SMLOUVA O POSKYTOVÁNÍ SLUŽEB PODPORY A SERVISU SOFTWARE
uzavřená dle § 1746 odst. 2. zákona č. 89/2012 Sb., občanský zákoník, v platném znění, (dále jen „zákon č. 89/2012 Sb.")

BCV solutions s. r. o.

zapsána: dne 5. 3. 2008 v Obchodním rejstříku vedeném u Městského soudu v Praze v oddíle C, vložce 136075.
se sídlem: 7. května 1168/70, Praha 4 – Chodov, 14900
IČO: 28360851 DIČ: CZ28360851
zastoupena: Zdeňkem Burdou, jednatelem
bankovní spojení: [redacted]
číslo účtu: [redacted]

jako **poskytovatel** na straně jedné (dále jen „**poskytovatel**" nebo „**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: Česká národní banka
číslo účtu: 24035021/0710

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

(poskytovatel a objednatel dále též souhrnně jako „**smluvní strany**")

Smluvní strany uzavírají po vzájemném projednání a shodě dnešního dne, měsíce a roku na základě výsledku **nadlimitní veřejné zakázky** s názvem „**Podpora Identity managementu**", **vyhlášené otevřeným řízením** dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších přepisů (dále jen „z. č. 134/2016 Sb.") a zveřejněné ve Věstníku veřejných zakázek. pod ev. č. **Z2023-044821** ze dne 09.10.2023 **a v Úředním věstníku Evropské unie pod č. 2023/S 196-614117, oznámení o zahájení zadávacího řízení ze dne 11.10.2023** (dále jen „veřejná zakázka"), v souladu s ustanovením § 1746 odst. 2. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále též „zákon" či „zákon č. 89/2012 Sb."), tuto

S M L O U V U O P O S K Y T O V Á N Í S L U Ž E B
P O D P O R Y A S E R V I S U S O F T W A R E

(dále též „**smlouva**")

I. Předmět plnění smlouvy

1. Předmětem plnění této smlouvy je závazek poskytovatele poskytovat objednateli servis, rozvoj a podporu stávajícího Identity managementu (dále jen „IdM" nebo „SW řešení") pro minimálně 7000 identit objednatele.
2. Součástí poskytování podpory bude údržba SW licencí, systémová podpora, uživatelská podpora a exitová součinnost, jejichž bližší specifikace je popsána v příloze č. 1 smlouvy.
3. Objednatel se touto smlouvou zavazuje zaplatit odměnu za poskytnutí podpory dle tohoto článku smlouvy v souladu s podmínkami sjednanými touto smlouvou.
4. Poskytovatel se stává plněním dle této smlouvy poskytovatelem systémů, technologií a služeb, na kterých je provozována základní služba: Poskytování zdravotních služeb dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „ZKB"). Objednatel je orgánem nebo osobou provozující základní službu podle ZKB § 3 písm. f) a provozování základní služby Objednatelem podle ZKB je závislé na provozování řešení poskytovaného poskytovatelem.
5. Místem plnění je sídlo objednatele.

II. Způsob poskytování podpory software

1. Konkrétní specifikace podpory je blíže specifikována v příloze č. 1 této smlouvy.
2. Oprávněné osoby objednatele a poskytovatele, které mohou pracovat s Helpdeskem objednatele jsou uvedeny v příloze č. 4 smlouvy.

III. Cena a platební podmínky

1. Cena za služby poskytované objednateli dle čl. I. a přílohy č. 1 (vyjma bodu 1.4 přílohy č. 1) této smlouvy je stanovena dohodou smluvních stran ve výši **745 200** Kč bez DPH ročně.
2. Cena služeb na vyžádání dle bodu č. 1.4 přílohy č. 1 této smlouvy je stanovena dohodou smluvních stran na částku **2000** Kč bez DPH za 1 člověkohodinu práce poskytovatele.

