Financováno Evropskou unií
NextGenerationEU

SMLOUVA– AUDIT SYSTÉMŮ A VYTVOŘENÍ HARDENINGOVÝCH BEZPEČNOSTNÍCH POLITIK

DoxoLogic, s.r.o.
zapsána: dne 22. května 2007 v obchodním rejstříku vedeném u Městského soudu v Praze C 125420
se sídlem: Karolinská 661/4, Praha 8, 186 00
IČO: 279 03 656 DIČ: CZ 279 03 656
zastoupena: Bc. Martin Listopad, jednatelem a Moore Technology CZ s.r.o., jednatelem, při výkonu funkce zastoupena Ing. Miloslavem Rutem
bankovní spojení: xxxxx
číslo účtu: xxxxx

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

a

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

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

uzavírají dnešního dne na základě výsledků veřejné zakázky malého rozsahu s názvem **„Audit systémů a vytvoření hardeningových bezpečnostních politik",** zadávané v otevřeném řízení (dále jen „veřejná zakázka"), v souladu s ustanovením § 1746 odst. 2, § 2079 a násl. a § 2586 a násl. 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 plnění smlouvy

1. Předmětem plnění dle této smlouvy je:

   a) provedení auditu nastavení a konfigurace jednotlivých operačních systémů, databázových systémů a dalších platforem objednatele, které jsou porovnány s benchmarky (doporučení výrobce nebo institucí pro kybernetickou bezpečnost), best practice a požadavky prostředí objednatele a následně jsou vytvořeny závazné hardeningové bezpečnostní politiky pro jednotlivé systémy. Na základě hardeningu je dosaženo zabezpečení konfigurace systému takovým způsobem, který omezí výskyt zranitelností využitelných útočníkem.

   b) služby technického specialisty na vyžádání v rozsahu maximálně 10 MD (80 člověkohodin) po dobu 24 měsíců po akceptaci dodaných služeb uvedených v předchozím bodě a) čl. I, odst. 1.

Cílem auditu a následného nasazení hardeningových bezpečnostních politik na systémy a databáze objednatele je:

- zvýšení úrovně bezpečnosti provozovaných systémů v souladu s mezinárodními standardy, best practice a zkušenostmi poskytovatele,
- zajištění efektivního řízení zranitelností a ověření shody s hardeningovými politikami,
- snížení pracnosti a rizik plynoucích z existujících zranitelností, konfiguračních neshod nebo provozu ICT objednatele,
- definice konfiguračního standardu pro používané systémy odpovídající potřebám prostředí objednatele, který lze vyžadovat i po externích dodavatelích,
- kompletní přehled o nastavení jednotlivých systémů, včetně možnosti ověření neshod oproti hardeningovým politikám.

V rámci předmětu plnění dle článku I, odst. 1, bodu a) této smlouvy je:

1) z důvodu zajištění vysoké úrovně bezpečnosti systémů/platforem (dále také „systémů") objednatele provedení činností v následujících fázích:

a) **Audit**– v úvodní fázi poskytovatel povede audity nastavení jednotlivých systémů, které jsou předmětem hardeningu (viz kap. Vymezení rozsahu auditovaných systémů). Tyto systémy budou objednatelem zvoleny dle jejich kritičnosti a významu, které jsou pro zajištění základních služeb objednatele nezbytné. Auditní zjištění budou pro jednotlivé systémy zdokumentovány. Na základě stanovených systémů budou poskytovatelem zvoleny vhodné nástroje nebo skripty pro automatizovanou kontrolu nastavení po celou dobu realizace předmětu plnění dle čl. I, odst. 1 bod a). Součástí této fáze bude osobní prezentace výstupu u objednatele.

b) **Vytvoření hardeningových bezpečnostních politik** – zjištění z auditu systémů budou poskytovatelem porovnány s již existujícími a prověřenými standardy (např. CIS Benchmarky, NIST a jiné), best practice a s požadavky vyplývající z prostředí objednatele. Na základě tohoto porovnání poskytovatel vypracuje hardeningové bezpečnostní politiky v takové podobě, aby bylo možné jejich nasazení v prostředí objednatele a bylo zřejmé jaké parametry nebo specifikace bude nezbytné v systémech upravit nebo nastavit. Dalším využitím těchto politik je jejich použitelnost pro následné vyhodnocování manuální nebo automatizované kontroly (audity) jak na stávajících, tak i nově konfigurovaných systémech.

