SMLOUVA – ŘEŠENÍ ZAJIŠŤUJÍCÍ VYROVNÁVÁNÍ ZATÍŽENÍ PRO DISTRIBUCI SÍŤOVÉHO NEBO APLIKAČNÍHO PROVOZU S INTELIGENTNÍ SPRÁVOU SÍŤOVÉHO PROVOZU – BALANCER S WEBOVÝM APLIKAČNÍM FILTREM

Simac Technik ČR, a.s.
zapsána v obchodním rejstříku vedeném Městským soudem v Praze oddíl B, vložka 3190
se sídlem: Radlická 740/113c, 158 00, Praha 5
IČ: 63079496 DIČ: CZ63079496
zastoupena: Ing. Dušan Bruoth, předseda představenstva
Ing. Martin Jireček, člen představenstva
Ing. Jaroslav Štefl, člen představenstva
Ing. Ivo Němeček, člen představenstva
Jménem společnosti jednají vždy dva členové představenstva společně.

bankovní spojení: ČSOB
číslo účtu: 8010-616133653/0300

jako **dodavatel** na straně jedné (dále jen „dodavatel")

a

Všeobecná fakultní nemocnice v Praze
se sídlem: U Nemocnice 499/2, 128 08 Praha 2
IČ: 000 64 165 DIČ: CZ00064165
zastoupena: prof. MUDr. Davidem Feltlem, Ph.D., MBA, ředitelem
bankovní spojení: ČNB
číslo účtu: 24035021/0710

jako **objednatel** na straně druhé (dále jen „objednatel")

Dodavatel a objednatel společně též jako „smluvní strany"

uzavírají dnešního dne na základě výsledku **nadlimitní veřejné zakázky** s názvem „**Implementace balanceru s webovým aplikačním filtrem**", **vyhlášené otevřeným řízením** dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „z. č. 134/2016 Sb.") a zveřejněné ve Věstníku veřejných zakázek. pod ev. č. Z2024-041434 ze dne 28.08.2024 **a uveřejněna na profilu zadavatele pod ID veřejné zakázky VZ0197998 ze dne 28.8.2024** (dále jen „veřejná zakázka"), v souladu s ustanovením § 1746 odst. 2., zákona č. 89/2012 Sb., občanský zákoník, v platném znění, (dále jen „zákon č. 89/2012 Sb."), tuto smlouvu (dále jen „smlouva")

Preambule

Realizace předmětu plnění je spolufinancována Evropskou unií z prostředků Nástroje pro oživení a odolnost (RRF) prostřednictvím Národního plánu obnovy ČR z výzvy č. 25 (předem definovaný projekt, komponenta 1. 2 Digitální systémy veřejné správy, Investice 3: Kybernetická bezpečnost).

I. Předmět smlouvy

1. Předmětem plnění dle této smlouvy je dodávka na dodání řešení zajišťující vyrovnávání zatížení pro distribuci síťového nebo aplikačního provozu s inteligentní správou síťového provozu - balancer s webovým aplikačním filtrem (Hardwarové řešení F5 BIG-IP r2600 v HA konfiguraci s moduly LTM AWAF a APMa licencí pro BIG-IP Intelligence) jako HW appliance v režimu high availability (HA) včetně veškerého SW nezbytného pro provoz HW appliance dle minimálních funkčních a technických požadavků objednatele uvedených v příloze č. 2 této smlouvy (dále také „řešení" nebo „předmět plnění").

Nedílnou součástí předmětu plnění je:

a) **provedení předimplementační analýzy**, která bude obsahovat vypracovaný detailní technický popis cílového stavu, vypracovaný implementační postup a způsob ověření funkčnosti řešení.

V rámci předimplementační analýzy budou navrženy nebo definovány tyto oblasti řešení:

- detailní technický popis cílového stavu:
  - architektura řešení,
  - požadavky na infrastrukturu,
  - způsob integrace,
  - nezbytné součinnosti objednatele,
- implementační postup a harmonogram,
- požadavky na součinnost objednatele v jednotlivých etapách implementace,
- způsob zaškolení,
- způsob ověření funkčnosti prostřednictvím:
  - testovacího provozu,
  - požadavky na pilotní provoz,
- testovací scénáře pro akceptační testy,
- podmínky spuštění do produkčního prostředí.

b) **dodání HW (Appliance)** včetně veškerého SW nezbytného pro provoz HW appliance dle minimálních funkčních a technických požadavků objednatele uvedených v příloze č. 2 této smlouvy, tj. jeho montáž, instalace HW, základní konfigurace a zprovoznění v režimu vysoké dostupnosti (dále také „HA"), předání souvisejících dokladů a včetně všech komponent potřebných pro připojení k síti objednatele.

c) **implementační práce, které obsahují:**

- instalaci a případnou konfiguraci,
- systémovou konfiguraci,
- integraci do technologického prostředí objednatele,
- konfiguraci systému:
  - konfiguraci 10 WAF politik
  - konfiguraci APM

d) **dodání technické, provozní a administrátorské dokumentace:**
Dodavatel vypracuje a předá podrobnou dokumentaci k řešení v CZ (českém) jazyce, zahrnující popis nebo postupy minimálně pro tyto oblasti:

- Technická dokumentace – popis architektury, systémů, konfigurací, nastavení a integrace řešení,
- Provozní dokumentace – návody a postupy k správě řešení od její údržby, přes zálohování a záchranné mechanismy až po postupy obnovy při havárii,
- Uživatelská příručka pro administrátory.

e) **zaškolení administrátorů**
Zajištění školení dodavatelem pro dodané řešení v rozsahu provozní a administrátorské dokumentace pro zaměstnance objednatele (min. 7 zaměstnanců objednatele).

f) **spuštění testovacího a pilotního provozu**
Před překlopením do produkčního provozu dodavatel provede v rámci testovacího nebo pilotního provozu ověření základní funkčnosti řešení dle požadavků objednatele s aktivní podporou dodavatele prostřednictvím specialisty na místě nebo jeho online reakcí (např. Teams, Skype) na případné kolize nebo nejasnosti po celou dobu testovacího/pilotního provozu.
Zjištěné kolize nebo nesoulady ve funkčnosti (závady) jsou po ukončení testovacího anebo pilotního provozu dodavatelem odstraněny a případně zaneseny do zpracované dokumentace. Bez odstranění zjištěných závad nelze zahájit akceptační testy.

g) **akceptační testy**
Akceptační testy budou provedeny dle objednatelem připravených testovacích scénářů. Akceptační testy pokrývají požadované funkčnosti definované v požadavcích na řešení. Úspěšná akceptace je podmíněna následujícími podmínkami (kritéria):

- výsledky scénářů nesmí obsahovat žádné vady – Akceptace bez výhrad
- výsledky scénářů obsahují vady – Akceptace s výhradou
  - žádné podstatné vady typu A
  - maximálně 2 vady méně závažného typu B
  - maximálně 7 vad ostatního typu C
- při překročení jakékoli z vad typu A nebo B anebo C uvedených v předchozím bodě (Akceptace s výhradou) nebude řešení akceptováno.

<u>Vada typu A:</u>

- způsobuje, že systém neposkytuje některou z kritických funkcionalit řešení (řešení nesplňuje účel, pro který byl vytvořen, nebo uživatelé nemohou používat všechny používané funkcionality) nebo/a zároveň,
- činí zcela nefunkčním některou z komponent řešení nebo/a zároveň,
- způsobuje, že řešení vykazuje nepřiměřeně dlouhé odezvy nebo/a zároveň,

- řešení vykazuje nedostatek, kdy implementační projekt zjevně neobsahuje části sjednané smlouvou nebo zadávací dokumentací, či zcela chybí podstatná část řešení.

Vada typu B:
- způsobuje, že je systém schopen omezeného provozu nebo neposkytuje některou z nekritických funkcionalit (řešení splňuje účel, pro který byl vytvořen; uživatelé mohou používat všechny klíčové funkcionality) nebo/a zároveň;
- způsobuje, že některá z funkcionalit systému není plně činná nebo ztěžuje užívání u některého koncového uživatele, avšak tento stav má jen zanedbatelné dopady na provoz u objednatele nebo/a zároveň.

Vada typu C:
- jsou ostatní závady/incidenty, které nejsou typu „A" ani „B".

h) spuštění produkčního prostředí a provoz řešení
Na základě splnění akceptačních kritérií dle čl. I. odst. 1 písm. g) je řešení přeneseno objednatelem do produkčního prostředí v součinnosti s dodavatelem.

i) záruku a zajištění poskytování záručního servisu

j) služby na vyžádání
Služby na vyžádání technického specialisty nad rámec předmětu plnění, který je uveden v čl. I. odst. 1 písm. a) až i) této smlouvy budou realizovány v průběhu plnění této smlouvy na základě písemných objednávek objednatele, které budou zaslány na e-mailovou adresu kontaktní osoby dodavatele. Za písemnou formu se považuje rovněž její elektronická forma. Rozsah těchto služeb je sjednán na maximálně 40 MD po dobu platnosti záruky a záručního servisu v hodinové sazbě stanovené touto smlouvou.

Bližší specifikace předmětu plnění je uvedena v příloze č. 1 této smlouvy.

2. Vzhledem k tomu, že se dodávané řešení v okamžiku uvedení do produkčního provozu stává informačním systémem základní služby, poskytování zdravotních služeb dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále též „ZKB"), stává se i dodavatel řešení provozovatelem informačního systému základní služby v souladu s požadavky ZKB. Dodavatel bere na vědomí, že se v okamžiku podpisu smlouvy o dodávce řešení a služeb stává orgánem nebo osobou dle § 3 písm. f) ZKB.
3. Dodavatel rovněž bere na vědomí, že v době uzavření smlouvy nesmí být dodávané technické nebo programové prostředky označeny NÚKIB jako hrozba. Následně poskytované služby nesmí být provozované na technických nebo programových prostředcích označených NÚKIB jako hrozba.
4. Dodavatel je povinen neprodleně informovat objednatele prostřednictvím dodavatelem určené odpovědné osoby: Manažera kybernetické bezpečnosti, e-mail: xxxxx, o kybernetických bezpečnostních incidentech souvisejících s implementací nebo při zajištění záručního servisu dodávaného řešení.
5. Součástí předmětu plnění dle této smlouvy je rovněž zajištění záruky na dodaný předmět plnění dle podmínek uvedených v čl. III smlouvy. Dodavatel prohlašuje, že je certifikovaným partnerem výrobce, jehož produkty jsou předmětem plnění této smlouvy.
6. Dodavatel se zavazuje dodat zařízení specifikované v čl. I a příloze č. 1 této smlouvy a objednatel se zavazuje uhradit dodavateli cenu specifikovanou v čl. IV. této smlouvy.

II. Dodání předmětu plnění

1. Dodavatel se zavazuje dodat objednateli předmět plnění dle čl. I. a přílohy č. 1 této smlouvy **nejpozději do 180 kalendářních dnů od uzavření této smlouvy.**
2. Část předmětu plnění spočívající v dodání HW dle čl. I. odst. 1 písm. b) smlouvy (dále jen „HW") bude dodána do sídla objednatele. Předání dalších částí plnění bude uskutečněno dle dohody odpovědných zástupců smluvních stran.
3. Dodavatel bude informovat objednatele o přesném termínu dodávky HW i dalších částí plnění, a to nejméně 5 pracovních dní před realizací dodávky. Při předání a převzetí HW bude pověřenými osobami obou smluvních stran podepsán dodací list.

