SMLOUVA NA DODÁVKU ŘEŠENÍ KAMEROVÉHO SYSTÉMU

Clarystone s.r.o.
zapsána v obchodním rejstříku vedeném u Městského soudu v Praze, spisová značka C 206322
se sídlem: Na Větrově 889/13, 142 00 Praha 4
IČO: 277 45 422 DIČ: CZ27745422
zastoupena: Mgr. Petrem Kochem, jednatelem
bankovní spojení: Komerční banka a.s.
číslo účtu: 43-51220257/0100

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

a

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

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

Dodavatel a objednatel společně též jako „smluvní strany"

uzavírají dnešního dne, měsíce a roku dle ustanovení § 2079 a násl. zákona č. 89/2012 Sb., občanský zákoník, v platném znění (dále jen „z. č. 89/2012 Sb."), a na základě vyhodnocení výsledků veřejné zakázky malého rozsahu s názvem „**Migrace kamerového systému**" realizované poptávkovým řízením a ID veřejné zakázky na profilu zadavatele: VZ0221755 ze dne 18. 6. 2025 (dále jen „veřejná zakázka"), tuto

smlouvu na dodávku řešení kamerového systému
(dále jen „smlouva")

I. Předmět smlouvy

1. Předmětem plnění dle této smlouvy je dodávka On-Premise řešení kamerového systému Milestone xProtect Professional+ (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 harmonogram.

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,
- 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 2 kusů HW (Serverů) včetně** veškerého SW potřebného ke správnému fungování uvedených serverů, montáže a instalace všech HW komponent do technologických stojanů (RACK) včetně označení a vyvázání kabelů a předání souvisejících dokladů.

c) **dodání časově neomezených užívacích práv (multilicence) k SW kamerového systému** (dále také „Video management systém" nebo „VMS") pro minimálně 100 uživatelů a instalace a nastavení virtuálního serveru pro řízení a správu kamerového systému včetně dodání všech dalších případných licencí, které dodávané řešení vyžaduje pro připojení min. 350 kamer objednatele k VMS.

V případě provedení úprav (patches), aktualizací (updates), vylepšení (upgrades) či jiných změn softwarového řešení, které je předmětem smlouvy ze strany poskytovatele, je licence poskytnuta i k takto změněnému software.

d) implementační práce, které obsahují:
- instalaci SW nutného k funkčnosti řešení *(instalaci klientů provede objednatel*),
- systémovou konfiguraci,
- konfiguraci řešení včetně uživatelského/správcovského rozhraní,
- migraci aktuálních pohledů a uživatelů ze současného systému nebo jejich vytvoření v novém prostředí.

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

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

f) zaškolení administrátorů a obsluhy
Zajištění školení dodavatelem pro dodaný kamerový systém v rozsahu provozní a administrátorské dokumentace pro zaměstnance objednatele (min. 10 zaměstnanců objednatele).

g) 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) budou po ukončení testovacího anebo pilotního provozu dodavatelem odstraněny a případně zaneseny do zpracované dokumentace. Bez odstranění zjištěných závad nelze zahájit akceptační testy.

h) 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 kamerového systému 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.

<u>Vada typu B:</u>
- 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.

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

i) záruku a zajištění poskytování záručního servisu

Bližší specifikace předmětu plnění je uvedena v příloze č. 1 této smlouvy. Záruka a způsob jejího poskytování je rovněž blíže řešena v čl. III. 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: ManazerKB@vfn.cz, 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 Video management systému, který je předmětem plnění této smlouvy.

5. Dodavatel se zavazuje dodat předmět plnění specifikovaný 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 3 měsíců od účinnosti 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: xxxxx, tel. xxxxx, email: xxxxx
   Za systémovou/technickou dodávku/: xxxxx, tel. xxxxx, email: xxxxx
   Za převzetí HW: Bc. Zbyněk Pecka, tel. xxxxx, email: xxxxx
   Za podpis akceptačního protokolu: xxxxx, tel. xxxxx, email: xxxxx
   K nahlašování požadavků na záruční servis: xxxxx, tel. xxxxx, email: xxxxx a xxxxx, tel. xxxxx, email: xxxxx
   Za identifikaci případného kybernetického útoku v průběhu plnění předmětu plnění dle této smlouvy: manažer KB, e-mail: xxxxx
   Za ochranu osobních údajů: xxxxx

   Kontaktní a odpovědná osoba za dodavatele: xxxxx, tel. xxxxx, email: 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 nahlašování požadavků na záruční servis: 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, email: 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, nikoliv však výlučně, jakost zařízení.

