakturu za základní 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.

## 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.

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

## Objednatel neposkytuje zálohové platby.

## Převezme-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.

## 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.

# Práva a povinnosti smluvních stran

## Poskytovatel je povinen realizovat dodávku a implementaci Software, včetně podpory, 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.

## 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.

## 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.

## 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.

## 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.

## 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.

## 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.

## 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.

## 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.

## 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.

## 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.

## Instalace a implementace Software, jakož i základní 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.

# Odpovědnost za vady

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

## 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.

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

## právo na bezplatné odstranění vad,

## právo na přiměřenou slevu z ceny,

## 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.

# Ochrana osobních údajů, důvěrné informace

## 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) 2016/679, 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.

## 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.

## 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.

## 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.

## 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.

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

## 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.

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

## je-li přístup k takovýmto souborům chráněn heslem nebo,

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

## 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.

## 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.

## Povinnost ochrany důvěrných informací se nevztahuje na informace, které:

## mohou být zveřejněny bez porušení této smlouvy,

## byly písemným souhlasem dotčené smluvní strany zproštěny těchto omezení,

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

## příjemce je zná dříve, než mu je předá druhá smluvní strana,

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

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

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

## 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.

# Sankční ujednání

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

## 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,

## 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,

## při prodlení poskytovatele s odstraněním vad či nedodělků Software uvedených v akceptačním protokolu, smluvní pokutu ve výši 3.000,- Kč za každý i započatý den prodlení, to za každou vadu či nedodělek zvlášť,

* + 1. při porušení povinnosti poskytovatele uvedené v čl. 4 odst. 4.1. až 4.3. této smlouvy, smluvní pokutu ve výši 10.000,- Kč za každý jednotlivý případ zvlášť, a to i opakovaně,

## při porušení povinnosti poskytovatele uvedené v čl. 7 této smlouvy, smluvní pokutu ve výši 50.000,- Kč za každý jednotlivý případ zvlášť, a to i opakovaně,

## 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,

## 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.

## 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.

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

# Pověřené osoby

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

## Jméno a příjmení: xxx

## tel: xxx

## email: xxx

Pověřenou osobou ve věcech plnění této smlouvy na straně objednatele ve věcech

## technických je:

## Jméno a příjmení: xxx

tel: xxx

email: xxx

## Pověřenou osobou ve věcech plnění této smlouvy na straně poskytovatele ve věcech smluvních

## Jméno a příjmení: xxx

## tel: xxx

## email: [xxx](mailto:odedek@ngss.cz)

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

## Jméno a příjmení: xxx

## tel: xxx

## email: [xxx](mailto:rnavratil@ngss.cz)

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

# Samostatné ujednání – registr smluv

## 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.

## 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.

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

## 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.

# Závěrečná ustanovení

## 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.

## 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 se jí z jakéhokoliv důvodu doručit.

## 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.

## 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.

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

## 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.

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

## 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.

## Nedílnou součástí této smlouvy jsou následující přílohy:

## Příloha č. 1 – Technická specifikace předmětu plnění

## Příloha č. 2 - Požadavky na zajištění kybernetické bezpečnosti

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

|  |  |
| --- | --- |
| Podepsáno elektronicky | Podepsáno elektronicky |
| ……………………………………………….  **Next Generation Security Solutions s.r.o.**  Mgr. Ondřej Dedek  jednatel | ……………………………………………….  **Oblastní nemocnice Mladá Boleslav, a.s., nemocnice Středočeského kraje**  JUDr. Ladislav Řípa  předseda představenstva |
|  | ……………………………………………….  **Oblastní nemocnice Mladá Boleslav, a.s., nemocnice Středočeského kraje**  Mgr. Daniel Marek  místopředseda představenstva |