3. Cena za poskytované služby dle čl. III. odst. 1. této smlouvy bude objednatelem hrazena v pravidelných čtvrtletních platbách ve výši **186 300** Kč bez DPH. Dnem uskutečnění zdanitelného plnění bude poslední kalendářní den příslušného čtvrtletí.
4. Cena za služby na vyžádání dle čl. III. odst. 2 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.
5. Ceny dle čl. III. této smlouvy budou hrazeny na základě faktur – daňových dokladů (dále jen „**faktura**") vystavených poskytovatelem, přičemž tyto musí obsahovat všechny údaje uvedené v § 29 odst. 1 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a dále též dle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů.
6. Poskytovatel se touto smlouvou zavazuje, že jím vystavená faktura bude obsahovat všechny náležitosti řádného daňového dokladu dle platné právní úpravy.
7. Splatnost faktury činí 60 dní ode dne doručení faktury objednateli do jeho sídla, přesněji na Ekonomický úsek, Odbor účetnictví nebo elektronicky ve formátu PDF nebo ISDOC na e-mailovou adresu: xxxxx.
8. Pokud faktura nebude obsahovat všechny zákonem a touto smlouvou stanovené náležitosti, je objednatel oprávněn ji do 15 dnů ode dne doručení vrátit poskytovateli s tím, že poskytovatel je poté povinen vystavit fakturu novou. Pro odstranění jakékoliv pochybnosti smluvní strany berou na vědomí, že za předpokladu vystavení nové faktury počíná běh nové doby splatnosti ve smyslu čl. III odst. 7 této smlouvy, tedy že v tomto případě objednatel není v prodlení s úhradou faktury.
9. Úhrada faktury bude provedena formou převodu na účet druhé smluvní strany uvedený na faktuře, přičemž tento bude shodný s účtem uvedeným v záhlaví této smlouvy.
10. Smluvní strany prohlašují, že povinnost objednatele zaplatit poskytovateli řádně vyfakturovanou cenu v souladu s touto smlouvou je splněna dnem odeslání platby z účtu objednatele.
11. Smluvní strany se dohodly, že pokud průměrná roční míra inflace vyjádřená přírůstkem průměrného indexu spotřebitelských cen (CPI – Consumer Price Index) dle údajů publikovaných Českým statistickým úřadem na jeho oficiálních internetových stránkách, přesáhne v České republice za posledních 12 po sobě jdoucích měsíců kalendářního roku hodnotu 5 bodů (procent) oproti míře inflace za kalendářní rok předcházející, na možnosti zvýšení kupní ceny o výši meziročního rozdílu míry inflace v uvedeném období, a to vždy od 1. ledna následujícího kalendářního roku a maximálně jednou v každém kalendářním roce účinnosti této smlouvy, nejdříve však od 1.1.2026. Poskytovatel je povinen tento nárůst inflace objednateli prokázat, ke zvýšení ceny za plnění se vyžaduje souhlas objednatele. Zvýšení ceny je účinné až po uzavření písemného číslovaného dodatku podepsaného oběma smluvními stranami.

IV. Trvání smlouvy

1. Smlouva se uzavírá na dobu neurčitou.
2. Smlouva může být ukončena:
    - písemnou dohodou smluvních stran
    - písemnou výpovědí ze strany objednatele nebo poskytovatele i bez udání důvodu; výpovědní doba činí 6 měsíců a počíná běžet první den následujícího měsíce, ve kterém byla písemná výpověď druhé smluvní straně doručena.
    - odstoupením od smlouvy ze strany objednatele nebo poskytovatele.
3. Kterákoliv ze smluvních stran je oprávněna odstoupit od smlouvy v případě, že druhá smluvní strana hrubě poruší nebo opakovaně porušuje své smluvní závazky vyplývající z této smlouvy a přes písemnou výzvu odmítá odstranit vady svého jednání, anebo nečiní žádné kroky k nápravě vzniklého vadného stavu nebo v případě porušení závazku mlčenlivosti druhou smluvní stranou. Za hrubé porušení smluvních závazků ze strany objednatele se považuje prodlení objednatele s úhradou faktur poskytovateli překračujícím termín splatnosti o 90 dnů a na straně poskytovatele, pokud dojde k porušení povinnosti jemu uložené ust. čl. IX odst. 6 této smlouvy
4. Odmítne – li smluvní strana, jíž je adresována zásilka, obsahující výpověď či odstoupení od této smlouvy, tuto zásilku převzít, považuje se tato zásilka za doručenou dnem odmítnutí takové zásilky.
5. Účinností výpovědi či odstoupením od smlouvy není dotčen nárok objednatele na náhradu škody vzniklé porušením podmínek této smlouvy, ani nárok na zaplacení smluvní pokuty.