6. Dodavatel odpovídá za dodržení přepravních podmínek po dobu přepravy HW k objednateli, tak aby nebylo zařízení znehodnoceno. HW bude dopraven do místa plnění na vlastní náklady a nebezpečí dodavatele.

7. Dodávka předmětu plnění se považuje podle této smlouvy za řádně splněnou, pokud:
   - byla objednatelem odsouhlasena předimplementační analýza,
   - předmět plnění (HW i SW) byl řádně doručen a naimplementován,
   - byly dodavatelem předány veškeré podklady a informace potřebné k výkonu licence, a to zejména licenční kódy a příslušná dokumentace,
   - bylo objednateli předáno oficiální potvrzení lokálního zastoupení výrobce dodávané HW části řešení (HW) o tom, že zařízení je nové, nepoužité a určené pro koncového zákazníka „Všeobecná fakultní nemocnice v Praze",
   - byl objednateli předán certifikát ze kterého je zřejmé, že dodavatel je certifikovaným partnerem výrobce Video management systému, který je předmětem plnění této smlouvy,
   - bylo provedeno zaškolení administrátorů a obsluhy 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. Dodavatel se zavazuje plnit předmět plnění prostřednictvím projektového týmu, tedy za přítomnosti osob, které jsou uvedeny v příloze č. 5 této smlouvy, jejichž prostřednictvím prokázal splnění kritérií technické kvalifikace v rámci veřejné zakázky, na jejímž základě byla uzavřena tato smlouva nebo další osoby, které budou odsouhlaseny dle čl. II odst. 11 této smlouvy.

11. V případě změny členů projektového týmu je dodavatel povinen vyžádat si předchozí písemný souhlas objednatele. Nový člen projektového týmu musí splňovat příslušné požadavky na kvalifikaci stanovené původními zadávacími podmínkami, což je dodavatel povinen objednateli doložit odpovídajícími dokumenty.

12. Pro případ jakékoliv změny ve složení projektového týmu se smluvní strany dohodly, že není potřeba uzavírat k tomu odpovídající dodatek této smlouvy, a taková změna je účinná dnem doručení písemného souhlasu objednatele dodavateli.

13. 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, kdy tento dokument tvoří přílohu č. 4 smlouvy.

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 řádného 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), poskytování aktualizací driverů pro nové modely podporovaných kamer,
   - 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 bude 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 kamerového systému, 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 kamerového systému. 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 funkčnosti provozu systému v režimu 24 hodin denně, 7 dní v týdnu (dále také „24x7") 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 24 hodin	do 3 dnů
Porucha**	24x7	do 3 pracovních dnů	do 7 pracovních dnů

Úroveň závady	Parametry služby		
	Provozní doba služby Hot-line	Maximální reakční doba od nahlášení požadavku:	Maximální doba odstranění závady
Chyba* **	24x7	do 3 pracovních dnů	do 14 dnů

Maximální reakční doba na odstranění závady se počítá od okamžiku zadání hlášení závady objednatelem do systému ServiceDesk 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 kamerového systému 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 ServiceDesku objednatele.
- Oprava vad, chyb a zranitelností.
- Zajištění souladu se zákony a normativy ČR a EU.
- Reakce na dotazy oprávněných osob objednatele.
- 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, a to zejména, nikoliv však výlučně, provozní, uživatelské a administrátorské.
- 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 Milestone a DELL 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 objednatele (viz kontaktní osoby uvedené v čl. II. odst. 3), 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	**1 934 300 Kč**
DPH	**406 203 Kč**
Cena vč. DPH	**2 340 503 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. Objednatel se zavazuje zaplatit cenu uvedenou v čl. IV. odst. 1 této smlouvy na základě faktury vystavené dodavatelem. Dodavatel předá fakturu objednateli spolu s akceptačním protokolem, jehož součástí bude dodací list, popřípadě zašle objednateli do 14 dnů po řádném předání a převzetí předmětu plnění. Fakturována může být pouze celá dodávka předmětu plnění, dílčí fakturace není povolena. Na faktuře budou rozepsány jednotlivé položky dle předmětu plnění.

