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

STAPRO s. r. o.
zapsána v obchodním rejstříku vedeném u Krajského soudu v Hradci Králové, oddíl C, spisová vložka číslo 148
se sídlem: Pernštýnské náměstí 51, 530 02 Pardubice
IČO: 135 83 531 DIČ: CZ699004728
zastoupena: Ing. Leošem Raibrem, jednatelem
bankovní spojení: ČSOB a.s.
číslo účtu: 271810793/0300

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 laboratorního systému FONS Openlims**", **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. Z2025-063680 ze dne 12. 11. 2025, a ID veřejné zakázky na profilu zadavatele VZ0233904 (dále jen „veřejná zakázka"), v souladu s ustanovením § 1746 odst. 2. zákona č. 89/2012 Sb., občanský zákoník, v platném znění, (dále jen „zákon č. 89/2012 Sb."), tuto

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 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 a podporu stávajícího laboratorního informačního systému FONS Openlims (dále jen „SW řešení" či „SW" případně též „předmět plnění" nebo „podpora") a dále poskytovat podporu všech vývojových úprav software.
2. Součástí poskytování podpory bude údržba SW licencí, systémová podpora, uživatelská podpora, reporting a exitová součinnost, jejichž bližší specifikace je popsána v příloze č. 1 smlouvy.
3. Objednatel se touto smlouvou zavazuje zaplatit poskytovateli odměnu za podporu dle tohoto článku smlouvy v souladu s podmínkami sjednanými touto smlouvou.
4. Poskytovatel bere na vědomí, že dle zákona č. 264/2025 Sb. o kybernetické bezpečnosti (nový ZKB) je objednatel po dobu trvání přechodného období dle ZKB orgánem nebo osobou provozující základní službu podle § 3 písm. f) zákona č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB) a provozování základní služby objednatelem podle dosavadního ZKB je závislé na provozování řešení poskytovaného poskytovatelem. Poskytovatel se stává plněním dle této smlouvy Poskytovatelem systémů, technologií a služeb, na kterých je provozována základní služba dle ZKB.
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. 3 smlouvy.

III. Cena a platební podmínky

1. Cena za služby poskytované objednateli dle čl. I. a přílohy č. 1 (vyjma bodu 7.5 přílohy č. 1 smlouvy) této smlouvy je stanovena dohodou smluvních stran ve výši **12 772 044,-** Kč bez DPH ročně.
2. Cena služeb na vyžádání dle bodu č. 7.5 přílohy č. 1 této smlouvy je stanovena dohodou smluvních stran na částku **1 980,- Kč** bez DPH za 1 hodinu práce poskytovatele.

3. Cena za poskytované služby dle čl. III. odst. 1. této smlouvy bude objednatelem hrazena v pravidelných měsíčních platbách ve výši **1 064 337,- Kč** bez DPH. Dnem uskutečnění zdanitelného plnění bude poslední kalendářní den příslušného měsíce.
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. Cena za plnění, které se stane součástí této smlouvy na základě ustanovení "Další podmínky plnění" odpovídajícím způsobem navýší cenu uvedenou v čl. III. odst. 1 a 3 této smlouvy, a to za předpokladu, že se navýší počet PC stanic objednatele využívajících SW řešení FONS Openlims objednatele, a to dle přílohy č. 2 této smlouvy.
6. 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.
7. Poskytovatel se touto smlouvou zavazuje, že jím vystavená faktura bude obsahovat všechny náležitosti řádného daňového dokladu dle platné právní úpravy.
8. Splatnost faktury činí 60 dní ode dne doručení faktury objednateli. Faktura bude zaslána elektronicky ve formátu PDF na e-mailovou adresu: xxxxx.
9. 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. 8 této smlouvy, tedy že v tomto případě objednatel není v prodlení s úhradou faktury.
10. 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.
11. Smluvní strany prohlašují, že povinnost objednatele zaplatit poskytovateli s touto smlouvou řádně vyfakturovanou cenu je splněna dnem odeslání platby z účtu objednatele.
12. 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 1.1.2027. 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. X 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. 4 této smlouvy „Používání sítě VFN externími uživateli".
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. 3 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 kap. 7 v bodě 7.4.5 a 7.4.6. této smlouvy.
7. Objednatel se zavazuje po dohodě s poskytovatelem zajistit přístup k technickým prostředkům: komponenty (hardwarové, softwarové) nebo služby, které nejsou předmětem smlouvy a jsou nutné pro zajištění provozu SW řešení nebo činností poskytovatele podle této smlouvy, a to dle svých možností a na základě zdůvodněných požadavků poskytovatele. Pokud nebude přístup na tyto prostředky zajištěn, neodpovídá poskytovatel za případné neplnění či omezené plnění poskytovaných služeb a činností. V případě nutnosti zajištění přístupu k technických prostředků objednatele, je poskytovatel povinen o této skutečnosti objednatele informovat s dostatečným časovým předstihem.

8. Objednatel se zavazuje, že do aplikace SW řešení dodaného poskytovatelem nebude provádět žádné zásahy narušující struktury databáze nebo jeho funkce, včetně napojení jiných systémů na databázi bez předchozího písemného souhlasu poskytovatele. V případě porušení takového závazku poskytovatel negarantuje bezchybný chod aplikace SW řešení a je oprávněn odstoupit od této smlouvy.
9. Objednatel je oprávněn provádět datové a konfigurační změny v SW řešení. Pokud tyto změny budou mít negativní dopad na služby a činnosti zajišťované poskytovatelem, pak poskytovatel neodpovídá za případné neplnění či omezené plnění poskytovaných služeb a činností prokazatelně způsobené zásahem objednatele. Objednatel se v takovémto případě zavazuje vyvolat jednání s poskytovatelem k zajištění nápravy.

VI. Závazky poskytovatele

1. Poskytovatel se zavazuje plnit své povinnosti vyplývající z této smlouvy s maximální odpovědností tak, aby SW řešení bylo udržováno 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 SW řešení 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 i v případě nedodržení podmínek sjednaných v rámci bodu 7.7 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: manazerKB@vfn.cz, neprodleně informovat o kybernetických bezpečnostních incidentech souvisejících s předmětem plnění.
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 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 dle této smlouvy, 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 se zavazuje, že veškeré poskytované služby dle této smlouvy nesmí být provozované na technických nebo programových prostředcích, které jsou zveřejněny na stránkách Národního centra kybernetické bezpečnosti (provozované NÚKIB) za hrozbu. Poskytovatel a jeho poddodavatel nebo výrobce technického nebo programového prostředku nesmí být z území či oblastí označených NÚKIB za hrozbu.
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. 3 této smlouvy).
12. Poskytovatel se zavazuje zajistit objednateli přístup a nakládání s veškerými daty objednatele uloženými v SW FONS Openlims po celou dobu trvání smlouvy v režimu Read-Only realizovaném v produkční databázi. Poskytovatel je povinen umožnit objednateli přístup k veškerým datům postupem dle čl. IX smlouvy.
13. Poskytovatel se zavazuje splňovat/dodržet relevantní požadavky na řízení bezpečnosti informací uvedené v příloze č. 5 této smlouvy „Požadavky systému řízení bezpečnosti informací na Dodavatele" vztahující se na prostředí a činnosti poskytovatele.

Další podmínky plnění:

1. Objednatel si vyhrazuje po dobu trvání této smlouvy právo na poskytnutí dalších služeb, a to za situace, kdy dojde k rozšíření stávajícího SW řešení na další PC stanice objednatele. Za poskytnutí těchto dalších služeb má poskytovatel nárok na adekvátní navýšení ceny plnění smlouvy.
2. Poskytovatel se zavazuje v případě rozšíření stávajícího SW řešení na další PC stanice objednatele provádět služby odpovídající rozsahu této smlouvy, a to dle podmínek stanovených touto smlouvou. Za poskytnutí těchto dalších služeb má poskytovatel nárok na adekvátní navýšení ceny plnění smlouvy.
3. Cena za tyto další služby je stanovena v příloze č. 2 této smlouvy.