V. Závazky objednatele

1. Objednatel se zavazuje zaplatit poskytovateli dohodnuté ceny za služby poskytnuté dle této smlouvy.
2. Objednatel se zavazuje, že umožní poskytovateli poskytování předmětu plnění vzdáleným přístupem při dodržení požadavků a podmínek uvedených v příloze č. 5 této smlouvy.
3. Objednatel se zavazuje zajistit poskytovateli jím požadované potřebné informace věcného i systémového charakteru pro plnění této smlouvy.
4. 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 a materiálů k plnění této smlouvy. Objednatel může tyto oprávněné osoby zaměnit jinými, které budou vhodné pro výkon prací, a to po předchozím písemném vyrozumění poskytovatele, bez nutnosti uzavřít písemný dodatek ke smlouvě (seznam oprávněných osob je přílohou č. 4 této smlouvy).
5. Oprávněné osoby objednatele odpovídají za obsah a správnost předaných požadavků a informací.
6. Objednatel se zavazuje přidělit každému požadavku v rámci poskytované podpory závažnost dle podmínek specifikovaných v příloze č. 1 této smlouvy.

VI. Závazky poskytovatele

1. Poskytovatel se zavazuje plnit své povinnosti vyplývající z této smlouvy s maximální odpovědností tak, aby systém byl udržován nepřetržitě v provozuschopném a funkčním stavu, který je řádně zdokumentován. Poskytovatel odpovídá za kvalitu a včasnost vykonaných prací ve smyslu výše uvedených ustanovení.

2. Poskytovatel je povinen systém zabezpečit tak, aby nedošlo k přihlášení nebo přístupu osoby, která nemá příslušné oprávnění do systému. Za jakékoli škody, s výjimkou fyzického zabezpečení serverů, způsobené objednateli zásahem neoprávněně přihlášené osoby odpovídá poskytovatel.
3. Poskytovatel se zavazuje zajistit objednateli přístup a nakládání s veškerými daty objednatele uloženými v SW řešení nepřetržitě a bez omezení po celou dobu trvání této smlouvy i po skončení účinnosti této smlouvy, a to v případě nedodržení podmínek sjednaných v rámci bodu 1.5 Přílohy č. 1 této smlouvy – Exitová součinnost.
4. Poskytovatel je odpovědný za škodu, která objednateli vznikne prokazatelným neplněním nebo vadným plněním závazků poskytovatele z této smlouvy vyplývajících.
5. Poskytovatel neodpovídá za jakékoli škody, opožděná nebo neposkytnutá plnění, pokud toto bude zapříčiněno neposkytnutím potřebných informací či dokumentů objednatelem nebo zásahem třetí strany do systému. Rozsah potřebných informací požadovaných poskytovatelem specifikuje objednateli poskytovatel, a to po nahlášení nebo potvrzení přijetí každého jednotlivého požadavku.
6. Poskytovatel musí objednatele, a to odpovědnou osobu: manažera kybernetické bezpečnosti, e-mail: xxxxx, neprodleně informovat o kybernetických bezpečnostních incidentech souvisejících s poskytovaným řešením.
7. Poskytovatel je povinen objednatele informovat prostřednictvím manažera kybernetické bezpečnosti o způsobu řízení rizik na straně poskytovatele a o zbytkových rizicích souvisejících s plněním smlouvy v půl ročním intervalu nebo v případě zjištění nových rizik nebo změn stávajících rizik informovat bezodkladně.
8. Poskytovatel je povinen informovat manažera kybernetické bezpečnosti objednatele o významné změně v ovládání poskytovatele podle dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích ve znění pozdějších předpisů nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných poskytovatelem k plnění podle této smlouvy.
9. Poskytovatel je povinen v případě zjištění nebo podezření na probíhající kybernetický útok v průběhu poskytování služeb poskytovatelem, provést nezbytné kroky poskytovatelem k zdokumentování a zajištění forenzních důkazů a okamžitému nahlášení kontaktní osobě za objednatele (viz kontaktní osoby), která rozhodne, zda budou práce ukončeny nebo bude v pracích pokračováno a za jakých podmínek.
10. Poskytovatel bere na vědomí, že služby poskytované dle této smlouvy nesmí být provozované na technických nebo programových prostředcích označených NÚKIB jako hrozba.
11. Poskytovatel je povinen určit oprávněné osoby pro styk s objednatelem, které budou po dobu platnosti této smlouvy zabezpečovat nezbytnou součinnost mezi objednatelem a poskytovatelem a k zajištění potřebných informací a materiálů k plnění této smlouvy. Poskytovatel může tyto oprávněné osoby zaměnit jinými, které budou vhodné pro výkon prací, a to po předchozím písemném vyrozumění a odsouhlasení ze strany objednatele (seznam oprávněných osob tvoří přílohu č. 4 této smlouvy).
12. Poskytovatel se zavazuje splňovat/dodržet relevantní požadavky na řízení bezpečnosti informací uvedené v příloze č. 6 této smlouvy „Požadavky systému řízení bezpečnosti informací na Dodavatele" vztahující se na prostředí a činnosti poskytovatele.