4. Faktura musí dále obsahovat všechny údaje uvedené v § 29 odst. 1 zákona č. 235/2004 Sb., o dani z přidané hodnoty a dle zákona č. 563/1991 Sb., o účetnictví. Splatnost faktury činí 60 dnů od jejího doručení objednateli. Faktura bude zaslána elektronicky ve formátu PDF na e-mailovou adresu: xxxxx. K faktuře bude přiložena kopie řádně opatřeného akceptačního protokolu, jehož součástí bude kopie dodacího listu.

5. 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.

6. Platby budou probíhat výhradně v CZK a rovněž veškeré cenové údaje budou v této měně.

7. 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.

3. V případě odstoupení od smlouvy ze strany objednatele se dodavatel zavazuje uvést technické prostředí objednatele do původního stavu, a to do 14 dnů od data doručení odstoupení od smlouvy objednatelem, pokud se smluvní strany nedohodnou jinak.

VI. Sankce

1. Pro případ prodlení objednatele s úhradou ceny dle čl. IV. této smlouvy má dodavatel nárok na zaplacení úroku z prodlení ze strany objednatele ve výši 0,01 % z částky, s jejíž platbou je objednatel v prodlení, za každý den takového prodlení. Smluvní strany se dohodly, že dodavatel je oprávněn požadovat zaplacení úroku z prodlení až po uplynutí 30 dnů od sjednané lhůty splatnosti.

2. V případě dodání jiného předmětu plnění než objednaného a při nedodržení dodací lhůty je objednatel oprávněn požadovat zaplacení jednorázové smluvní pokuty ve výši 200.000,- Kč. Dále je objednatel oprávněn požadovat zaplacení další smluvní pokuty ve výši 0,1 % z ceny plnění dle čl. IV. odst. 1 smlouvy bez DPH za každý započatý den prodlení s dodáním předmětu plnění, jestliže se s dodavatelem nedohodne jinak. Objednatel je dále v těchto případech 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 10.000,- Kč za každý započatý den 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 5.000,- Kč za každý započatý pracovní den 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 každý započatý den prodlení za jednotlivý případ.

6. V případě prodlení dodavatele s dodržením termínů odstranění vad předmětu plnění, jsou-li uvedeny v akceptačním protokolu o předání a převzetí předmětu plnění dle čl. II. odst. 10 smlouvy, je objednatel oprávněn požadovat zaplacení smluvní pokuty ve výši 0,1% z celkové ceny předmětu plnění bez DPH za každý i započatý den prodlení.

7. V případě nedodržení některé z povinností dodavatele stanovených v čl. VIII. odst. 2 - 4 smlouvy má objednatel právo účtovat smluvní pokutu ve výši 10.000,- Kč.
8. Za nedodržení povinností uvedených v čl. I. odst. 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. Za nedodržení povinnosti vedené v čl. V. odst. 3 smlouvy má objednatel právo účtovat smluvní pokutu ve výši 200.000,- Kč.
9. 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.
10. 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., o zadávání veřejných zakázek 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., o zadávání veřejných zakázek 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.

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. Pokud je smlouva podepisována elektronicky, je vyhotovena v jednom stejnopise podepsaném oběma smluvními stranami elektronickým podpisem dle zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.
4. Autentičnost této smlouvy potvrzují smluvní strany svými 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 – Projektový tým

V Praze dne dle el. podpisu:

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

V Praze dne dle el. podpisu:

Mgr. Petr Koch
jednatel Clarystone s.r.o.

Příloha č. 1 smlouvy - Technická a funkční specifikace předmětu plnění

Řešení migrace kamerového systému zahrnuje dodávku rozšířeného a spolehlivého systému Milestone xProtect v úrovni licence Professional+ a servery DELL v konfiguraci odpovídající požadavkům výrobce software. Tato kombinace je plně funkční a odpovídá technickým a funkčním požadavkům objednatele.