Příloha č. 1

**Technická specifikace předmětu plnění**

**Oblast SIEM řešení**

|  |
| --- |
| **Technická specifikace nabízeného zařízení** |
| Řešení musí v rámci licence podporovat zpracování 1000 EPS s možností rozšíření až na 10000 EPS a 10 000 flows (síťových toků) za minutu | Ano |
| Řešení musí mít schopnost uchovat nejméně 6 TB dat (v komprimovaném formátu), aniž by vyžadovalo použití externích paměťových zařízení | Ano |
| Minimální administrace /výběr zařízení ze seznamu od výrobce/pro připojení dalších zdrojů událostí (např. servery Windows, Unix/Linux, switch, routery) | Ano |
| Sběr log záznamů z prostředí Windows a Linux/Unix. Sběr Windows EVT záznamů i z Windows Server | Ano |
| Sběr logů z dalších bezpečnostních a síťových systémů | Ano |
| Počet zdrojů pro sběr logů minimálně 40 000 | Ano |
| Řešení musí být dodáno jako virtual all-in-one | Ano |
| Řešení musí podporovat protokoly: Syslog, Windows Events Collection (WinRM/ RPC), FTP, S/TP/SCP, SNMP, ODBC/JDBC, log file protokol | Ano |
| Řešení musí umožňovat bez-agentový sběr logů (sběr bez nutnosti instalovat agenta na cílový systém) | Ano |
| Řešení musí umožňovat sběru logů lokálním kolektorem s přeposíláním do SIEMu | Ano |
| Řešení musí podporovat možnost záložního uložení logů (rozšiřitelné úložiště neodpovídá tomuto požadavku) | Ano |
| Řešení má centrální management všech komponent a administrativních funkcí ve webovém uživatelském rozhraní | Ano |
| Řešení musí umožňovat definovat uživatelům SIEMu přístup k jednotlivým zařízením, jejich skupinám či síťovým segmentům | Ano |
| Řešení musí podporovat automatickou identifikaci systémů – zdrojů logů | Ano |
| Řešení musí podporovat šifrovanou komunikaci mezi zdroji logů a SIEM | Ano |
| Řešení musí umožňovat integraci s adresářovým systémem (LDAP, Active Directory) pro potřeby autentizace uživatelů | Ano |
| Log Management s minimální postimplementační administrací. /agregace událostí dle typů, analýza, vyhodnocování/ pro případy jako je zavedení nového zdroje událostí, nastavení pravidel pro sběr dat a archiv událostí | Ano |
| Řešení musí umožňovat automatické aktualizace | Ano |
| Řešení poskytuje webové uživatelské rozhraní pro management, analýzu a reporting | Ano |
| Řešení musí poskytovat automatický backup proces | Ano |
| Řešení musí poskytovat interní kontroly stavu zařízení (healthcheck) a upozornění uživatele v případě problému | Ano |
| Řešení musí poskytovat analytické a korelační funkce bez dalších zásahů a činností (out-of-the-box) | Ano |
| Řešení musí být volně výkonově rozšiřitelné. | Ano |
| Řešení musí umožňovat rozšíření výběrů o uživatelské položky z obsahu logů | Ano |
| Řešení musí zajišťovat integritu nasbíraných dat | Ano |
| Řešení umožňuje nárůst zdrojů událostí bez nutnosti pořizování dalšího hardware | Ano |
| Řešení musí poskytovat Near-real-time analýzu událostí | Ano |
| Řešení poskytuje analýzu dlouhodobých trendů událostí | Ano |
| Řešení musí umožňovat agregaci události z logů i podle položek které nejsou standardně zahrnuty v řešení | Ano |
| Řešení musí podporovat normalizaci časových značek z různých časových zón | Ano |
| Řešení musí podporovat sběr textových logů ze souborů | Ano |
| Způsob zadávání vyhledávání: Vyhledávací rozhraní systému správy logů musí poskytovat podporu jak pro zadání dotazu s použitím Booleovy logiky, tak pro regulární výrazy | Ano |
| Řešení musí poskytovat alertování na detekované anomálie, změny chování sítě a změny v generování logů a událostí. | Ano |
| Řešení musí poskytnout alerting vycházející z detekovaných bezpečnostních hrozeb od monitorovaných zařízení. | Ano |
| Řešení musí podporovat rozšíření o alerting porušení bezpečnostních pravidel, založený na stanovené bezpečnostní politice | Ano |
| Řešení musí umožňovat kombinované hledání v indexovaných i neindexovaných datech v systému správy logů s použitím regulárních výrazů a fulltextového vyhledávání v nestrukturovaném textu současně | Ano |
| Korelační modul musí poskytovat již po instalaci (out-of-the-box) metody korelačních pravidel, která automatizují zjišťování incidentů a související workflow procesy | Ano |
| Řešení musí podporovat korelaci mezi zařízeními již po instalaci (out-of-the-box). Zjišťování chyb autentizace, chování perimetru a výskytu červů bez potřeby specifikovat typy sledovaných zařízení | Ano |
| Řešení musí podporovat vykonávání akci v závislosti na přijatém logu jako např. zaslat email, notifikaci nebo spustit předem definovaný skript | Ano |
| Řešení musí umožňovat pracovat s IP geolokacemi (botnet kanály atp.) | Ano |
| Řešení musí podporovat generování alertů při výpadku logů z konkrétního zařízení | Ano |