VII. Smluvní pokuty, sankce

1. Pro případ prodlení objednatele s úhradou ceny dle čl. III 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. V případě, že nebude dodržen požadavek na dostupnost provozu identity managementu v režimu SLA 99,5 %, uvedený v kapitole č. 1.3.2 v příloze č. 1 této smlouvy, je objednatel oprávněn za nedodržení dostupnosti řešení požadovat smluvní pokutu ve výši 10.000,- Kč za každý i započatý den nedostupnosti.
3. Na výše uvedené smluvní pokuty nemá objednatel nárok, prokáže-li se, že problém byl způsoben jednáním objednatele, selháním nebo jinými problémy na straně objednatele.
4. V případě nedodržení povinností poskytovatele dle čl. IX odst. 2, 6 a 7 této smlouvy, má objednatel právo účtovat poskytovateli smluvní pokutu ve výši 50 000,- Kč za každé jednotlivé porušení povinnosti.
5. V případě nedodržení povinností poskytovatele dle čl. VI odst. č. 6 až 12 a čl. VIII. této smlouvy, má objednatel právo účtovat poskytovateli smluvní pokutu ve výši 200 000,- Kč za každé jednotlivé porušení povinnosti.
6. V případě nedodržení povinnosti stanovené v čl. IX. odst. 9 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.
7. 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.
8. Smluvní pokuta bude vyúčtovaná samostatným daňovým dokladem, splatnost smluvní pokuty činí 30 dní ode dne doručení vyúčtování poskytovateli.
9. Zaplacením smluvní pokuty není dotčen nárok objednatele na náhradu škody, včetně náhrady škody, která převyšuje smluvní pokutu.

VIII. Mlčenlivost

1. Poskytovatel 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. Poskytovatel 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 poskytovatel 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 poskytovatelem 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. Poskytovatel 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. Poskytovatel se zavazuje zajistit informovanost svých pracovníků (včetně poddodavatelů) o povinnostech vyplývajících z této smlouvy. Poskytovatel 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. Poskytovatel se zavazuje informovat své poddodavatele o povinnosti mlčenlivosti dle této smlouvy. V případě porušení mlčenlivosti za strany poddodavatele, odpovídá poskytovatel 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. IX smlouvy, 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., a dle zákona o registru smluv uveřejnit tuto smlouvu včetně případných dodatků, příloh a objednávek vystavených na základě této smlouvy, 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 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. Poskytovatel bere na vědomí, že objednatel je povinným subjektem podle zák. č. 106/1999 Sb., zákona o svobodném přístupu k informacím, ve znění pozdějších předpisů.
4. Poskytovatel se zavazuje dodržovat nařízení objednatele, kterým je zakázáno kouření ve všech prostorách i plochách areálu objednatele s výjimkou vyhrazených míst.
5. Obě strany se zavazují, že v souvislosti s plněním smlouvy učiní opatření k zajištění ochrany před šířením počítačových virů a nelegálních programů.
6. 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 20.000.000,- Kč.
7. Poskytovatel je povinen udržovat výše uvedené pojištění po celou dobu trvání smlouvy. 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 poskytovatel povinen učinit příslušná opatření tak, aby pojištění bylo udrženo tak, jak je požadováno v tomto ustanovení smlouvy.