Software Milestone xProtect je multiserverový a umožňuje v nasazení podle topologie dle bodu 3, funkčních požadavků. Níže je soupis jednotlivých licencí a komponent

Licence Milestone xProtects Professional+

1x licence *XProtect Professional+ Base License (BL)* - základní licence systému

350x licence *XProtect Professional + Device License (DL)* – licence pro jednotlivé zařízení (kamera) připojená do systému

350x podpora *5 Years Care Plus for XProtect Professional+ DL* – 5-ti letá podpora VSM systému obsahující poskytování aktualizací programových prostředků (nové verze, opravné verze, bezpečnostní záplaty), poskytování aktualizací driverů pro nové modely podporovaných kamer

2x server **DELL POWEREDGE R760XS SERVER, 4x8TB, PS 5Y**

Základna	PowerEdge R760xs
Trusted Platform	Module Trusted Platform Module 2.0 V3
Chassi	3.5" Chassis with up to 12 Hard Drives (SAS/SATA) PERC11
Processor	Intel Xeon Silver 4410Y 2G, 12C/24T, 16GT/s, 30M Cache, Turbo, HT(150W) DDR5-4000
Paměť	32 GB 5600MT/s RDIMMs
Konfigurace RAID	RAID 1 + RAID 5
Řadič pole RAID	PERC H755 Adapter, Low Profile
Pevné disky (o.s.)	2x 480GB SSD SATA Read Intensive 6Gbps 512 2.5in Hot-plug AG Drive,3.5in HYB CARR, 1 DWPD
Pevné disky (data)	4x 8TB 7.2K RPM SATA 6Gbps 512e 3.5in Hot-plug Hard Drive
Fans	High Performance Fan x5
Napájecí zdroj	Dual, Hot-Plug, Power Supply, Redundant (1+1), 700W MM HLAC (ONLY FOR 200-240Vac) Titanium
PCIe Riser	Riser Config 0, No Riser, 1x16 + 1x8 (1 CPU), with OCP
Motherboard	PowerEdge R760xs Motherboard with Broadcom 5720 Dual Port 1Gb On-Board LOM
Síťový adaptér	Broadcom 57416 Dual Port 10GbE BASE-T Adapter, OCP NIC 3.0
Provedení	PowerEdge 2U Standard Bezel, Rack Rails Cable Management Arm, 2U, Rack Rails ReadyRails Sliding Rails
Operating System	Windows Server 2025 Standard,16CORE,FI,No Med,No CAL,Multi Language
OS Media Kits	Windows Server 2025 Standard,16CORE,DF Recovery Image, Multi Lang
Rozšířené služby	ProSupport Next Business Day Onsite Service Initial, 36 měsícu
Rozšířené služby	ProSupport Next Business Day Onsite Service Extension, 24 měsíců

Příloha č. 2 – Minimální technické a funkční požadavky objednatele

Minimální technická a funkční specifikace

1. Pojmy a zkratky

- AD – Active Directory - adresářová služba od firmy Microsoft
- CA – Certifikační Autorita
- CCTV – kamerový systém (Closed-circuit television, uzavřený televizní okruh)
- DB – databáze
- DC1 – Datové centrum 1, Budova A5
- DC2 – Datové centrum 2, Budova
- GDPR - General Data Protection Regulation - obecné nařízení o ochraně osobních údajů
- HW – hardware
- Log - záznam činnosti softwaru
- NDAA - National Defense Authorization Act – Americký federální zákon, který definuje zákaz používání vybraných produktů video dohledu
- NBDoS záruka – Next Business Day on Site – druhý pracovní den bude vyslán profesionální servisní technik, který se postará o odstranění závady,
- NÚKIB - Národní úřad pro kybernetickou a informační bezpečnost
- On-Premise - řešení představuje software či hardware, který je uložen v interní infrastruktuře a prostoru společnosti
- OS – operační systém
- PRTG - software pro centrální monitorování IT infrastruktury
- SCCM – Microsoft System Center Configuration Manager
- SW – software
- ÚIDT - Úsek informatiky a digitální transformace
- VFN – Všeobecná fakultní nemocnice v Praze
- VMS – Video Management Systém
- VMWare – virtualizační platforma

2. Technologické prostředí objednatele

Kapitola obsahuje popis technologického prostředí objednatele, ve kterém bude dodavatel realizovat požadované řešení.

