Financováno Evropskou unií
NextGenerationEU

PO 890/S/23

SMLOUVA – ŘEŠENÍ PRO ŘÍZENÍ A SPRÁVU PRIVILEGOVANÝCH OPRÁVNĚNÍ (PIM/PAM)

Be a Future s.r.o.
zapsána: v obchodním rejstříku vedeném Městským soudem v Praze pod sp. zn oddíl C, vložka 285925
se sídlem: Karlovo náměstí 313/8, Nové Město, 120 00 Praha 2
IČ: 04876041 DIČ: CZ04876041
zastoupená: Ing. Petrem Šindelářem, jednatelem společnosti

bankovní spojení: xxxxx
číslo účtu: xxxxx

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
zastoupená: prof. MUDr. Davidem Feltlem, Ph.D., MBA, ředitelem
bankovní spojení: ČNB
číslo účtu: 24035021/0710

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

uzavírají dnešního dne na základě výsledku **nadlimitní veřejné zakázky** s názvem „**Řešení pro řízení a správu privilegovaných oprávnění (PIM/PAM)**", **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. Z2023-038364 ze dne 31.8. 2023 **a v Úředním věstníku Evropské unie pod č. oznámení o zahájení zadávacího řízení 2023/S 168-525629 ze dne 01.09.2023** (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 HW appliance v režimu high availability (HA) včetně časově neomezených užívacích práv k SW nástroji pro řízení a správu privilegovaných oprávnění (PIM/PAM) název Password Safe pro 105 uživatelů/administrátorů (30 interních a 75 externích) pro zabezpečení napojení na 150 koncových systémů objednatele a pro zabezpečení 25-ti aplikačních účtů (dále také „řešení" nebo „předmět plnění").

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,
  - návrhy procesů,
  - 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 dodání časově neomezených užívacích práv k SW, tj. jeho montáž, instalace HW včetně všech komponent v místě plnění, základní konfigurace HW a zprovoznění v režimu vysoké dostupnosti (dále také HA) a předání souvisejících dokladů.
Na základě technických a funkčních specifikací uvedených v příloze č. 1 a provedené předimplementační analýzy (čl. I. odst. 1a)) bude dodán HW a SW v následujícím rozsahu, kde dodavatel zajistí:

- montáž a instalaci všech HW komponent do technologických stojanů (RACK) včetně označení a vyvázání kabelů,
- instalaci softwarového vybavení a instalační konfiguraci systému PIM/PAM,
- předání souvisejících dokladů.

c) implementační práce, které obsahují:

- instalaci SW,
- systémovou konfiguraci,
- nastavení procesů/postupů nezbytných k zavedení a správě privilegovaných účtů,
- integrace na vyjmenované systémy/aplikace/služby v rozsahu účtů uvedené v příloze č. 2 této smlouvy.
- napojení nebo přenesení privilegovaných účtů pod správu řešení PIM/PAM,
- vytvoření záložních/záchranných přístupů při nedostupnosti/nefunkčnosti řešení PIM/PAM (např. lokální účty, Break Glass účet),
- nastavení zálohování a postupů obnovy,
- zdokumentování instalačních, konfiguračních, integračních, záložních a záchranných postupů,
- ověření systémového a integračního nastavení.

d) dodání technické, provozní a administrátorské dokumentace:
Dodavatel vypracuje a předá podrobnou dokumentaci PIM/PAM v CZ jazyce, zahrnující popis nebo postupy minimálně pro tyto oblasti:

- Technická dokumentace – popis architektury, systémů, konfigurací, nastavení a integrace řešení,
- Procesní dokumentace – nastavení postupů a procesů pro zavedení a správu privilegovaných účtů,
- 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 a auditory.

e) zaškolení administrátorů a auditorů
Zajištění školení dodavatelem pro dodaný systém PIM/PAM v rozsahu provozní a administrátorské dokumentace pro zaměstnance VFN (min. 10 zaměstnanců objednatele):

- na procesy a postupy zavedení a správy privilegovaných účtů,
- správy řešení PIM/PAM,
- používání a schvalování přiřazení privilegovaných oprávnění,
- nastavení monitorovacích funkcí a kontrolních zásad/politik/omezení,
- způsob vyhodnocení a možnosti vyhledání činností v zaznamenaných relacích,
- sledování relací v reálném čase s možností zásahů do jejich průběhu,
- nastavení alertingu a blokačních pravidel,
- možnosti auditování a využití jako forensní důkazy (auditní stopa),
- a dalších pokročilých funkcí řešení (např. behaviorální biometrie, osobní trezor, rizikové chování účtů, vyhodnocení nekalých praktik apod.).

f) spuštění testovacího prostředí a pilotní provoz
Před překlopením do produkčního provozu dodavatel provede ověření postupů při zavádění a použití privilegovaných účtů spolu s napojením na spravované systémy nebo aplikace v testovacím nebo pilotním provozu tak, aby při spuštění nedošlo ke kolizním nebo omezujícím stavům při zajištění provozu těchto systémů a aplikací. Současně dodavatel v rámci tohoto testovacího nebo pilotního provozu provede ověření základní funkčnosti 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 systému (systém nesplňuje účel, pro který byl vytvořen, nebo uživatelé nemohou používat všechny používané funkcionality) nebo/a zároveň,

- činí zcela nefunkčním některou z komponent systému PIM/PAM nebo/a zároveň,
- způsobuje, že systém vykazuje nepřiměřeně dlouhé odezvy nebo/a zároveň,
- systém 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 (systém 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 bod g) je řešení přeneseno objednatelem do produkčního prostředí v součinnosti s dodavatelem.

i) audit nastavení
Součástí dodávaného řešení bude provedení auditu nastavení řešení zaměřené na:
- změny nastavení řešení a jeho konfigurace,
- zavedených procesů/postupů,
- nastavených integrací,
- napojených účtu,
- kontrolních nebo blokačních mechanismů,
- alertingu,
- uchovávaných relací,

Výstupní zpráva bude obsahovat doporučení a návrhy změn nastavení nebo fungování celého řešení PIM/PAM dle doporučení výrobce, „best practice" a zkušeností techniků dodavatele.

Audit nastavení bude dodavatelem proveden 2 x, a to v intervalu po 6-ti měsících ode dne akceptace dodaného řešení a po 12-ti měsících od akceptace dodaného řešení. Každý z Auditu nastavení bude proveden a výstupní zpráva bude předložena objednateli k odsouhlasení nejpozději do 14-ti kalendářních dnů ode dne zahájení jednotlivého Auditu nastavení.

j) záruku a zajištění poskytování záručního servisu

k) služby na vyžádání
Služby na vyžádání technického specialisty nad rámec předmětu plnění, který je uveden v čl. I. odst. 1 a) až j) 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. Dodavatel 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.
3. 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.
4. 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.
5. 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 150 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 3 pracovní dny před realizací dodávky. Při předání a převzetí HW bude pověřenými osobami obou smluvních stran podepsán dodací list.

Kontaktní a odpovědná osoba za objednatele:
Za systémovou/technickou dodávku/: xxxx, tel.: xxxxx, e-mail: xxxxx
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: xxxxx
Za identifikaci případného kybernetického útoku v průběhu plnění předmětu plnění dle této smlouvy: manažer KB, e-mail: xxxxx
Za ochranu osobních údajů: Pověřenec, e-mail: xxxxx

Kontaktní a odpovědná osoba za dodavatele: xxxxx, jednatel společnosti, tel. xxxxx, e-mail: xxxxx

Za systémovou/technickou dodávku: xxxxx, tel. xxxxx, email: xxxxx
Za předání HW: xxxxx, tel.: xxxxx, email: xxxxx
Za akceptaci předmětu plnění: xxxxx, tel.: xxxxx, email: xxxxx
K poskytování záručního servisu: xxxxx, tel.: xxxxx, email: xxxxx
Za identifikaci případného kybernetického útoku v průběhu plnění předmětu plnění dle této smlouvy: xxxxx, tel.: xxxxx, email: 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 a auditorů 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 SW 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 řádné 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 řádné 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. 5 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 systému PIM/PAM, 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 systému PIM/PAM. Hlavní úlohou je zajištění bezvýpadkového provozu systému, realizace proaktivních činností, kterými se bude výpadkům předcházet a v případě výpadku uvedení systému 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 funkčnost provozu systému 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 12 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 systému PIM/PAM nebo/a zároveň,
- způsobuje, že systém vykazuje nepřiměřeně dlouhé odezvy nebo/a zároveň,
- systém 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 (systém 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,

*****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 systému, které jsou vyžadovány pro zajištění bezpečnosti systému nebo rozvojových aktivit, včetně zajištění funkčnosti celého sytému po provedeném upgradu.
- Aktualizace dokumentace.
- Ostatní nevyjmenované práce nutné pro zajištění funkčnosti systému.