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. Při nedodržení termínu pro odstranění závady v kategorii „havárie" specifikované v bodě 7.4.5 přílohy č. 1 této smlouvy, je objednatel oprávněn požadovat na poskytovateli smluvní pokutu ve výši 5.000,- Kč za každou započatou hodinu prodlení za jednotlivý případ.
3. Při nedodržení termínu pro odstranění závady v kategorii „závada" specifikované v bodě 7.4.5 přílohy č. 1 této smlouvy, je objednatel oprávněn požadovat na poskytovateli smluvní pokutu ve výši 3.000,- Kč za každou započatou hodinu prodlení za jednotlivý případ.
4. Při nedodržení termínu pro odstranění závady v kategorii „chyba" specifikované v bodě 7.4.5 přílohy č. 1 této smlouvy, je objednatel oprávněn požadovat na poskytovateli smluvní pokutu ve výši 5.000,- Kč za každý započatý pracovní den prodlení za jednotlivý případ.
5. V případě, že nebude dodržen požadavek na dostupnost provozu v režimu SLA, uvedených v bodě 7.4.4 přílohy 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 každého jednotlivého SLA.
6. Na výše uvedené smluvní pokuty nemá objednatel nárok, prokáže-li se, že problém byl způsoben jednáním objednatele, selháním nebo jinými problémy na straně objednatele.
7. V případě nedodržení povinností poskytovatele dle čl. X odst. 2, 6 a 7 této smlouvy, má objednatel právo účtovat poskytovateli smluvní pokutu ve výši 50.000,- Kč za každé jednotlivé porušení povinnosti.
8. V případě nedodržení povinností poskytovatele dle čl. VI odst. 6 až 13 a čl. VIII této smlouvy, má objednatel právo účtovat poskytovateli smluvní pokutu ve výši 200.000,- Kč za každé jednotlivé porušení povinnosti.
9. V případě nedodržení povinnosti stanovené v čl. XI odst. 3 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.
10. 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.
11. Smluvní pokuta bude vyúčtovaná samostatným daňovým dokladem, splatnost smluvní pokuty činí 30 dní ode dne doručení vyúčtování Poskytovateli.
12. 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. 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. Zpřístupnění dat

1. Objednatel požaduje technicky zajistit přístup k veškerým datům uloženým objednatelem do SW řešení (zejména pacientská data) uloženým v databázích SW řešení. Přístup bude řízený na úrovni externí služby objednatele mimo SW řešení (webové služby a exporty dat pomocí datových pump) a souvisejícího logování (auditní stopy) o těchto přístupech, resp. čerpání dat. Objednatel bude mít k dispozici náhled do databází a na základě požadavku objednatele bude pumpa poskytovatelem upravena/rozšířena o další data.
2. Zajištění bezpečnosti zpracování takto exportem získaných dat, zejména osobních a citlivých údajů pacientů, je od okamžiku jejich exportu z databází SW řešení výlučně v odpovědnosti objednatele.

X. Ostatní ujednání

1. Poskytovatel bere na vědomí, že objednatel je povinen dle ustanovení § 219 odst. 1 zákona č. 134/2016 Sb., a dle zákona č. 340/2015 Sb., o registru smluv, uveřejnit tuto smlouvu včetně případných dodatků, 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 smluvní 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. 4 této smlouvy.
9. Veškerá data uložená nebo ukládaná a zpracovávána uživateli objednatele v laboratorním informačním systému FONS Openlims (zejména pacientská data) jsou výhradním vlastnictvím objednatele.
10. Objednatel se zavazuje umožnit pracovníkům poskytovatele:
    - přístup na příslušná pracoviště v místech instalace technologií dotčených smlouvou,
    - bezpečné, nezávadné a zdraví neohrožující pracovní prostředí.

XI. 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 předpisů České republiky. Změny a doplnění této smlouvy lze učinit pouze na základě písemné dohody smluvních stran. Takové dohody musí mít podobu datovaných, vzestupně číslovaných dodatků této smlouvy podepsanými jejich statutárními zástupci.
3. Poskytovatel je oprávněn postoupit pohledávku vyplývající z plnění dle této smlouvy na třetí osobu pouze s předchozím písemným souhlasem objednatele.
4. Tato smlouva včetně příloh je vyhotovena ve 2 stejnopisech, z nichž každá strana obdrží po jednom vyhotovení. Obě vyhotovení jsou rovnocenná a mají platnost originálu. Pokud je smlouva podepisována elektronicky, je vyhotovena v jednom stejnopise podepsaném oběma smluvními stranami elektronickým podpisem dle zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.
5. Autentičnost této smlouvy potvrzují smluvní strany svými podpisy.

Přílohy:
Příloha č. 1 – Specifikace předmětu plnění
Příloha č. 2 – Položkový ceník_cenová kalkulace
Příloha č. 3 – Seznam oprávněných osob
Příloha č. 4 – Používání sítě VFN externími uživateli
Příloha č. 5 – Požadavky systému řízení bezpečnosti informací na dodavatele

V Praze dne dle el. podpisu

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

V Pardubicích dne dle el. podpisu

Ing. Leoš Raibr
jednatel společnosti STAPRO s. r. o.

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

PŘÍLOHA Č. 1 - SPECIFIKACE PŘEDMĚTU PLNĚNÍ: PODPORA LABORATORNÍHO INFORMAČNÍHO SYSTÉMU FONS OPENLIMS

VŠEOBECNÁ FAKULTNÍ NEMOCNICE V PRAZE
Úsek informatiky a digitální transformace |
U Nemocnice 499/2, 128 08 Praha 2 | www.vfn.cz

1 Manažerské shrnutí

Dokument je určen mimo jiné i jako podklad pro provedení veřejné zakázky s názvem „Podpora laboratorního informačního systému FONS Openlims" společnosti Stapro s. r. o., vyhlášené otevřeným řízením dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších přepisů (dále jen „z. č. 134/2016 Sb.").

2 Předmět veřejné zakázky / smlouvy

Všeobecná fakultní nemocnici v Praze (dále **VFN**) v současné době využívá laboratorní informační systém FONS Openlims (dále **systém**), který byl pořízen od společnosti Stapro s. r. o. na základě smlouvy o dílo a k němuž má VFN na neomezenou dobu právo k užití licence.

Předmětem této veřejné zakázky je poskytování služeb podpory provozu laboratorního informačního systému FONS Openlims" a služeb na vyžádání v tomto rozsahu:

1. Údržba software (maintenance).
2. Uživatelská podpora.
3. Systémová podpora.
4. Řešení závad.
5. Reporting.
6. Poskytování služeb na vyžádání.

Objednatel poskytne poskytovateli ke splnění tohoto závazku nezbytnou součinnost.

3 Popis stávajícího systému

3.1 Rozsah spravovaného prostředí

Všeobecná fakultní nemocnici v Praze (dále VFN) v současné době využívá laboratorní informační systém „Openlims" (dále systém), který byl pořízen od společnosti Stapro s. r. o. na základě smlouvy o dílo a k němuž má VFN na neomezenou dobu právo k užití licence. Systém se aplikován na různých pracovištích a skládá se z těchto modulů:

1. Jedná se zde o 2 hlavní databáze
   - DB pro centrální laboratoře VFN
   - DB pro laboratoř UDMP a FTO
2. Laboratoře
   - Biochemie
   - Hematologie a 1. interní klinika
   - Imunologie
   - Národní laboratoř pro tkáňové helmintózy
   - Toxikologická laboratoř
   - Laboratoř ústavu dědičných metabolických poruch
   - Pracoviště fakultního transfuzního oddělení – dále FTO (laboratoř, krevní banka, odběrové centrum a výroba)

VŠEOBECNÁ FAKULTNÍ NEMOCNICE V PRAZE
Úsek informatiky a digitální transformace |
U Nemocnice 499/2, 128 08 Praha 2 | www.vfn.cz

3. Servery a systémové služby
   - svr-olas1 (centrální laboratoře VFN) – 5 služeb pro aplikaci, 4 pro komunikaci s analyzátory
   - svr-olas2 (laboratoř UDMP a FTO) – 1 služba pro aplikaci a komunikaci s analyzátory
   - svr-kom – komunikace (výsledky, elektronické žádanky)
   - svr-weblis – webová aplikace s modulem WebLIMS, odběrové centrum (aktualizace času odběru v odeslaných elektronických žádankách), messenger pro zasílání výsledků pacientům
   - svr-toxikologie – skenování žádanek a jejich ukládání
   - svr-OpenlimsDB – databáze všech 3 instalací Openlims (centrální laboratoře VFN , UDMP, FTO)
   - ukb-Openlims – lokální server lokální instalace pro záložní provoz biochemie
   - hema-Openlims – lokální server lokální instalace pro záložní provoz hematologie
   - WKS-PILNIK – pečetění výsledkových listů od eIdentity a.s.
   - SVR-IDM-PROXY.vfn.cz – komunikace s IdM systém společnosti BCV Solutions