Obecné standardy

- Produkční prostředí je realizováno v On-Premise prostředí objednatele.
- Objednatel provozuje dvě datová centra, která jsou geograficky oddělená a pracující v režimu HA clustrovém řešení.

Virtualizační standardy

- VMWare vSphere 8 Enterprise Plus (8.0.3).

Parametry klientské pracovní stanice

Objednatel požaduje dodání řešení, které bude bez jakýchkoliv problémů (doba odezvy, zatížení, velikost úložiště apod.) fungovat s níže uvedenými minimálními parametry pracovní stanice (není součástí dodávky):

- Procesor min. 6 jader (Intel řady i5 min 8.generace).
- Paměť RAM: 8GB.
- HDD/SSD 250GB.
- Disk je zašifrovaný nástrojem Bitlocker.
- Integrovaná grafická karta.
- OS: Windows 10 Pro/Ent nebo vyšší.
- Antivir: MS Defender.
- Standardní SW výbava: PC v doméně VFN s user právy, NIS Medea, MS Office, webový prohlížeč MS Edge Chromium.

Popis stávajícího CCTV

Objednatel provozuje 280 kamer, které jsou připojeny do systému Cisco Safety and Security Desktop verze 7.11.1.5, který je spravován pomocí systému Cisco Video Surveillance Operations Manager verze 7.11.1.

Ze 175 kamer je záznam uchováván po dobu 5 dní v maximální možné kvalitě s minimálně 12 snímky za sekundu.

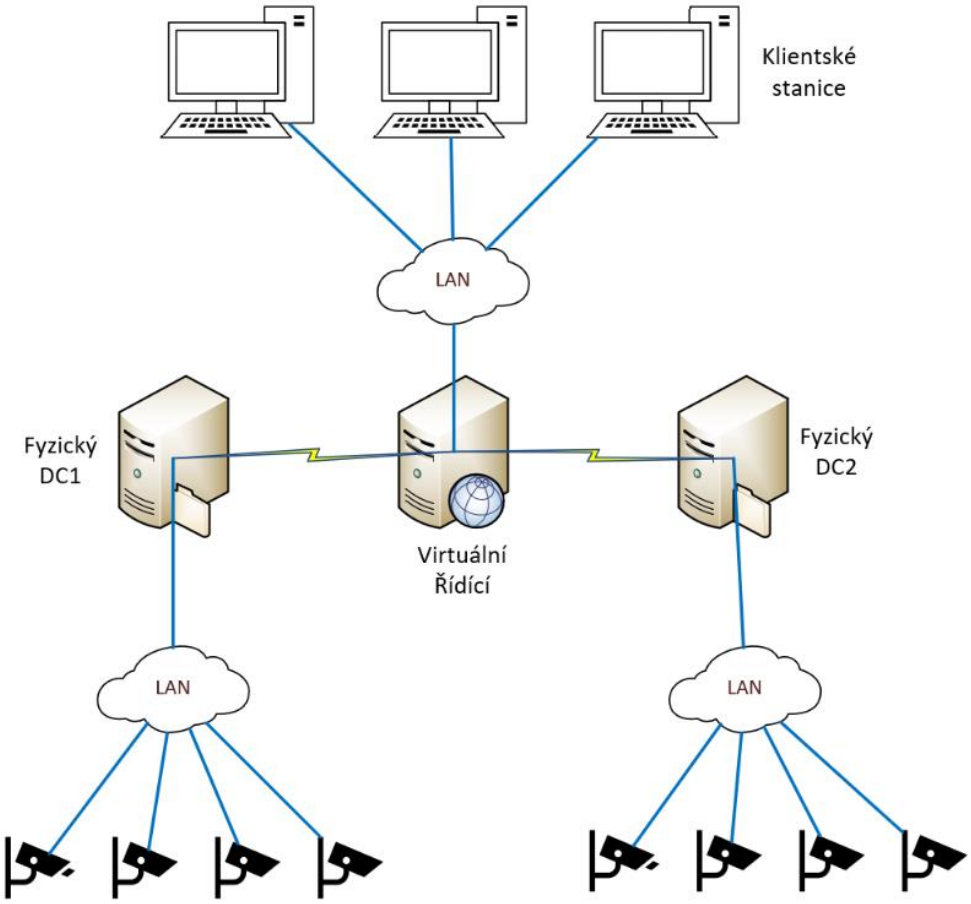
Na jedné pracovní stanici je zobrazováno maximálně 16 kamer.