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 60 měsíců, 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 za VFN (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 této smlouvy byla sjednána ve výši:

Celková cena bez DPH	**6 997 224,00 Kč**
DPH	**1 469 417,04 Kč**
Cena vč. DPH	**8 466 641,04 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 k) této smlouvy činí **1875,00 bez DPH** za hodinu práce dodavatele.
4. Objednatel se zavazuje zaplatit cenu uvedenou v čl. IV. odst. 1 této smlouvy na základě faktur vystavené dodavatelem na základě plnění. 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 může být zaslána elektronicky ve formátu PDF nebo ISDOC na e-mailovou adresu: xxxxx nebo poštou ve dvou vyhotoveních na Ekonomický úsek objednatele, odbor účetnictví. K faktuře bude přiložena kopie řádně opatřeného dodacího listu způsobem sjednaným výše v čl. II. V případě zaslání faktury elektronicky bude dodací list přiložen v neskenované podobě.
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 čísla projektu. CZ.31.1.01/MV/23_50/0000050 a CZ.31.2.0/0.0/0.0/22_054/0007984
10. Faktury se platí bankovním převodem na účet druhé smluvní strany uvedený na faktuře. Povinnost objednatele zaplatit dodavateli vyúčtovanou dohodnutou 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 kupující 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 objednatelem nedohodne jinak. Objednatel je dále v těchto případech 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 5.000,- 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 3.000,- 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. Za nedodržení termínu odevzdání výstupní zprávy uvedeného v čl. I, odst. 1 bodu i) do 14-ti kalendářních dnů ode dne zahájení jednotlivého auditu nastavení, má objednatel právo účtovat jednorázovou smluvní pokutu ve výši 50.000,- Kč. Dále je objednatel oprávněn požadovat zaplacení další smluvní pokuty ve výši 1.000,- Kč za každý započatý kalendářní den prodlení za jednotlivý případ.
7. 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.
8. 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.
9. Za nedodržení povinností uvedených v čl. I. odst. 2 a 3 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.
10. 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.
11. 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.
12. 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. VIII, 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 zákona 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 2031 nebo po dobu nejméně 5 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 2033 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 včetně příloh je vyhotovena ve 2 stejnopisech, z nichž každá strana obdrží po jednom vyhotovení. Obě vyhotovení jsou rovnocenná a mají platnost originálu.
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:

---

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

V Praze dne:

Ing. Petr Šindelář
jednatel společnosti

Příloha č. 1 smlouvy

ŘEŠENÍ PRO ŘÍZENÍ A SPRÁVU PRIVILEGOVANÝCH OPRÁVNĚNÍ (PIM/PAM)

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 (tab. č.1), která slouží pro posouzení zadavatelem, zdali nabízené řešení splňuje požadavky na HW/SW.

Tabulka č. 1

#	Oblast	Popis požadavku	Odpověď uchazeče (ANO/NE/pozn.)
	Funkční požadavky		
1	Řízení přístupů	Řešení poskytuje nástroj pro správu privilegovaných účtů, řízení přístupu k těmto účtům a monitoring veškerých aktivit privilegovaných účtů. Uživatelské přístupy jsou řízeny bezpečnostní politikou, kdy má vybraný uživatel práva přístupu pouze k definovaným účtům a systémům. Účty a systémy, ke kterým nemá práva přístupu, nejsou pro uživatele viditelné.	ANO
2	Striktní oddělení přístupových oprávnění	Systém plně podporuje multi-tenant prostředí. Uživatelé/skupiny uživatelů mají přístup pouze k vybraným účtům, systémům, auditním záznamům, konfiguraci atp. I správce/administrátor řešení má povolen přístup pouze k vybraným složkám a konfiguraci.	ANO
3	Oddělení administrátorských oprávnění	Řešení musí umožňovat napojení na MS AD Tier model nebo možnost aplikování oddělení privilegovaných (administrátorských) oprávnění do 3 vrstev (doménová, serverová, klientská stanice), kdy přístup do nižší vrstvy je blokován a do vyšší vrstvy je ověřován (schvalován).	ANO

#	Oblast	Popis požadavku	Odpověď uchazeče (ANO/NE/pozn.)
4	Víceúrovňové schvalování přístupů	Řešení umožňuje víceúrovňové schvalování správcovských přístupů k cílovým systémům – přístupy lze omezit dle vybraného účtu, nebo na daný časový úsek. Schvalování přístupu lze vynutit odděleně pro přístup přihlašovacím údajům privilegovaného účtu, nebo pro připojení na koncový systém. O nových žádostech, schválení a zamítnutí budou uživatelé upozornění emailem, vytvořením ticketu v helpdesk systému apod.	ANO
5	Bezpečnostní parametry	Řešení zaručuje vysokou bezpečnost přenášených a uložených informací (confidentiality, integrity, availability). Uložené informace, včetně nahrávek a spravovaných přihlašovacích údajů, jsou uloženy v jedné centrální a vysoce zabezpečené databázi. Řešení musí umožňovat omezení práv správce systému tak, aby neměl sám přístup k uloženým přihlašovacím údajům, logům, nebo nahrávkám, bez autorizace vlastníků dat. Systém jako celek musí být certifikovaný bezpečnostním standardem Common Criteria anebo ekvivaletní certifikaci.	ANO
6	Uživatelské rozhraní	Přístup k uživatelskému rozhraní je požadovaný přes webový portál s možností ověření přes LDAP/MS Active Directory a druhým faktorem (minimálně PKI karty, RSA ID, Radius server, ...).	ANO
7	Silná autentizace	Nástroj umožňuje vynutit silnou autentizaci uživatelů pro přístup k uloženým údajům i pro bezpečné vzdálené připojení. Silnou autentizací je míněna minimálně možnost kombinace jméno/heslo + druhý faktor (RADIUS, PKI, certifikát, atp...). Řešení umožňuje integraci s MFA nástroji třetích stran, minimálně Microsoft a Cisco.	ANO

#	Oblast	Popis požadavku	Odpověď uchazeče (ANO/NE/pozn.)
8	Šifrování a zabezpečení dat	Řešení musí splňovat standard FIPS 140-2 a šifrovací algoritmy minimálně na úrovni AES-256 a RSA-2048. Řešení umožňuje zadavateli splnit compliance požadavky pro ZKB, GDPR, PCI-DSS, SOX, HIPAA atd.	ANO
9	Jednorázové povýšení oprávnění	Nástroj umožňuje povýšení oprávnění běžných (neprivilegovaných) uživatelů na koncových systémech bez nutnosti instalace agentského řešení. Řešení umožňuje povyšování oprávnění na základě požadavku, příslušnosti do AD skupiny, případně na časově omezené období.	ANO
	Password Management		
10	Vyhledávání a přidávání privilegovaných účtů	Řešení umožňuje vyhledávat privilegované účty v operačních systémech/LDAP/Active Directory a přidat je (manuálně i automaticky) do systému řízení přístupu dle bezpečnostní politiky. Vyhledávání účtů nevyužívá instalaci agentů na koncová zařízení. Systém umožňuje vyhledávání v on-premise i cloud prostředí (např. AWS).	ANO
11	Řízení hesel a SSH klíčů	Řešení umožňuje automatickou výměnu hesel a SSH klíčů privilegovaných účtů po ukončení relace (jednorázové heslo), nebo v pravidelných intervalech dle bezpečnostní politiky. Rotaci hesla/SSH klíče lze vynutit i uživatelem. Hesla a SSH klíče se vyměňují bez agentů.	ANO
12	Ověřování hesel	Řešení kontroluje v pravidelných intervalech shodu uloženého hesla v systému řízení přístupů a cílovém bodu. V případě neshody vynutí synchronizaci, nebo zašle upozornění správci.	ANO
13	Řízení servisních účtů	Systém umožňuje vyhledat účty v MS Windows prostředí a jejich návaznost na další služby/aplikace (services, sheduled tasks, IIS pool, COM+ object, ...). Při vynucení změny	ANO