c) **Nasazení hardeningových bezpečnostních politik (dále také jen „politik") ** – nasazení politik na jednotlivých systémech bude provedeno objednatelem v součinnosti s poskytovatelem v testovacím prostředí objednatele (pokud je testovací prostředí vytvořeno) a to tak, aby bylo zajištěno řešení případných kolizních stavů konfigurace systémů a předešlo se omezení provozu z důvodu kolizí. Všechny případné změny zjištěné při testování budou poskytovatelem zaneseny do finální podoby hardeningových bezpečnostních politik. Po úspěšném „odladění" kolizních stavů bude objednatelem v součinnosti s poskytovatelem provedeno nasazení finálních politik na jednotlivé produkční systémy objednatele.

   Finální verze politik budou aplikovány pouze na typové servery podle specifikace v kap. Vymezení rozsahu auditovaných systémů a rollout na zbývající systémy objednatele bude proveden objednatelem podle dodaných skriptů, nástrojů nebo postupů poskytovatele.

2) dodání následujících výstupů:

- zdokumentování výstupů z auditu (např. výstup z nástroje, systémové služby, skriptu, manuálního ověření) a celkové vyhodnocení jednotlivých systémů do zprávy z auditu, která bude obsahovat následují oblasti:
  - výstupní konfigurace a nastavení jednotlivých systémů,
  - zjištěné odchylky od doporučení a standardů,
  - doporučení změn politik a konfigurací systémů,
  - celkové vyhodnocení stavu auditovaných systémů a prostředí objednatele,
- dokumenty nebo technické konfigurace finálních hardeningových bezpečnostních politik pro jednotlivé systémy ve formě, která umožní jejich budoucí aktualizaci zadavatelem (např. excel, xml),
- skripty (případně nástroje) nebo postupy pro následné ověření nastavených politik na zbývajících nebo nově konfigurovaných systémech objednatele.

- **Akceptace** – k akceptaci dodávané služby je nezbytné splnit následující:
  - provedení auditu všech systémů zadavatele,
  - vytvoření všech politik k nasazení na systémy zadavatele,
  - nasazené finální politiky bez kolizních stavů,
  - dodání všech požadovaných výstupů v elektronické podobě.

Minimální požadavky na hardeningové bezpečnostní politiky
K nastavení bezpečné konfigurace jednotlivých operačních systémů, databázových systémů a dalších platforem je nezbytné zajistit implementaci níže uvedených opatření do hardeningových bezpečnostních politik:

- nastavení protokolů auditu (zohlednění zákonné doby uchování, velikosti a rotace logů),
- nastavení minimálních povolených služeb,
- nastavit běžící služby pouze s minimálními právy,
- pokud je to možné: provoz běžících služeb v izolovaném prostředí,
- omezení přístupu k příkazovému řádku a PowerShellu,
- omezení přístupu k možnostem Ovládacích panelů,
- omezení přístupu ke konfiguračním souborům operačního systému,
- omezení přístupu do registru,
- minimální přiřazení práv pro rozhraní údržby a přístupy,