Kontaktní a odpovědná osoba za objednatele:

Za převzetí HW: xxxxx, tel.: xxxxx, e-mail: xxxxx
Za akceptaci předmětu plnění: xxxxx, tel.: xxxxx, e-mail: xxxxx
K nahlašování požadavků na záruční servis: xxxxx, tel.: xxxxx, e-mail: xxxxxx
Za identifikaci případného kybernetického útoku v průběhu plnění předmětu plnění dle této smlouvy: manažer KB, e-mail: xxxxx
Za ochranu osobních údajů: xxxxx

Kontaktní a odpovědná osoba za dodavatele:

Za předání HW: xxxxx, tel.: xxxxx, e-mail: xxxxx
Za akceptaci předmětu plnění: xxxxx, tel.: xxxxx, e-mail: xxxxx
K poskytování záručního servisu: xxxxx, tel: xxxxx, e-mail: xxxxx
Za identifikaci případného kybernetického útoku v průběhu plnění předmětu plnění dle této smlouvy: xxxxx, tel.: xxxxx, e-mail: xxxxx
Za ochranu osobních údajů: xxxxx, tel.: xxxxx, e-mail: xxxxx

4. Dodací list podepíší a opatří otisky razítek oprávnění zaměstnanci obou smluvních stran. Takto opatřený dodací list slouží jako doklad o řádném předání a převzetí HW (je nedílnou součástí akceptačního protokolu).
5. Okamžikem protokolárního předání a převzetí HW přechází na objednatele vlastnické právo HW a nebezpečí škody na HW. Objednatel není povinen převzít HW či jeho část, která je poškozena nebo která jinak nesplňuje podmínky této smlouvy, zejména pak jakost zařízení.
6. Dodavatel odpovídá za dodržení přepravních podmínek po dobu přepravy HW k objednateli, tak aby nebylo zařízení znehodnoceno. Předmět plnění (HW) bude dopraven do místa plnění na vlastní náklady a nebezpečí dodavatele.
7. Dodávka se považuje podle této smlouvy za splněnou, pokud:
    - byla objednatelem odsouhlasena předimplementační analýza,
    - předmět plnění (HW i SW) byl řádně doručen a naimplementován,
    - bylo objednateli předáno oficiální potvrzení lokálního zastoupení výrobce dodávaného HW o tom, že zařízení je nové, nepoužité a určené pro koncového zákazníka Všeobecná fakultní nemocnice v Praze,
    - bylo provedeno zaškolení administrátorů objednatele,
    - byla předána veškerá potřebná dokumentace,
    - byly provedeny akceptační testy,
    - předmět plnění byl řádně předán a převzat způsobem sjednaným níže,
    - byla provedena akceptace řádného předání a převzetí předmětu plnění včetně aktivace maintenance výrobce.
8. Po splnění a předání celého předmětu plnění vystaví dodavatel akceptační protokol, který bude obsahovat níže uvedené náležitosti:
    - název a sídlo dodavatele a objednatele,
    - číslo smlouvy,
    - datum řádného předání/převzetí předmětu plnění,
    - stav HW a SW v okamžiku jeho předání a převzetí,
    - akceptace či výhrady,
    - jiné náležitosti důležité pro předání a převzetí dodaného předmětu plnění.
9. Dodací list podepíší a opatří otisky razítek oprávnění zaměstnanci obou smluvních stran. Takto opatřený dodací list slouží jako doklad o řádném předání a převzetí zboží (HW) (je nedílnou součástí akceptačního protokolu).
10. Objednatel není povinen akceptovat předání a převzetí předmětu plnění v případě, že předmět plnění bude vykazovat vady a nedodělky. Pokud vada nebo nedodělek nebrání převzetí předmětu plnění smlouvy, musí být vždy uveden v akceptačním protokolu s uvedením data odstranění. Nebude-li objednatelem akceptováno předání a převzetí předmětu plnění z důvodů vad a nedodělků, bude o této skutečnosti sepsán zápis s výčtem zjištěných vad nebo nedodělků, které zjistil objednatel včetně způsobu a lhůt k jejich odstranění. Tento zápis bude současně podepsán zástupci obou smluvních stran.
11. Dodavatel je při plnění dle této smlouvy povinen postupovat v souladu s vnitřními předpisy objednatele, se kterými byl prokazatelně seznámen, zejména SM-UI-02 Používání sítě VFN externími uživateli.
12. Dodavatel se zavazuje splňovat/dodržet relevantní požadavky na řízení bezpečnosti informací uvedené v příloze č. 5 této smlouvy „Požadavky systému řízení bezpečnosti informací na Dodavatele" vztahující se na prostředí a činnosti dodavatele.

III. Způsob poskytování záruky

1. Dodavatel se zavazuje zajistit záruku včetně záručního servisu u dodaného předmětu plnění dle čl. I. a přílohy č. 1 této smlouvy po dobu 60 měsíců ode dne předání a převzetí celého předmětu plnění.
2. Záruční servis předmětu plnění obsahuje:
    - odstraňování vad, součinnost s výrobcem,
    - poskytování aktualizací programových prostředků (nové verze, opravné verze, bezpečnostní záplaty),
    - soulad se zákony a normativy ČR a EU,
    - odstranění zjištěných zranitelností (penetrační testy, hrozba nebo opatření NÚKIB, výrobce nebo veřejně zdokumentovaných),
    - pomoc při řešení provozních problémů,
    - podpora na místě při implementaci aktualizací programových prostředků, a to na základě výzvy objednatele,
    - záruční servis v režimu 24x7 s reakční dobou uvedenou v čl. III odst. 4 této smlouvy.

3. K zajištění elektronické komunikace mezi objednatelem a dodavatelem je určen helpdeskový nástroj objednatele ServiceDesk VFN. V tomto nástroji budou probíhat hlášení událostí, které bude dodavatel řešit podle kategorie, závažnosti a úrovni dostupnosti služeb (SLA). Za tímto účelem bude určeným pracovníkům dodavatele zřízen přístup do ServiceDesku objednatele. Pokud má dodavatel k dispozici svůj interní helpdeskový nástroj, je také možné provést jeho integraci s nástrojem objednatele.
   V případě technických potíží, které zabraňují objednateli komunikovat s dodavatelem prostřednictvím ServiceDesku objednatele dle předchozího odstavce, lze požadavky odeslat formou elektronické pošty na určenou emailovou adresu dodavatele xxxxx. Tato komunikace má z hlediska úrovně služeb stejnou váhu jako komunikace v ServiceDesku objednatele. Pro operativní komunikaci mezi objednatelem a dodavatelem bude zřízena telefonní Hot Line dodavatele na určeném telefonním čísle **xxxxx**.

4. V rámci záručního servisu se dodavatel zavazuje poskytovat/zajistit:
    - služby potřebné pro zajištění bezproblémového běhu řešení, včetně drobného rozvoje, který je spjatý zejména s konfiguračními změnami. Pro zajištění záručního servisu bude dodavateli umožněn vzdálený přístup formou VPN.
    - služby potřebné pro bezchybný běžný provoz řešení. Hlavní úlohou je zajištění bezvýpadkového provozu řešení, realizace proaktivních činností, kterými se bude výpadkům předcházet a v případě výpadku uvedení řešení do provozního stavu.
    - na všechny použité technologie, které jsou součástí dodávky, zajistit záruku výrobce obsahující právo instalace nových verzí po celou dobu záruční doby.

5. Součástí záručního servisu je zajištění funkčnosti provozu řešení v režimu 24 hodin denně, 7 dní v týdnu (dále též „24x7") při dostupnosti 99,86 % s následujícími parametry služby:

Úroveň závady	Parametry služby		
	Provozní doba služby Hot-line	Maximální reakční doba od nahlášení požadavku:	Maximální doba odstranění závady
Havárie*	24x7	do 2 hodin	do 24 hodin
Porucha**	24x7	do 8 hodin	do 48 hodin
Chyba***	24x7	do 48 hodin	do 120 hodin

Maximální reakční doba na odstranění závady se počítá od okamžiku zadání hlášení závady objednatelem do systému Helpdesk objednatele.
Do doby na odstranění závady se nezapočítává doba, po kterou jsou dodávány doplňující či upřesňující informace nutné pro řešení objednatelem.
Řešení chyb a provozních problémů není omezeno počtem hodin / měsíc.

Kategorie incidentů/závad
Za závadu nebo incident je považována jakákoliv událost, která narušuje nebo by mohla narušit funkčnost dodaného plnění. Tyto události jsou reprezentovány servisním záznamem se stanovenou závažností. Za incident se nepovažuje porucha způsobená vyšší mocí, tj. živelnou pohromou, válečným konfliktem nebo teroristickým útokem anebo jinými podobnými událostmi, jež nastaly nezávisle na vůli dodavatele a brání mu ve splnění jeho povinností, jestliže nelze rozumně předpokládat, že by dodavatel tuto překážku nebo její následky odvrátil nebo překonal a dále, že by v době vzniku závazku tuto překážku předvídal.
Za závadu nebo incident se nepovažuje výpadek systému způsobený závadou HW objednatele.

Pro účely této smlouvy jsou definovány následující úrovně závad:

***Havárie:** Havárií se rozumí stav, který:
- způsobuje, že systém neposkytuje některou z kritických funkcionalit systému (systém nesplňuje účel, pro který byl vytvořen, nebo uživatelé nemohou používat všechny používané funkcionality) nebo/a zároveň,
- činí zcela nefunkčním některou z komponent řešení nebo/a zároveň,
- způsobuje, že řešení vykazuje nepřiměřeně dlouhé odezvy nebo/a zároveň,
- řešení vykazuje nedostatek, kdy implementační projekt zjevně neobsahuje části sjednané smlouvou nebo zadávací dokumentací, či zcela chybí podstatná část řešení.

****Porucha:** Poruchou se rozumí stav, který:
- způsobuje, že je systém schopen omezeného provozu nebo neposkytuje některou z nekritických funkcionalit (řešení splňuje účel, pro které bylo vytvořeno; uživatelé mohou používat všechny klíčové funkcionality) nebo/a zároveň;
- způsobuje, že některá z funkcionalit řešení není plně činná nebo ztěžuje užívání u některého koncového uživatele, avšak tento stav má jen zanedbatelné dopady na provoz u objednatele nebo/a zároveň.

*****Chyba**: Chybou se rozumí stav, kdy:
- jsou ostatní závady/incidenty, které nespadají do kategorie „Havárie" ani „Porucha".

<u>Záruční servis předmětu plnění obsahuje:</u>

- Reakce na nahlášené chyby, problémy a požadavky.
- Analytická podpora řešení problémů zadaných do Helpdesku objednatele.
- Oprava vad, chyb a zranitelností.
- Zajištění souladu se zákony a normativy ČR a EU.
- Reakce na dotazy oprávněných osob objednatele.
- Monitoring preventivní.
- Kontroly provozních logů.
- Obnova provozu systému po výpadcích.
- Instalace oprav a nových verzí SW produktů, které byly dodány jako součást řešení, které jsou vyžadovány pro zajištění bezpečnosti systému nebo rozvojových aktivit, včetně zajištění funkčnosti celého řešení po provedeném upgradu.
- Aktualizace dokumentace.
- Ostatní nevyjmenované práce nutné pro zajištění funkčnosti řešení.

6. Záruka se nevztahuje na poruchy, které byly způsobeny neodbornou obsluhou a údržbou, živelnou pohromou, nedodržením návodu od výrobce, nedodržením provozních podmínek nebo jiným způsobem než obvyklým provozem.
7. Po dobu záruční lhůty je objednatel povinen využívat dodaná zařízení dle pokynů dodavatele, popřípadě dle pokynů výrobce **F5, Inc.**, výlučně v souladu s jejich posláním a příslušnými technickými podmínkami. Případná technická zlepšení nebo úpravy může vykonat jen na základě písemného souhlasu dodavatele nebo výrobce.
8. V případě zjištění nebo podezření na probíhající kybernetický útok v průběhu poskytování služeb (záruky) dodavatele, musí být provedeny nezbytné kroky dodavatelem k zdokumentování a zajištění forenzních důkazů a okamžitému nahlášení

kontaktní osobě objednatele (viz kontaktní osoby), která rozhodne, zda budou práce ukončeny nebo bude v pracích pokračováno a za jakých podmínek.

IV. Cena a platební podmínky

1. Cena za předmět plnění dle čl. I. odst. 1 písm. a) až i) této smlouvy byla sjednána ve výši:
   Celková cena bez DPH 4 970 379,00 Kč
   DPH 1 043 779,59 Kč
   Cena vč. DPH 6 014 158,59 Kč
   (dále jen „cena")
2. Celková cena je stanovena jako konečná a zahrnuje cenu za celý předmět plnění a veškeré náklady dodavatele na plnění dle této smlouvy.
3. Cena služby technického specialisty poskytnuté objednateli na základě jeho emailových požadavků dle čl. I. odst. 1 písm. j) této smlouvy činí 2 062,50 Kč bez DPH za hodinu práce dodavatele.
4. Objednatel se zavazuje zaplatit cenu uvedenou v čl. IV. odst. 1 této smlouvy na základě faktury vystavené dodavatelem. Dodavatel předá fakturu objednateli spolu s akceptačním protokolem, jehož součástí bude dodací list, popřípadě zašle objednateli do 14 dnů po řádném předání a převzetí předmětu plnění. Fakturována může být pouze celá dodávka předmětu plnění. Na faktuře budou rozepsány jednotlivé položky dle předmětu plnění.
5. Cena za poskytované služby dle čl. IV. odst. 3. této smlouvy bude objednatelem hrazena na základě faktury vystavené dodavatelem na základě výkazu provedených služeb, který odsouhlasí obě smluvní strany.
6. Faktura musí dále obsahovat všechny údaje uvedené v § 29 odst. 1 zákona č. 235/2004 Sb., o dani z přidané hodnoty a dle zákona č. 563/1991 Sb., o účetnictví. Splatnost faktury činí 60 dnů od jejího doručení objednateli. Faktura bude zaslána elektronicky ve formátu PDF na e-mailovou adresu: xxxxx. K faktuře bude přiložena kopie řádně opatřeného dodacího listu způsobem sjednaným výše v čl. II.
7. V případě, že dodavatelem vystavená faktura bude obsahovat nesprávné či neúplné údaje, je právem objednatele takovou fakturu do 15 dnů od jejího převzetí vrátit dodavateli. Ten podle charakteru nedostatků fakturu opraví anebo vystaví novou. U opravené nebo nové faktury běží nová lhůta splatnosti.
8. Platby budou probíhat výhradně v CZK a rovněž veškeré cenové údaje budou v této měně.
9. Faktura musí obsahovat registrační číslo projektu CZ.31.1.01/MV/23_50/0000050 a CZ.31.2.0/0.0/0.0/22_054/0007984 a musí obsahovat informaci, že se jedná o projekt financovaný z NPO, tzn. faktura musí obsahovat větu „Financováno Evropskou unií –Next Generation EU".
10. Faktury se platí bankovním převodem na účet druhé smluvní strany uvedený na faktuře. Povinnost objednatele zaplatit dodavateli vyúčtovanou cenu je splněna dnem odeslání platby z účtu objednatele.