#	Oblast	Popis požadavku	Odpověď uchazeče (ANO/NE/pozn.)
		hesla je heslo propsáno i do návazných služeb.	
14	Vyhledání tzv. backdoor účtů a automatický onboarding	Systém umožňuje pravidelné vyhledávání účtů, které nejsou řešením spravovány, ale jsou používány pro přístupy na koncové systémy. Systém takové účty dokáže vyhledat, upozornit na jejich použití a případně automaticky zařadit do správy. Řešení zároveň umožňuje detekci nespravovaných účtů v reálném čase a automatické uložení a vynucení změny hesla.	ANO
15	Customizace Password Management	Řešení musí umožňovat možnost úpravy systému password management, tak aby bylo možné integrovat další systémy zadavatele. Úpravy je možné provádět pomocí nástroje dodávaného výrobcem a případně úpravou konfiguračních souborů.	ANO
	Řízení vzdálených relací		
16	Izolace relací	Správcovský přístup na cílový systém bude zprostředkován pomocí tzv. terminal/jump serveru prostřednictvím zvoleného komunikačního protokolu, aplikace a příslušného privilegovaného účtu tak, aby koncový uživatel neměl přístup k přihlašovacím údajům. Izolace přístupu je možná až na úroveň aplikace (typu webový prohlížeč s konkrétní URL, MMC konzole s vybraným snap-in, konkrétní aplikace... např. MS SQL Management Studio, WinSCP atp.), kdy uživatel nemá možnost přistupovat k jiným službám, aplikacím v rámci dané relace. Po ukončení aplikace se uzavře spojení celé relace. Vzdálené připojení k relaci lze navázat jak přes vlastní GUI dodaného řešení, tak i pomocí standardních protokolů RDP a SSH a standardních klientů typu putty a remote desktop manager. U všech možností	ANO

#	Oblast	Popis požadavku	Odpověď uchazeče (ANO/NE/pozn.)
		připojení ke vzdálené relaci musí být podporováno vynucení silné autentizace (minimálně integrace s LDAP a RADIUS).	
17	Izolace SSH relací	Správcovský přístup prostřednictvím SSH protokolu se bude provádět přes SSH Proxy, kde bude uživatel ověřený svými přihlašovacími údaji (je možné spárovat s MS Active Directory) a bude připojený zvoleným privilegovaným účtem na cílový systém bez zadávání hesla a dle bezpečnostní politiky. Pro připojení pomocí SSH Proxy je vyžadována podpora silné autentizace (minimálně integrace s LDAP, RADIUS, či autentizace pomocí SSH klíče).	ANO
18	Připojení do webových relací	Řešení umožňuje zprostředkovat uživateli bezpečné připojení na vybrané webové aplikace a sociální sítě pomocí tzv. Webové proxy. Řešení umožní uživateli přihlášení do vybrané webové aplikace pomocí standardního (neprivilegovaného) účtu, webová proxy následně zprostředkuje přihlášení do koncové aplikace pomocí silného "privilegovaného" účtu. Uživatel nemusí znát hesla privilegovaných účtů a je mu umožněno transparentní SSO.	ANO
19	Vzdálené připojení pomocí prohlížeče	Řešení poskytuje možnost připojení na vzdálené relace pouze pomocí prohlížeče a protokolu HTTPS (není nutné otevírat z klientské stanice RDP protokol, mezi uživatelem a jump serverem bude otevřený pouze bezpečný WebSocket protokol, port 443).	ANO

#	Oblast	Popis požadavku	Odpověď uchazeče (ANO/NE/pozn.)
20	Nahrávání relací	Řešení musí umožňovat monitoring a nahrávání celé relace a aktivit privilegovaných účtů ve video formátu s možností kontextového vyhledávání, bez nutnosti instalace agentů na koncový systém. Záznam relace musí být vytvářen kontinuálně, nikoliv formou screenshotů. V nahrávkách je možné zpětně vyhledávat v záznamu ve formě metadat – minimálně u RDP spuštěné aplikace a události, u SSH relací jednotlivé příkazy, u Webových aplikací click na jednotlivé odkazy, u jiných typů relací alespoň stisky kláves. Pro přehrávání nahrávek není potřeba instalace nástrojů třetích stran (flash, java, codec atp.) a je dostupné z GUI dodávaného řešení.	ANO
21	Automatické označení podezřelých aktivit v nahrávkách	Systém poskytuje možnost automaticky vyhodnocovat a označovat nahrávky relací na základě vybraných spuštěných příkazů a aplikací, tak aby bylo možné vyhledávat potenciálně nebezpečné činnosti. Systém zároveň umožňuje alerting takových událostí, včetně možnosti exportu logů v reálném čase pomocí syslog na SIEM atp.	ANO
22	Pozastavení/terminace relací	Řešení nabízí možnost automatického pozastavení, nebo terminace potenciálně nebezpečných relací. Pravidla pro detekci potenciálně nebezpečných relací je možné plně editovat – typ události, uživatelé (možnost nastavení výjimek na úrovni skupin v AD) a typ reakce.	ANO
23	Možnost sledování relací v reálném čase	Řešení umožňuje sledovat aktivní relace dalším uživatelem (například auditor) a v případě nutnosti ukončit sledovanou relaci. Sledování "živých" relací je také možné pomocí prohlížeče a protokolu HTTPS (není nutné otevírat z klientské stanice RDP protokol).	ANO

#	Oblast	Popis požadavku	Odpověď uchazeče (ANO/NE/pozn.)
24	Kontrola relací	Systém umožňuje autorizovanému personálu centrálně vyhledávat v nahrávkách podle data, uživatele a spuštěného příkazu. Řešení umožnuje označovat nahrávky relací pomocí skóre podle spuštěných aplikací, akcí a příkazů v dané relaci.	ANO
25	Analýza a detekce potenciálně škodlivého chování	Součástí řešení je nástroj umožňující provádět průběžnou analýzu využívání privilegovaných účtů a následnou detekci potenciálně škodlivého chování – uživatel se připojuje z nestandardní IP, uživatel se připojuje na systémy, na které běžně nemá přístup, uživatel používá privilegovaný přístupy v nestandardní časy atp. Zároveň řešení umožňuje detekci útoků na úrovni zranitelností Kerberos typu OverPass the Hash, PAC attack a Golden ticket.	ANO
26	Detekce a blokování podezřelých aktivit	Systém umožňuje detekci podezřelých aktivit chování uživatelů v reálném čase a musí umožňovat automatické vynucení nápravných opatření – alerting, změna přihlašovacích údajů, terminace/pozastavení relací.	ANO
	Audit a reporting		
27	Zobrazení aktivit uživatele	Systém musí umožňovat audit jednotlivých akcí uživatelů s privilegovanými účty – zobrazení hesla, změny uložených údajů, vytvoření relace.	ANO
28	Audit administrátorských akcí	Řešení musí umožňovat vygenerování reportu veškerých aktivit administrátora řešení.	ANO
29	Přístup k reportům	Řešení umožňuje nastavení přístupu k reportům pouze pro vybrané uživatele.	ANO
30	Export auditních dat	Systém musí umožňovat export auditních záznamů pro nástroje typu Crystal reports.	ANO
31	Nezpochybnitelný auditní záznam	Řešení zaručuje nezpochybnitelnou auditovatelnost jednotlivých	ANO

#	Oblast	Popis požadavku	Odpověď uchazeče (ANO/NE/pozn.)
		operací, možnosti reportování a textové logy.	
32	Zabezpečení auditních záznamů	Řešení musí umožňovat nesmazatelnost logů po dobu minimálně 30 dní. Auditní záznamy musí být bezpečně uloženy v zašifrované podobě, tak aby k nim měl přístup pouze oprávněný uživatel.	ANO
33	Monitoring pomocí RestAPI	Systém umožňuje monitoring jednotlivých komponent pomocí RestAPI – integrace s monitoring systémy zadavatele.	ANO
	Integrace a podporované platformy		
34	Podpora systémů zadavatele	Systém musí umožňovat správu privilegovaných účtů pro různé druhy koncových systémů – minimálně v rozsahu viz. bod: "Podpora řízení hesel a bezpečné přístupy pro systémy". Případně možnost konfigurace a vývoje vlastních konektorů pro změnu hesel a vzdálených přístupů.	ANO
35	Seznam podporovaných systémů	Výrobce musí poskytovat veřejně dostupný (ideálně URL na veřejnou webovou stránku) seznam integrovatelných řešení na úrovni Password Management, Remote Session Management, SIEM.	ANO
36	Integrace s ticketing nástroji	Řešení musí umožňovat integraci s ticketing nástroji třetích stran – žádost o schválení přístupu, přístup na základě existujícího ticektu, atp. Systém musí obsahovat WebApi/RestAPI rozhraní umožňující všechny integrační funkce. Součástí dodávky je popis rozhraní, včetně ukázek použití.	ANO
37	Podpora MS Active Directory	Řešení nabízí plnou integraci s Microsoft Active Directory na úrovni informací o uživatelích, příslušnosti ke skupinám a emailech. Integrace musí umožňovat mapování rolí v PAM řešení v návaznosti na skupiny v AD.	ANO
38	MFA – multi factor autentizace	Řešení musí podporovat integraci s nástroji třetích stran	ANO