3.2 Hardwarová infrastruktura

VFN využívá pro provoz systému tyto technické prostředky ve svém vlastnictví:

Určení serveru / zařízení	Typ	Označení serveru / zařízení	Operační systém
Openlims - Aplikační server (CHL, UKIA, UKBLD)	VM	SVR-OLAS1	Win 2016, Datacenter, 64-bit
Openlims - Aplikační server (FTO, UDMP)	VM	SVR-OLAS2	Win 2016, Datacenter, 64-bit
Openlims – DB server	VM	SVR-OpenlimsDB	Win 2016, Std, 64-bit
Openlims - záložní provoz STATIM - ÚLBLD	VM	ukb-Openlims	Win 2016, Std, 64-bit, SQL 2017
Openlims - záložní provoz STATIM - CHL	VM	Hema-Openlims	Win 2016, Std, 64-bit
Openlims - WEBLims	VM	SVR-WebLIS	Win 2016, Std, 64-bit
Úložiště výsledkových listů Openlims - pracovní archiv	VM	SVR-FS2	Win 2016, Std, 64-bit
Openlims - toxikologie	VM	SVR-Toxikologie	Win 2016, Datacenter, 64-bit
Openlims – pečetění výsledkových listů	VM	WKS-PILNIK	Win 2016, Datacenter, 64-bit
Openlims - komunikační prostředník	VM	SVR-Kom	Win 2016, Std, 64-bit

3.2.1 Hardwarová infrastruktura pro centrální laboratoře a ÚDMP

- Počet PC: 508
- Počet uživatelů: 563
- Počet analyzátorů: 137, typ komunikace: souborová, RS2, TCP
- Počet tiskáren: 130

- Počet BC tiskáren: 62
- Počet PDA u křesel v odběrovém centru: 20
- OMR čtečka pro načítání metod z papírových žádanek 1x
- Fujitsu skener pro toxikologii (plánováno rozšíření na biochemii, hematologii, imunologii)

3.2.2 Hardwarová infrastruktura pro provoz FTO

- Počet PC: 104
- Počet uživatelů: 150
- Počet analyzátorů: 16
- Počet tiskáren: 54 tiskáren (15 tiskáren čárových kódů EPL i ZPL)
- Počet čteček čárových kódů: 62
- 1 off-line instalace na 3 NTB (Evidence, Lékař, Odběr) – pro výjezdy FTO

4 Funkční specifikace, integrace a činnosti nad LIS

4.1 Pro centrální laboratoře a ÚDMP

- Oddělené číselníky metod pro jednotlivé laboratoře, oddělené příjmy, mezilaboratorní výpočty
- Synchronizace číselníků s NIS MEDEA (včetně registru pacientů) a ServiceBroker s KIS FONS Enterprise
- Pečetění výsledkových listů službou ELDAX (elektronický zdravotní archív) od společnosti Seyfor a.s., a odesílání odkazů na archivované dokumenty do MEDEA a FONS Enterprise
- Odesílání výsledků do dvou nemocničních NIS a externích systémů (MISE, ÚHKT)
- Příjem elektronických žádanek z více nemocničních NIS – MEDEA a FONS Enterprise a dalších externích žadatelů (ÚHKT, IKEM)
- Modul Sady komunikačních kódů pro komunikaci mimo VFN umožňující správnou identifikaci metod s různými NČLP
- Modul Automatické hlášení výsledků Covid do ISIN
- Modul Automatické odesílání výsledků do NRHZS
- B2B komunikace s portálem VZP (kontrola čísel pojištěnců)

4.1.1 Zajišťované činnosti nad Openlims:

- Školení uživatelů a administrátorů.
- Konzultace k optimalizaci laboratorních procesů.
- Analýza nových procesů, návrh řešení, předání požadavků vývojovému oddělení, testování a implementace nové funkcionality.
- Pravidelná aktualizace a správa systému.
- Údržba číselníků metod a skupin metod.
- Zakládání nových bloků, jejich konfigurace a zařazení do laboratorních procesů.
- Úprava tiskových předloh dle požadavků laboratoře a požadavků akreditace.
- Aktualizace kódů NČLP.

VŠEOBECNÁ FAKULTNÍ NEMOCNICE V PRAZE
Úsek informatiky a digitální transformace |
U Nemocnice 499/2, 128 08 Praha 2 | www.vfn.cz

- Správa modulu „Sady komunikačních kódů" pro komunikaci s externími systémy.
- Aktualizace číselníků metod v systému Medee pro příjem výsledků a export požadavků.
- Nastavení a podpora odesílání výsledků externím žadatelům.
- Nastavení a podpora importu elektronických požadavků od externích žadatelů.
- Kontrola a řešení správného zobrazování výsledků v systému Medee.
- Kontrola a řešení příjmu elektronických žádanek do laboratoří.
- Spolupráce při údržbě stromu žadatelů.
- Údržba číselníků pro zdravotní pojišťovny a nastavení vyúčtování.
- Kontrola činnosti analyzátorů.
- Kontrola naplánovaných úloh.
- Kontrola a řešení pečetění výsledkových listů a jejich zálohování.
- Definice předdefinovaných textů dle požadavků laboratoře.
- Podpora při instalaci pracovních stanic a tiskáren.
- Připojování nových analyzátorů.
- Konfigurace tiskových sestav dle požadavků uživatelů.
- Provádění profylaktických protokolů (4× ročně).
- Podpora při kontrole a opravách dat pro zdravotní pojišťovny.
- Instalace certifikátů (pečetění a B2B komunikace).
- Definice výpočtových vztahů a rozporů dle požadavků.
- Konfigurace štítků v jazycích EPL a ZPL.
- Úprava RPL pro tisk štítků a komunikaci s analyzátory.
- Kalibrace tiskáren štítků.
- Pravidelná kontrola deníků a notifikací.

4.2 Pro provoz FTO

- 2 provozy (laboratoř dárců a pacientů), 14 bloků
- 3562 žadatelů
- 482 metod
- export výsledků do NIS - Medea a FONS Enterprise
- export výsledků - Vidia Diagnostika
- import požadavků - FONS Enterprise
- Odběrová centra (přenos UNL souborů): Rokycany, Příbram
- Externí žadatelé (komunikace v DASTA 4): Kladno, ÚHKT (Amadeus) – import požadavků/export výsledků
- synchronizace dat po Výjezdech s Off-line klienty
- NROVDK – zasílání povinných údajů, on-line kontrola dárců i odběrů
- ÚZIS – export transfuzních dat
- Navision – ekonomický systém ve VFN – export dat z uzávěrky

VŠEOBECNÁ FAKULTNÍ NEMOCNICE V PRAZE
Úsek informatiky a digitální transformace |
U Nemocnice 499/2, 128 08 Praha 2 | www.vfn.cz

4.2.1 Zajišťované činnosti nad Openlims:

- Aktualizace instalací pro off-line klienta
- Údržba číselníku metod, skupin metod
- Pomoc při údržbě stromu žadatelů
- Údržba číselníků pro ZP (odbornosti, IČP – každý měsíc)
- Školení uživatelů (noví uživatelé, zaškolení při instalaci verze)
- Kontrola procesu ukončování žádanek
- Kontrola procesu výroby
- Kontrola činnosti analyzátorů - logy
- Kontrola naplánovaných úloh
- Definice předdefinovaných textů dle požadavků
- Generování provozních štítků
- Podpora při instalaci stanic a tiskáren
- Připojování nových přístrojů
- Konfigurace tiskových sestav dle požadavků
- Validace systému – 1x za 2 roky velká validace, malá validace před instalací každé verze
- Pomoc při přípravě kontroly SUKL, řešení požadavků od SUKL
- Podpora zvaní dárců na KN, Zbraslav i výjezdy
- Kontrola dat pro ZP, generování dat pro ZP, pomoc při opravě dat
- Kontrola dat před uzávěrkou, export dat z uzávěrky pro účtárnu VFN
- Kontrola kvality – definice a úprava parametrů
- Look back - – definice a úprava parametrů
- Údržba skladových karet
- Údržba typů odběrů
- Roční statistiky
- Instalace certifikátů (NROVDK, Transnet)
- Opravy dat pro uzávěrku (skladové doklady TP i zboží)
- Definice výpočtových vztahů a rozporů dle požadavků
- Definice parametrů pro uvolňování a propouštění TP
- Konfigurace štítků v jazyce EPL i ZPL
- Kalibrace tiskáren štítků
- Kontrola zásilek, řešení kolizí
- Podpora při rozesílání daňového potvrzení
- Pravidelná kontrola deníků a notifikací (analyzátory, komunikace, rozesílání SMS dárcům, NROVDK,...)
- Analýza nových procesů, návrh řešení, , otestování a implementace nové funkcionality
- Příprava elektronického importu požadavků na objednávání TP
- Pravidelná aktualizace a správa systému

VŠEOBECNÁ FAKULTNÍ NEMOCNICE V PRAZE
Úsek informatiky a digitální transformace |
U Nemocnice 499/2, 128 08 Praha 2 | www.vfn.cz

5 Technologické a technické prostředí systému

Kapitola obsahuje popis technologického prostředí systému a aktuální technické prostředí, které se může změnit v budoucnosti.