8. Poskytovatel se zavazuje při plnění této smlouvy dodržovat povinnosti uvedené v dokumentu „Používání sítě VFN externími uživateli", který je přílohou č. 5 této smlouvy.
9. Poskytovatel je oprávněn postoupit pohledávku vyplývající z plnění dle této smlouvy na třetí osobu pouze s předchozím písemným souhlasem objednatele.

X. Závěrečná ujednání

1. Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti uveřejněním v registru smluv.
2. Tato smlouva se řídí právním řádem České republiky a případné spory z ní, které nebudou urovnány smírnou cestou, budou rozhodovány věcně a místně příslušným soudem ČR, za kterýžto pro účely této smlouvy smluvní strany označují obecný soud objednatele.
3. Právní vztahy touto smlouvou neupravené, jakož i právní poměry z ní vznikající a vyplývající, se řídí příslušnými ustanoveními občanského zákoníku v platném znění a předpisy souvisejícími.
4. Jakékoliv změny této smlouvy mohou být prováděny pouze formou písemných dodatků k této smlouvě a musí být podepsány oprávněnými zástupci smluvních stran. Tyto případné dodatky budou tvořit nedílnou součást této smlouvy.
5. 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.
6. Práva a závazky, které pro smluvní strany ze smlouvy vyplývají, přecházejí na jejich případné právní nástupce.
7. Smluvní strany prohlašují, že si tuto smlouvu přečetly, a že byla ujednána po vzájemném projednání podle jejich svobodné vůle, určitě, vážně a srozumitelně, nikoliv v tísni za nápadně nevýhodných podmínek.

Přílohy:
Příloha č. 1 - Specifikace podpory SW řešení
Příloha č. 2 – Technická dokumentace řešení IdM objednatele
Příloha č. 3 – Položkový ceník cenová kalkulace
Příloha č. 4 - Seznam oprávněných osob
Příloha č. 5 – Používání sítě VFN externími uživateli
Příloha č. 6 – Požadavky systému řízení bezpečnosti informací na dodavatele

V Praze dne	V Praze dne
---	---
prof. MUDr. David Feltl, Ph.D., MBA	Zdeněk Burda
ředitel Všeobecné fakultní nemocnice v Praze	jednatel

1 Servis a podpora

Dodavatel poskytuje servis a podporu v těchto oblastech:

a) Údržba software.
b) Systémová podpora.
c) Uživatelská podpora.
d) Služby na vyžádání
e) Exitová součinnost.

Objednatel poskytne poskytovateli ke splnění tohoto závazku nezbytnou součinnost.

1.1 Údržba software

Poskytovatel se zavazuje udržovat identity management (dále jen „IdM") aktuální, správně licencovaný, splňující veškeré požadavky kladené na bezpečnost, ochranu osobních údajů a v souladu s legislativou.
Poskytovatel se zavazuje po dobu platnosti tohoto závazku dále poskytovat zejména:

- Opravu zjištěných chyb v programovém kódu IdM formou aktuálně vydávaných softwarových opravných kódů (hot-fix nebo patch).
- Updaty a upgrady IdM, které byly výrobcem uvolněny na trh. Dodavatel musí zajistit aktuálnost IdM na všech aktivních i neaktivních nodech použité virtualizace.
- Proaktivní řešení bezpečnostních chyb a zranitelnosti IdM.
- Odstraňuje zranitelnosti identifikované nezávislými subjekty (např. NIST), NÚKIB a z penetračních testů objednatele (provádí smluvní dodavatel objednatele).
- Aktualizaci IdM tak, aby byl v souladu s relevantními platnými právními předpisy ČR a EU.