Kamerové náhledy jsou na 80 pracovištích.

Modely kamer jsou Axis 210, Axis 211, CIVS-IPC-2521V, Axis 211M, CIVS-IPC-2621V, CIVS-IPC-2630V, AXIS M1013, CIVS-IPC-3520, CIVS-IPC-3530, AXIS M1011, CIVS-IPC-3050, CIVS-IPC-4300, AXIS P3367, CIVS-IPC-3535, P3265-LV, CIVS-IPC-8030, AXIS P3245-LV, AXIS P3245-LVE, Axis P3267-LV/LVE, Axis P1455-LE, AXIS M4215-V, AXIS M3215-LVE, AXIS M4308-PLE panoramic.

3. Funkční požadavky

Funkční schéma



Systém musí být schopen obsloužit minimálně 350 kamer. Na jeden fyzický server bude aktivních maximálně 200. **Pokud připojení kamer k VMS vyžaduje licence, tak tyto licence musí být součástí nabídky dodavatele (tzn. součástí celkové nabídkové ceny dodavatele) a budou uvedeny v nabídce dodavatele, a to pro požadovaných minimálně 350 kamer.**

Logické schéma zapojení

Software pro management videa musí podporovat centrální správu, poskytovat efektivní správu všech připojených kamer a poskytovat kompletní přehled o systému.

Dodané řešení musí umožnovat šifrovanou komunikaci mezi servery a klienty pomocí zabezpečených digitálních certifikátů CA.

Klient na koncové stanice bude distribuován nástrojem SCCM. Dodavatel ve spolupráci s objednatelem připraví instalační balíček.

Klient na koncových stanicích musí umět zobrazit obsah na více monitorech.

Klient na koncových stanicích se bude přihlašovat k Virtuálnímu serveru.

Klient na koncových stanicích musí jít spustit automaticky po startu PC a bez použití klávesnice a myši.

Systém musí podporovat stávající modely kamer. Tuto skutečnost musí uchazeč na požádání doložit, případně předvést v rámci posuzovaní nabídek.

SW pro správu videa musí nativně podporovat možnost ověření uživatelů služby Windows Active Directory prostřednictvím protokolu Microsoft NTLM, ověření Kerberos a/nebo nabízet možnost integrace externích poskytovatelů identit pomocí protokolu OpenID Connect a OAuth2 bez nutnosti dalšího licencování.

SW pro management videa musí mít integrován reportovací nástroj pro vypsání kompletní stávající konfigurace, která zajišťuje kompletní dokumentaci systému pro GDPR/NIS 2 ověření.

SW pro správu videa musí být otevřenou platformou s minimálně 400 integracemi, které byly ověřeny nebo certifikovány výrobcem softwaru pro management videa. Software pro management videa musí umožňovat integraci na úrovni SDK/API bez nutnosti podepsání dohody o mlčenlivosti. Nejsou vyžadovány žádné další licenční poplatky ani náklady.

SW musí mít transparentní licenční politiku. Klientské aplikace (například klienti pro prohlížení, mobilní klienti a další) nejsou licencovány.

Objednatel nepožaduje přenos záznamů ze současného systému CCTV.

4. Nefunkční požadavky

V kapitole jsou uvedené nefunkční požadavky na řešení.

Řízení přístupů

Řešení musí umožnit nastavení rolí podle elementárních práv dodaným nástrojem nebo funkcí v SW (např admin modul).

Monitoring

Na servery bude objednatelem nasazená služba PRTG pro monitorování zdrojů. Monitoring bude zahrnovat nepřetržitý dohled nad důležitými prvky řešení a jejich funkcemi včetně průběžného vyhodnocování tak, aby bylo možné předejít většině hrozících výpadků a selhání.