- auditování protokolu NTLM,
- centrálně spravovat bránu firewall systému Windows pomocí zásad skupiny,
- sledování změn nastavení objektu zásad skupiny,
- změna všech existujících výchozích hesel hesly podle interních zásad hesel objednatele,
- řídit zásady Applockeru nebo omezení softwaru,
- nastavení filtrace a šifrování provozu včetně zmapování využívaných portů a jejich případná aktivace/deaktivace,
- zohlednit známé zranitelnosti (např. omezení SSL certifikátů, zakázání TLS 1.0/1.1, povolení 1.2/1.3, vynucení podepisování SMB pomocí zásad skupiny apod.),
- zakázání vlastností, např.:
    - chybové nebo ladicí zprávy pro koncové uživatele,
    - nezabezpečená, zastaralá a/nebo nepotřebná rozhraní,
    - zabránit ukládání hodnot hash systému,
    - anonymní překlad SID / Name Translation,
    - odebrání anonymních uživatelů z oprávnění Everyone,
    - protokolu používaný k překladu adres IP na názvy hostitelů: Link local Multicast Name Resolution (LLMNR),
    - nepotřebné mechanismy automatického spouštění,
    - nepotřebné komponenty operačního systému včetně služeb na pozadí,
- aktivování:
    - spořič obrazovky s ochranou heslem,
    - silný nástroj pro řízení uživatelských účtů (UAC),
    - antivirový program během procesu spouštění,
    - protokolování,
    - funkce zabezpečení CPU,
    - přístupové heslo systému BIOS,
    - zadaná spouštěcí sekvence.

Vymezení rozsahu auditovaných systémů
Pro hardening jsou zvoleny následující systémy/platformy objednatele:

- Microsoft Windows Server (2008, 2012, 2016, 2019),
- Microsoft SQL (2016, 2017, 2019),
- Linux (CentOS, Debian, Rocky, Ubuntu, SUSE/SLES, RHEL/Oracle),
- PostgreSQL 14,
- FirebirdSQL,
- VMware (7.0),

Vždy se bude jednat o jeden typický server, pokud není nastavení systému odlišné (jiné komponenty/služby) nebo specifické (např. Doménový kontrolér, Web Server, Exchange Server), to znamená, že pro každý odlišný/specifický budou tyto rozdíly zdokumentovány formou samostatné hardeningové politiky. Součástí hardeningu bude i specifikace/konfigurace nastavení auditování pro jednotlivé systémy.

V rámci předmětu plnění dle článku I, odst. 1, bodu b) této smlouvy je:

Objednatel požaduje, aby služby technického specialisty na vyžádání (*nad rámec předmětu plnění uvedeného v článku I, odst. 1 bodu a) této smlouvy*) byly realizovány:

- na základě písemných požadavků objednatele elektronicky formou objednávky na adresu uvedené kontaktní osoby poskytovatele. Objednávka bude obsahovat specifikaci služby (následné konzultace ke správě a nastavení systému nebo databáze objednatele).
- za poskytnuté a objednatelem akceptované služby přísluší poskytovateli za hodinu práce odměna v dohodnuté výši.

Předpokládaný celkový počet případných služeb na vyžádání, tzn. následných konzultací ke správě a nastavení systému objednatele je v jejich součtu omezen na 10 MD (man day) a doba pro vyžádání služby je omezena na 24 měsíců po akceptaci předmětu plnění uvedeného v článku I, odst. 1, bodu a) této smlouvy.

II. Dodání předmětu plnění

1. Poskytovatel se zavazuje zrealizovat předmět plnění:
    - dle čl. I, odst. 1, bodu a) této smlouvy nejpozději do 150 kalendářních dnů ode dne nabytí účinnosti smlouvy,
    - dle čl. I, odst. 1, bodu b) této smlouvy v termínu objednávky vzájemně odsouhlasené smluvními stranami.
2. Realizace předmětu plnění se považuje podle této smlouvy za splněnou, pokud:
    - předmět plnění dle čl. I, odst. 1, bodu a) této smlouvy byl řádně zrealizován a případně dle čl. I, odst. 1, bodu b) této smlouvy byl realizován dle objednávky objednatele,
    - předmět plnění byl řádně akceptován způsobem sjednaným v čl. II. odst. 3 této smlouvy.
3. Po zrealizování předmětu plnění vystaví poskytovatel akceptační protokol, který bude obsahovat níže uvedené náležitosti:
    - označení akceptačního protokolu a jeho číslo,
    - název a sídlo poskytovatele a objednatele,
    - číslo této smlouvy/objednávky,
    - označení dodané služby a jejího množství,
    - datum zrealizování služby,
    - výsledek akceptačního řízení,
    - jiné náležitosti důležité pro předání a převzetí dodané služby.
4. 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 lhůty k jejich odstranění. Tento zápis bude současně podepsán zástupci obou smluvních stran.
5. Poskytovatel se zavazuje, že bude poskytovat služby s vynaložením veškeré odborné péče, že bude dodržovat obecně závazné předpisy a vnitřní předpisy objednatele:
    - Používání sítě VFN externími uživateli (SM-UI-02) uvedené v příloze č. 2 této smlouvy, která mu byla objednatelem poskytnuta, a se kterou byl prokazatelným způsobem seznámen před podpisem této smlouvy. Požadavky, definované předmětem smlouvy, znamenají výjimky z některých pravidel, definované v předpisu.
6. Veškeré činnosti při realizaci předmětu plnění je poskytovatel povinen provádět osobami, které mají odpovídající kvalifikaci.
7. Kontaktní a odpovědná osoba za poskytovatele:

    Za realizaci předmětu plnění: xxxxx (Tel.: xxxxx E-mail: xxxxx)
    Za akceptaci předmětu plnění: xxxxx (Tel.: xxxxx E-mail: xxxxx)
    Za identifikaci případného kybernetického útoku v průběhu plnění předmětu plnění dle této smlouvy: xxxxx (Tel.: xxxxx E-mail: xxxxx)

    Kontaktní a odpovědná osoba za objednatele:

    Za systémovou oblast: xxxxx (Tel.: xxxxx E-mail: xxxxx
    Za bezpečnost systémů: xxxxx (Tel.: xxxxx E-mail: xxxxx
    Za akceptaci předmětu plnění: xxxxx (Tel.: [redacted] E-mail: xxxxx
    Za identifikaci případného kybernetického útoku v průběhu plnění předmětu plnění dle této smlouvy: xxxxx

III. Cena a platební podmínky

1. Cena za předmět dle čl. I, odst. 1, bodu a) této smlouvy byla sjednána ve výši:

    Celková cena bez DPH **528 000 Kč**
    DPH **110 880 Kč**
    Cena vč. DPH **638 880 Kč** (dále jen „cena")

Celková cena je stanovena jako konečná a zahrnuje cenu za celý předmět plnění dle čl. I, odst. 1, bodu a) této smlouvy a veškeré náklady poskytovatele na plnění dle této smlouvy.

2. Cena služeb na vyžádání dle čl. I, odst. 1, bodu b) této smlouvy je stanovena dohodou smluvních stran ve výši **1 400 Kč** bez DPH za 1 hodinu práce poskytovatele.

3. Objednatel nebude poskytovat zálohy. Cena za plnění dle čl. I, odst. 1, bodu a) této smlouvy bude uhrazena až po řádné akceptaci a předání celého předmětu plnění článku dle čl. I, odst. 1, bodu a) této smlouvy této smlouvy.

4. Objednatel se zavazuje zaplatit cenu na základě faktury vystavené dodavatelem do 14 dnů po řádné akceptaci a předání celého předmětu plnění dle článku I, odst. 1, bodu a) této smlouvy.

5. Cena za služby na vyžádání dle čl. I, odst. 1, bodu b) této smlouvy bude objednatelem hrazena po akceptaci každé jednotlivé realizace na základě objednávky. Přílohou jednotlivé faktury za jednotlivou realizaci služeb na vyžádání bude akceptační protokol příslušné fakturované realizace, který bude podepsán oběma smluvními stranami.

6. 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 zaslána poštou ve dvou vyhotoveních na Ekonomický úsek objednatele, odbor účetnictví. K faktuře bude přiložena kopie řádně opatřeného akceptačního protokolu způsobem sjednaným níže. V případě zaslání faktury elektronicky bude akceptační protokol přiložen v neskenované podobě.

7. Faktura musí obsahovat všechny údaje uvedené v § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, dle zákona č. 563/1991 Sb., o účetnictví. V případě, že dodavatelem vystavená faktura bude obsahovat nesprávné či neúplné údaje, je právem objednatele takovou fakturu do 15 dnů od jejího převzetí vrátit poskytovateli. Ten podle charakteru nedostatku fakturu opraví anebo vystaví novou. U opravené nebo nové faktury běží nová lhůta splatnosti.