#	Oblast	Popis požadavku	Odpověď uchazeče (ANO/NE/pozn.)
		pro vynucení multi factor autentizace. Minimálně na úrovní LDAP/S, RADIUS, PKI, RSA.	
39	SIEM integrace	Systém musí umožňovat integraci s nástroji SIEM – volitelně konfigurovatelný rozsah záznamů, které jsou posílány do SIEM.	ANO
40	HSM integrace	Systém musí umožňovat integraci s nástroji HSM – uložení šifrovacích klíčů k databázi řešení.	ANO
	Podpora řízení hesel a bezpečné přístupy pro systémy		
41	Podporované systémy	Windows 7, 8, 8.1, 10, 11 Windows Server 2008, 2012, 2016, 2019 Active Directory HP iLO, Dell DRAC, IBM Windows Services, Windows Scheduled Tasks, IIS Application Pool, Windows Registry COM+ VMWare, Red Hat, Suse, Unix, Ubuntu, Debian MS SQL, MySQL, PostreSQL, Oracle, DB2 Cisco, Juniper, F5, HP, Office 365, Microsoft Azure Application Keys	ANO
	Architektura		
42	Architektura řešení	Veškeré komponenty řešení musí splňovat nároky na vysoké zabezpečení a automaticky vynucovat tzv. hardening. Úložiště dat, kde jsou uloženy jednotlivé účty, přihlašovací údaje, nahrávky relací a auditní záznamy, je vysoce zabezpečeno a odděleno od ostatních komponent řešení. Databáze dat je součástí řešení a není nutné využívat nástroje třetích stran. Tento požadavek platí pro veškerá data v rámci řešení, tj. i pro HA a DR.	ANO
43	Vysoká dostupnost řešení	Řešení musí podporovat nasazení ve vysoké dostupnosti a vlastní technologické možnosti (nejsou používány nástroje/SW třetích stran) pro zabezpečení High Availability ve dvou geograficky oddělených	ANO

#	Oblast	Popis požadavku	Odpověď uchazeče (ANO/NE/pozn.)
		lokalitách, Disaster Recovery a zálohování tak, aby citlivá data byla stále vysoce zabezpečená a dostupná pouze vlastníkům dat.	
44	Disaster recovery	Disaster recovery a HA proces je plně automatický a není závislý na nástrojích třetích stran (MS cluster atp.).	ANO
45	Zálohování systému	Řešení musí umožňovat bezpečné zálohování dat systému – zálohy musí být šifrované a přístup k zálohovaným datům je umožněn pouze pomocí zabezpečených Disaster Recovery klíčů.	ANO
46	Automatická instalace	Veškeré komponenty řešení musí umožňovat automatickou instalaci v on-premise prostředí. Řešení minimálně poskytuje skripty pro kopírování instalačních souborů, instalaci pre-requisite, instalaci komponent, hardening a základní konfiguraci. Automatickou instalaci je možné řešit například pomocí Ansible roles.	ANO
	Požadavky na zařízení (HW)		
47	Redundance napájení	Centrální část a komponenty pro dodávané řešení musí obsahovat min. 2 redundantní napájecí zdroje.	ANO
48	Umístění zařízení	Zařízení musí být montovatelné do standardního 19" technologického stojanu o hloubce 800 mm (1U, 2U, případně 3U velikost).	ANO
49	Síťové požadavky	Zařízení musí obsahovat min. 2x LAN port, každý alespoň 10Gbit/s, lépe 25Gbpss podporou LACP.	ANO
50	Úložiště	Řešení musí mít vlastní úložiště na nahrávání relací jeho velikost musí odpovídat počtu licencí a době uchování relací, který je stanoven na 18 měsíců.	ANO
51	Zálohování a obnova	Řešení musí mít možnost zálohování a obnovy veškerého svého nastavení, tzn. konfigurace, včetně definice dashboardů, reportů,	ANO

#	Oblast	Popis požadavku	Odpověď uchazeče (ANO/NE/pozn.)
		definovaných procesů, uživatelských nastavení apod.	
52	Appliance	Pro zajištění vysoké dostupnosti řešení je požadováno dodání HW jedním z následujících způsobů: • dodání jednotlivých komponent HW i SW od jednoho výrobce (označované za „Apppliance“), • kombinace hardwarové appliance s virtuální appliance na platformě VMware ESX od různých výrobců, ale i v tomto případě musí dodavatel garantovat plnou kompatibilitu HW a SW, tj. pokud dojde k závadě, musí být tato řešena dodavatelem jako vada dodávaného řešení bez ohledu na to, zda se jedná o závadu HW nebo SW.	ANO
	Podpora výrobce		
53	Síť certifikovaných partnerů na lokálním trhu	Výrobce garantuje certifikovaného partnera na lokálním trhu, kde je zaručena technická znalost řešení, zkušenosti s implementací a řízením projektů PAM.	ANO
54	Konzultační služby	Výrobce poskytuje vlastní konzultační služby v rámci projektů implementace PAM řešení. V rámci služeb jsou poskytovány konzultace a best practices ohledně zabezpečení privilegovaných účtů, vedení PAM projektů a postupná analýza aktuálního stavu zabezpečení zadavatele.	ANO
55	Assessment tool	Výrobce zákazníkům poskytuje nástroj, včetně odborných konzultací, který umožňuje pravidelné vyhodnocení zabezpečení privilegovaných účtů v prostředí zadavatele, vzhledem k předem definovaným rizikům. Celý koncept Assessment nástroje umožní zákazníkům postupné povyšování bezpečnosti a	ANO

#	Oblast	Popis požadavku	Odpověď uchazeče (ANO/NE/pozn.)
		případné porovnání aktuálního stavu s anonymními údaji tisíců zákazníků po celém světě.	
56	Program zabezpečení privilegovaných účtů	Výrobce poskytuje metodologii postupného zabezpečení privilegovaných účtů, včetně osobních konzultací na lokálním trhu. Metodologie popisuje základní témata a rizika svázaná s oblastí privilegovaných přístupů do IT infrastruktury a zároveň navrhuje patřičná nápravná opatření.	ANO
57	Discovery tool	Výrobce poskytuje zdarma nástroj na vyhledání privilegovaných účtů v prostředí zadavatele a s nimi svázaných zranitelností. Zároveň poskytuje vlastní konzultační služby pro vyhodnocení a před-implementační podporu.	ANO
	Licenční model		
58	Druh licence	Řešení musí být dimenzované minimálně pro 105 uživatelů a 150 koncových systémů (aplikací, kusů HW). Součástí licence je instalace v HA v rámci dvou lokalit (HA v každé lokalitě i mezi lokalitami) a testovacího prostředí (včetně HA).	ANO
59	Dostupnost	Řešení musí podporovat minimálně 30 současných připojení přes RDP, SSH a/nebo VNC.	ANO
60	Počty licencí v rámci dodávky	Licence je požadována minimálně pro 30 uživatelů s licenčním oprávněním ke všem funkcím systému. Tuto licenci budou využívat kmenoví zaměstnanci Zadavatele. Licence je požadována minimálně pro 75 uživatelů s omezenou funkcionalitou. Tato licence bude určena pro externí firmy spolupracující se Zadavatelem. U této licence nebudou požadovány následující vlastnosti: • sledování, vyhodnocování a	ANO