V. Odstoupení od smlouvy

1. Kterákoliv ze smluvních stran je oprávněna od této smlouvy odstoupit v případě jejího podstatného porušení druhou smluvní stranou. Pro účely této smlouvy se za podstatné porušení smluvních povinností považuje takové porušení, u kterého strana porušující smlouvu měla nebo mohla předpokládat, že při takovémto porušení smlouvy, s přihlédnutím ke všem okolnostem, by druhá smluvní strana neměla zájem smlouvu uzavřít; zejména:
   - na straně objednatele nezaplacení ceny plnění podle této smlouvy ve lhůtě delší 60 dní po dni splatnosti příslušné faktury, přestože byl dodavatelem na neplnění této smlouvy písemně upozorněn,
   - na straně dodavatele zejména jednání uvedená v čl. VI. odst. 2 této smlouvy, tj. jestliže nedodá řádně a včas předmět plnění, pokud dodavatel nezjednal nápravu, přestože byl objednatelem na neplnění této smlouvy písemně upozorněn.
2. Odstoupení od smlouvy musí být provedeno písemným oznámením o odstoupení, které musí obsahovat důvod odstoupení a musí být doručeno druhé smluvní straně. Účinky odstoupení nastanou okamžikem doručení písemného vyhotovení odstoupení druhé smluvní straně.

VI. Sankce

1. Pro případ prodlení objednatele s úhradou ceny dle čl. IV. této smlouvy má dodavatel nárok na zaplacení úroku z prodlení ze strany objednatele ve výši 0,01 % z částky, s jejíž platbou je objednatel v prodlení, za každý den takového prodlení. Smluvní strany se dohodly, že dodavatel je oprávněn požadovat zaplacení úroku z prodlení až po uplynutí 30 dnů od sjednané lhůty splatnosti.
2. V případě dodání jiného předmětu plnění než objednaného a při nedodržení dodací lhůty je objednatel oprávněn požadovat zaplacení jednorázové smluvní pokuty ve výši 50.000,- Kč. Dále je objednatel oprávněn požadovat zaplacení další smluvní pokuty ve výši 0,1 % z ceny plnění dle čl. IV. odst. 1 smlouvy bez DPH za každý započatý den prodlení s dodáním předmětu plnění, jestliže se s dodavatelem nedohodne jinak. Objednatel je dále v těchto případech rovněž oprávněn odstoupit od smlouvy.
3. Za nedodržení termínu uvedeného ve čl. III. odst. 5 smlouvy, tzn. odstranění závady v úrovni „Havárie", má objednatel právo účtovat smluvní pokutu ve výši 3.000,- Kč za každou započatou hodinu prodlení za jednotlivý případ.
4. Za nedodržení termínu uvedeného ve čl. III. odst. 5 smlouvy, tzn. odstranění závady v úrovni „Porucha", má objednatel právo účtovat smluvní pokutu ve výši 2.000,- Kč za každou započatou hodinu prodlení za jednotlivý případ.
5. Za nedodržení termínu uvedeného ve čl. III. odst. 5 smlouvy, tzn. odstranění závady v úrovni „Chyba", má objednatel právo účtovat smluvní pokutu ve výši 1.000,- Kč za každou započatou hodinu prodlení za jednotlivý případ.
6. V případě prodlení dodavatele s dodržením termínů odstranění vad předmětu plnění, jsou-li uvedeny v akceptačním protokolu o předání a převzetí předmětu plnění dle čl. II. odst. 10 smlouvy, je objednatel oprávněn požadovat zaplacení smluvní pokuty ve výši 0,1% z celkové ceny předmětu plnění bez DPH za každý i započatý den prodlení.
7. V případě nedodržení některé z povinností dodavatele stanovených v čl. VIII. odst. 2-4 smlouvy má objednatel právo účtovat smluvní pokutu ve výši 10.000,- Kč.
8. Za nedodržení povinností uvedených v čl. I. odst. 3 a 4 nebo čl. II. odst. 12 nebo v čl. III. odst. 8 nebo čl. VII., má objednatel právo účtovat smluvní pokutu ve výši 200.000,- Kč za každé jednotlivé porušení povinnosti.

9. V případě nedodržení některé z povinností dodavatele stanovených v čl. VIII. odst. 7 a 8 smlouvy má objednatel právo účtovat dodavateli smluvní pokutu ve výši sankce uložené objednateli Vlastníkem komponenty NPO (Ministerstvem vnitra ČR) za nedodržení povinností stanovených v Podmínkách rozhodnutí o poskytnutí dotace nebo ve výši zkrácení dotace z téhož důvodu.
10. V případě nedodržení povinnosti stanovené v čl. VIII. odst. 5 smlouvy má objednatel právo účtovat smluvní pokutu ve výši pohledávky, která byla postoupena v rozporu s touto smlouvu. Objednatel má zároveň právo odstoupit od smlouvy.
11. Smluvní pokuta bude vyúčtovaná samostatným daňovým dokladem a její splatnost činí 30 dní ode dne doručení daňového dokladu. Zaplacením smluvní pokuty není dotčeno právo na náhradu škody vzniklé smluvní straně požadující zaplacení smluvní pokuty.

VII. Mlčenlivost

1. Dodavatel se zavazuje zachovávat mlčenlivost ve vztahu ke všem informacím a skutečnostem, které se dozví o objednateli, jeho zaměstnancích, pacientech atd. v souvislosti s uzavřením a plněním smlouvy, pokud tyto informace mají povahu obchodního tajemství, osobních údajů nebo mají být z jiných důvodů chráněny před zveřejněním. Dodavatel je povinen nakládat s osobními údaji a zejména s údaji o zdravotním stavu, genetickými a biometrickými údaji (dále jen „Osobní údaje") v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 (dále jen GDPR) a příslušnými ustanoveními zákona č. 110/2019 Sb., o zpracování osobních údajů.
2. Povinnost mlčenlivosti platí rovněž o skutečnostech, na něž se vztahuje povinnost mlčenlivosti zdravotnických pracovníků, zejména podle ustanovení § 51 zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (Zákon o zdravotních službách), a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení Osobních údajů.
3. Pokud dodavatel přijde při plnění smlouvy do styku s Osobními údaji a bude v postavení zpracovatele ve smyslu GDPR a Zákona o zpracování osobních údajů, zavazuje se nakládat s Osobními údaji pouze za účelem splnění závazků z této smlouvy a žádným jiným způsobem, a to v souladu příslušnými ustanoveními GDPR a Zákona o zpracování osobních údajů v rozsahu nezbytném pro plnění smlouvy a po dobu nezbytnou k plnění smlouvy. Zpracovávání Osobních údajů v rozsahu údajů poskytnutých objednatelem a týkajících se zdravotnické dokumentace pacientů, jimž jsou objednatelem poskytovány zdravotní služby, a dále v rozsahu Osobních údajů zaměstnanců objednatele dodavatelem může zahrnovat odstranění potíží za účelem zabránění, vyhledávání a opravy problémů zjištěných při poskytování služeb dle této smlouvy, může také zahrnovat zlepšování funkcí informačních systémů, vyhledávání hrozeb uživatelům a ochrany uživatelů informačních systémů. Osobní údaje nebudou použity k jinému účelu, ani z nich nebudou odvozovány informace pro žádné reklamní či jiné komerční účely. Dodavatel se zavazuje za účelem ochrany osobních údajů objednatele a jeho pacientů a zaměstnanců před neoprávněným přístupem, použitím, zveřejněním nebo zničením, resp. před jejich náhodnou ztrátou či změnou uplatňovat technická a organizační bezpečnostní opatření, interní kontroly a rutiny zabezpečení osobních údajů zajišťující splnění všech povinností dle GDPR a Zákona o ochraně osobních údajů, zejména zajistit, aby data obsažená ve zdravotnické dokumentaci byla šifrována způsobem, který znemožní nahlížení do těchto údajů neoprávněným osobám.
4. Dodavatel se zavazuje zajistit informovanost svých pracovníků (včetně poddodavatelů) o povinnostech vyplývajících z této smlouvy. Dodavatel se zavazuje zajistit, aby jeho pracovníci, kteří budou přicházet do styku s osobními údaji, byli smluvně vázáni povinností mlčenlivosti ve smyslu GDPR a Zákona o zpracování osobních údajů a poučeni o možných následcích porušení těchto povinností s tím, že povinnost důvěrnosti bude jimi dodržována i po skončení jejich smluvního vztahu k objednateli. Toto ujednání je sjednáno ve smyslu ustanovení čl. 28 GDPR. Dodavatel se zavazuje informovat své poddodavatele o povinnosti mlčenlivosti dle této smlouvy. V případě porušení mlčenlivosti za strany poddodavatele, odpovídá dodavatel objednateli za vzniklou škodu, jako kdyby povinnost porušil sám.
5. Smluvní strany se zavazují zachovat mlčenlivost též o všech ostatních skutečnostech, ve vztahu, k nimž o to budou druhou stranou písemně požádány. Smluvní strany se též zavazují nevyužít informace podle prvé věty tohoto odstavce ve svůj prospěch nebo ve prospěch třetích osob v rozporu s účelem jejich předání.
6. Smluvní strany jsou povinny zajistit, že nebudou neoprávněně pořizovány kopie informací či jiné záznamy nad rámec plnění dle této smlouvy, a nebudou zjišťovány informace, které nejsou nezbytně nutné ke splnění povinností vyplývajících z této smlouvy.
7. Smluvní strany se zavazují pro případ, že se v průběhu plnění dle této smlouvy dostanou do kontaktu s údaji druhé smluvní strany vyplývajícími z její provozní činnosti, tyto údaje v žádném případě nezneužít, nezměnit ani jinak nepoškodit, neztratit či neznehodnotit.
8. Dodavatel se zavazuje plně respektovat bezpečnostní požadavky objednatele k zajištění ochrany Osobních údajů pacientů a zaměstnanců objednatele.
9. Povinnost mlčenlivosti o informacích a skutečnostech obchodního charakteru trvá po dobu 5 let od ukončení této smlouvy, o informacích obsahujících Osobní údaje trvá bez časového omezení.
10. Smluvní strany vylučují povinnosti jim uložené ve smyslu čl. VII., a to za předpokladu plnění povinností jim uložených platnými právními předpisy, především, nikoliv však výlučně zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů (dále též „**registr smluv**").

VIII. Ostatní ujednání

1. Dodavatel bere na vědomí, že objednatel je povinen dle ustanovení § 219 odst. 1 z. č. 134/2016 Sb., a dle zákona č. 340/2015 Sb., o registru smluv, uveřejnit tuto smlouvu včetně případných dodatků, zákonem stanoveným způsobem.
2. Dodavatel je povinen v souladu s ustanovením § 105 z. č. 134/2016 Sb. předložit do 10 pracovních dnů od doručení oznámení o výběru dodavatele objednateli seznam, ve kterém uvede, jaké části předmětu plnění a v jakém rozsahu bude plnit prostřednictvím poddodavatele, spolu s identifikací poddodavatele a uvedením rozsahu jeho plnění, pokud mu jsou známi. Poddodavatelé, kteří nebyli tímto způsobem identifikováni a kteří se následně zapojí do plnění veřejné zakázky, musí být identifikováni dodatečně, a to nejpozději před zahájením plnění veřejné zakázky tímto poddodavatelem.
3. Dodavatel je povinen mít v platnosti a udržovat pojištění odpovědnosti za škodu způsobenou objednateli či třetím osobám při výkonu podnikatelské činnosti, která je předmětem této smlouvy, s limitem pojistného plnění v minimální výši 10.000.000,- Kč.