V případě dodání nové verze nebo update musí být zachovány všechny funkcionality uvedené v příloze č. 2 této smlouvy a dodání nové verze nebo update musí být v souladu se standardním technologickým prostředím objednatele, pokud nebude dohodnuto jinak.

1.2 Systémová podpora

Poskytovatel se zavazuje udržovat realizované řešení v aktuálním stavu, splňující veškeré požadavky kladené na funkčnost, bezpečnost a ochranu osobních údajů.
Poskytovatel se zavazuje po dobu platnosti podpory dále poskytovat zejména:

- Správa produkčního i testovacího prostředí objednatele.
- Služby řešení bezpečnostních chyb, hackerských/kybernetických útoků a zjištěných zranitelností řešení.
- Služby migrace řešení – převod řešení na vyšší verzi databázového prostředí a operačního systému.
- Služby zahrnující monitoring, zálohování a logování v souladu s požadavky objednatele.

1.3 Uživatelská podpora

Poskytovatel se zavazuje poskytovat uživatelskou podporu softwarového řešení druhé a vyšší úrovně.
Objednatel má podporu systému první úrovně plně ve své kompetenci, s řízenou distribucí na interní podporu nebo podporu poskytovatele. Pro řádné poskytování služeb poskytovatele zajistí objednatel součinnost interního servisního týmu technických specialistů pro řešení poruch a požadavků s týmem poskytovatele.

Služby spojené s uživatelskou podporou

Poskytovatel se zavazuje po dobu platnosti této podpory zajistit pro objednatele služby spojené s podporou řešení

1. Uvedené služby jsou součástí dodávky a nejsou zpoplatněny vysoutěženou hodinovou sazbou.
2. Jsou to služby poskytované zpravidla v místě objednatele, služby mohou být poskytnuty i vzdáleně. O poskytnutých službách je vždy zapsán řešitelem záznam do příslušného Ticketu v ServiceDesku VFN, resp. integrované aplikaci Helpdesku poskytovatele.
3. Služby spojené s podporou zahrnují:
   - Dílčí konzultační činnost pro uživatele a správce systému,
   - zaškolení uživatelů při rutinním provozu na pracovišti objednatele,
   - zaškolení správce systému při implementaci nových verzí,
   - metodická podpora při rutinním používání systému,
   - sledování využití systému a vypracování návrhů na jeho zlepšení,
   - průběžná aktualizace veškeré dokumentace systému.

1.3.1 Komunikační cesty

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

1.3.2 Řešení závad

Závadou se rozumí nefunkčnost jakékoli funkcionality systému, která bude poskytovatelem řešena v rámci sjednané úrovně poskytování služeb (SLA).
U dané závady určuje příslušnou úroveň poskytování služeb vždy objednatel. Poskytovatel má právo se proti určené úrovni odvolat, pokud byla průkazně určena chybně.
Provoz řešení je v režimu 24 x 7 při dostupnosti 99,7 % za rok, garantovaná podpora je uvedena v následující tabulce podle příslušné úrovně SLA.

Úroveň SLA	Příjem hlášení	Reakční doba (doba od nahlášení do zahájení řešení Incidentu)	Maximální doba od nahlášení do obnovy služby
1 - KRITICKÁ	8:30 – 16:30 HotLine – 8x5 HelpDesk – 24x7	4 hodiny	Do 3 pracovních dní
2 - VÁŽNÁ	8:30 – 16:30 HotLine – 8x5 HelpDesk – 24x7	Do 8 hodin	Do 5 pracovních dní
3 - BĚŽNÁ	8:30 – 16:30 HotLine – 8x5 HelpDesk – 24x7	Do 24 hodin	Do 7 pracovních dní

Reakční doba je v pracovních hodinách.
Řešení závad není omezeno počtem hodin / měsíc.