#	Oblast	Popis požadavku	Odpověď uchazeče (ANO/NE/pozn.)
		ukončování relací jiných uživatelů, • přístup k záznamům relací jiných uživatelů, • role administrátora systému a přidělování práv uživatelům systému, • možnost zobrazení hesel k cílovým systémům a jejich manuální změna.	
61	Ostatní licenční požadavky	Licence nesmí být omezena na počet cílových zařízení nebo řízených účtů. Součástí licence musí být i řešení redundance všech komponent a taktéž geo-redundance (minimálně active-passive) s dodatečnou místní redundancí v druhé geolokaci. Licence musí umožnit instalaci separátního trvalého testovacího prostředí s plnou funkčností a v plném rozsahu. Součástí dodávky musí být také všechny potřebné licence pro operační systémy, databáze a případné další potřebné komponenty systému. Pro části řešení, které budou provozovány ve virtuálním prostředí Zadavatele a jejichž operační systém bude MS Windows Server 2012 – 2019, může Dodavatel využít stávající licence Zadavatele z edice MS Server DataCenter.	ANO
62	Podpora řešení	Dodávka musí obsahovat zajištění podpory výrobce (maintenance) po celou dobu poskytování záruční podpory, včetně práva na instalaci nových verzí SW, jeho oprav a patchů.	ANO
	Řízení aplikačních účtů		
63	Řízení aplikačních účtů	Řešení poskytuje zabezpečení aplikačních a technických privilegovaných účtů a jejich přihlašovacích údajů. Řešení umožňuje odstranění tzv. hard-coded přihlašovacích údajů ze skriptů, konfiguračních souborů a aplikací. Systém musí	ANO

#	Oblast	Popis požadavku	Odpověď uchazeče (ANO/NE/pozn.)
		umožňovat různé API pro bezpečné vyzvedávání přihlašovacích údajů pro aplikace a skripty.	
64	Bezpečná autentizace aplikací	Řešení musí umožňovat silnou autentizaci skriptů a aplikací pro vyzvedávání přihlašovacích údajů, a to minimálně na úrovni – hostname/IP adresa aplikačního serveru, certifikátu, uživatele, pod kterým je aplikace/skript spuštěna, cesty k aplikaci, případně MD5 hash.	ANO
65	Lokální cache	Systém umožňuje poskytování přihlašovacích údajů aplikacím a skriptům pomocí agentského řešení, které obsahuje možnost bezpečné cache. V případě síťového výpadku bude aplikace/skript mít stále k dispozici přihlašovací údaje k privilegovanému účtu.	ANO
66	Popis SDK	Výrobce musí poskytnout popis jednotlivých API a SDK pro konfiguraci skriptů a aplikací. Ideálně s konkrétními příklady nasazení.	ANO
	Postup nasazení		
67	Předimplementační analýza	Dodavatel zpracuje předimplementační analýzu dle požadavků definovaných v kapitole „Předimplementační analýza“.	ANO
68	Implementace	Dodavatel implementuje řešení dle požadavků definovaných v kapitole „Implementace“.	ANO
69	Školení	Dodavatel realizuje školení dle požadavků definovaných v kapitole „Školení“.	ANO
70	Technické a provozní dokumentace	Dodavatel zpracuje technickou a provozní/administrátorskou dokumentaci dle požadavků definovaných v kapitole „Zpracování technické a provozní/administrátorské dokumentace“.	ANO
71	Testovací a pilotní provoz	Dodavatel zajistí součinnosti při testovacím a pilotním provozu dle požadavků definovaných v kapitole „Testovací a pilotní provoz“.	ANO

#	Oblast	Popis požadavku	Odpověď uchazeče (ANO/NE/pozn.)
72	Akceptační testy	Dodavatel zajistí součinnosti při akceptačních testech dle požadavků definovaných v kapitole „Akceptační testy“.	ANO
73	Produkční prostředí a provoz řešení	Dodavatel zajistí součinnosti při přenesení do produkčního prostředí definovaných v kapitole „Produkční prostředí a provoz řešení“.	ANO
74	Audit nastavení	Dodavatel provede audit nastavení dle požadavků definovaných v kapitole „Audit nastavení“.	ANO
75	Backdoor	Dodavatel zajistí součinnost při tvorbě a implementaci schémat pro případ backdoor přístupu při výpadku systému PIM/PAM.	ANO
	Záruka a záruční servis		
76	Záruční podpora na provoz systému PIM/PAM	Dodavatel splní požadavky na zajištění záruky a záručního servisu jsou definovány níže v kapitole Záruční podpora na provoz systému PIM/PAM.	ANO
	Služby na vyžádání		
77	Objednání služeb na vyžádání	Dodání služeb technického specialisty na vyžádání nad rámec předmětu plnění.	ANO

Příloha č. 2 – Minimální technické a funkční požadavky objednatele

Minimální technické a funkční požadavky

Řešení pro správu privilegovaných oprávnění (PIM/PAM)

Popis prostředí objednatele pro nasazení řešení PIM/PAM

Prostředí objednatele 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 (omezeně Windows 7).
U informačních systémů objednatele 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 řešení PIM/PAM

Řešením správy privilegovaných účtů je nasazení systému PIM/PAM, který je možné rozdělit do následujících, úzce souvisejících oblastí:

1. Správa hesel – centrální správa a ochrana privilegovaných účtů v šifrovaném a zabezpečeném úložišti s automatickou rotací hesel v koncových systémech;

2. Správa procesů udělování privilegovaných práv – prostřednictvím automatizovaných, kontrolovaných a zabezpečených procesů se zajišťuje správa přístupu na základě rolí a automatizovaných pracovních postupů;

3. Nahrávání a monitorování relací – zaznamenávání všech aktivit při práci s privilegovanými účty (snímání/nahrávání obrazovek, evidování stisků kláves, indexace, ukládání apod.), které mají tyto auditní záznamy odolné proti neoprávněné manipulaci;

4. Sledování a blokace v reálném čase – možnost sledování a reakce (nastavená pravidla, odeslaní aletru, manuální blokace apod.) na monitorované relace v reálném čase;

5. Provádění analýzy uživatelského chování – umožňující identifikace vnitřní nebo vnější hrozby, odhalování a zastavení podezřelých aktivit;

6. Uživatelská behaviorální biometrie – algoritmy kontroly charakteristiky chování uživatele, např. vzorce chování, dynamika stisku kláves, analýza pohybu myši apod.;

7. Podpora blacklist a whitelist příkazů a názvů oken – umožňující omezení/povolení protokolů, síťových služeb, příkazů a specifických názvů oken, které lze povolit/zakázat pro jednotlivé skupiny privilegovaných účtů;

8. Možnost napojení/integraci s ticketingovými systémy – proces zažádání a schválení udělování privilegovaných práv nebo procesů;

9. Kontrola přístupu – rozšíření možností v přidělování oprávnění k užití privilegovaných účtů při přístupu ke koncovým systémům, možná detekce a ochrana proti vybraným činnostem na základě definovaných pravidel;

10. Osobní trezor hesel – možnost ukládat jakákoliv hesla a generovat náhodná hesla pro nefederované účty do osobního trezoru hesel;

11. Fulltextové vyhledání – možnost provádět fulltextové vyhledávání jak pro příkazy, tak pro jakýkoli zobrazený text uživatelem v obsahu relací.

objednatel připouští pouze tuto variantu možného řešení: On-premise: dodávka a implementace HW a SW v místě objednatele.

Minimální funkční a technické požadavky

Dodávka a implementace řešení:

#	Oblast	Popis požadavku
	Funkční požadavky	
1	Řízení přístupů	Řešení poskytuje nástroj pro správu privilegovaných účtů, řízení přístupu k těmto účtům a monitoring veškerých aktivit privilegovaných účtů. Uživatelské přístupy jsou řízeny bezpečnostní politikou, kdy má vybraný uživatel práva přístupu pouze k definovaným účtům a systémům. Účty a systémy, ke kterým nemá práva přístupu, nejsou pro uživatele viditelné.
2	Striktní oddělení přístupových oprávnění	Systém plně podporuje multi-tenant prostředí. Uživatelé/skupiny uživatelů mají přístup pouze k vybraným účtům, systémům, auditním záznamům, konfiguraci atp. I správce/administrátor řešení má povolen přístup pouze k vybraným složkám a konfiguraci.
3	Oddělení administrátorských oprávnění	Řešení musí umožňovat napojení na MS AD Tier model nebo možnost aplikování oddělení privilegovaných (administrátorských) oprávnění do 3 vrstev (doménová, serverová, klientská stanice), kdy přístup do nižší vrstvy je blokován a do vyšší vrstvy je ověřován (schvalován).
4	Víceúrovňové schvalování přístupů	Řešení umožňuje víceúrovňové schvalování správcovských přístupů k cílovým systémům – přístupy lze omezit dle vybraného účtu, nebo na daný časový úsek. Schvalování přístupu lze vynutit odděleně pro přístup přihlašovacím údajům privilegovaného účtu, nebo pro připojení na koncový systém. O nových žádostech, schválení a zamítnutí budou uživatelé upozornění emailem, vytvořením ticketu v helpdesk systému apod.
5	Bezpečnostní parametry	Řešení zaručuje vysokou bezpečnost přenášených a uložených informací (confidentiality, integrity, availability). Uložené informace, včetně nahrávek a spravovaných přihlašovacích údajů, jsou uloženy v jedné centrální a vysoce zabezpečené databázi. Řešení musí umožňovat omezení práv správce systému tak, aby neměl sám přístup k uloženým přihlašovacím údajům, logům, nebo nahrávkám, bez autorizace vlastníků dat. Systém jako celek musí být certifikovaný bezpečnostním standardem Common Criteria anebo ekvivaletní certifikaci.
6	Uživatelské rozhraní	Přístup k uživatelskému rozhraní je požadovaný přes webový portál s možností ověření přes LDAP/MS Active Directory a druhým faktorem (minimálně PKI karty, RSA ID, Radius server, ...).
7	Silná autentizace	Nástroj umožňuje vynutit silnou autentizaci uživatelů pro přístup k uloženým údajům i pro bezpečné vzdálené připojení. Silnou autentizací je míněna minimálně možnost kombinace jméno/heslo + druhý faktor (RADIUS, PKI, certifikát, atp...). Řešení umožňuje integraci s MFA nástroji třetích stran, minimálně Microsoft a Cisco.
8	Šifrování a zabezpečení dat	Řešení musí splňovat standard FIPS 140-2 a šifrovací algoritmy minimálně na úrovni AES-256 a RSA-2048. Řešení umožňuje objednateli splnit compliance požadavky pro ZKB, GDPR, PCI-DSS, SOX, HIPAA atd.
9	Jednorázové povýšení oprávnění	Nástroj umožňuje povýšení oprávnění běžných (neprivilegovaných) uživatelů na koncových systémech bez nutnosti instalace agentského řešení. Řešení umožňuje povyšování oprávnění na základě požadavku, příslušnosti do AD skupiny, případně na časově omezené období.
	Password Management	
10	Vyhledávání a přidávání privilegovaných účtů	Řešení umožňuje vyhledávat privilegované účty v operačních systémech/LDAP/Active Directory a přidat je (manuálně i automaticky) do systému řízení přístupu dle bezpečnostní politiky. Vyhledávání účtů nevyužívá instalaci agentů na koncová zařízení. Systém umožňuje vyhledávání v on-premise i cloud prostředí (např. AWS).
11	Řízení hesel a SSH klíčů	Řešení umožňuje automatickou výměnu hesel a SSH klíčů privilegovaných účtů po ukončení relace (jednorázové heslo), nebo v pravidelných intervalech dle bezpečnostní politiky. Rotaci hesla/SSH klíče lze vynutit i uživatelem. Hesla a SSH klíče se vyměňují bez agentů.
12	Ověřování hesel	Řešení kontroluje v pravidelných intervalech shodu uloženého hesla v systému řízení přístupů a cílovém bodu. V případě neshody vynutí synchronizaci, nebo zašle upozornění správci.
13	Řízení servisních účtů	Systém umožňuje vyhledat účty v MS Windows prostředí a jejich návaznost na další služby/aplikace (services, sheduled tasks, IIS pool, COM+ object, ...). Při vynucení změny hesla je heslo propsáno i do návazných služeb.

#	Oblast	Popis požadavku
14	Vyhledání tzv. backdoor účtů a automatický onboarding	Systém umožňuje pravidelné vyhledávání účtů, které nejsou řešením spravovány, ale jsou používány pro přístupy na koncové systémy. Systém takové účty dokáže vyhledat, upozornit na jejich použití a případně automaticky zařadit do správy. Řešení zároveň umožňuje detekci nespravovaných účtů v reálném čase a automatické uložení a vynucení změny hesla.
15	Customizace Password Management	Řešení musí umožňovat možnost úpravy systému password management, tak aby bylo možné integrovat další systémy objednatele. Úpravy je možné provádět pomocí nástroje dodávaného výrobcem a případně úpravou konfiguračních souborů.
	Řízení vzdálených relací	
16	Izolace relací	Správcovský přístup na cílový systém bude zprostředkován pomocí tzv. terminal/jump serveru prostřednictvím zvoleného komunikačního protokolu, aplikace a příslušného privilegovaného účtu tak, aby koncový uživatel neměl přístup k přihlašovacím údajům. Izolace přístupu je možná až na úroveň aplikace (typu webový prohlížeč s konkrétní URL, MMC konzole s vybraným snap-in, konkrétní aplikace... např. MS SQL Management Studio, WinSCP atp.), kdy uživatel nemá možnost přistupovat k jiným službám, aplikacím v rámci dané relace. Po ukončení aplikace se uzavře spojení celé relace. Vzdálené připojení k relaci lze navázat jak přes vlastní GUI dodaného řešení, tak i pomocí standardních protokolů RDP a SSH a standardních klientů typu putty a remote desktop manager. U všech možností připojení ke vzdálené relaci musí být podporováno vynucení silné autentizace (minimálně integrace s LDAP a RADIUS).
17	Izolace SSH relací	Správcovský přístup prostřednictvím SSH protokolu se bude provádět přes SSH Proxy, kde bude uživatel ověřený svými přihlašovacími údaji (je možné spárovat s MS Active Directory) a bude připojený zvoleným privilegovaným účtem na cílový systém bez zadávání hesla a dle bezpečnostní politiky. Pro připojení pomocí SSH Proxy je vyžadována podpora silné autentizace (minimálně integrace s LDAP, RADIUS, či autentizace pomocí SSH klíče).
18	Připojení do webových relací	Řešení umožňuje zprostředkovat uživateli bezpečné připojení na vybrané webové aplikace a sociální sítě pomocí tzv. Webové proxy. Řešení umožní uživateli přihlášení do vybrané webové aplikace pomocí standardního (neprivilegovaného) účtu, webová proxy následně zprostředkuje přihlášení do koncové aplikace pomocí silného "privilegovaného" účtu. Uživatel nemusí znát hesla privilegovaných účtů a je mu umožněno transparentní SSO.
19	Vzdálené připojení pomocí prohlížeče	Řešení poskytuje možnost připojení na vzdálené relace pouze pomocí prohlížeče a protokolu HTTPS (není nutné otevírat z klientské stanice RDP protokol, mezi uživatelem a jump serverem bude otevřený pouze bezpečný WebSocket protokol, port 443).
20	Nahrávání relací	Řešení musí umožňovat monitoring a nahrávání celé relace a aktivit privilegovaných účtů ve video formátu s možností kontextového vyhledávání, bez nutnosti instalace agentů na koncový systém. Záznam relace musí být vytvářen kontinuálně, nikoliv formou screenshotů. V nahrávkách je možné zpětně vyhledávat v záznamu ve formě metadat – minimálně u RDP spuštěné aplikace a události, u SSH relací jednotlivé příkazy, u Webových aplikací click na jednotlivé odkazy, u jiných typů relací alespoň stisky kláves. Pro přehrávání nahrávek není potřeba instalace nástrojů třetích stran (flash, java, codec atp.) a je dostupné z GUI dodávaného řešení.
21	Automatické označení podezřelých aktivit v nahrávkách	Systém poskytuje možnost automaticky vyhodnocovat a označovat nahrávky relací na základě vybraných spuštěných příkazů a aplikací, tak aby bylo možné vyhledávat potenciálně nebezpečné činnosti. Systém zároveň umožňuje alerting takových událostí, včetně možnosti exportu logů v reálném čase pomocí syslog na SIEM atp.
22	Pozastavení/terminace relací	Řešení nabízí možnost automatického pozastavení, nebo terminace potenciálně nebezpečných relací. Pravidla pro detekci potenciálně nebezpečných relací je možné plně editovat – typ události, uživatelé (možnost nastavení výjimek na úrovni skupin v AD) a typ reakce.
23	Možnost sledování relací v reálném čase	Řešení umožňuje sledovat aktivní relace dalším uživatelem (například auditor) a v případě nutnosti ukončit sledovanou relaci. Sledování "živých" relací je také možné pomocí prohlížeče a protokolu HTTPS (není nutné otevírat z klientské stanice RDP protokol).
24	Kontrola relací	Systém umožňuje autorizovanému personálu centrálně vyhledávat v nahrávkách podle data, uživatele a spuštěného příkazu. Řešení umožnuje označovat nahrávky relací pomocí skóre podle spuštěných aplikací, akcí a příkazů v dané relaci.
25	Analýza a detekce potenciálně škodlivého chování	Součástí řešení je nástroj umožňující provádět průběžnou analýzu využívání privilegovaných účtů a následnou detekci potenciálně škodlivého chování – uživatel se připojuje z nestandardní IP, uživatel se připojuje na systémy, na které běžně nemá přístup, uživatel používá privilegovaný přístupy v nestandardní časy atp. Zároveň řešení umožňuje detekci útoků na úrovni zranitelností Kerberos typu OverPass the Hash, PAC attack a Golden ticket.