4. Dodavatel je povinen udržovat výše uvedené pojištění po celou dobu trvání smlouvy. V případě porušení této povinnosti je objednatel oprávněn od smlouvy, která bude uzavřena na základě výsledku tohoto zadávacího řízení odstoupit. Na žádost objednatele je dodavatel povinen předložit objednateli dokumenty prokazující, že pojištění v požadovaném rozsahu a výši trvá. Pokud by v důsledku pojistného plnění nebo jiné události mělo dojít k zániku pojištění, k omezení rozsahu pojištěných rizik, ke snížení stanovené min. výše pojistného plnění, nebo k jiným změnám, které by znamenaly zhoršení podmínek oproti původnímu stavu, je dodavatel povinen učinit příslušná opatření tak, aby pojištění bylo udrženo tak, jak je požadováno v tomto ustanovení.
5. Dodavatel je oprávněn postoupit pohledávku vyplývající z plnění dle této smlouvy na třetí osobu pouze s předchozím písemným souhlasem objednatele.
6. Dodavatel se zavazuje dodržovat nařízení objednatele, kterým je zakázáno kouření ve všech prostorách i plochách areálu objednatele s výjimkou vyhrazených míst.
7. Dodavatel je povinen uchovávat veškeré doklady související s realizací plnění předmětu smlouvy (způsobem dle zákona o účetnictví) včetně účetních dokladů minimálně do konce roku 2036 nebo po dobu nejméně 10 let ode dne poslední platby za provedené práce, přičemž závazná je lhůta, která je delší. Dále je povinen zajistit, aby také všichni jeho poddodavatelé, partneři, dodavatelé partnerů uchovávali veškeré dokumenty související s prováděním plnění předmětu této smlouvy.
8. Minimálně do konce roku 2036 resp. ve lhůtách dle předchozího odstavce je dodavatel povinen poskytovat požadované informace a dokumentaci související s realizací projektu objednateli, zaměstnancům nebo zmocněncům pověřených orgánů (MV ČR, MZ ČR, MPO ČR, MF ČR, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů veřejné správy), a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu, poskytnout jim při provádění kontroly součinnost a být fyzicky přítomen kontrolám v místě plnění.

IX. Závěrečná ujednání

1. Tato smlouva nabývá platnosti dnem podpisu smluvními stranami a účinnosti dnem uveřejnění v registru smluv.
2. Veškeré právní vztahy založené, resp. vyplývající z této smlouvy, které zde nejsou výslovně upravené, včetně eventuálních řešení vzájemných sporů, se řídí ustanoveními příslušných právních předpisů České republiky. Změny a doplnění této smlouvy lze učinit pouze na základě písemné dohody smluvních stran. Takové dohody musí mít podobu datovaných, vzestupně číslovaných dodatků této smlouvy podepsanými jejich statutárními zástupci.
3. Tato smlouva je vyhotovena ve dvou stejnopisech s platností originálu, z nichž každá ze smluvních stran obdrží po jednom vyhotovení. Pokud je smlouva podepisována elektronicky, je vyhotovena v jednom stejnopise podepsaném oběma smluvními stranami elektronickým podpisem dle zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce. Nedílnou součástí této smlouvy jsou přílohy dle textu smlouvy.
4. Autentičnost této smlouvy potvrzují smluvní strany svými vlastnoručními podpisy.

Přílohy:
Příloha č. 1 – Technická a funkční specifikace předmětu plnění
Příloha č. 2 – Minimální technické a funkční požadavky objednatele
Příloha č. 3 – Položkový ceník
Příloha č. 4 - Používání sítě VFN externími uživateli
Příloha č. 5 – Požadavky systému řízení bezpečnosti informací na dodavatele

V Praze dne dle el. podpisu:

prof. MUDr. David Feltl, Ph.D., MBA
ředitel Všeobecné fakultní nemocnice v Praze

V Praze dne dle. el. podpisu

Simac Technik ČR, a.s.

ŘEŠENÍ ZAJIŠŤUJÍCÍ VYROVNÁVÁNÍ ZATÍŽENÍ PRO DISTRIBUCI SÍŤOVÉHO NEBO APLIKAČNÍHO PROVOZU S INTELIGENTNÍ SPRÁVOU SÍŤOVÉHO PROVOZU – BALANCER S WEBOVÝM APLIKAČNÍM FILTREM

Posouzení splnění vlastností a funkcionalit nabízeného řešení

Zadavatel požaduje splnění všech požadavků vyplývajících ze zadávacích podmínek a všech jejich příloh. Každý účastník zadávacího řízení je povinen vyplnit níže uvedenou tabulku (tabulka č.1), která slouží pro posouzení zadavatelem, zdali nabízené řešení splňuje požadavky na HW/SW.

Tabulka č. 1 **Požadovaná funkcionalita/vlastnost**	**Nabízené řešení splňuje/nesplňuje požadavek (doplní dodavatel)** **ANO/NE**
Platforma	
Nasazení redundantních HW zařízení ve funkci load-balancer s podporou autentizace uživatelů, SSL akcelerátoru a webového aplikačního firewallu.	Ano
Každé zařízení podporuje připojení 4 x 10/1 Gbps metalické RJ45 porty a alespoň 4x 25/10 Gbps optické SFP+ porty.	Ano
Datová propustnost zařízení alespoň 18 Gbps či více na L4 a 11 Gbps či více na L7	Ano
Minimální propustnost HTTP požadavků: 800 tis.za sekundu	Ano
Minimální propustnost L7 požadavků: 470 tis. za sekundu	Ano
Počet současných L4 spojení: 17 mil.	Ano
Offload – HW komprese – propustnost min. 5 Gbps	Ano
Ano SSL akcelerace v HW	Ano
Počet SSL transakcí za sekundu min. 6500 (při použití 2K klíče)	Ano
Počet SSL transakcí za sekundu min. 4000 (při použití ECDSA P-256 klíče)	Ano
Celkový šifrovací výkon 7 Gbps	Ano
Nezávislé rozhraní pro management	Ano
Redundantní napájení	Ano
K dispozici jako autonomní box nebo ve formě šasi	Ano
Management: sériový port, GUI, příkazový řádek, iLO	Ano
Operační systém	
Full-Proxy architektura (plné oddělení klientského a serverového spojení)	Ano
Podpora IPv4	Ano
Plná podpora IPv6, IPv4/IPv6 gateway	Ano
Podpora externích šifrovacích karet pro SSL (HSM)	Ano
Podpora ověření certifikátů vydaných podřízenou CA (intermediate CA)	Ano
Podpora Spanning Tree Protokolu (STP)	Ano
Možnost přidat vlastní funkce pomocí skriptování	Ano
Podpora HTTP/2	Ano
Podpora IPSec IKEv2	Ano
Podpora konfigurace a správu zařízení přes REST API	Ano
Podpora SNMP (v1/v2c/v3)	Ano
Možnost aktivovat následující funkce na jedné HW platformě: - L4-7 loadbalancing - ICSA certifikovaný Web aplikační firewall Možnost dodatečně aktivovat další funkcionalitu zakoupením licencí: - ICSA certifikovaný síťový firewall - Autorizace a autentizace aplikací, SSL VPN - DNS služby a DNS firewall - IP reputační databáze	Ano

Možnost používat knihovny JavaScript třetích stran k úpravě a správě provozu	Ano
Podpora Active-Active a Active-Pasive módu	Ano
Možnost vytvoření HA clusteru mezi Virtuální a Hardware platformou	Ano
Web aplikační Firewall	
Integrace s nástrojem na detekci zranitelností webových aplikací	Ano
Detekce a blokování širokého spektra útoků na aplikační vrstvě, minimálně podle OWASP top10	Ano
Možnost doprogramovat si filtrovaci pravidla pro aplikace	Ano
Automatická korelace zranitelností do jednoho bezpečnostního incidentu	Ano
Ochrana AJAX a JSON aplikací	Ano
Ochrana proti L7 DDoS útokům, web scrapingu a útokům pomocí hrubé síly (brute force)	Ano
Podpora Captcha metody	Ano
Automatické odlišení skutečných uživatelů od robotů	Ano
Integrovaný XML firewall	Ano
Podpora maskování/odstranění citlivých informací – čísla kreditních karet, číslo pojištění…	Ano
Automatické nahrávání a aplikování nových signatur	Ano
Podpora pozitivního a negativního bezpečnostního modelu	Ano
Blokování útočníků na základě geolokace	Ano
Podpora ICAP pro antivirovou kontrolu – pro HTTP, SOAP a SMTP	Ano
Ochrana SMTP a FTP na aplikační úrovni	Ano
Podpora SSL (šifrování a dešifrování)	Ano
Podpora různých typů reportů – PCI, geolokační reporty	Ano
Podpora standardů PCI DSS, HIPAA, Basel II a SOX	Ano
Integrované bezpečnostní politiky pro Microsoft Outlook Web Access, Oracle Applications, Wordpress a Microsoft SharePoint	Ano
Podpora pro analýzu HTTP provozu (Top URL, Top klienti, nejpoužívanější HTTP metody, návštěvnost stránek podle geogr. Regionu)	Ano
Možnost importu zranitelnosti aplikací z alespoň některých z následujících skenerů: ● Cenzic Hailstorm ● WhiteHat Sentinel ● IBM Rational AppScan ● QualysGuard Web Application Scanning	Ano
Podpora aplikačního firewallu ve virtuálních kontextech	Ano
Podpora aplikačního firewallu v cloudu	Ano
Rozšířená podpora CSHUI – detekce aktivity klávesnice a myši, detekce změn URL od klienta za krátkou dobu	Ano
Ochrana proti Session Highjacking pomocí Browser Fingerprintingu	Ano
Detekce a ochrana před DoS útoky na specifické URL, které mohou zatížit back-end systémy (např. vyhledávací URL apod.)	Ano
Vynucení přístupu uživatele k chráněné aplikaci přes přihlašovací stránku aplikace	Ano

Podpora nastavení bezpečnostních politik podle IP adresy, doménového jména a URI	Ano
Podpora a filtrování WebSocket provozu	Ano
Blacklistování IP adres, které opakovaně snaží překonat bezpečnostní opatření v politice	Ano
Možnost ochrany proti Credential Stuffing útokům	Ano
Možnost doplnění modulu pro přístup k online databázi nejnovějších útoků	Ano
Možnost rozšířit DoS ochranu proti přetížení napojením na čističku provozu přes cloud.	Ano
Řízení provozu	
Možnost připojení k monitorovacím nástrojům třetích stran prostřednictvím otevřeného API	Ano
Podpora REST API	Ano
Autentizace klientů přes LDAP/Radius	Ano
Povolení/zakázání ICMP a ARP pro VIP	Ano
Podpora vysokorychlostního granulárního logování / logování per aplikace / bez omezení výkonnosti zařízení	Ano
Podpora rozvažování zátěže alespoň pro následující metody: - Round Robin - Least Connections - Ratio - Ratio Least Connections - Ratio Session - Weighted Least Connections - Least Sessions - Fastest Server - Fastest Application	Ano
Podpora filtrace paketů	Ano
Podpora ToS, QoS (marking/preservation/mimic)	Ano
Podpora SNMP (v1/v2c/v3)	Ano
Podpora rozvažování zátěže založené na poměrech (ratio) s perzistencí	Ano
Podpora SSL perzistence	Ano
Podpora perzistentních záznamů na základě vlastních parametrů	Ano
Podpora SSL certifikátů podepsaných SHA-2 algoritmem	Ano
Podpora práce s 4096-bit klíči	Ano
Současná podpora ECC a RSA certifikátu	Ano
Podpora Camellia šifer SSL	Ano
Podpora pro TLS 1.2 a TLS 1.3	Ano
Podpora ECC a DH šifer v HW	Ano
Podpora SSL Forward proxy	Ano
Stavové filtrované paketů (ACL)	Ano
Podpora vlastních skriptů pro monitorování zdraví a dostupnosti služeb	Ano
Podpora monitorování služeb na základě výkonu konkrétních hostů	Ano
TCP optimalizace síťových toků	Ano
Komprese a cachování specifických služeb	Ano

Podpora zrcadlení SSL relací a SSL spojení v HA clusteru	Ano
Podpora optimalizace dynamické velikosti TLS bloků (TLS record size)	Ano
Podpora autentizace: - HTTP basic - HTML form - Certificate - OCSP - CRLDP - Radius - LDAP - Active Directory - NTLM v1/v2 - Kerberos - SAML - SerurID - OAM - Tacacs+ - Local DB	Ano
Import uživatelských identit IF-MAP	Ano
Podpora externích přihlašovacích stránek aplikací	Ano
Podpora vysoké dostupnosti AAA serverů	Ano
OTP (generování a ověření)	Ano
Podpora CAPTCHA	Ano
SAML: - SP role - IdP role	Ano
Modifikace SAML atributů	Ano
Podpora SAML 2.0	Ano
Podpora pro vytvoření Single Sign-On (SSO): - HTTP basic - HTML form - NTLM v1/v2 - Kerberos - SAML	Ano
Uchování přihlašovacích údajů v paměti a jejich přeposlání k ověření (User identity credential caching, SSO proxy)	Ano
Podpora federace (SSO napříč různými doménami, např. on-prem a SaaS)	Ano
Podpora Kerberos ticketing	Ano
PCoIP proxy	Ano
RDP proxy	Ano
Patching (maskování) webových portálů: - HTML - JavaScript	Ano