5.1 Datové centrum a infrastruktura

VFN disponuje dvěma datovými centry, která jsou geograficky oddělená a pracující v režimu clustrovém provedení, kde provozuje využívané technologie na virtualizační platformě VMware 8.0.

5.2 Technologie využívané objednatelem

1. Aplikace a databáze jsou postaveny na podporovaných technologiích, které mají garantovaný vývojový cyklus minimálně na příštích 5 let. Tyto technologie musí být pravidelně aktualizovány.
2. Modulární architektura umožňuje rozšiřování funkcionalit.
3. Objednatel využívá následující technologie:

Oblast	Technologie	Doplňující informace
Virtualizační platforma	VMware	Verze 8.0
Zálohovací systém	Veeam	Objednatel provádí v pracovní dny zálohy inkrementální a o víkendu plné. Zálohy jsou prováděny v nočních hodinách.
Monitorovací systém	PRTG	
Logování	SIEM IBM QRadar	Nástroj pro sběr a hodnocení logů.
Vzdálený přístup	VPN Cisco AnyConnect s vícefaktorovým ověřením	Vzdálený přístup pro management prostředí je umožněn pomocí VPN objednatele.
Řízení privilegovaných oprávnění (PIM/PAM)	BeyondTrust	Privilegovaný přístup na spravované technologie prostřednictvím nástroje PIM/PAM s MFA ověřením.

5.3 Řízení přístupů

1. Aplikace podporuje systém Single Sign On objednatele, s využitím integrace na Active Directory objednatele.
2. Umožňuje řízení všech rolí v aplikaci prostřednictvím skupin v Active Directory objednatele, podporuje víceúrovňová uživatelská oprávnění a umožňuje nastavení rolí podle elementárních práv.

5.4 Přístupová práva

1. Rozdělení přístupových práv do rolí s umožňuje uživateli povolit pouze některé činnosti dle pracovního zařazení.
2. Umožňuje definovat neslučitelné role.

3. Systém umožňuje supervizorovi (např. IT administrátorovi nebo vedoucímu lékárníkovi) spravovat uživatelská oprávnění, tj. nastavovat přístupová práva jednotlivým zaměstnancům lékárny k jednotlivým funkcím systému.
4. Systém umožňuje přenos a aplikaci předdefinovaných vzorů oprávnění, a to bez nutnosti zásahu dodavatele.

5.5 Monitoring

1. Monitoring musí zahrnovat nepřetržitý dohled nad důležitými prvky ASW a jejich funkcemi včetně průběžného vyhodnocování tak, aby bylo možné předejít většině hrozících výpadků a selhání.
2. Monitoring musí zahrnovat zejména prvky jako servery, aplikace, databáze, a integrační prvky se souvisejícími systémy.

5.6 Logování

1. Systém logování zahrnuje logy transakční, aplikační a bezpečnostní a logování práce každého uživatele.
2. V rámci systému pro logování je zajištěno:
   - logování všech transakcí aktivních operací v aplikaci, DB a systémech včetně předávání dat do nástroje SIEM,
   - správně nastavené časové značky na všech zdrojích (tj. synchronizovaný čas, jeho jednotný formát).
   - dostatečné kapacity pro logování a jejich uchovávání po určenou dobu,
   - dostupnost logů i v případě poruchy systému (zálohování).

5.7 Zálohování dat

1. Zálohování dat provádí objednatel na základě zálohovacího plánu zpracovaného dodavatelem.
2. Zálohovací plány předpisují, jak ochránit ASW a data při neočekávané události, pádem systému počínaje a fyzickým zničením zařízení konče.

5.8 Obnova po havárii

1. Obnovu dat provádí objednatel ve spolupráci s dodavatelem na základě plánu obnovy zpracovaného dodavatelem.
2. Plány obnovy provozu ASW po rozsáhlém výpadku musí být zpracovány pro nejpravděpodobnější havárie s největším dopadem na činnost objednatele tak, aby snížily na minimum dobu zásahu, chybovost a riziko ze zanedbání důležitých souvislostí.
3. Plány obnovy provozu ASW po havárii musí být pravidelně revidovány a testovány.
4. Plány obnovy musí obsahovat:
   - Umístění a popis záloh.
   - Pořadí a způsob obnovy jednotlivých komponent systémů.
   - Způsob ověření úspěšného obnovení dat ze zálohy.
   - Maximální časy obnovy.
   - Kontaktní údaje servisních organizací.
   - Metodika testování plánů obnovy.

6 Požadavky na bezpečnost

1. Dodávané technické nebo programové prostředky nesmí být prostředky, které jsou zveřejněny na stránkách Národního centra kybernetické bezpečnosti (provozované NÚKIB) za hrozbu. Žádné poskytované služby nesmí být provozované na výše uvedených technických nebo programových prostředcích označených NÚKIB za hrozba. Dodavatel/Poskytovatel služeb a jeho poddodavatel nebo výrobce technického nebo programového prostředku nesmí být z území či oblastí označených NÚKIB za hrozbu.
2. Dodavatel musí udržovat procesní a technickou dokumentaci v souladu s mezinárodní normou ISO/IEC 27001:2022 (resp. 2023), ISO 27799:2019 (doporučení a požadavky na řízení bezpečnosti informací ve zdravotnických zařízeních), NIST SP 800 řady, metodiky OWASP v souladu s příslušnou legislativou vztahující se na celý předmět dodávky (zejména nařízením EU č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR) a zákona č. 110/2019 Sb., o zpracování osobních údajů) a to v níže uvedeném rozsahu.

6.1 Požadavky na vývoj, test a provoz ASW

1. Dodavatel musí zajistit ve své vlastní (firemní) infrastruktuře z pohledu zajištění bezpečnosti prostředí:
   - Vývojové a testovací prostředí musí být zcela oddělena v sítích a musí být podporována oddělenými stroji.
   - Provozní servery objednatele nesmí vyžadovat překladače a systémové utility, které nejsou nezbytné pro jejich správu nebo provoz.
   - Testování a vývoj nových verzí systémů, aplikací i zařízení se nesmí provádět v provozním prostředí.
2. Dodavatel musí dodržovat při vývoji svých produktů zásady SDL (Secure Development Lifecycle).

6.2 Ochrana před škodlivým kódem

1. Pokud je součástí podporovaného ASW, musí být zajištěna a popsána ochrana:
   - Komunikace ve vnitřní síti.
   - Ochrana serverů a sdílených datových úložišť.
   - Popis požadavků na zajištění bezpečnosti pracovních stanic (HW klientů, popř. VDI).

6.3 Ověření zranitelnosti celého ASW

1. Součástí vývoje jsou i bezpečnostní testy a proces kontroly kódu (codereview) dodavatelem, jejichž cílem je odhalit chyby a zranitelnosti dříve, než je aplikace schválena do provozu.
2. V případě provedené významné změny nebo změny celkové architektury ASW musí podléhat nezávislému bezpečnostnímu testování (penetrační testy), které jsou prováděny objednatelelm prostřednictvím 3. strany (na náklady objednatele) v souladu s normami ISO/IEC 27005:2022 a ISO/IEC 27002:2022 dle obecně uznávané metodiky (např. OSSTMM, OWASP, NIST apod.).
3. Rozsah testů bude zaměřen na infrastrukturu a aplikační vrstvu. Tyto testy budou provedeny objednatelem (prostřednictvím 3. strany) a zjištěné zranitelnosti musí být dodavatelem odstraněny před uvedením ASW do produkčního provozu. V případě potřeby bude odstranění zranitelností ASW ověřeno retesty objednatelem.