#	Oblast	Popis požadavku
26	Detekce a blokování podezřelých aktivit	Systém umožňuje detekci podezřelých aktivit chování uživatelů v reálném čase a musí umožňovat automatické vynucení nápravných opatření – alerting, změna přihlašovacích údajů, terminace/pozastavení relací.
	Audit a reporting	
27	Zobrazení aktivit uživatele	Systém musí umožňovat audit jednotlivých akcí uživatelů s privilegovanými účty – zobrazení hesla, změny uložených údajů, vytvoření relace.
28	Audit administrátorských akcí	Řešení musí umožňovat vygenerování reportu veškerých aktivit administrátora řešení.
29	Přístup k reportům	Řešení umožňuje nastavení přístupu k reportům pouze pro vybrané uživatele.
30	Export auditních dat	Systém musí umožňovat export auditních záznamů pro nástroje typu Crystal reports.
31	Nezpochybnitelný auditní záznam	Řešení zaručuje nezpochybnitelnou auditovatelnost jednotlivých operací, možnosti reportování a textové logy.
32	Zabezpečení auditních záznamů	Řešení musí umožňovat nesmazatelnost logů po dobu minimálně 30 dní. Auditní záznamy musí být bezpečně uloženy v zašifrované podobě, tak aby k nim měl přístup pouze oprávněný uživatel.
33	Monitoring pomocí RestAPI	Systém umožňuje monitoring jednotlivých komponent pomocí RestAPI – integrace s monitoring systémy objednatele.
	Integrace a podporované platformy	
34	Podpora systémů objednatele	Systém musí umožňovat správu privilegovaných účtů pro různé druhy koncových systémů – minimálně v rozsahu viz. bod: "Podpora řízení hesel a bezpečné přístupy pro systémy". Případně možnost konfigurace a vývoje vlastních konektorů pro změnu hesel a vzdálených přístupů.
35	Seznam podporovaných systémů	Výrobce musí poskytovat veřejně dostupný (ideálně URL na veřejnou webovou stránku) seznam integrovatelných řešení na úrovni Password Management, Remote Session Management, SIEM.
36	Integrace s ticketing nástroji	Řešení musí umožňovat integraci s ticketing nástroji třetích stran – žádost o schválení přístupu, přístup na základě existujícího ticektu, atp. Systém musí obsahovat WebApi/RestAPI rozhraní umožňující všechny integrační funkce. Součástí dodávky je popis rozhraní, včetně ukázek použití.
37	Podpora MS Active Directory	Řešení nabízí plnou integraci s Microsoft Active Directory na úrovni informací o uživatelích, příslušnosti ke skupinám a emailech. Integrace musí umožňovat mapování rolí v PAM řešení v návaznosti na skupiny v AD.
38	MFA – multi factor autentizace	Řešení musí podporovat integraci s nástroji třetích stran pro vynucení multi factor autentizace. Minimálně na úrovní LDAP/S, RADIUS, PKI, RSA.
39	SIEM integrace	Systém musí umožňovat integraci s nástroji SIEM – volitelně konfigurovatelný rozsah záznamů, které jsou posílány do SIEM.
40	HSM integrace	Systém musí umožňovat integraci s nástroji HSM – uložení šifrovacích klíčů k databázi řešení.
	Podpora řízení hesel a bezpečné přístupy pro systémy	
41	Podporované systémy	Windows 7, 8, 8.1, 10, 11 Windows Server 2008, 2012, 2016, 2019 Active Directory HP iLO, Dell DRAC, IBM Windows Services, Windows Scheduled Tasks, IIS Application Pool, Windows Registry COM+ VMWare, Red Hat, Suse, Unix, Ubuntu, Debian MS SQL, MySQL, PostreSQL, Oracle, DB2 Cisco, Juniper, F5, HP, Office 365, Microsoft Azure Application Keys
	Architektura	
42	Architektura řešení	Veškeré komponenty řešení musí splňovat nároky na vysoké zabezpečení a automaticky vynucovat tzv. hardening. Úložiště dat, kde jsou uloženy jednotlivé účty, přihlašovací údaje, nahrávky relací a auditní záznamy, je vysoce zabezpečeno a odděleno od ostatních komponent řešení. Databáze dat je součástí řešení a není nutné využívat nástroje třetích stran. Tento požadavek platí pro veškerá data v rámci řešení, tj. i pro HA a DR.
43	Vysoká dostupnost řešení	Řešení musí podporovat nasazení ve vysoké dostupnosti a vlastní technologické možnosti (nejsou používány nástroje/SW třetích stran) pro zabezpečení High

#	Oblast	Popis požadavku
		Availability ve dvou geograficky oddělených lokalitách, Disaster Recovery a zálohování tak, aby citlivá data byla stále vysoce zabezpečená a dostupná pouze vlastníkům dat.
44	Disaster recovery	Disaster recovery a HA proces je plně automatický a není závislý na nástrojích třetích stran (MS cluster atp.).
45	Zálohování systému	Řešení musí umožňovat bezpečné zálohování dat systému – zálohy musí být šifrované a přístup k zálohovaným datům je umožněn pouze pomocí zabezpečených Disaster Recovery klíčů.
46	Automatická instalace	Veškeré komponenty řešení musí umožňovat automatickou instalaci v on-premise prostředí. Řešení minimálně poskytuje skripty pro kopírování instalačních souborů, instalaci pre-requisite, instalaci komponent, hardening a základní konfiguraci. Automatickou instalaci je možné řešit například pomocí Ansible roles.
	Požadavky na zařízení (HW)	
47	Redundance napájení	Centrální část a komponenty pro dodávané řešení musí obsahovat min. 2 redundantní napájecí zdroje.
48	Umístění zařízení	Zařízení musí být montovatelné do standardního 19" technologického stojanu o hloubce 800 mm (1U, 2U, případně 3U velikost).
49	Síťové požadavky	Zařízení musí obsahovat min. 2x LAN port, každý alespoň 10Gbit/s, lépe 25Gbpss podporou LACP.
50	Úložiště	Řešení musí mít vlastní úložiště na nahrávání relací jeho velikost musí odpovídat počtu licencí a době uchování relací, který je stanoven na 18 měsíců.
51	Zálohování a obnova	Řešení musí mít možnost zálohování a obnovy veškerého svého nastavení, tzn. konfigurace, včetně definice dashboardů, reportů, definovaných procesů, uživatelských nastavení apod.
52	Appliance	Pro zajištění vysoké dostupnosti řešení je požadováno dodání HW jedním z následujících způsobů: • dodání jednotlivých komponent HW i SW od jednoho výrobce (označované za „Apppliance"), • kombinace hardwarové appliance s virtuální appliance na platformě VMware ESX od různých výrobců, ale i v tomto případě musí dodavatel garantovat plnou kompatibilitu HW a SW, tj. pokud dojde k závadě, musí být tato řešena dodavatelem jako vada dodávaného řešení bez ohledu na to, zda se jedná o závadu HW nebo SW.
	Podpora výrobce	
53	Síť certifikovaných partnerů na lokálním trhu	Výrobce garantuje certifikovaného partnera na lokálním trhu, kde je zaručena technická znalost řešení, zkušenosti s implementací a řízením projektů PAM.
54	Konzultační služby	Výrobce poskytuje vlastní konzultační služby v rámci projektů implementace PAM řešení. V rámci služeb jsou poskytovány konzultace a best practices ohledně zabezpečení privilegovaných účtů, vedení PAM projektů a postupná analýza aktuálního stavu zabezpečení objednatele.
55	Assessment tool	Výrobce zákazníkům poskytuje nástroj, včetně odborných konzultací, který umožňuje pravidelné vyhodnocení zabezpečení privilegovaných účtů v prostředí objednatele, vzhledem k předem definovaným rizikům. Celý koncept Assessment nástroje umožní zákazníkům postupné povyšování bezpečnosti a případné porovnání aktuálního stavu s anonymními údaji tisíců zákazníků po celém světě.
56	Program zabezpečení privilegovaných účtů	Výrobce poskytuje metodologii postupného zabezpečení privilegovaných účtů, včetně osobních konzultací na lokálním trhu. Metodologie popisuje základní témata a rizika svázaná s oblastí privilegovaných přístupů do IT infrastruktury a zároveň navrhuje patřičná nápravná opatření.
57	Discovery tool	Výrobce poskytuje zdarma nástroj na vyhledání privilegovaných účtů v prostředí objednatele a s nimi svázaných zranitelností. Zároveň poskytuje vlastní konzultační služby pro vyhodnocení a před-implementační podporu.
	Licenční model	
58	Druh licence	Řešení musí být dimenzované minimálně pro 105 uživatelů a 150 koncových systémů (aplikací, kusů HW). Součástí licence je instalace v HA v rámci dvou lokalit (HA v každé lokalitě i mezi lokalitami) a testovacího prostředí (včetně HA).
59	Dostupnost	Řešení musí podporovat minimálně 30 současných připojení přes RDP, SSH a/nebo VNC.
60	Počty licencí v rámci dodávky	Licence je požadována minimálně pro 30 uživatelů s licenčním oprávněním ke všem funkcím systému. Tuto licenci budou využívat kmenoví zaměstnanci objednatele.