- CSS - Java	
Podpora uživatelského portálu při publikaci služeb v režimu jednoho URL	Ano
Uživatelský portál, kde se zobrazují aplikace podle přístupových práv	Ano
Podpora L7 ACL	Ano
Podpora importu dynamických ACL z AAA	Ano
Podpora dynamického řízení přístupu	Ano
Podpora zabezpečení vzdálené pracovní plochy vzdáleného uživatele	Ano
Síťová SSL VPN DTLS	Ano
Podpora publikace aplikací formou portálu	Ano
Podpora vzdáleného přístupu k aplikacím bez nutnosti použití tlustého klienta	Ano
Podpora OS: - Windows - MAC - Linux - iOS - Android	Ano
Nativní podpora MDM	Ano
Podpora Oauth 2.0	Ano
Kontrola nastavení zabezpečení koncových bodů (klientů), validace politik, detekce AV a verze, certifikátů aj. parametrů na straně klienta	Ano
Filtrování URL	Ano
URL kategorizační databáze	Ano
Podpora pro vytváření flexibilní a granulární přístupové politky	Ano
GUI pro vizuální nastavení přístupových bezpečnostních politik a logiky autentizace	Ano
Podpora Microsoft ActiveSync a Outlook Anywhere s klientskou NTLM autentizací	Ano
Zjednodušené řízení přístupové politiky pro VDI technologie Citrix XenApp a XenDesktop	Ano
Podpora „Step-up“ autentizace	Ano
IP reputační databáze	
Napojení na globální databázi škodlivých IP adres s automatickým obnovováním a možnost jejich blokování	Ano
Rozpoznání zdrojů Phishingu, Anonymních Proxy a spojení na Command and Control centra Botnetů	Ano
Možnost napojení na CDN	Ano

Příloha č. 2 – Minimální technické a funkční požadavky objednatele

Minimální technické a funkční požadavky

Balancer s webovým aplikačním filtrem

Popis prostředí zadavatele

Prostředí zadavatele se skládá z virtuálních serverů na platformě VMware ESX, několika fyzických serverů, které není možné, či vhodné, z jejich podstaty virtualizovat, z fyzických a virtuálních pracovních stanic, síťových prvků v topologii hvězda, tj. s centrálním přepínačem, a dalších zařízení.
Servery s datovými úložišti komunikují prostřednictvím SAN Fibre Channel sítě vybavené redundantními Cisco MDS přepínači. Maximální, a současně preferovaná, linková rychlost je 16 Gbit.
Fyzické pracovní stanice jsou vybaveny operačním systémem a Windows 10 a vyšší (omezeně Windows 7).
U informačních systémů zadavatele je v maximální efektivní míře implementována funkce Single Sign-On s využitím služby Microsoft Active Directory (autentizační protokol Kerberos). Uživatel se autentizuje pouze do domény a při spuštění aplikace již není zadávání jména/hesla zpravidla nutné. Samozřejmě existuje množství aplikací, kde SSO není možné. Navíc existují uživatelé bez doménových účtů.

Požadavky na balancer s WAF

1. Správa aplikačního provozu:

Požadované řešení musí inteligentně spravovat náš síťový provoz, aby naše aplikace byly vždy spolehlivé, rychlé a optimalizované. Potřebujeme, aby řešení škálovalo podle aktuálních požadavků na provoz, zlepšovalo dobu načítání a celkovou uživatelskou zkušenost. Důležitá je také možnost přizpůsobení pravidel a programovatelnost. Toto řešení bude zajišťovat ochranu dat zákazníků pomocí vysokého výkonu a viditelnosti SSL pro příchozí i odchozí provoz, a poskytovat ICAP pro integraci s ochranou proti ztrátě dat a virům.

2. Bezpečný a centralizovaný přístup:

Potřebujeme nástroj, který zajistí bezpečný, jednoduchý a centralizovaný přístup ke všem našim aplikacím, API a datům. Měl by umožnit nasazení modelu „Zero Trust" na základě granulárního kontextu, čímž zabezpečí každý požadavek na přístup k aplikacím jednotlivě. Dále by měl provádět kontrolu zabezpečení a integrity zařízení a poskytovat přístup k VPN na úrovni jednotlivých aplikací bez zásahu uživatele. Tento nástroj musí poskytovat možnost získat šifrovaná data s vysokou mírou přizpůsobení autentizace a kontroly přístupu k jednotlivým aplikacím, sítím a zdrojům.

3. Ochrana proti aplikačním útokům (Webový Aplikační Firewall):

Hledáme řešení, které bude chránit naše aplikace, API a data proti nejčastějším útokům, jako jsou útoky „Zero day," DoS/DDoS útoky na aplikační vrstvě OSI modelu, hrozby vyjmenované v seznamu OWASP Top 10, převzetí aplikace a Boty. Toto řešení musí umět jak transparentní režim bezzásahové kontroly, tak rovněž režim automatického omezení podezřelého provozu. Řešení musí být napojeno na IP reputační databázi. Důležitá je také flexibilita v možnostech nasazení a správy, aby vyhovovalo našim specifickým potřebám.
Zadavatel připouští pouze tuto variantu možného řešení: On-premise: dodávka a implementace HW v místě zadavatele.

Požadovaná funkcionalita/vlastnost
Platforma
Nasazení redundantních HW zařízení ve funkci load-balancer s podporou autentizace uživatelů, SSL akcelerátoru a webového aplikačního firewallu.
Každé zařízení podporuje připojení 4 x 10/1 Gbps metalické RJ45 porty a alespoň 4x 25/10 Gbps optické SFP+ porty.
Datová propustnost zařízení alespoň 18 Gbps či více na L4 a 11 Gbps či více na L7
Minimální propustnost HTTP požadavků: 800 tis.za sekundu
Minimální propustnost L7 požadavků: 470 tis. za sekundu
Počet současných L4 spojení: 17 mil.
Offload – HW komprese – propustnost min. 5 Gbps
SSL akcelerace v HW
Počet SSL transakcí za sekundu min. 6500 (při použití 2K klíče)
Počet SSL transakcí za sekundu min. 4000 (při použití ECDSA P-256 klíče)
Celkový šifrovací výkon 7 Gbps
Nezávislé rozhraní pro management
Redundantní napájení
K dispozici jako autonomní box nebo ve formě šasi
Management: sériový port, GUI, příkazový řádek, iLO
Operační systém
Full-Proxy architektura (plné oddělení klientského a serverového spojení)
Podpora IPv4
Plná podpora IPv6, IPv4/IPv6 gateway
Podpora externích šifrovacích karet pro SSL (HSM)
Podpora ověření certifikátů vydaných podřízenou CA (intermediate CA)
Podpora Spanning Tree Protokolu (STP)
Možnost přidat vlastní funkce pomocí skriptování
Podpora HTTP/2
Podpora IPSec IKEv2
Podpora konfigurace a správu zařízení přes REST API
Podpora SNMP (v1/v2c/v3)
Možnost aktivovat následující funkce na jedné HW platformě: - L4-7 loadbalancing - ICSA certifikovaný Web aplikační firewall Možnost dodatečně aktivovat další funkcionalitu zakoupením licencí: - ICSA certifikovaný síťový firewall - Autorizace a autentizace aplikací, SSL VPN - DNS služby a DNS firewall - IP reputační databáze
Možnost používat knihovny JavaScript třetích stran k úpravě a správě provozu
Podpora Active-Active a Active-Pasive módu
Možnost vytvoření HA clusteru mezi Virtuální a Hardware platformou
Web aplikační Firewall
Integrace s nástrojem na detekci zranitelností webových aplikací
Detekce a blokování širokého spektra útoků na aplikační vrstvě, minimálně podle OWASP top10
Možnost doprogramovat si filtrovaci pravidla pro aplikace
Automatická korelace zranitelností do jednoho bezpečnostního incidentu

Ochrana AJAX a JSON aplikací
Ochrana proti L7 DDoS útokům, web scrapingu a útokům pomocí hrubé síly (brute force)
Podpora Captcha metody
Automatické odlišení skutečných uživatelů od robotů
Integrovaný XML firewall
Podpora maskování/odstranění citlivých informací – čísla kreditních karet, číslo pojištění…
Automatické nahrávání a aplikování nových signatur
Podpora pozitivního a negativního bezpečnostního modelu
Blokování útočníků na základě geolokace
Podpora ICAP pro antivirovou kontrolu – pro HTTP, SOAP a SMTP
Ochrana SMTP a FTP na aplikační úrovni
Podpora SSL (šifrování a dešifrování)
Podpora různých typů reportů – PCI, geolokační reporty
Podpora standardů PCI DSS, HIPAA, Basel II a SOX
Integrované bezpečnostní politiky pro Microsoft Outlook Web Access, Oracle Applications, Wordpress a Microsoft SharePoint
Podpora pro analýzu HTTP provozu (Top URL, Top klienti, nejpoužívanější HTTP metody, návštěvnost stránek podle geogr. Regionu)
Možnost importu zranitelnosti aplikací z alespoň některých z následujících skenerů: ● Cenzic Hailstorm ● WhiteHat Sentinel ● IBM Rational AppScan ● QualysGuard Web Application Scanning
Podpora aplikačního firewallu ve virtuálních kontextech
Podpora aplikačního firewallu v cloudu
Rozšířená podpora CSHUI – detekce aktivity klávesnice a myši, detekce změn URL od klienta za krátkou dobu
Ochrana proti Session Highjacking pomocí Browser Fingerprintingu
Detekce a ochrana před DoS útoky na specifické URL, které mohou zatížit back-end systémy (např. vyhledávací URL apod.)
Vynucení přístupu uživatele k chráněné aplikaci přes přihlašovací stránku aplikace
Podpora nastavení bezpečnostních politik podle IP adresy, doménového jména a URI
Podpora a filtrování WebSocket provozu
Blacklistování IP adres, které opakovaně snaží překonat bezpečnostní opatření v politice
Možnost ochrany proti Credential Stuffing útokům
Možnost doplnění modulu pro přístup k online databázi nejnovějších útoků
Možnost rozšířit DoS ochranu proti přetížení napojením na čističku provozu přes cloud.
Řízení provozu
Možnost připojení k monitorovacím nástrojům třetích stran prostřednictvím otevřeného API
Podpora REST API
Autentizace klientů přes LDAP/Radius
Povolení/zakázání ICMP a ARP pro VIP
Podpora vysokorychlostního granulárního logování / logování per aplikace / bez omezení výkonnosti zařízení

Podpora rozvažování zátěže alespoň pro následující metody: - Round Robin - Least Connections - Ratio - Ratio Least Connections - Ratio Session - Weighted Least Connections - Least Sessions - Fastest Server - Fastest Application
Podpora filtrace paketů
Podpora ToS, QoS (marking/preservation/mimic)
Podpora SNMP (v1/v2c/v3)
Podpora rozvažování zátěže založené na poměrech (ratio) s perzistencí
Podpora SSL perzistence
Podpora perzistentních záznamů na základě vlastních parametrů
Podpora SSL certifikátů podepsaných SHA-2 algoritmem
Podpora práce s 4096-bit klíči
Současná podpora ECC a RSA certifikátu
Podpora Camellia šifer SSL
Podpora pro TLS 1.2 a TLS 1.3
Podpora ECC a DH šifer v HW
Podpora SSL Forward proxy
Stavové filtrované paketů (ACL)
Podpora vlastních skriptů pro monitorování zdraví a dostupnosti služeb
Podpora monitorování služeb na základě výkonu konkrétních hostů
TCP optimalizace síťových toků
Komprese a cachování specifických služeb
Podpora zrcadlení SSL relací a SSL spojení v HA clusteru
Podpora optimalizace dynamické velikosti TLS bloků (TLS record size)
Podpora autentizace: - HTTP basic - HTML form - Certificate - OCSP - CRLDP - Radius - LDAP - Active Directory - NTLM v1/v2 - Kerberos - SAML - SerurID - OAM - Tacacs+ - Local DB
Import uživatelských identit IF-MAP
Podpora externích přihlašovacích stránek aplikací
Podpora vysoké dostupnosti AAA serverů