6.4 Požadavky na logovací aparát

1. Pro operace logování v systému musí být zajištěna bezpečnost a integrita log záznamů (ochrana před zneužitím, změněním nebo vymazáním) napříč celým log management systémem (dle možné závažnosti zneužití).
2. Zaznamenané události musí být zpracovatelné (strukturované, strojově čitelné) nezávislým prostředkem pro ochranu získaných informací před neoprávněným čtením nebo změnou a pro další vyhodnocování (SIEM).

6.5 Aplikační bezpečnost

Dodavatel zajistí v rámci ASW:

1. Trvalou ochranu aplikací a informací před neoprávněnou činností, popřením provedených činností, kompromitací nebo neautorizovanou změnou.
2. Trvalou ochranu transakcí před jejich nedokončením, nesprávným směrováním, neautorizovanou změnou předávaného datového obsahu, kompromitací, neautorizovaným duplikováním nebo opakováním.
3. Aplikace neumožňuje trvalé a nenávratné smazání dokumentu. Aplikace vždy vytvoří pouze revizi dokumentu se změnou.
4. Automatické odhlašování po konfiguračně definované době neaktivity uživatele. Doba neaktivity musí být nastavitelná až na úroveň oddělení, pokud nebude nastavena pro konkrétní oddělení, platí centrální systémový parametr.

6.6 Ochrana dat

Dodavatel zajistí v rámci spravovaného/podporovaného ASW:

1. Nastavení ochrany dat zpracovaných nebo uchovávaných v ASW, a to především osobních údajů nebo citlivých údajů, kdy bude kladen důraz na data dostupná z vnější sítě. Budou zohledněna rizika:
   - Neoprávněného přístupu
   - Nedovolených činností nad rámec svých práv
   - Popření provedených činností
   - Kompromitace
   - Porušení integrity dat
   - Nedostupnosti dat
   - Neautorizované změny
2. Ochranu prováděných transakcí nebo změn dat:
   - Před jejich nedokončením
   - Nesprávným směrováním
   - Neautorizovanou změnou předávaného datového obsahu
   - Kompromitací
   - Neautorizovaným duplikováním nebo opakováním, a to v souladu s legislativními nebo normativními požadavky, např. daňové, účetní, na ochranu dat

3. Při významné změně ASW musí být provedena analýza rizik a posouzení vlivu na ochranu osobních údajů (DPIA – Data Protection Impact Assessment) v souladu s GDPR ve spolupráci s objednatelem a následné zajištění implementace adekvátních opatřeních na straně dodavatele.

6.7 Zálohování dat

1. Zálohovací plány musí předpisovat, jak ochránit ASW a data při neočekávané události, pádem systému počínaje a fyzickým zničením zařízení konče. Zálohovací plán definuje, jaká data, jakým způsobem a jak často se mají zálohovat, aby byly splněny požadavky uživatelů na:
   - Přijatelnou lhůtu obnovení dat ze zálohy
   - Přípustný objem dat, který nebude možno obnovit (data od poslední zálohy)
   - Dobu a termín omezení provozu IT z důvodu zálohování (zálohovací okno)
2. Zálohovací plán musí obsahovat:
   - Způsob zálohování (technologie, metoda)
   - Stanovení četnosti a cyklů záloh pro technologie, systémy a data
   - Termíny zálohování (zálohovací okna)
   - Pravidla pro manipulaci s médii (bezpečnost uložení, skartace)
   - Stanovení Recovery Time Objective (RTO; jak rychle je možno data obnovit)
   - Stanovení Recovery Point Objective (RPO; jak staré mohou být zálohy)
   - Definice odpovědností
   - Testování záloh (ověření obnovitelnosti a čitelnosti)
3. Smyslem upřesnění ze strany dodavatele je specifikace zálohování jak a co bude zálohováno a samotné jeho nastavení a provádění je na straně objednatele.

6.8 Kryptografické prostředky

V případě využití kryptografických prostředků pro činnost ASW, dodavatel zajistí použití kryptografických algoritmů a kryptografických klíčů v úrovni odolnosti vyplývající z analýzy rizik. Kryptografické klíče musí být uloženy v bezpečném prostředí s možností auditu přístupu ke klíčům.

6.9 Zabezpečení síťových služeb

1. Realizace a dokumentace způsobu zabezpečení síťových služeb.
2. Virtuální servery v prostředí objednatele jsou umístěny ve Virtuální síti, která je propojena s on-premises datovým centrem objednatele. Hybridní propojení zajišťuje objednatel. Komunikace mezi jednotlivými funkčními celky je řízená na úrovni síťových služeb a protokolů s pomocí network security groups. Povolena je pouze vzájemná komunikace, která je nezbytná pro funkci systému.
3. Vstupní, výstupní i vzájemná síťová komunikace mezi jednotlivými částmi systému je monitorována.

6.10 Aktualizace

1. Aktualizace a úpravy aplikace(í) na serverech a na koncových stanicích provádí dodavatel.
2. Aktualizace OS bude prováděna objednatelem v rámci pravidelných aktualizací virtuálních serverů v prostředí objednatele.

7 Požadavky na podporu provozu

Poskytovatel poskytuje servis a podporu v těchto oblastech:

a) Údržba software.
b) Systémová podpora.
c) Uživatelská podpora.
d) Řešení závad.
e) Reporting.
f) Exitová součinnost.

Objednatel poskytne poskytovateli ke splnění tohoto závazku nezbytnou součinnost.

7.1 Údržba software (maintenance)

Poskytovatel se zavazuje udržovat databáze a aplikační software" (dále jen „ASW") 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 ASW formou aktuálně vydávaných softwarových opravných kódů (hot-fix nebo patch).
- Updaty a upgrady ASW, které byly výrobcem uvolněny na trh. Poskytovatel musí zajistit aktuálnost ASW na všech aktivních i neaktivních nodech použité virtualizace.
- Proaktivní řešení bezpečnostních chyb a zranitelnosti ASW.
- Poskytovatel je povinen identifikovat a odstraňovat technické zranitelnosti ASW spojené s bezpečnostním nastavením nebo fungováním ASW. Odstranění uvedených zranitelností se vztahuje i na zranitelnosti identifikované NÚKIB, objednatelem nebo zveřejněné v mezinárodní databázi zranitelností (např. NIST - https://nvd.nist.gov/, CISA - https://www.cisa.gov/news-events/cybersecurity-advisories).
- Aktualizaci ASW tak, aby byl v souladu s relevantními platnými právními předpisy ČR a EU.
- Dodavatel se zavazuje bez prodlení informovat Objednatele o veškerých softwarových produktech, nebo jejich částech, uvolňovaných v rámci této podpory a rovněž o všech nově samostatně dodávaných funkcích a modulech ASW.

Systém musí být udržován v souladu s platnými legislativními normami, které upravují provoz ASW v České republice. Tyto normy zahrnují rovněž požadavky na veškerou komunikaci s institucemi. Důraz je kladen zejména na komunikaci se zdravotními pojišťovnami, SÚKL, Ministerstvem zdravotnictví a ÚZIS.

Dodavatel je povinen zajistit, aby všechny legislativní změny byly promítnuty do aktuální verze ASW a jeho datových rozhraní. Úpravy musí být implementovány tak, aby ASW byl neustále v souladu s právními předpisy. Tyto aktualizace musí být poskytovány v rámci touto smlouvou sjednané podpory, a nikoliv formou zakázkových úprav ze strany objednatele.

7.2 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:

- 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.