8. Platby budou probíhat výhradně v CZK (česká koruna) 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 poskytovateli vyúčtovanou dohodnutou cenu je splněna dnem odeslání platby z účtu objednatele.

IV. 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,
   - na straně poskytovatele kromě ujednání uvedeného v čl. V. odst. 2 této smlouvy, také jestliže nedodá řádně a včas předmět plnění a pokud 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.

V. Sankce

1. Pro případ prodlení objednatele s úhradou ceny dle čl. IV této smlouvy má poskytovatel 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 poskytovatel je oprávněn požadovat zaplacení úroku z prodlení až po uplynutí 30 dnů od sjednané lhůty splatnosti.

2. Poskytovatel je v případě nedodržení termínu plnění dle čl. II. této smlouvy povinen uhradit objednateli smluvní pokutu ve výši 0,1 % z celkové ceny plnění dle této smlouvy za každý i započatý den prodlení, jestliže se s objednatelem nedohodne jinak. Objednatel je dále v těchto případech oprávněn odstoupit od smlouvy.

3. V případě porušení povinnosti dle čl. VIII. a čl. IX odst. 6 této smlouvy, je objednatel oprávněn požadovat uhrazení smluvní pokuty ve výši 200.000,- Kč za každé jednotlivé porušení povinnosti.

4. V případě porušení povinnosti dle čl. IX. odst. 3 a 4 této smlouvy, je objednatel oprávněn požadovat uhrazení smluvní pokuty ve výši 50.000,- Kč za každé jednotlivé porušení povinnosti.

5. V případě nedodržení povinnosti stanovené v čl. IX. odst. 5 smlouvy má objednatel právo účtovat smluvní pokutu ve výši pohledávky, která byla postoupena v rozporu s touto smlouvou. Objednatel má zároveň právo odstoupit od smlouvy.

6. V případě nedodržení některé z povinností dodavatele stanovených v čl. IX. 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.

7. 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.
8. Uplatněním nároku na zaplacení smluvní pokuty, ani jejím skutečným uhrazením nezanikne povinnost poskytovatele splnit povinnost, jejíž plnění bylo zajištěno smluvní pokutou, a poskytovatel tak bude nadále povinen ke splnění takovéto povinnosti.

VI. Závazky objednatele

1. Objednatel se zavazuje zaplatit poskytovateli dohodnutou cenu za plnění zrealizované dle této smlouvy.
2. Objednatel se zavazuje, že umožní poskytovateli poskytování předmětu plnění vzdáleným přístupem.
3. Objednatel se zavazuje zajistit poskytovateli jím požadované potřebné informace věcného i systémového charakteru pro plnění této smlouvy.
4. Požadavky poskytovatele na zdroje a na nutnou součinnost objednatele uvedené v příloze č. 3 této smlouvy.
5. Objednatel je povinen určit oprávněné osoby pro styk s poskytovatelem, které budou po dobu platnosti této smlouvy zabezpečovat nezbytnou součinnost mezi poskytovatelem a objednatelem a k zajištění potřebných informací k plnění této smlouvy. Objednatel může tyto oprávněné osoby zaměnit jinými, které budou vhodné pro výkon prací, a to po předchozím písemném vyrozumění poskytovatele. Oprávněné osoby objednatele odpovídají za obsah a správnost předaných požadavků a informací.

VII. Závazky poskytovatele

1. Poskytovatel se zavazuje dodat plnění specifikované v čl. I této smlouvy a odpovídá za kvalitu a včasnost zrealizovaného předmětu plnění ve smyslu výše uvedených ustanovení.
2. Poskytovatel je odpovědný za škodu, která objednateli vznikne prokazatelným neplněním nebo vadným plněním jeho závazků vyplývajících z této smlouvy.
3. Poskytovatel neodpovídá za jakékoli škody, opožděná nebo neposkytnutá plnění, pokud toto bude zapříčiněno neposkytnutím potřebné součinnosti objednatele dle přílohy č. 3 této smlouvy nebo zásahem třetí strany do systému.