OTP (generování a ověření)
Podpora CAPTCHA
SAML: - SP role - IdP role
Modifikace SAML atributů
Podpora SAML 2.0
Podpora pro vytvoření Single Sign-On (SSO): - HTTP basic - HTML form - NTLM v1/v2 - Kerberos - SAML
Uchování přihlašovacích údajů v paměti a jejich přeposlání k ověření (User identity credential caching, SSO proxy)
Podpora federace (SSO napříč různými doménami, např. on-prem a SaaS)
Podpora Kerberos ticketing
PCoIP proxy
RDP proxy
Patching (maskování) webových portálů: - HTML - JavaScript - CSS - Java
Podpora uživatelského portálu při publikaci služeb v režimu jednoho URL
Uživatelský portál, kde se zobrazují aplikace podle přístupových práv
Podpora L7 ACL
Podpora importu dynamických ACL z AAA
Podpora dynamického řízení přístupu
Podpora zabezpečení vzdálené pracovní plochy vzdáleného uživatele
Síťová SSL VPN DTLS
Podpora publikace aplikací formou portálu
Podpora vzdáleného přístupu k aplikacím bez nutnosti použití tlustého klienta
Podpora OS: - Windows - MAC - Linux - iOS - Android
Nativní podpora MDM
Podpora Oauth 2.0
Kontrola nastavení zabezpečení koncových bodů (klientů), validace politik, detekce AV a verze, certifikátů aj. parametrů na straně klienta
Filtrování URL
URL kategorizační databáze
Podpora pro vytváření flexibilní a granulární přístupové politky
GUI pro vizuální nastavení přístupových bezpečnostních politik a logiky autentizace
Podpora Microsoft ActiveSync a Outlook Anywhere s klientskou NTLM autentizací
Zjednodušené řízení přístupové politiky pro VDI technologie Citrix XenApp a XenDesktop
Podpora „Step-up“ autentizace

IP reputační databáze
Napojení na globální databázi škodlivých IP adres s automatickým obnovováním a možnost jejich blokování
Rozpoznání zdrojů Phishingu, Anonymních Proxy a spojení na Command and Control centra Botnetů
Možnost napojení na CDN

Příloha č. 3 – Položkový ceník

Příloha č. 7 ZP

Předmět plnění VZ	Množství	Jednotka	Nabídková cena/jednotka		Nabídková cena celkem		
			(bez DPH)	(s DPH)	(bez DPH)	Samostatně DPH (základní sazba)	(s DPH)
Řešení pro inteligentní správu síťového provozu - balancer s webovým aplikačním filtrem v souladu se zadávacími podmínkami a s návrhem smlouvy							
Předimplementační analýza dle čl. I., odst. 1 písm.a) návrhu smlouvy	**1**	**různé**	82 500,00 Kč	99 825,00 Kč	82 500,00 Kč	17 325,00 Kč	99 825,00 Kč
Dodání HW appliance (HA) včetně veškerého SW nezbytného pro provoz HW appliance dle čl I., odst. 1 písm. b) návrhu smlouvy včetně záruky a záručního servisu **(60 měsíců)**	1	ks	4 673 379,00 Kč	5 654 788,59 Kč	4 673 379,00 Kč	981 409,59 Kč	5 654 788,59 Kč
Implementační práce dle čl. I., odst. 1 písm. c) návrhu smlouvy	1	různé	132 000,00 Kč	159 720,00 Kč	132 000,00 Kč	27 720,00 Kč	159 720,00 Kč
Dodání technické a provozní/administrátorské dokumentace dle čl. I., odst. 1 písm. d) návrhu smlouvy	1	různé	49 500,00 Kč	59 895,00 Kč	49 500,00 Kč	10 395,00 Kč	59 895,00 Kč
Zaškolení administrátorů objednatele dle čl. I., odst. 1 písm. e) návrhu smlouvy.	1	různé	33 000,00 Kč	39 930,00 Kč	33 000,00 Kč	6 930,00 Kč	39 930,00 Kč
Služby technického specialisty nad rámec předmětu plnění VZ (předmět plnění VZ dle čl.I. odst. 1 písm. a) - i) návrhu smlouvy**) tj. dle čl. I., odst. 1 písm. j) návrhu smlouvy.**	40	MD (Man Day)	16 500,00 Kč	19 965,00 Kč	660 000,00 Kč	138 600,00 Kč	798 600,00 Kč
Celková nabídková cena za celý předmět plnění bez DPH *					5 630 379,00 Kč		

*) Hodnotící kritérium dle bodu 8 ZP

**) Množství doplní dodavatel dle nabízeného řešení

VŠEOBECNÁ FAKULTNÍ NEMOCNICE V PRAZE
U Nemocnice 499/2, 128 08 Praha 2 | www.vfn.cz, http://intranet.vfn.cz

POUŽÍVÁNÍ SÍTĚ VFN EXTERNÍMI UŽIVATELI

Obsah

1 Účel a oblast platnosti dokumentu 2
2 Pojmy a zkratky 2
3 Odpovědnosti a pravomoci 2
4 Postup (popis činností) 3
4.1 Procesy externího přístupu 3
4.1.1 Podmínky schvalování 3
4.1.2 Postup zřízení přístupu 3
4.1.3 Zrušení přístupu 4
4.2 Povinnosti, pravidla a restrikce 4
4.2.1 Povinnosti externích uživatelů 4
4.2.2 Požadavky na připojené zařízení 4
4.2.3 Bezpečnostní incident nebo kybernetický útok 4
4.2.4 Zakázané činnosti 5
4.2.5 Monitoring činností 5
4.2.6 Porušení pravidel a povinností 5
4.3 Revize externího připojení 5
5 Závěrečná ustanovení 6
6 Vznikající dokumenty a údaje 6
7 Související dokumenty 6
8 Přílohy 6
Příloha č. 1 – Povinnosti při připojování zařízení do sítě VFN 6
Příloha č. 2 – Postup zřízení přístupu externímu uživateli do počítačové sítě VFN 6
Příloha č. 3 – Povinnost administrátora v případě bezpečnostního incidentu nebo kybernetického útoku 6

Zpracovatel: [redacted]	**Účinnost dokumentu od:** 23. 7. 2020	**Schválil:** [redacted]
Garant: [redacted] Vedoucí odboru správy ICT	**První vydání dne:** 1. 1. 2008	**Dne:** 23. 7. 2020

POUŽÍVÁNÍ SÍTĚ VFN EXTERNÍMI UŽIVATELI

1 Účel a oblast platnosti dokumentu

Účelem této směrnice je stanovení podmínek pro používání sítě VFN externími uživateli včetně životního cyklu přístupu a povinností, pravidel a restrikcí vztahující se na externí uživatele přistupující do VFN.

2 Pojmy a zkratky

AD	Active Directory
Externí uživatel	Osoba využívající prostředky ICT VFN, která není v pracovně právním poměru k VFN
Garant	Zaměstnanec VFN, který zodpovídá za přístup a práci externího uživatele v síti VFN.
ICT	Informační a komunikační technologie
ISE	Cisco Identity Services Engine
OSICT	Odbor správy ICT
ServiceDesk	Nástroj na zaznamenání, evidenci a sledování stavu incidentů nebo požadavků zaměstnanců VFN a pracovníků externích dodavatelských firem řešených Úsekem informatiky a digitální transformace.
ÚI	Úsek informatiky a digitální transformace
VFN	Všeobecná fakultní nemocnice v Praze
VPN	Virtual Private Network – vzdálený zabezpečený přístup do lokální sítě

3 Odpovědnosti a pravomoci

Garant – zodpovídá za přístup, rozsah oprávnění a práci externího uživatele v síti VFN.

Externí uživatel – externí pracovník, kterému je na základě smluvního vztahu zřízen externí přístup, který je schválen garantem externího přístupu ve VFN (Garant). Výkon práce provádí v souladu se smluvním ujednáním a v souladu s náležitostmi dodržovat povinnosti, pravidla a zákazy uvedené v kap. 4.2.

Pracoviště Dispečinku ÚI (Odbor podpory uživatelů) – zodpovídá za ověření externího uživatele, schválení požadavku Garantem a za zadání požadavku do ServiceDesku.

OSICT – zodpovídá za zpracování a řešení požadavku o VPN přístup.

4 Postup (popis činností)

4.1 PROCESY EXTERNÍHO PŘÍSTUPU

4.1.1 Podmínky schvalování

Externí uživatel musí vyplnit formulář F-VFN-463 Žádost o zřízení přístupu externího uživatele do sítě VFN, kde je uveden garant externího přístupu za VFN (dále jen Garant), na jehož základě dojde k ověření identity žadatele a o schválení validity požadovaného přístupu a rozsahu přístupu Garantem. Po splnění těchto podmínek je možné zřízení účtu externího uživatele.

4.1.2 Postup zřízení přístupu

4.1.2.1 Externí uživatel

Detailní postup pro zřízení účtu externího uživatele je uveden v příloze (Příloha č. 2 – Postup zřízení přístupu externímu uživateli do počítačové sítě VFN) a zároveň dostupný na webové stránce https://www.vfn.cz/externista. Pokud je součástí externího přístupu i požadavek o zřízení vzdáleného přístupu je postupováno dle kapitoly 4.1.2.2 (Vzdálený přístup - VPN). Platnost externího účtu je max. 1 rok od zřízení, pokud nebyl zřizován na dobu určitou. Žadatel bude 1 měsíc před expirací upozorněn na kontaktní e-mail uvedený v žádosti, obdobně i Garant bude upozorněn na svůj pracovní mail 1 měsíc před. O prodloužení přístupového účtu žádá Garant e-mailem – jako odpověď na e-mail s upozorněním na expiraci.

4.1.2.2 Vzdálený přístup - VPN

Externí pracovníci se mohou do sítě VFN připojit pomocí VPN TLS tunelu s multifaktorovou autentizaci. Detailní postup pro žadatele je na stránce https://www.vfn.cz/vpn. O VPN přístup žádá Garant prostřednictvím požadavku do ServiceDesku, kde musí být uvedeno:

- jméno a příjmení externisty,
- účet externisty ve VFN,
- firma,
- telefon,
- e-mail,
- oblast činnosti ve vztahu k VFN,
- na které zařízení (modality, servery) má mít externí uživatel přístup a v jakém rozsahu (IP, porty),
- doba platnosti VPN přístupu, pokud má být na dobu určitou.

Požadavek dále zpracuje pracovník správy sítí OSICT v následujících krocích:

- předá ke schválení vedoucímu OSICT,
- předá na externí firmu Simac, která podle něj nastaví profil v ISE,
- předá na správu serverů OSICT.

Požadavek dále zpracuje pracovník správy serverů OSICT v následujících krocích:

- nastaví profil v AD,
- pošle informace o vytvoření VPN přístupu externímu uživateli,
- ukončí požadavek Garanta v ServiceDesku (čímž dojde k vygenerování a zaslání notifikačního emailu Garantovi).

4.1.3 Zrušení přístupu

Ke zrušení externího účtu nebo VPN přístupu může dojít za následujících podmínek:

- v oprávněných případech, kdy externí uživatel porušil pravidla a povinnosti uvedené v příloze č. 1, Povinnosti při připojování zařízení do sítě VFN,
- pokud je podezření na zavinění bezpečnostního nebo provozního incidentu či byl jakýmkoliv způsobem zapojen do kybernetického útoku na VFN,
- uplynula stanovená doba externího účtu nebo VPN přístupu (výchozí je 1 rok) nebo Garant nepotvrdil prodloužení externího účtu (čímž zanikne i související VPN přístup)
- nebo byl zadán požadavek na zrušení/ukončení externího účtu anebo VPN přístupu,
- požadavek je zpracován pracovníkem OSICT, který odebere členství v odpovídající AD skupině a následně předá na externí firmu Simac, která zruší profil v ISE.

4.2 POVINNOSTI, PRAVIDLA A RESTRIKCE

4.2.1 Povinnosti externích uživatelů

Uživatel v rámci připojení do sítě VFN:

- smí používat připojení pouze k účelům souvisejícím s výkonem smluvní činnosti v takovém rozsahu, který odpovídá potřebám uživatele pro výkon této činnosti,
- je povinen používat své připojení takovým způsobem, který nenaruší funkci sítě, informačních systémů a jejich dat ani práva ostatních uživatelů,
- je povinen chránit svá hesla před vyzrazením a v případě podezření, že heslo zná jiná osoba, heslo musí změnit přes portál http://www.office.com a tuto situaci neprodleně nahlásit jako incident dle bodu 4.2.1.1,
- je povinen zabránit využití či zneužití jeho vzdáleného připojení (VPN) třetí osobou,
- v případě podezření na bezpečnostní incident, nestandardní chování připojení nebo informačních systémů či jakékoliv náznaku na kybernetický útok neprodleně nahlásit toto podezření dle bodu 4.2.1.1,
- je povinen chovat se v souladu s dobrými mravy a právním řádem České republiky.

4.2.1.1 Nahlášení incidentu

V pracovní dny:

- od 7:00 do 16:00 na Dispečink ÚI na te[redacted]
- od 16:00 do 7:00 na Pohotovost ÚI na t[redacted]

O víkendu a svátcích na Pohotovost ÚI na tel. +[redacted]

4.2.2 Požadavky na připojené zařízení

Požadavky a povinnosti vztahující se na zařízení, které je používáno pro externí nebo VPN přístup, jsou uvedeny v příloze č. 1 (Povinnosti při připojování zařízení do sítě VFN) tohoto dokumentu.