7.3 Provoz a údržba serverů ASW serverového centra

V rámci servisních služeb se poskytovatel zavazuje zajistit provoz a údržbu technických prostředků

Určení serveru / zařízení	Typ	Označení serveru / zařízení	Operační systém	Správce infrastruktury	Správce OS
Openlims - Aplikační server (CHL, UKIA, UKBLD)	VM	SVR-OLAS1	Win 2016, Datacenter, 64-bit	OBJEDNATEL	DODAVATEL
Openlims - Aplikační server (FTO, UDMP)	VM	SVR-OLAS2	Win 2016, Datacenter, 64-bit	OBJEDNATEL	DODAVATEL
Openlims – DB server	VM	SVR-OpenlimsDB	Win 2016, Std, 64-bit	OBJEDNATEL	DODAVATEL
Openlims - záložní provoz STATIM - ÚLBLD	VM	ukb-Openlims	Win 2016, Std, 64-bit, SQL 2017	OBJEDNATEL	OBJEDNATEL
Openlims - záložní provoz STATIM - CHL	VM	Hema-Openlims	Win 2016, Std, 64-bit	OBJEDNATEL	OBJEDNATEL
Openlims - WEBLims	VM	SVR-WebLIS	Win 2016, Std, 64-bit	OBJEDNATEL	DODAVATEL
Úložiště výsledkových listů Openlims - pracovní archiv	VM	SVR-FS2	Win 2016, Std, 64-bit	OBJEDNATEL	OBJEDNATEL
Openlims - toxikologie	VM	SVR-Toxikologie	Win 2016, Datacenter, 64-bit	OBJEDNATEL	DODAVATEL
Openlims – pečetění výsledkových listů	VM	WKS-PILNIK	Win 2016, Datacenter, 64-bit	OBJEDNATEL	OBJEDNATEL
Openlims - komunikační prostředník	VM	SVR-Kom	Win 2016, Std, 64-bit	OBJEDNATEL	DODAVATEL

- **Omezení sjednaných služeb:**

HW, Hypervisor (pokud je) pro technické prostředky, u nichž je uveden jako správce infrastruktury objednatel, spravuje úsek informatiky a digitální transformace Objednatele,

Operační systém (OS) spravuje objednatel nebo dodavatel, jak je uvedeno v tabulce této kapitoly.

7.3.1 Zálohování dat serverů a ASW ze serverového centra

Zálohování je prováděno v součinnosti poskytovatele a objednatele:

7.3.2 Zálohování virtuálních serverů a aplikační vrstvy ASW serverů

Zálohování virtuálních serverů (VM) je realizováno pomocí centrálního zálohovacího systému Veeam, které zajišťuje Objednatel v režimu 1 x denně inkrementální a 1 x týdně plná záloha.

7.3.3 Zálohování DB

1. Zálohování DB je realizováno prostředky MS SQL Serveru, konkrétně pomocí SQL maintenance plánu a zajišťuje ho Dodavatel. Plán se skládá z následujících kroků:
2. Každé 2 hod se provádí on-line zálohy transakčních logů všech aplikačních DB na lokální disky serveru
3. 1x denně se spouští plná on-line záloha všech aplikačních DB na lokální disky serveru.
4. Z lokálních disků serveru se odstraní staré zálohy tak, aby na něm byla vždy poslední sada záloh (historie 1 den). Tento krok navazuje na předchozí.
5. Aktuální sada záloh se přenese na zálohovací server SVR-OffBackup. Tento krok navazuje na předchozí.
6. Dále se na serveru SVR-OffBackup odstraní staré zálohy tak, aby na něm bylo uloženo 5 posledních sad záloh (historie 5 dní). Tento krok navazuje na předchozí.

7.3.4 Archivace záloh DB

Archivaci záloh ze serveru SVR-OffBackup provádí objednatel v periodě 1x týdně

7.3.5 Činnosti vykonávané kontinuálně

Poskytovatel se zavazuje poskytovat následující služby pro servery ASW

Monitoring provozu 24x7 pro servery SVR-OLAS1 , SVR-OLAS2, SVR-OpenlimsDB , SVR-Kom

7.3.6 Činnosti vykonávané alespoň 1x měsíčně

Poskytovatel se zavazuje poskytovat následující služby pro servery ASW:

- Preventivní prohlídky – kontrola funkčnosti, zabezpečení a optimalizace provozu serveru ASW, včetně vystavení zprávy/protokolu a jeho uložení do úložiště dokumentů objednatele nebo portálu dodavatele přístupném objednateli.
- Preventivní prohlídky zahrnují především kontrolu konfigurace a nastavení serveru včetně výkonnostních parametrů serveru, kontrolu zaplnění diskových subsystémů, kontrolu systémových logů, kontrolu zálohování dat.
- Virtualizaci a její zabezpečení spravuje objednatel.

7.3.7 Činnosti vykonávané alespoň 1x ročně

Zálohovací plán – Příprava a aktualizace zálohovacího plánu představuje poskytnutí součinnosti dodavatele pro objednatele při aktualizaci zálohovacího plánu pro všechny části SW řešení. Aktualizace zálohovacího plánu spočívá v zajištění těchto činnosti:

1. Identifikace datových aktiv (data i SW), stanovení maximální doby ztráty dat, definice zálohovacích postupů.
2. Součástí je rovněž součinnost na aktualizaci dokumentace: Zálohovací plán, Recovery plán, Havarijní plán a plán kontinuity služeb, Analýza rizik.

Test obnovy – V součinnosti s garantem zálohování objednatele zajistí dodavatel jednou ročně test obnovy SW řešení spočívající v obnově všech části SW řešení (uživatelské rozhraní, aplikační logika a data). Test obnovy spočívá v zajištění těchto činnosti:

- obnova dat ze záloh,
- ověření validity dat,
- ověření funkčností ASW řešení.

Objednatel poskytne součinnost zejména poskytnutím potřebné infrastruktury a prostředí pro provedení Testu obnovy

7.4 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 provozu ASW

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 (proškolení uživatelů ASW, organizační opatření, posílení, doplnění nebo přesuny techniky apod.).
   - Metodická podpora konfigurace systému a přípravy číselníků ASW,
   - Vytváření databázových view na základě požadavků Objednatele,
   - Konfigurace a kontrola přenosů dat mezi aplikacemi,

VŠEOBECNÁ FAKULTNÍ NEMOCNICE V PRAZE
Úsek informatiky a digitální transformace |
U Nemocnice 499/2, 128 08 Praha 2 | www.vfn.cz

- Nastavení přístupových práv aplikací,
- Kontrola a nastavování číselníků a parametrů aplikací pro jednotlivá oddělení.
- průběžná aktualizace veškeré dokumentace systému.

Pro provoz centrální laboratoře VFN a UDMP

- Školení uživatelů a administrátorů.
- Konzultace k optimalizaci laboratorních procesů.
- Analýza nových procesů, návrh řešení, předání požadavků vývojovému oddělení, testování a implementace nové funkcionality.
- Pravidelná aktualizace a správa systému.
- Údržba číselníků metod a skupin metod.
- Zakládání nových bloků, jejich konfigurace a zařazení do laboratorních procesů.
- Úprava tiskových předloh dle požadavků laboratoře a požadavků akreditace.
- Aktualizace kódů NČLP.
- Správa modulu „Sady komunikačních kódů" pro komunikaci s externími systémy.
- Aktualizace číselníků metod v systému Medee pro příjem výsledků a export požadavků.
- Nastavení a podpora odesílání výsledků externím žadatelům.
- Nastavení a podpora importu elektronických požadavků od externích žadatelů.
- Kontrola a řešení správného zobrazování výsledků v systému Medee.
- Kontrola a řešení příjmu elektronických žádanek do laboratoří.
- Spolupráce při údržbě stromu žadatelů.
- Údržba číselníků pro zdravotní pojišťovny a nastavení vyúčtování.
- Kontrola činnosti analyzátorů.
- Kontrola naplánovaných úloh.
- Kontrola a řešení pečetění výsledkových listů a jejich zálohování.
- Definice předdefinovaných textů dle požadavků laboratoře.
- Podpora při instalaci pracovních stanic a tiskáren.
- Připojování nových analyzátorů.
- Konfigurace tiskových sestav dle požadavků uživatelů.
- Provádění profylaktických protokolů (4× ročně).
- Podpora při kontrole a opravách dat pro zdravotní pojišťovny.
- Instalace certifikátů (pečetění a B2B komunikace).
- Definice výpočtových vztahů a rozporů dle požadavků.
- Konfigurace štítků v jazycích EPL a ZPL.
- Úprava RPL pro tisk štítků a komunikaci s analyzátory.
- Kalibrace tiskáren štítků.
- Pravidelná kontrola deníků a notifikací

VŠEOBECNÁ FAKULTNÍ NEMOCNICE V PRAZE
Úsek informatiky a digitální transformace |
U Nemocnice 499/2, 128 08 Praha 2 | www.vfn.cz