#	Oblast	Popis požadavku
		Licence je požadována minimálně pro 75 uživatelů s omezenou funkcionalitou. Tato licence bude určena pro externí firmy spolupracující se objednatelem. U této licence nebudou požadovány následující vlastnosti: • sledování, vyhodnocování a ukončování relací jiných uživatelů, • přístup k záznamům relací jiných uživatelů, • role administrátora systému a přidělování práv uživatelům systému, • možnost zobrazení hesel k cílovým systémům a jejich manuální změna.
61	Ostatní licenční požadavky	Licence nesmí být omezena na počet cílových zařízení nebo řízených účtů. Součástí licence musí být i řešení redundance všech komponent a taktéž geo-redundance (minimálně active-passive) s dodatečnou místní redundancí v druhé geolokaci. Licence musí umožnit instalaci separátního trvalého testovacího prostředí s plnou funkčností a v plném rozsahu. Součástí dodávky musí být také všechny potřebné licence pro operační systémy, databáze a případné další potřebné komponenty systému. Pro části řešení, které budou provozovány ve virtuálním prostředí objednatele a jejichž operační systém bude MS Windows Server 2012 – 2019, může Dodavatel využít stávající licence objednatele z edice MS Server DataCenter.
62	Podpora řešení	Dodávka musí obsahovat zajištění podpory výrobce (maintenance) po celou dobu poskytování záruční podpory, včetně práva na instalaci nových verzí SW, jeho oprav a patchů.
	Řízení aplikačních účtů	
63	Řízení aplikačních účtů	Řešení poskytuje zabezpečení aplikačních a technických privilegovaných účtů a jejich přihlašovacích údajů. Řešení umožňuje odstranění tzv. hard-coded přihlašovacích údajů ze skriptů, konfiguračních souborů a aplikací. Systém musí umožňovat různé API pro bezpečné vyzvedávání přihlašovacích údajů pro aplikace a skripty.
64	Bezpečná autentizace aplikací	Řešení musí umožňovat silnou autentizaci skriptů a aplikací pro vyzvedávání přihlašovacích údajů, a to minimálně na úrovni – hostname/IP adresa aplikačního serveru, certifikátu, uživatele, pod kterým je aplikace/skript spuštěna, cesty k aplikaci, případně MD5 hash.
65	Lokální cache	Systém umožňuje poskytování přihlašovacích údajů aplikacím a skriptům pomocí agentského řešení, které obsahuje možnost bezpečné cache. V případě síťového výpadku bude aplikace/skript mít stále k dispozici přihlašovací údaje k privilegovanému účtu.
66	Popis SDK	Výrobce musí poskytnout popis jednotlivých API a SDK pro konfiguraci skriptů a aplikací. Ideálně s konkrétními příklady nasazení.
	Postup nasazení	
67	Předimplementační analýza	Dodavatel zpracuje předimplementační analýzu dle požadavků definovaných v kapitole „Předimplementační analýza".
68	Implementace	Dodavatel implementuje řešení dle požadavků definovaných v kapitole „Implementace".
69	Školení	Dodavatel realizuje školení dle požadavků definovaných v kapitole „Školení".
70	Technické a provozní dokumentace	Dodavatel zpracuje technickou a provozní/administrátorskou dokumentaci dle požadavků definovaných v kapitole „Zpracování technické a provozní/administrátorské dokumentace".
71	Testovací a pilotní provoz	Dodavatel zajistí součinnosti při testovacím a pilotním provozu dle požadavků definovaných v kapitole „Testovací a pilotní provoz".
72	Akceptační testy	Dodavatel zajistí součinnosti při akceptačních testech dle požadavků definovaných v kapitole „Akceptační testy".
73	Produkční prostředí a provoz řešení	Dodavatel zajistí součinnosti při přenesení do produkčního prostředí definovaných v kapitole „Produkční prostředí a provoz řešení".
74	Audit nastavení	Dodavatel provede audit nastavení dle požadavků definovaných v kapitole „Audit nastavení".
75	Backdoor	Dodavatel zajistí součinnost při tvorbě a implementaci schémat pro případ backdoor přístupu při výpadku systému PIM/PAM.
	Záruka a záruční servis	
76	Záruční podpora na provoz systému PIM/PAM	Dodavatel splní požadavky na zajištění záruky a záručního servisu jsou definovány níže v kapitole Záruční podpora na provoz systému PIM/PAM.

#	Oblast	Popis požadavku
	Služby na vyžádání	
77	Objednání služeb na vyžádání	Dodání služeb technického specialisty na vyžádání nad rámec předmětu plnění.

Příloha č. 3 – Položkový ceník

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 sběr, detekci a vyhodnocení kybernetických bezpečnostních událostí (SIEM) v souladu se zadávacími podmínkami a s návrhem smlouvy							
Časově neomezená užívací práva k SW nástroji pro řízení a správu privilegovaných oprávnění (PIM/PAM) dle čl. I., odst. 1 návrhu smlouvy včetně záruky a záručního servisu **(60 měsíců)**	1	licence	4 810 044,00 Kč	5 820 153,24 Kč	4 810 044,00 Kč	1 010 109,24 Kč	5 820 153,24 Kč
HW appliance (HA) dle čl I., odst. 1 b) návrhu smlouvy včetně záruky a záručního servisu **(60 měsíců)**	1	ks	363 180,00 Kč	439 447,80 Kč	363 180,00 Kč	76 267,80 Kč	439 447,80 Kč
Předimplementační analýza dle čl. I., odst. 1 a) návrhu smlouvy	1	různé	306 000,00 Kč	370 260,00 Kč	306 000,00 Kč	64 260,00 Kč	370 260,00 Kč
Implementační práce dle čl. I., odst. 1 c) návrhu smlouvy	1	různé	489 600,00 Kč	592 416,00 Kč	489 600,00 Kč	102 816,00 Kč	592 416,00 Kč
Dodání technické a provozní/administrátorské dokumentace dle čl. I., odst. 1 d) návrhu smlouvy	1	různé	122 400,00 Kč	148 104,00 Kč	122 400,00 Kč	25 704,00 Kč	148 104,00 Kč
Zaškolení administrátorů a auditorů objednatele dle čl. I., odst. 1 e) návrhu smlouvy.	1	různé	122 400,00 Kč	148 104,00 Kč	122 400,00 Kč	25 704,00 Kč	148 104,00 Kč
Provedení Auditu nastavení dle čl. I., odst. 1 i) návrhu smlouvy.	2	různé	91 800,00 Kč	111 078,00 Kč	183 600,00 Kč	38 556,00 Kč	222 156,00 Kč
Služby technického specialisty nad rámec předmětu plnění VZ dle čl. I., odst. 1k) návrhu smlouvy.	40	MD (Man Day)	15 000,00 Kč	18 150,00 Kč	600 000,00 Kč	126 000,00 Kč	726 000,00 Kč
Celková nabídková cena za celý předmět plnění bez DPH *					6 997 224,00 Kč		

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

Zpracovatel:	Účinnost dokumentu od:	Schválil:
[redacted]	23. 7. 2020	[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 tel. [redacted]
- od 16:00 do 7:00 na Pohotovost ÚI na tel. [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 tel. [redacted]
    - od 16:00 do 7:00 na Pohotovost ÚI na tel. [redacted]
  - o víkendu a svátcích na Pohotovost ÚI na tel. [redacted]

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.