4.2.3 Bezpečnostní incident nebo kybernetický útok

V případě bezpečnostní hrozby nebo kybernetického útoku má VFN právo zrušit povolení přístupu externího uživatele anebo VPN přístupu na dobu nezbytnou k analyzování hrozby nebo útoku a zabránění jakéhokoliv ohrožení sítě, informačních systémů a dat VFN. Pokud externí uživatel vykonává nebo má práva správce nebo

administrátora IS VFN, je povinen konat bezodkladně a zajistit dostatek důkazního materiálu dle povinností uvedených v příloze (Příloha č. 3 – Povinnost administrátora v případě bezpečnostního incidentu nebo kybernetického útoku).

4.2.4 Zakázané činnosti

Externí uživatel připojený do sítě VFN nesmí:

- v žádném případě poskytovat informace o přístupu, postupech, přístupová hesla, certifikáty, další citlivé informace a ani jejich části třetím osobám,
- umožnit přístup do sítě jiným osobám (např. umožnit přihlášení pod svým jménem),
- se jakýmkoliv způsobem angažovat při rozesílání a distribuci protiprávních, pomlouvačných, hanlivých, reklamních, agitačních a jiných zpráv,
- v žádném případě předávat jakékoli důvěrné informace získané tímto přístupem třetím osobám (osobní údaje, číselníky, databáze, atd.),
- v síti VFN vyhledávat důvěrné nebo jinak citlivé informace, snažit se získat neautorizovaný přístup k souborům a informacím,
- jakýmkoliv způsobem narušit funkci sítě, informačních systémů a dostupnost jejich dat,
- omezit práva uživatelů/správců ICT nebo získat práva nad rámec svých činností a oprávnění,
- v rámci VFN instalovat nebo ukládat jakýkoli neautorizovaný, nelegální nebo škodlivý software.

4.2.5 Monitoring činností

Veškeré činnosti externího připojení do sítě VFN jsou monitorovány a logovány a pravidelně vyhodnocovány architektem kybernetické bezpečnosti nebo jiným pověřeným zaměstnancem ÚI.

4.2.6 Porušení pravidel a povinností

Externímu uživateli, který poruší pravidla, nedodrží povinnosti nebo provádí zakázané činnosti (viz kap. 4.2):

- bude právo přístupu do sítě VFN neprodleně odebráno,
- porušení může být posuzováno jako závažné porušení povinností vyplývajících z právních předpisů a smluvního vztahu vztahujících se k externímu uživateli vykonávané práci a jednání v rozporu se zájmy VFN a uzavřeného smluvního vztahu.

Externí uživatel připojený do sítě VFN:

- plně zodpovídá za škody vzniklé v důsledku zneužití jeho přístupu zaviněného nedbalostí, nebo poskytnutím přístupu do sítě VFN třetí osobě,
- je plně zodpovědný za obsah svého datového prostoru.

4.3 REVIZE EXTERNÍHO PŘIPOJENÍ

Za oprávněnost, platnost a rozsah externího připojení odpovídá Garant, který v případě jakékoliv změny (zrušení, odebrání/přidání práv, apod.) zadá tuto změnu formou požadavku do ServiceDesku.

V rámci kontrolních mechanizmů je minimálně 1x ročně prováděna kontrola povolených externích uživatelů a připojení VPN v rámci pravidelných auditů KB prováděné auditorem KB nebo jiným pověřeným subjektem.

5 Závěrečná ustanovení

Tato směrnice je závazná pro všechny výše uvedené zaměstnance a externí subjekty v kap. 3 Odpovědnosti a pravomoci.

Porušení této směrnice bude posuzováno jako závažné porušení povinností vyplývajících z právních předpisů a smluvního vztahu vztahujících se k externímu uživateli vykonávané práci a jednání v rozporu se zájmy VFN a uzavřeného smluvního vztahu.

Tato směrnice podléhá revizi nejméně jednou ročně. Za provedení revize dokumentu odpovídá zpracovatel této směrnice.

6 Vznikající dokumenty a údaje

Název	Uchovává	Doba uchování

7 Související dokumenty

RD-VFN-11 Řád používání informačních systémů

F-VFN-463 Formulář: Žádost o zřízení přístupu externího uživatele do sítě VFN

8 Přílohy

Příloha č. 1 – Povinnosti při připojování zařízení do sítě VFN

Příloha č. 2 – Postup zřízení přístupu externímu uživateli do počítačové sítě VFN

Příloha č. 3 – Povinnost administrátora v případě bezpečnostního incidentu nebo kybernetického útoku

VŠEOBECNÁ FAKULTNÍ NEMOCNICE V PRAZE
U Nemocnice 499/2, 128 08 Praha 2 | www.vfn.cz, http://intranet.vfn.cz

POVINNOSTI PŘI PŘIPOJOVÁNÍ ZAŘÍZENÍ DO SÍTĚ VFN

Povinnosti při připojování zařízení do sítě VFN:

1) Připojení každého zařízení do LAN sítě VFN musí být předem konzultováno s Odborem správy ICT Úsekem informatiky a digitální transformace (dále jen ÚI) VFN.
2) Instalace a provozování jakéhokoli software v síti VFN musí být předem konzultováno s Odborem vývoje a správy SW ÚI VFN.
3) Je zakázáno svévolně zapojovat zařízení do LAN sítě a jakkoli měnit LAN síť VFN.
4) Je zakázáno měnit, instalovat a nahrávat jakýkoli softwarový obsah na zařízení VFN.
5) Je zakázáno jakýmkoli způsobem měnit a zasahovat do hardware vybavení VFN.
6) Je zakázáno využívat pro vzdálený přístup na připojovaná zařízení jiných než ÚI VFN schválených metod - viz níže.
7) Při umisťování IT zařízení (server, PC) do sítě VFN je vlastník IT zařízení povinen na své náklady, pokud není ve smlouvě uvedeno jinak, udržovat toto zařízení:
   a. v aktuálním (aktualizace operačního systému, aktualizace antivirového programu)
   b. v bezpečném (nemožnost jednoduše zneužít, používání silných přístupových hesel...) stavu.

   ÚI provádí náhodné testy zneužitelnosti zařízení. V případě zjištění hrozeb nebo nedostatků je vlastník IT zařízení povinen na své náklady zjištěné hrozby a nedostatky neprodleně odstranit.
8) Vlastník IT zařízení je povinen, na vyžádání ÚI, předložit ke kontrole konfiguraci IT zařízení. V situaci, kdy připojené zařízení způsobuje jakékoliv bezpečnostní anebo technické problémy v síti VFN, má VFN možnost takovéto zařízení bez předchozího upozornění odpojit od sítě VFN a externí účet (včetně VPN připojení) zablokovat nebo i zrušit.

Případné dotazy, požadavky nebo problémy je možné řešit na:

- od 7:00 do 16:00 Dispečink ÚI na tel. [redacted]

Metoda vzdáleného přístupu

K připojovaným zařízením je možné, pokud tomu nebrání další důvody, zřídit vzdálený přístup typu VPN připojení (IPSec tunel nebo jeho obdoba). Je nutná instalace Cisco VPN klienta.

Info: https://www.vfn.cz/vpn nebo Pohotovosti ÚI: [redacted] (mimo pracovní hodiny Dispečinku ÚI).

VŠEOBECNÁ FAKULTNÍ NEMOCNICE V PRAZE
U Nemocnice 499/2, 128 08 Praha 2 | www.vfn.cz, http://intranet.vfn.cz

POSTUP ZŘÍZENÍ PŘÍSTUPU EXTERNÍMU UŽIVATELI DO POČÍTAČOVÉ SÍTĚ VFN

Postup

Postup žádosti o povolení přístupu do počítačové sítě VFN:

- Žadatel si stáhne, vytiskne a vyplní formulář F-VFN-463.
- Žadatel se dostaví s vyplněným a NEPODEPSANÝM formulářem na Dispečink Úseku informatiky a digitální transformace (dále jen Dispečink ÚI) ve VFN (Budova ředitelství A5, pracovní dny 7:00 – 16:00).
- Pracovník Dispečinku ÚI ověří identitu žadatele (OP, pas). Žadatel podepíše formulář.
- Pracovník Dispečinku ÚI zašle na uvedeného Garanta e-mail s žádostí o schválení validity požadovaného přístupu a rozsahu přístupu. V případě požadavku na VPN připojení, je Garant upozorněn.
- Po obdržení potvrzení od Garanta bude vytvořen přístupový účet externího uživatele a případně VPN přístup.
- Žadatel bude o schválení a zřízení přístupového účtu informován e-mailem.
- Žadatel se dostaví na Dispečink ÚI a vyzvedne si uživatelské jméno a heslo. Heslo je doporučeno si na místě změnit.
- Expirace přístupového účtu je max. po 1 roce od zřízení. Žadatel i Garant bude 1 měsíc před expirací upozorněn na zadaný e-mail. O prodloužení přístupového účtu žádá Garant e-mailem – jako odpověď na e-mail s upozorněním na expiraci.

Upozornění: *Přístup do počítačové sítě VFN se nezřizuje na počkání!*

Povinnosti, pravidla a omezení

Po dobu platnosti účtu externího uživatele je externí uživatel povinen dodržovat následující:

- stanovené povinnosti, pravidla a případné restrikce v kap. 4.2 Řádu používání sítě VFN externími uživateli (SM-UI-02),
- při používání VPN přístupu:
  - stanovené povinnosti pro připojování zařízení do sítě VFN definované v příloze č. 1 (SM-UI-02),
  - návody a postupy pro VPN připojení do sítě VFN uvedené na webových stránkách https://www.vfn.cz/vpn,
- aktuální informace uvedená na webových stránkách https://www.vfn.cz/externista.

Dokumenty ke stažení

- Formulář F-VFN-463 Žádost o zřízení přístupu externího uživatele do sítě VFN
- Řád používání sítě VFN externími uživateli (SM-UI-02)

Kontakt

Dispečink ÚI

- Všeobecná fakultní nemocnice v Praze, U Nemocnice 499/2, 128 08 Praha 2
- Telefon: [redacted]
- E-mail: [redacted]

VŠEOBECNÁ FAKULTNÍ NEMOCNICE V PRAZE
U Nemocnice 499/2, 128 08 Praha 2 | www.vfn.cz, http://intranet.vfn.cz

POVINNOST ADMINISTRÁTORA V PŘÍPADĚ BEZPEČNOSTNÍHO INCIDENTU NEBO KYBERNETICKÉHO ÚTOKU

Povinnosti administrátora

V případě podezření či probíhajícím bezpečnostním incidentu nebo kybernetickém útoku je povinností správce nebo administrátora konat bezodkladně a zajistit dostatek důkazního materiálu:

- k identifikaci zdroje nebo příčiny,
- k čemu došlo nebo jak se projevuje,
- důsledkům a možným dopadům,

u tohoto incidentu či útoku je vždy povinen:

- zajistit kopie logů nebo transakčních záznamů, pokud by to nezpůsobilo jejich poškození nebo smazání,
- iniciovat nebo pozastavit šíření či poškození, zamezit incidentu nebo útoku,
- nemazat jakákoliv data o kybernetickém bezpečnostním incidentu bez svolení VFN, Policie ČR nebo NÚKIB,
- nahlásit toto podezření neodkladně na Pohotovost ÚI jako bezpečnostní nebo kybernetický incident:
  - v pracovní dny:
    - od 7:00 do 16:00 na Dispečink ÚI na t[redacted]
    - od 16:00 do 7:00 na Pohotovost ÚI na
  - o víkendu a svátcích na Pohotovost ÚI na tel.

Příloha č. 5 - Požadavky systému řízení bezpečnosti informací na dodavatele

1 Účel

Účelem toho dokumentu je stanovit požadavky vyplývající ze systému řízení bezpečnosti informací ve VFN pro Dodavatele jako provozovatele, Poskytovatele služeb nebo zajišťující podporu základních služeb: zdravotních služeb dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen ZKB).
Příloha vymezuje obecná pravidla a zásady kybernetické bezpečnosti vztahující se na smluvní plnění Dodavatele, pokud nejsou detailně specifikovány Smlouvou. Tato příloha nerozšiřuje předmět plnění Dodavatele vymezený smlouvou, ale pouze specifikuje relevantní požadavky systému řízení bezpečnosti informací ve VFN, které musí Dodavatel při plnění dodržovat.
Dodavatel je povinen prokazatelně seznámit všechny své zainteresované zaměstnance s obsahem tohoto dokumentu.

2 Bezpečnostní požadavky

Dodavatel ve vztahu k předmětu plnění smlouvy musí definovat v interních předpisech, konfiguračních a instalačních manuálech, postupech nebo jiných dokumentech sloužících k předmětu dodávané služby či musí plnit zde popsané povinnosti.