| Řešení musí obsahovat vestavěný mechanismus na klasifikaci systémů podle typu (např. mail server vs. databázový server) | Ano |
| Řešení umožňuje vyhodnocení chybějících sekvencí (např. služba přestala běžet) | Ano |
| Řešení musí podporovat schopnost monitorovat historii útoků (typů událostí) na kritické komponenty a historii útoků jednotlivých uživatelů v případě rozšíření o sledování síťových toků | Ano |
| Řešení musí podporovat schopnost korelovat události DHCP, VPN a Active Directory a sledovat průběh uživatelské relace (session) v rámci celé instituce (přesná identifikace uživatele) v případě rozšíření o sledování síťových toků | Ano |
| Řešení musí podporovat schopnost korelovat data o událostech se statickými a dynamickými seznamy označujícími položky, které mají či nemají být v síti povoleny (tj. seznam nezabezpečených protokolů) v případě rozšíření o sledování síťových toků | Ano |
| Řešení musí poskytovat rozhraní pro reporting, pomocí kterého lze vytvářet nové sestavy bez nutnosti sestavovat SQL dotazy | Ano |
| Řešení musí podporovat nezměněnou funkcionalitu reportingu i při změně nebo náhradě některé technologie jako např. firewallu nebo IDS | Ano |
| Řešení musí být rozšiřitelné o funkci sledování síťové komunikace (síťové toky) pomocí rozšíření licence | Ano |
| Nabízené řešení musí poskytovat webové uživatelské rozhraní pro správu, analýzy, reportovaní a podobně. Rozhraní by nemělo obsahovat pluginy nebo být založeno na technologiích Java, Flash nebo na bázi tlustého klienta. | Ano |
| Řešení musí obsahovat nativní podporu vysoké dostupnosti (HA) bez rozšiřujících komponent/software třetích stran. | Ano |
| HA musí být možné připojit v jakékoliv fázi, bez nutnosti reinstalace a celého řešení. | Ano |
| Nabízené řešení musí poskytovat automatické aktualizace řešení bez pomoci profesionálních služeb vendora. | Ano |
| Některá zařízení v síti často mění svou IP adresu. Nabízené řešení musí být schopno udržet databázi zařízení konzistentní i v těchto případech. Popište, jak řešení splňuje tento požadavek. | Ano |
| Řešení musí nabízet přístup k datům skrze otevřené REST API pro integraci s dalšími systémy. Popište, jak řešení splňuje tento požadavek. | Ano |
| Řešení musí být navrženo tak, aby bylo schopno pracovat s interními překrývajícími se rozsahy adres spolu se síťovými toky, událostmi a zařízeními v síti. Popište, jak řešení splňuje tento požadavek. | Ano |
| Řešení musí uchovávat logy jak v normalizovaném formátu, tak i v „raw“ formátu. | Ano |
| Řešení nebude licenčně omezeno počtem používaných korelačních pravidel. | Ano |
| Řešení nebude licenčně omezeno počtem generovaných reportů | Ano |
| Systém disponuje prostředky pro zobrazení aktuálních provozních informací o infrastruktuře a prostředky pro zobrazení reportů pro podporu řízení. | Pro zobrazení aktuálních provozních informací je využita kombinace nástrojů PostgreSQL/Grafana. Pro tvorbu a reportování statistických informací pro podporu řízení je využit nástroj PowerBI. |
| Systém musí zobrazovat stav monitorovaných celků se zpožděním maximálně v řádu jednotek vteřin. | Nástroj je závislý na zdroji informací, tedy systémech, které provádí samotné měření. Od získání těchto dat, jsou přehledy dostupné v řádu vteřin. Data jsou načítána přehledovými grafy v okamžik jejich zobrazení. |
| Vyhodnocené údaje jsou ukládány do datového skladu a slouží jako podklad pro statistické vyhodnocení provozu. | Naměřené hodnoty jsou jednou denně přeneseny do datového skladu. Ten slouží jako podklad pro PowerBI reporty. |
| Architektura systému umožňuje vyvinout a integrovat datový konektor na nové datové zdroje. | Systém disponuje mechanismem datových konektorů na kterých je zbytek systému nezávislý. Tyto konektory transformují specifická data od jednotlivých systémů do interního formátu systému. |
| Systém umožňuje nastavit oprávnění na čtení a zápis na složky, do kterých jsou organizovány provozní přehledy a manažerské reporty. | Systém umožňuje vybraným uživatelům z uživatelského rozhraní zobrazit dialog pro přiřazení oprávnění do složek. |
| Systém lze konfigurovat z uživatelského webového rozhraní bez nutnosti zásahů na straně serveru. | Ano, systém lze konfigurovat z uživatelského rozhraní v modulu "Nastavení systému". |
| Systém umožňuje načítat a synchronizovat uživatelské účty a uživatelské skupiny z MS Active Directory a autentizovat tyto uživatele proti MS AD | Systém disponuje plnou integrací na MS Active Directory. |
| Systém umožňuje nastavit oprávnění na čtení a zápis na složky, do kterých jsou organizovány provozní přehledy a manažerské reporty. | Systém umožňuje vybraným uživatelům z uživatelského rozhraní zobrazit dialog pro přiřazení oprávnění do složek. |