Pro provoz FTO

- Aktualizace instalací pro off-line klienta
- Údržba číselníku metod, skupin metod
- Pomoc při údržbě stromu žadatelů
- Údržba číselníků pro ZP (odbornosti, IČP – každý měsíc)
- Školení uživatelů (noví uživatelé, zaškolení při instalaci verze)
- Kontrola procesu ukončování žádanek
- Kontrola procesu výroby
- Kontrola činnosti analyzátorů - logy
- Kontrola naplánovaných úloh
- Definice předdefinovaných textů dle požadavků
- Generování provozních štítků
- Podpora při instalaci stanic a tiskáren
- Připojování nových přístrojů
- Konfigurace tiskových sestav dle požadavků
- Validace systému – 1x za 2 roky velká validace, malá validace před instalací každé verze
- Pomoc při přípravě kontroly SUKL, řešení požadavků od SUKL
- Podpora zvaní dárců na KN, Zbraslav i výjezdy
- Kontrola dat pro ZP, generování dat pro ZP, pomoc při opravě dat
- Kontrola dat před uzávěrkou, export dat z uzávěrky pro účtárnu VFN
- Kontrola kvality – definice a úprava parametrů
- Look back - – definice a úprava parametrů
- Údržba skladových karet
- Údržba typů odběrů
- Roční statistiky
- Instalace certifikátů (NROVDK, Transnet)
- Opravy dat pro uzávěrku (skladové doklady TP i zboží)
- Definice výpočtových vztahů a rozporů dle požadavků
- Definice parametrů pro uvolňování a propouštění TP
- Konfigurace štítků v jazyce EPL i ZPL
- Kalibrace tiskáren štítků
- Kontrola zásilek, řešení kolizí
- Podpora při rozesílání daňového potvrzení
- Pravidelná kontrola deníků a notifikací (analyzátory, komunikace, rozesílání SMS dárcům, NROVDK,...)
- Analýza nových procesů, návrh řešení, , otestování a implementace nové funkcionality
- Příprava elektronického importu požadavků na objednávání TP
- Pravidelná aktualizace a správa systému

Preventivní prohlídky, dílčí konzultační činnost pro uživatele a správce systému

1. V prvním roce platnosti smlouvy bude provedena alikvotní část preventivních prohlídek.
2. Termíny preventivních prohlídek a konzultačních návštěv se stanoví vzájemnou dohodou, s přihlédnutím k jejich rovnoměrnému rozložení v průběhu kalendářního roku a vycházejí z požadavků objednatele.
3. Preventivní prohlídky jsou realizovány vzdálenou správou nebo návštěvami pracovníků poskytovatele na pracovišti objednatele. O způsobu provedení rozhoduje poskytovatel.
4. Konzultační návštěvy jsou realizovány návštěvami pracovníků poskytovatele na pracovišti objednatele.
5. Jednotlivé konzultační návštěvy jsou zaměřeny vždy na konkrétní oblast. Maximální rozsah konzultační návštěvy je jeden člověkoden (tj. 8 hodin běžné pracovní doby). Do této doby je zahrnuta příprava poskytovatele na provedení konzultační návštěvy, samotné provedení návštěvy a následné zpracování výsledků návštěvy formou protokolu.
6. Konzultační návštěvy slouží dle požadavků objednavatele ke konzultacím, ke školení uživatelů při rutinním provozu na pracovišti objednatele, k nastavení a konfiguraci systému (zejména u nových nebo dosud nevyužívaných funkcí systému), ke sledování využití aplikačního software a vypracování návrhů na jeho zlepšení.
7. O provedení preventivní prohlídky a konzultační návštěvy bude pracovníkem poskytovatele sepsán protokol.
8. Preventivní prohlídky zahrnují především kontrolu konfigurace a nastavení ASW včetně DB prostředí, kontrolu platnosti a aktuálnosti číselníků, kontrolu výstupů, kontrolu metodických postupů používání ASW a využívání možností funkcionality ASW uživateli, včetně nastavení přístupových práv.

7.4.1 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 [redacted] ato 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 čísl[redacted]

7.4.2 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.

7.4.3 Kategorizace dostupnosti dle jednotlivých pracovišť objednatele

Aplikace	Dostupnost	Pracoviště
FONS Openlims	A1	statimové pracoviště ÚLBLD *
FONS Openlims	A1	statimové pracoviště CHL *
FONS Openlims	A2	ostatní pracoviště, systém jako celek, celá nemocnice
FONS Openlims FTO	A2	ostatní pracoviště , systém jako celek, celá nemocnice, všechny areály

* Pracoviště má samostatný aktualizovaný server s ASW pro nouzový provoz umístěný přímo v laboratoři. ASW pro nouzový provoz spouští pracovníci laboratoře.

7.4.4 Definice kategorií dostupnosti

Kód	Varianta	Max. doba spuštění náhradního řešení	Celková max. doba neplánovaného výpadku za kalendářní měsíc	Max. doba jedné plánované servisní odstávky	Max. doba plánovaných i neplánovaných odstávek ročně	Dostupnost [%]
A1	Nepřetržitá kritická	10 minut bez uložených dat	8 hodin	24 hodin mimo *	72 hodin	99,18%
			4 hodiny **	2 hodiny v *	12 hodin **	99,73% **
A2	Nepřetržitá významná	120 minut	8 hodin	24 hodin mimo *	72 hodin	99,18%
			4 hodiny **	2 hodiny v *	12 hodin **	99,73%**

* V pracovní době, tedy v pracovní dny 7:00-16:00.

** Maximální možná souběžná nefunkčnost základního i náhradního řešení bez uložených dat při odstraňování poruchy vyžadující obnovu dat ze záložního archivu s on-line dostupným archivem dat (replika DB, záloha na rychlých discích, ne pásková knihovna)

Ze zajištění dostupnosti jsou vyjmuty případy, kdy se aktualizuje / mění aplikační software a technické prostředky z důvodů inovace (plánované akce).

Dostupnost aplikace je stav, kdy uživatel může využívat sjednané služby nutné pro zajištění jeho pracovní činnosti.

7.4.5 Definice SLA pro kategorii dostupnosti

Provoz řešení je v režimu 24x7 při roční dostupnosti dle definované kategorie dostupnosti (viz kap 7.4.4 tohoto dokumentu) garantovaná podpora je uvedena v následující tabulce podle příslušné úrovně SLA.

Kategorie incidentu	Příjem hlášení	Reakční doba (doba od nahlášení do zahájení řešení)	Maximální doba od nahlášení do odstranění závady

Havárie	Nepřetržitě Hotline - 24 x 7 Vyhrazený GSM nebo HelpDesk – 9 x 5 (pracovní dny 07:00 – 16:00)	Neprodleně po přijetí oznámení	Nejpozději do 90 minut po přijetí oznámení
Závada		Nejpozději do 24 hodin po přijetí oznámení	Nejpozději do 72 hodin po přijetí oznámení
Chyba	HelpDesk – 9 x 5 (pracovní dny 07:00 – 16:00)	Nejpozději následující pracovní den po přijetí oznámení	Do 70 kalendářních dnů

Do doby na odstranění závady se nezapočítává doba, po kterou jsou dodávány doplňující či upřesňující informace nutné pro řešení nebo poskytována jiná součinnost (např. záloha dat)..

Odstávky systému je nezbytné plánovat s odpovědnými pracovníky objednatele. Maximální doba neplánované odstávky jsou 2 hodiny. Neplánovaná odstávka SW řešení musí být schválená objednatelem. Není omezeno počtem odpracovaných hodin. Maximální doba na odstranění závady se počítá od okamžiku zadání hlášení závady do helpdesku nebo telefonického nahlášení na určené kontakty poskytovatele, se zajištěním zpětné vazby o jejím přijetí.

7.4.6 Definice kategorie incidentu

Definice - klasifikace incidentu		
Kategorie incidentu	**Závažnost incidentu**	**Příklad**
Havárie **- přerušení provozu**	Služba aplikačního sw jako celku, jeho funkce nejsou pro uživatele dostupné a nelze pokračovat v užívání ASW. Celková ztráta funkcionality ASW, kdy není k dispozici žádné dočasné řešení problému.	Havárie db serveru. Nedostupný příjem pacientů. Nedostupné zadávání výsledků v LIS. Nefunkční komunikace s hlavním analyzátorem.
Závada **- významné omezení provozu**	Služba ASW nebo kritické funkce ASW jsou pro uživatele významně omezeny, problém způsobuje závažnou ztrátu služeb ASW. V používání ASW lze pokračovat pouze omezeně, některé z klíčových funkcionalit nelze použít. Není k dispozici žádné přijatelné náhradní řešení.	Významné (hromadné) chyby ve vykázaných dávkách. Nefunkční zálohování. Časté narušování denního souboru LIS a nutnost jeho obnovování. Neúměrně dlouhá doba odezvy ASW.
Chyba **– menší omezení provozu**	Služba ASW nebo kritické funkce ASW jsou pro uživatele dostupné, problém způsobuje omezení služeb ASW. V používání ASW lze pokračovat. Není ohroženo používání služby ASW pro uživatele.	Nefunkční tisk na jednom pracovišti. Nefunkční kontrola podmínek pořizování dokladů – výkazů pro pojišťovnu. Nesprávná konfigurace provozu pracoviště.