1.3.2.1 Definice kategorie incidentu

Kategorie incidentu	Závažnost incidentu
Kritická - přerušení provozu	Služba IdM jako celku není dostupná, více jak 4 hod. nejsou prováděny synchronizace a přenosy, nelze provádět aplikační správu, jeho funkce nejsou pro uživatele dostupné a nelze pokračovat v užívání IdM. Celková ztráta funkcionality IdM, kdy není k dispozici žádné dočasné řešení problému.
Vážná - významné omezení provozu	Služba IdM nebo kritické funkce IdM jsou pro uživatele významně omezeny, problém způsobuje závažnou ztrátu služeb IdM. V používání IdM lze pokračovat pouze omezeně, některé z klíčových funkcionalit nelze použít. Není k dispozici žádné přijatelné náhradní řešení.
Běžná – menší omezení provozu	Služba IdM nebo kritické funkce IdM jsou pro uživatele dostupné, problém způsobuje omezení služeb IdM. V používání IdM lze pokračovat. Není ohroženo používání služby IdM pro uživatele.

1.4 Služby na vyžádání

Poskytovatel se zavazuje po dobu platnosti podpory zajistit pro objednatele služby na vyžádání, tzn. služby nad rámec předmětu plnění. Předpokládaný rozsah je 196 MD (1 568 člověkohodin) za čtyři roky.

1. Služby na vyžádání budou realizovány na základě dílčích objednávek a budou hrazeny dle ceníku Služby na vyžádání (vysoutěžená hodinová sazba).

2. Jsou to služby poskytované zpravidla v místě objednatele, služby mohou být po dohodě poskytnuty i vzdáleně. Z poskytnutých služeb je vždy vypracována zpráva o realizaci.
3. Forma akceptace poskytnutých služeb nad rámec předmětu plnění této smlouvy je realizována oboustranně potvrzeným akceptačním protokolem.
4. Služby na vyžádání zahrnují zejména:
    - Konzultační a analytické služby zaměřené na požadovanou oblast,
    - poskytování systémových, programátorských a vývojových prací,
    - realizace požadavků na novou funkcionalitu nad rámec stávajícího řešení objednatele uvedeného v příloze č. 2 této smlouvy.

1.5 Exitová součinnost

Poskytovatel za účelem řádného a plynulého převedení všech činností spojených se servisem a podporou řešení při jejich ukončení poskytovatelem garantuje především tyto součinnosti:

- Poskytne náležitou a nezbytnou součinnost pro takové převedení,
- poskytne veškeré nezbytné informace a dokumentaci,
- předá objednateli data způsobem a ve formátu odsouhlaseném,
- uvedené služby v rámci exitové součinnosti jsou zpoplatněny vysoutěženou hodinovou sazbou.

1. [redacted]
   - [redacted]
2. [redacted]

[redacted]

3. [redacted]

- [redacted]

4. [redacted]

4.1. [redacted]

4.2. [redacted]

4.3. [redacted]

4.4. [redacted]

4.5. [redacted]

4.6. [redacted]

4.7. [redacted]

4.8. [redacted]

4.9. [redacted]

4.10. [redacted]

4.11. [redacted]

5. [redacted]

5.1. [redacted]

- [redacted]

6. [redacted]

6.1. [redacted]

6.2. [redacted]

7. [redacted]

7.1. [redacted]

7.1.1. [redacted]

7.1.2. [redacted]

7.1.3. [redacted]

7.1.4. [redacted]

7.2. [redacted]

7.2.1. [redacted]

7.2.2. [redacted]

7.2.3. [redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

[redacted]

7.3. [redacted]

[redacted]

7.4. [redacted]

[redacted]

7.5. [redacted]

[redacted]

7.6. [redacted]

[redacted]

8. [redacted]

8.1. [redacted]

8.1.1. [redacted]

8.1.2. [redacted]

8.1.3. [redacted]

8.1.4. [redacted]

8.1.5. [redacted]

8.1.6. [redacted]

8.1.7. [redacted]

8.1.8. [redacted]

9. [redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

10. [redacted]

10.1. [redacted]

Položka	Název	Položka	MJ	ks	jednotková cena bez DPH (Kč)	Celková cena bez DPH (Kč)
1	Podpora Identity managementu (dále jen IdM") (v souladu se zadávacími podmínkami)	Podpora IdM	rok	4	745 200,00 Kč	2 980 800,00 Kč
		Služby na vyžádání	člověkohodina	1568	2 000,00 Kč	3 136 000,00 Kč
Cena celkem v Kč bez DPH						**6 116 800,00 Kč**