2.1 Obecná pravidla bezpečnosti informací

Dodavatel je povinen:

- vydefinovat rozsah prací/služeb/podpory v kompetenci Dodavatele a podmínky spolupráce mezi smluvními stranami,
- specifikovat popis používání každé služby provozované nebo spravované Dodavatelem,
- stanovit cílové úrovně služby a neakceptovatelné nebo zakázané úrovně služby,
- vést seznam jednotlivců, kteří vzhledem ke svým předdefinovaným právům a privilegiím jsou oprávněni zajišťovat smluvní služby,
- umožnit VFN právo monitorovat nebo auditovat smluvní povinnosti i u Dodavatele,
- stanovit popis eskalace problému v případech řešení havárie s popisem pravidel pro řešení havarijních situací,
- zajistit školení zainteresovaných uživatelů a správců Dodavatele v metodách, postupech a v bezpečnosti,
- upřesnit podmínky spolupráce Dodavatele se subdodavateli (třetí stranou),
- informovat Objednatele o způsobu řízení rizik a o zbytkových rizicích,
- informovat o významné změně dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, či ekvivalentním postavení, nebo o změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy,
- provést neprodlené nahlášení identifikovaných bezpečnostních událostí a slabin kontaktní osobě za VFN.

2.2 Fyzická bezpečnost

Dodavatel je povinen:

- nastavit komplexní opatření fyzické bezpečnosti v prostředí Dodavatele, jež zabrání nebo sníží pravděpodobnost vzniku ohrožení IS základní služby, ztrát dat a jiného duševního vlastnictví, přerušení činností či poškozování jiných důležitých zájmů VFN,
- dodržovat režimová nebo organizační opatření VFN při vjezdu do objektů nebo vstupu do prostor nebo překonávání fyzických/logických zábran těchto objektů nebo prostor VFN,
- dobrovolně se podrobit případným kontrolám vnášených/vynášených osobních věcí nebo jakýchkoliv předmětů při vstupu nebo odchodu z objektů nebo prostor VFN prováděné oprávněnými zaměstnanci VFN (ostraha, vrátný, recepce apod.),
- neprovádět fotografování, video/audio záznam nebo kopírování/scanování dokumentů bez souhlasu oprávněného zaměstnance VFN. V prostorách kategorie zóny „C" (např. serverovna) pouze na základě písemného povolení vedení VFN.

2.3 Bezpečnost lidských zdrojů

Dodavatel je povinen:

- prokazatelně seznámit zaměstnance Dodavatele s dodržováním bezpečnostních pravidel a zásad požadovaných VFN,
- dodržovat ochranu aktiv VFN před neautorizovaným přístupem, vyzrazením, modifikací, zničením nebo narušením,
- zachovávat mlčenlivost o důvěrných údajích nebo sděleních VFN a o jejich ochraně,
- stanovit odpovědnosti zaměstnanců Dodavatele pro nakládání s informacemi,
- poučit zaměstnance Dodavatele hlásit zjištěné bezpečnostní události nebo jiná bezpečnostní rizika odpovědné osobě Dodavatele,
- provádět pravidelné školení zaměstnanců Dodavatele v souvislosti s bezpečností informací,
- při porušení pracovních povinnosti zaměstnance Dodavatele ve vztahu k bezpečnosti informací nebo způsobení bezpečnostního incidentu, musí být zahájeno formální disciplinární řízení. Způsob řízení odpovídá povaze porušení nebo incidentu a jeho dopadu na VFN.

2.4 Řízení přístupu

Dodavatel je povinen:

- dodržovat princip minimálních oprávnění: přidělovat oprávnění na nejnižší možné úrovni, která umožní jejich správnou funkci,
- dodržovat požadavky na řízení přístupu:
    - definovat procesy přidělování, správy oprávnění, pravidelně provádět audit přidělených oprávnění a odstraňovat účty při odchodu zaměstnance nebo změně jeho zařazení,
    - přidělovat privilegovaná oprávnění takovým způsobem, aby byla zajištěna jednoznačná auditovatelnost všech kroků provedených pod těmito účty ve vztahu ke konkrétním osobám.

2.5 Bezpečné chování uživatelů

Uvedené povinnosti se vztahují na prostředí VFN nebo zařízení používané ke správě nebo administraci předmětu smlouvy.
Zaměstnanec Dodavatele:

- nesmí šířit a vědomě používat SW získaný v rozporu s právními předpisy, zejména s autorským zákonem a SW, získaný v souladu s těmito předpisy nesmí užívat v rozporu se smlouvou,
- musí používat počítačové prostředky a SW vybavení VFN jen v rámci smluvního ujednání a stanovené kompetence,
- je povinen respektovat pravidla tvorby a nakládání s přístupovými hesly definovaná VFN,
- je povinen zachovávat důvěrnost hesel jemu přidělených v rámci své kompetence,
- nesmí žádnými prostředky se pokusit získat přístupová práva či privilegovaný stav, který mu nebyl přidělen,
- nesmí se pokusit získat přístup k chráněným informacím a datům jiných uživatelů nebo systémů,
- musí dodržovat předepsaná opatření pro užití prostředků pro vzdálený přístup (aktualizace systému, spuštěný FW a antivir, využití veřejných sítí apod.).

2.6 Bezpečnost mobilních zařízení a vzdáleného přístupu

Přístup externích zařízení do prostředí Objednatele je možný po provedení registrace zařízení při dodržení postupu „Přístup do počítačové sítě VFN pro externí zaměstnance/firmy“, zde uvedených povinností a směrnice Používání sítě VFN externími uživateli (SM-UI-02). Uživatel Dodavatele připojený do sítě VFN je povinen:

- používat je pouze k účelům a po dobu souvisejícím s výkonem smluvní činnosti v takovém rozsahu, který odpovídá potřebám uživatele pro výkon této činnosti,
- používat své připojení takovým způsobem, který nenaruší funkci sítě ani práva ostatních uživatelů,
- chránit svá hesla před vyzrazením, a v případě podezření, že heslo zná jiná osoba, tuto situaci neprodleně nahlásit Poskytovateli připojení,
- zabránit využití či zneužití jeho vzdáleného připojení třetí osobou,
- chovat se v souladu s dobrými mravy a právním řádem České republiky.

2.7 Ochrana před škodlivým kódem

Ve vztahu k dodavatelským pracím a službám zajišťujícím provoz a fungování základních služeb VFN musí být zajištěna ochrana vnějšího perimetru Dodavatele, komunikace, IS, úložišť a koncových stanic nebo mobilních zařízení před škodlivým kódem.

2.8 Zálohování a obnova dat

Dodavatel je povinen provádět zálohování dat a informací v provozovaných nebo spravovaných HW, IS a jejich datech k zajištění jejich dostupnosti v případě nestandardních událostí (chyba paměťového média, havárie systému, poškození integrity dat atp.), aby bylo možné zálohovaná data použít pro jejich obnovu nebo přesun do jiného prostředí.
Zálohovaná data musí splňovat požadavky:

- na kompletní obnovu dat,
- dodržet maximálně tolerovaný prostoj (MTD) definovaný ve smlouvě,
- pravidelné provádění záloh a testování jejich obnovy,
- zajištění ochrany záloh a obsažených dat včetně jejich integrity,
- vydefinovaná správa (včetně řízení přístupu), doba uchování, cykly a počet kopií zálohovaných dat.

2.9 Technické zranitelnosti

Dodavatel je povinen:

- identifikovat a odstraňovat technické zranitelnosti spojené s bezpečnostním nastavením nebo fungováním jím provozovaných/spravovaných zařízení nebo systémů,
- upozorňovat VFN na identifikované zranitelnosti zařízení nebo systémů ve správě VFN nebo subdodavatelů,
- provádět ověření/testování opravy zranitelnosti v testovacím nebo integračním prostředí před instalací opravy programového vybavení do produkčního prostředí.

2.10 Bezpečnost komunikační sítě

Dodavatel je povinen omezit riziko napadení systémů nebo služeb prostřednictvím počítačové sítě, např. využitím:

- šifrování,
- řízené kontroly přístupu,
- zamezením napadení aktivním útočníkem,
- řízením zátěže,
- zajištěním integrity dat,
- samostatné lokální sítě,
- víceúrovňovou bezpečností,
- využitím vhodné sítě.

2.11 Bezpečnostní zásady pro práci s daty

Dodavatel je povinen:

- dodržovat stanovená pravidla ochrany dat zahrnující speciální nakládání s tajnými, důvěrnými, osobními a citlivými údaji dle jednotlivých zákonů (např. nařízení č. 2016/679 - GDPR, zákona č. 110/2019 Sb., zákon č. 412/2005 Sb. apod.),
- zajistit řízení přístupu k datům s využitím principu minimálních oprávnění,
- ochránit data při přenosu, předání a v datovém úložišti,
- plnit povinnosti ochrany osobních údajů, a to především technická nebo organizační opatření, hlášení úniku osobních údajů, spolupráce na řešení incidentů nebo auditu ochrany osobních údajů apod.,
- dodržet závazek dodavatele (a subdodavatele) neporušovat integritu a dostupnost aktiv,
- stanovit omezení platná pro kopírování a šíření informací,
- přijmout opatření zajišťující vrácení či zničení informací po ukončení smluvního vztahu nebo v jeho průběhu,
- definovat postupy bezpečné likvidace dat.

2.12 Používání kryptografické ochrany

Dodavatel je povinen:

- využívat úrovně ochrany s ohledem na typ a sílu kryptografického algoritmu ve vztahu k citlivosti jednotlivých informačních aktiv,
- zohledňovat známá nebo odhalená rizika a zranitelnosti pro použité typy a síly kryptografických algoritmů výměnou za „bezpečné" (neprolomené) kryptografické algoritmy.

2.13 Akvizice, vývoj a údržba informačních systémů

Dodavatel je povinen:

- dodržovat bezpečnostní pravidla, noremy a best practices (např. OWASP - Open Web Application Security Project) v rámci celého životního cyklu nákupu a vývoje SW od zadání, návrhu, přes vývoj a testování až po nasazení do provozu,
- zavést oddělení rolí vývoje, testu a provozu; vytvářet a provozovat vývojové, integrační, testovací a provozní prostředí tak, aby byla zcela oddělena v sítích a byla podporována oddělenými stroji,
- zohlednit bezpečnostní požadavky VFN na dodávaný nebo vyvíjený SW, a to především:
    - podporované frameworky a platformy v prostředí VFN,
    - nefunkční bezpečnostní požadavky,
    - provádět ověření codereview v jednotlivých fázích vývoje a testování,
    - spolupracovat na bezpečnostním testování včetně penetračních testů,
    - dodávat systémové a provozní bezpečnostní dokumentace,
- stanovit způsob převzetí, akceptace a instalaci do produkčního prostředí,
- používat jasný a specifikovaný proces řízení změn.

2.14 Zvládání bezpečnostních incidentů

Dodavatel je povinen:

- mít ve svém prostředí zavedený systém hlášení, upozorňování a vyšetřování bezpečnostních nebo kybernetických incidentů a případů prolomení bezpečnosti,
- neprodleně oznámit Objednateli bezpečnostní nebo kybernetický incidenty a prolomení bezpečnosti v prostředí Dodavatele nebo Objednatele,
- spolupracovat s Objednatelem na vyšetření, vyhodnocení a přijetí opatření z bezpečnostního nebo kybernetického incidentu v prostředí Objednatele.

2.15 Řízení kontinuity činností

Dodavatel je povinen:

- vytvořit takové postupy a fungující prostředí, které umožní zajistit kontinuitu a obnovu klíčových procesů a činností základních služeb VFN provozovaných nebo spravovaných Dodavatelem HW, IS a jejich dat v případě jejich narušení nebo ztráty,
- provádět pravidelné testování, vyhodnocování a případně aktualizování havarijních plánů obnovy (DRP).

2.16 Legislativní a normativní požadavky

Dodavatel je povinen splnit legislativní a normativní požadavky:

- zákon č. 181/2014 Sb., o kybernetické bezpečnosti a vyhlášku č. 82/2018Sb., o kybernetické bezpečnosti,
- nařízení EU č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR),
- zákon č. 110/2019 Sb., zpracování osobních údajů,
- směrnici EU č. 2016/1148, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů (NIS),
- nařízení EU č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (eIDAS),
- standardy systému řízení bezpečnosti řady ISO/IEC 27000 – Information Security Management System (ISMS), především ISO/IEC 27001, ISO/IEC 27002 a ISO/IEC 27799,
- a související normy nebo best-practice.

2.17 Kontroly zavedení bezpečnostních opatření

Dodavatel je povinen provádět kontroly zavedených bezpečnostních opatření v prostředí Dodavatele v pravidelných intervalech a následně přijímat odpovídající preventivní nebo systémová nebo organizační opatření na zjištěné nedostatky nebo zranitelnosti a umožnit VFN ověření provádění kontrol a aplikaci následných opatření.

2.18 Audity plnění bezpečnostních požadavků

Dodavatel je povinen umožnit VFN provedení auditu plnění požadavků uvedených v tomto dokumentu nebo s kterými byl prokazatelně Dodavatel seznámen, a to po předchozím upozornění. Audit bude proveden zaměstnanci VFN nebo jím smluvně pověřeným subjektem.