Seznam služeb a procesů nutných ke sledování dodá dodavatel a zapracuje do provozní dokumentace.

Logování

Systém logování dodávaného řešení musí zahrnovat logy v níže uvedeném rozsahu a musí umožňovat jejich napojení na SIEM objednatele např. pomocí Syslog nebo Windows Event Log (prostřednictvím agenta WinCollect), případně JDBC.
V rámci dodávaného řešení musí být realizováno zaznamenání minimálně následujících událostí:

- Přihlášení a odhlášení uživatelů a administrátorů (včetně neúspěšných).
- Činnosti provedené privilegovanými účty (administrátorské účty, systémové účty, technické účty apod.).
- Činnosti vedoucí ke změně přístupových oprávnění (standardních i privilegovaných).
- Neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů.
- Zahájení a ukončení činností (včetně „pádů" nebo selhání) jednotlivých komponent systému.
- Činnosti spojené s přijímáním/odesíláním ze/do SW třetích stran (integrační logy).
- Automatická varovná nebo chybová hlášení komponent systému.
- Přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností.
- Použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení.
- Změny a výmaz datových záznamů včetně času, uživatele a identifikace pracovní stanice, ze které byl úkon proveden (transakční protokol).

Takto zaznamenané události musí být chráněny před neoprávněným čtením nebo změnou.

5. Požadavky na bezpečnost řešení

- Trvalou ochranu aplikací a informací před neoprávněnou činností, popřením provedených činností, kompromitací nebo neautorizovanou změnou.
- Trvalou ochranu transakcí/záznamů před jejich nedokončením, nesprávným směrováním, neautorizovanou změnou předávaného datového obsahu, kompromitací, neautorizovaným duplikováním nebo opakováním.
- Nastavení ochrany dat zpracovaných nebo uchovávaných v řešení, a to především osobních údajů nebo citlivých údajů, kdy bude kladen důraz na data dostupná z vnější sítě. Budou zohledněna rizika:
    - Neoprávněného přístupu,
    - Nedovolených činností nad rámec svých práv,
    - Popření provedených činností,
    - Kompromitace,
    - Porušení integrity dat,
    - Nedostupnosti dat,
    - Neautorizované změny,
- Ochranu prováděných transakcí nebo změn dat:
    - Před jejich nedokončením,
    - Nesprávným směrováním,

  - Neautorizovanou změnou předávaného datového obsahu,
  - Kompromitací,
  - Neautorizovaným duplikováním nebo opakováním, a to v souladu s legislativními nebo normativními požadavky, např. daňové, účetní, na ochranu dat.
- Definovat zálohovací plány, které řeší: jaká data, jakým způsobem a jak často se mají zálohovat, aby byly splněny požadavky na:
  - Přijatelnou lhůtu obnovení dat ze zálohy,
  - Přípustný objem dat, který nebude možno obnovit (data od poslední zálohy),
  - Dobu a termín omezení provozu IT z důvodu zálohování (zálohovací okno).
  - Stanovení četnosti a cyklů záloh pro technologie, systémy a data,
  - Způsob testování záloh (ověření obnovitelnosti a čitelnosti).
- Dodávané technické nebo programové prostředky nesmí být prostředky, které jsou zveřejněny na stránkách Národního centra kybernetické bezpečnosti (provozované NUKIB) jako hrozba. Veškeré poskytované služby nesmí být provozované na výše uvedených technických nebo programových prostředcích označených NUKIB jako hrozba.