## **Způsob řešení platformy pro SIEM**

**xxx**

Příloha č. 2

**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:

1. 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.
2. Na základě bezpečnostních potřeb a výsledků hodnocení rizik zavést příslušná bezpečnostní opatření v rozsahu poskytovaného předmětu plnění, monitorovat je, vyhodnocovat jejich účinnost.
3. 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.
4. 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.
5. Stanovit a udržovat aktuální opatření bezpečnosti ve formě procesů a technologií, které zajišťují naplnění bezpečnostní politiky.
6. **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:

1. 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.
2. **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:

1. Řídit vlastní rizika, která mohou ovlivnit poskytování předmětu plnění.
2. V minimálním intervalu 1x ročně vytvořit a předložit Zprávu o řízení kybernetických rizik, která bude minimálně pokrývat:
3. Vyhodnocení stavu kybernetické bezpečnosti za hodnocený rok
4. Identifikaci a hodnocení rizik s vazbou na předmět plnění
5. Realizovaná bezpečnostní opatření
6. Nepokrytá bezpečnostní rizika a návrh opatření
7. Vyhodnocení bezpečnostních událostí a incidentů
8. Aktuální stav souladu Poskytovatele s těmito Kybernetickými požadavky
9. **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:

1. 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.
2. 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.
3. **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:

1. 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.
2. 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.
3. **Bezpečnost lidských zdrojů**
4. 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:
5. 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.
6. 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.
7. 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.
8. 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:
9. Pro uložení a sdíleni dat a informací Objednatele využívaly pouze k tomu schválené prostředky (aktiva);
10. Neukládaly ani nesdílely data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno Objednatele;
11. Nestahovaly, nesdílely, neukládaly, nearchivovaly ani neinstalovaly datové a spustitelné soubory v rozporu s licenčními podmínkami nebo autorským zákonem;
12. Nenavštěvovaly internetové stránky s eticky nevhodným obsahem;
13. Nerealizovaly pokusy o neautorizovaný přístup ke zdrojům Objednatele ani ke zdrojům jiných subjektů;
14. 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;
15. Nepodílely se s prostředky Objednatele na šíření spamu ani škodlivého softwaru.
16. 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.
17. **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:

1. Zajistit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování předmětu plnění.
2. Na vyžádání poskytnout Objednateli přehled, report, či jinou adekvátní informaci o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře.
3. 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.
4. **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:

1. Přiměřeně reagovat na změny na straně Objednatele a upravit na své straně technická a organizační opatření tak, aby odpovídala novému stavu po provedení změny.
2. Aktivně spolupracovat při testování významné změny.
3. **Řízení přístupu**
4. 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:
5. Přidělovat oprávnění svým jednotlivým pracovníkům ve smyslu oprávnění k výkonu činností tak, aby byla minimalizována rizika nežádoucího přístupu k aktivům Objednatele.
6. 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.
7. 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).
8. 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.
9. Průběžně kontrolovat a vyhodnocovat oprávněnost a potřebu přístupu, jak fyzického, tak i logického, u všech osob na straně Poskytovatele, které přistupují do prostředí Objednatele.
10. 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.
11. Poskytovatel bere na vědomí, že přidělení oprávnění zaměstnanci Poskytovatele musí být řízeno principem nezbytného minima a není nárokové.
12. 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).
13. **Akvizice, vývoj a údržba**
14. 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:
15. Zajistit bezpečnou implementaci, inovaci, aktualizaci a testování technologií, které jsou předmětem plnění.
16. Předat Objednateli dokumentaci předmětu plnění minimálně v následujícím rozsahu:
17. dokumentaci všech bezpečnostních nastavení, funkcí a mechanismů,
18. dokumentaci obsahující popis autorizačního konceptu a oprávnění,
19. dokumentaci obsahující instalační a konfigurační postupy.
20. V případě, že předmět plnění zahrnuje vývoj softwaru, zavazuje se Poskytovatel:
21. Dodržovat a implementovat nejlepší praktiky pro bezpečný vývoj softwaru definované na základě smluvního vztahu.
22. 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.
23. 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.
24. 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.).
25. 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.
26. Zajistit bezpečnost testovacího prostředí u Poskytovatele a ochranu poskytnutých testovacích dat Objednatelem.
27. Zajistit, že do produkčního prostředí Objednatele bude dodán jen předmětem smlouvy specifikovaný kompilovaný, respektive spustitelný kód a další nezbytná data pro provozování předmětu plnění.
28. Zajistit, že v rámci poskytovaného plnění bude dodávaný software
29. v souladu s bezpečnostními politikami a standardy Objednatele
30. otestován na soulad s bezpečnostními politikami Objednatele (platí pro Poskytovatele, pokud byl s takovými bezpečnostními politikami seznámen)
31. Instalovat software pouze na základě Objednatelem předem schválených migračních postupů.
32. 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.
33. **Zvládání kybernetických bezpečnostních událostí a incidentů**
34. 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:
35. Stanovit a popsat na své straně činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání bezpečnostních incidentů.
36. 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.
37. Vyhodnocovat informace o bezpečnostních incidentech a uchovávat je pro budoucí použití s ohledem na požadavky platné české a evropské legislativy.
38. 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.
39. Bez zbytečného odkladu a po dohodě s Objednatelem realizovat opatření požadovaná Objednatelem v dohodnutých termínech ke snížení dopadu bezpečnostního incidentu nebo zamezení pokračování incidentu.
40. 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.
41. 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.
42. **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:

1. Zajistit adekvátní kontinuitu svých aktiv, které jsou potřebné k poskytování předmětu plnění.
2. Pravidelně kontrolovat a testovat, že je schopen kontinuitu aktiv zajistit dle sjednané úrovně služeb.
3. **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.

1. **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:

1. 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.
2. 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.
3. **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:

1. Realizovat bezpečnostní opatření pro odstranění nebo blokování síťového spojení/síťových spojení, které/která neodpovídají požadavkům na ochranu integrity komunikační sítě.
2. Realizovat přístup z mobilního zařízení do prostředí Objednatele pouze prostřednictvím zabezpečeného připojení virtuální privátní sítě (VPN) nebo zvolit adekvátní technické opatření.
3. 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.
4. 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.
5. Na aktiva Objednatele neinstalovat a nepoužívat v prostředí Objednatele tyto typy nástrojů, pokud nejsou součástí předmětu plnění:
6. Keylogger - software nebo hardware, který neautorizované zaznamenává stisky kláves s cílem narušit důvěrnost zadávaných dat a informací.
7. Sniffer - software nebo hardware umožňující odposlouchávání síťového provozu.
8. 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.
9. Backdoor - skrytý softwarový nebo hardwarový nástroj, který umožňuje obejití schválených autentizačních procedur, instalovaný s cílem budoucího snadnějšího a neautorizovaného přístupu do systému ICT.
10. Malware a jiný škodlivý software, který narušuje, obchází či jinak omezuje bezpečnostní opatření v prostředí Objednatele.
11. Připojovat do prostředí Objednatele pouze zařízení ICT, která jsou chráněna proti malware a jinému škodlivému softwaru, pokud to jejich technologie umožňuje.
12. 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.
13. 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.
14. Zajistit sběr informací o provozních a bezpečnostních činnostech v rozsahu předmětu plnění a ochranu získaných informací před jejich neoprávněným čtením nebo změnou.
15. Pro on-line transakce realizované prostřednictvím webových technologií implementovat TLS/SSL certifikáty s cílem zajistit jejich důvěrnost, integritu a identitu komunikujících protistran.
16. Veškeré neveřejné informace poskytnuté Objednatelem chránit vhodným šifrováním a proti neautorizovanému přístupu, a to zejména na mobilních zařízeních.
17. 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.
18. 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.