Příloha č. 4 Smlouvy – Seznam oprávněných osob

A. Seznam kontaktních osob poskytovatele oprávněných poskytovat podporu

Jméno	**Funkce**	**Telefonní číslo**
xxxxx	Servisní specialista	xxxxx
xxxxx	Servisní specialista	xxxxx
xxxxx	Vedoucí servisní podpory	xxxxx

B. Seznam kontaktních osob objednatele oprávněných k hlášení požadavků na poskytování podpory

Jméno	**Funkce**	**Telefonní číslo**
xxxxx	Vedoucí odboru provozu IT	xxxxx
xxxxx	Vedoucí odboru bezpečnosti IT	xxxxx
xxxxx	Vedoucí oddělení správy serverů	xxxxx

C. Seznam kontaktních osob objednatele určených k hlášení oznámení, požadavků, událostí nebo incidentů poskytovatele ve vztahu k ochraně osobních údajů nebo bezpečnosti informací nebo kybernetické bezpečnosti

Oblast	**Funkce**	**Kontakt**
Ochrana osobních údajů	Pověřenec pro ochranu osobních údajů	xxxxx
Bezpečnosti informací, kybernetické bezpečnost	Manažer bezpečnosti informací / kybernetické bezpečnosti	xxxxx

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

POUŽÍVÁNÍ SÍTĚ VFN EXTERNÍMI UŽIVATELI

Obsah

Zpracovatel:	Účinnost dokumentu od:	Schválil:
[redacted]	23. 7. 2020	[redacted]
Garant:	**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]

Požadavky systému řízení bezpečnosti informací na dodavatele

1 Účel

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

2 Bezpečnostní požadavky

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

2.1 Obecná pravidla bezpečnosti informací

Dodavatel je povinen:

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

2.2 Fyzická bezpečnost

Dodavatel je povinen:

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

2.3 Bezpečnost lidských zdrojů

Dodavatel je povinen:

- prokazatelně seznámit zaměstnance Dodavatele s dodržováním bezpečnostních pravidel a zásad požadovaných VFN,
- dodržovat ochranu aktiv VFN před neautorizovaným přístupem, vyzrazením, modifikací, zničením nebo narušením,
- zachovávat mlčenlivost o důvěrných údajích nebo sděleních VFN a o jejich ochraně,
- stanovit odpovědnosti zaměstnanců Dodavatele pro nakládání s informacemi,
- poučit zaměstnance Dodavatele hlásit zjištěné bezpečnostní události nebo jiná bezpečnostní rizika odpovědné osobě Dodavatele,
- provádět pravidelné školení zaměstnanců Dodavatele v souvislosti s bezpečností informací,

- při porušení pracovních povinnosti zaměstnance Dodavatele ve vztahu k bezpečnosti informací nebo způsobení bezpečnostního incidentu, musí být zahájeno formální disciplinární řízení. Způsob řízení odpovídá povaze porušení nebo incidentu a jeho dopadu na VFN.

2.4 Řízení přístupu

Dodavatel je povinen:

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

2.5 Bezpečné chování uživatelů

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

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

2.6 Bezpečnost mobilních zařízení a vzdáleného přístupu

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

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

2.7 Ochrana před škodlivým kódem

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

2.8 Zálohování a obnova dat

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

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

2.9 Technické zranitelnosti

Dodavatel je povinen:

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

2.10 Bezpečnost komunikační sítě

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

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

2.11 Bezpečnostní zásady pro práci s daty

Dodavatel je povinen:

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

2.12 Používání kryptografické ochrany

Dodavatel je povinen:

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

2.13 Akvizice, vývoj a údržba informačních systémů

Dodavatel je povinen:

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

2.14 Zvládání bezpečnostních incidentů

Dodavatel je povinen:

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

2.15 Řízení kontinuity činností

Dodavatel je povinen:

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

2.16 Legislativní a normativní požadavky

Dodavatel je povinen splnit legislativní a normativní požadavky:

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

2.17 Kontroly zavedení bezpečnostních opatření

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

2.18 Audity plnění bezpečnostních požadavků

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