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)
Migrace kamerového systému v souladu se zadávacími podmínkami a s návrhem smlouvy							
Časově neomezená užívací práva k SW (Video management systém (dále také "VSM")) pro minimálně 100 uživatelů dle čl. I., odst. 1 c) návrhu smlouvy včetně záruky a záručního servisu **(60 měsíců)** včetně všech dalších případných licencí, které nabízené řešení vyžaduje pro připojení min. 350 kamer zadavatele k VSM.	1	multilicence	1 427 500,00 Kč	1 727 275,00 Kč	1 427 500,00 Kč	299 775,00 Kč	1 727 275,00 Kč
HW (Server) dle čl I., odst. 1 b) návrhu smlouvy včetně záruky a záručního servisu **(60 měsíců)**	2	ks	181 400,00 Kč	219 494,00 Kč	362 800,00 Kč	76 188,00 Kč	438 988,00 Kč
Předimplementační analýza dle čl. I., odst. 1 a) návrhu smlouvy	1	různé	24 000,00 Kč	29 040,00 Kč	24 000,00 Kč	5 040,00 Kč	29 040,00 Kč
Implementační práce dle čl. I., odst. 1 d) návrhu smlouvy	1	různé	80 000,00 Kč	96 800,00 Kč	80 000,00 Kč	16 800,00 Kč	96 800,00 Kč
Dodání technické, provozní a administrátorské dokumentace dle čl. I., odst. 1 e) návrhu smlouvy	1	různé	24 000,00 Kč	29 040,00 Kč	24 000,00 Kč	5 040,00 Kč	29 040,00 Kč
Zaškolení administrátorů a obsluhy objednatele dle čl. I., odst. 1 f) návrhu smlouvy.	1	různé	16 000,00 Kč	19 360,00 Kč	16 000,00 Kč	3 360,00 Kč	19 360,00 Kč
Celková nabídková cena za celý předmět plnění bez DPH *					1 934 300,00 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: [redacted]	**Účinnost dokumentu od:** 23. 7. 2020	**Schválil:** [redacted]
Garant: [redacted] Vedoucí odboru správy ICT	**První vydání dne:** 1. 1. 2008	**Dne:** 23. 7. 2020

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

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. +420 224 962 119,
- od 16:00 do 7:00 na Pohotovost ÚI na tel. +420 702 083 578.

O víkendu a svátcích na Pohotovost ÚI na tel. +420 702 083 578.

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.

POUŽÍVÁNÍ SÍTĚ VFN EXTERNÍMI UŽIVATELI

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. +420 224 962 119.

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: +420 702 083 578 (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 te[redacted]
    - od 16:00 do 7:00 na Pohotovost ÚI na t[redacted]
  - o víkendu a svátcích na Pohotovost ÚI na tel. +[redacted]

Příloha č. 5 Projektový tým

Role	Zodpovědnost (náplň práce)	Jméno a příjmení	Vzdělání, praxe	Referenční zakázka	Vztah k dodavateli
Projektový manažer	Vedení projektu, zodpovědnost za plánování zdrojů, tvorba časového harmonogramu, zodpovědnost za dodržování hamonogramu, předání dokumentace a předmětu plnění	[redacted]	16 let praxe v řízení projektů	Vedení projektů: Kamerový systém pro rozvodny PRE Distribuce, kamerový systém Milestone xProtect pro Mercedes-Benz Česká republika, kamerový systém Milestone xProtect pro Daimler Truck Česká republika	kmenový zaměstanec
Technický specialista 1	technické konzultace, předimplementační analýza, implementace Milestone xProtect, konfigurace Milestone xProtect	[redacted]	21 let praxe - networking, 16 let praxe IP kamerové systémy, Milestone Certified Design Engineer Milestone Certified Integration Technician	Technická realizace projektů: Kamerový systém pro rozvodny PRE Distribuce, kamerový systém Milestone xProtect pro Mercedes-Benz Česká republika, kamerový systém Milestone xProtect pro Daimler Truck Česká republika	kmenový zaměstanec
Technický specialista 2	technické konzultace, předimplementační analýza, implementace Milestone xProtect, konfigurace Milestone xProtect	[redacted]	21 let praxe - networking, 11 let praxe IP kamerové systémy, Milestone Certified Design Engineer Cisco Certified Network Associate	Technická realizace projektů: Kamerový systém pro rozvodny PRE Distribuce, kamerový systém Milestone xProtect pro Mercedes-Benz Česká republika, kamerový systém Milestone xProtect pro Daimler Truck Česká republika	kmenový zaměstanec
Microsoft specialista	Technická podpora, návrh a konfigurace operačních systémů	[redacted]	Microsoft Certified Professional 30 letá praxe se správou Microsoft serverů	návrh, design, implementace a správa serverového prostředí kontaktního centra pro E.On Česká republika	kmenový zaměstanec