VIII. 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. Poskytovatel 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**").

IX. Ostatní ujednání

1. Poskytovatel 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. Poskytovatel je povinen v souladu s ustanovením § 105 z. č. 134/2016 Sb. předložit do 10 pracovních dnů od doručení oznámení o výběru poskytovatele 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. Poskytovatel 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 5.000.000,- Kč.

4. Poskytovatel 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 poskytovatel 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. Poskytovatel je oprávněn postoupit pohledávku vyplývající z plnění dle této smlouvy na třetí osobu pouze s předchozím písemným souhlasem objednatele.

6. V případě zjištění nebo podezření na probíhající kybernetický útok, musí poskytovatel provést nezbytné kroky k zdokumentování a zajištění forenzních důkazů a okamžitému nahlášení kontaktní osobě objednatele za identifikaci případného kybernetického útoku v průběhu plnění předmětu plnění dle této smlouvy, která je uvedena v čl. II, odst. 7 této smlouvy, která rozhodne, zda budou práce ukončeny nebo pokračováno, a za jakých podmínek.

7. Poskytovatel 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.

X. Závěrečná ujednání

1. Tato smlouva nabývá platnosti dnem jejího podpisu oběma 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 předpisy 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 - Položkový ceník
Příloha č. 2 – Používání sítě VFN externími uživateli
Příloha č. 3 - Požadavky na zdroje a nutnou součinnost objednatele

V Praze dne:

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

V Praze dne

_____
DoxoLogic, s.r.o.
Bc. Martin Listopad, jednatel

_____
Ing. Miloslav Rut
za Moore Technology CZ s.r.o., jednatel

Příloha č. 1 smlouvy PO 780/S/23

Položkový ceník

Předmět plnění VZ	Množství	Jednotka	Nabídková cena celkem		
			(bez DPH)	Samostatně DPH (základní sazba)	(s DPH)
Audit systémů zadavatele a vytvoření hardeningových bezpečnostních politik (v souladu se zadávacími podmínkami a návrhem smlouvy).	1	různé	528 000,00 Kč	110 880,00 Kč	638 880,00 Kč
Služby technického specialisty na vyžádání (v souladu se zadávacími podmínkami a návrhem smlouvy**)**	80	člověkohodin	112 000,00 Kč	23 520,00 Kč	135 520,00 Kč
Celková nabídková cena za celý předmět plnění bez DPH			640 000,00 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

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

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

Příloha č. 3 smlouvy č. PO 780/S/23

Požadavky na zdroje a nutnou součinnost objednatele

Požadavky poskytovatele na zdroje a nutnou součinnost objednatele dle oblastí:

- obecné požadavky,
- základní přehled o IS/ICT společnosti,
- na řízení komunikace,
- na provedení auditu OS/DB/platforem,
- k prezentaci výstupů z auditů,
- technické konzultace k nastavení OS/DB/platforem a provozovaných IS,
- k otestování a nasazení hardeningových bezpečnostních politik,
- k vypracování a předání finálních výstupů.

Požadavky na součinnost objednatele v následujících oblastech:

1) obecné požadavky – nutná součinnost s IT specialistou objednatele,
2) základní přehled o IS/ICT společnosti – nutná součinnost/úvodní schůze s IT manažerem objednatele,
3) na řízení komunikace – nutná součinnost/úvodní schůze s network administrátorem,
4) na provedení auditu OS/DB/platforem – nutná součinnost společně s interní auditorem objednatele,
5) k prezentaci výstupů z auditů – bez potřeby zapojení zaměstnance objednatele,
6) technické konzultace k nastavení OS/DB/platforem a provozovaných IS – nutná součinnost s IT specialistou objednatele,
7) k otestování a nasazení hardeningových bezpečnostních politik – nutná součinnost s IT specialistou objednatele,
8) k vypracování a předání finálních výstupů – bez potřeby zapojení zaměstnance objednatele.

Požadavky na zdroje:
Dle vzájemné domluvy mezi objednatelem a poskytovatelem v průběhu plnění předmětu veřejné zakázky.