Řešení chyb a provozních problémů není omezeno počtem hodin / měsíc.

7.5 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 96 MD za čtyři roky plnění.

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.

7.6 Reporting

Poskytovatel se zavazuje poskytovat objednateli reporting poskytnutých služeb a to tak, že report bude rozdělen na:

- Vyřešené závady a závady v řešení,
- vyřešené požadavky a požadavky vřešení,
- soupis poskytnutých a poskytovaných služeb spojených suživatelskou podporou,
- soupis poskytnutých a poskytovaných služeb na vyžádání, tzn. nad rámec předmětu plnění této smlouvy,
- přehled splněných a nesplněných SLA.

Tento report se dodavatel zavazuje poskytovat objednateli jednou měsíčně vždy za uplynulý měsíc, kposlednímu dni v měsíci. Reporting může být nahrazen on-line přístupem objednatele do HelpDesku dodavatele, pokud jsou požadované informace uvedeny u jednotlivých záznamů nebo takový reporting aplikace HelpDesku umožňuje on-line.

7.7 Exitová součinnost

Poskytovatel za účelem řádného exportu všech dat SW řešení při ukončení účinnosti smlouvy garantuje především tyto součinnosti:

- Poskytne náležitou a nezbytnou součinnost pro export a předání dat ASW,
- poskytne veškeré nezbytné informace a dokumentaci k exportu dat ASW,
- Data ASW ve stávajícím formátu budou objednateli předána bezúplatně, pokud bude objednatel požadovat jiný formát dat, mohou být práce související s převodem dat ASW do požadovaného formátu zpoplatněny,
- Na žádost objednatele provede poskytovatel protokolární likvidaci dat ASW a provozních údajů souvisejících s poskytováním údržby SW řešení a tímto zanikne možnost vedení jakéhokoliv i budoucího sporu.

Příloha č. 2 – Položkový ceník_cenová kalkulace

Podpora laboratorního systému FONS OpenLIMS									
Předmět plnění	Množství	Jednotka	Povinný dodavatel		Dodavatel		Cena celkem		
			bez DPH	s DPH	bez DPH	s DPH	bez DPH	DPH	s DPH
Podpora provozu stávajícího SW řešení s 620 PC stanic a služby dalšího rozvoje na vyžádání									
Údržba SW řešení	1	měsíc	277 850 Kč	336 198,50 Kč	27 785,00 Kč	33 619,85 Kč	305 635,00 Kč	64 183,35 Kč	369 818,35 Kč
	48	měsíců	13 336 800 Kč	16 137 528,00 Kč	1 333 680,00 Kč	1 613 752,80 Kč	14 670 480,00 Kč	3 080 800,80 Kč	17 751 280,80 Kč
Uživatelská podpora	1	měsíců	223 335 Kč	270 235,35 Kč	335 832,00 Kč	406 356,72 Kč	559 167,00 Kč	117 425,07 Kč	676 592,07 Kč
	48	měsíců	10 720 080 Kč	12 971 296,80 Kč	16 119 936,00 Kč	19 505 122,56 Kč	26 840 016,00 Kč	5 636 403,36 Kč	32 476 419,36 Kč
Systémová podpora	1	měsíc	114 020 Kč	137 964,20 Kč	85 515,00 Kč	103 473,15 Kč	199 535,00 Kč	41 902,35 Kč	241 437,35 Kč
	48	měsíců	5 472 960 Kč	6 622 281,60 Kč	4 104 720,00 Kč	4 966 711,20 Kč	9 577 680,00 Kč	2 011 312,80 Kč	11 588 992,80 Kč
Služby dalšího rozvoje na vyžádání	1	MD (Manday)	10 880 Kč	13 164,80 Kč	4 960,00 Kč	6 001,60 Kč	15 840,00 Kč	3 326,40 Kč	19 166,40 Kč
	96	MD (Manday)	1 044 480 Kč	1 263 820,80 Kč	476 160,00 Kč	576 153,60 Kč	1 520 640,00 Kč	319 334,40 Kč	1 839 974,40 Kč
Cena celkem za podporu provozu a služby dalšího rozvoje na vyžádání	**48**	**měsíců**	**30 574 320 Kč**	**36 994 927,20 Kč**	**22 034 496,00 Kč**	**26 661 740,16 Kč**	**52 608 816,00 Kč**	**11 047 851,36 Kč**	**63 656 667,36 Kč**
CELKOVÁ NABÍDKOVÁ CENA ZA CELÝ PŘEDMĚT PLNĚNÍ POLOŽKA A + SLUŽBY NA VYŽÁDÁNÍ*							**52 608 816,00 Kč**	**11 047 851,36 Kč**	**63 656 667,36 Kč**

Přehled navýšení měsíční ceny za služby podpory provozu pro každých 10 PC stanic	Množství	Jednotka	Povinný dodavatel		Dodavatel		Cena celkem		
			bez DPH	s DPH	bez DPH	s DPH	bez DPH	DPH	s DPH
Údržba SW řešení	1	měsíc	15 000,00 Kč	18 150,00 Kč	100,00 Kč	121,00 Kč	15 100,00 Kč	3 171,00 Kč	18 271,00 Kč
Uživatelská podpora	1	měsíc	3 649,00 Kč	4 415,29 Kč	400,00 Kč	484,00 Kč	4 049,00 Kč	850,29 Kč	4 899,29 Kč
Systémová podpora	1	měsíc	1 863,00 Kč	2 254,23 Kč	200,00 Kč	242,00 Kč	2 063,00 Kč	433,23 Kč	2 496,23 Kč

Příloha č. 3 Smlouvy – Seznam oprávněných osob

A. Seznam kontaktních osob poskytovatele oprávněných poskytovat podporu

Jméno	**Funkce**	**Telefonní číslo**
xxxxx	Manažer podpory	xxxxx
xxxxx	Vedoucí oddělení HD	xxxxx

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

Jméno	**Funkce**	**Telefonní číslo**
Hlášení požadavků na poskytování podpory je přes Service Desk objednatele: Help Desk Ivanti		
xxxxx	Vedoucí odboru vývoje a správy SW	xxxxx
Dispečink	Dispečink Úseku informatiky	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
Úsek informatiky a digitální transformace |
U Nemocnice 499/2, 128 08 Praha 2 | www.vfn.cz, http://intranet.vfn.cz

POUŽÍVÁNÍ SÍTĚ VFN EXTERNÍMI UŽIVATELI

Obsah

Dokument je nově vytvořen, změny nejsou vyznačeny.

Zpracovatel:	**Účinnost dokumentu od:**	**Schválil:**
[redacted]	1.8.2025	[redacted]
Garant:	**První vydání dne:**	**Dne:**
Vedoucí odboru provozu IT	1.1.2008	1.8.2025

Dokument zobrazený na intranetu VFN je řízen správcem dokumentace pracoviště.
Po vytištění slouží pouze pro informativní účely – nepodléhá pravidlům řízení dokumentace.

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

POUŽÍVÁNÍ SÍTĚ VFN EXTERNÍMI UŽIVATELI

1 Účel a oblast platnosti dokumentu

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

2 Pojmy a zkratky

AD	Active Directory
Externí uživatel	Osoba využívající prostředky IT 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
OPIT	Odbor provozu IT
	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.

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

POUŽÍVÁNÍ SÍTĚ VFN EXTERNÍMI UŽIVATELI

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 OPIT v následujících krocích:

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

Požadavek dále zpracuje pracovník správy serverů OPIT 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 OPIT, 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
- od 16:00 do 7:00 na Pohotovost ÚI na t

O víkendu a svátcích na Pohotovost ÚI na tel. +

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

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 provozu IT 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)

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 používámí 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:
  E-mail: [redacted]

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]

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

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

1 Účel

Účelem toho dokumentu je stanovit požadavky vyplývající ze systému řízení bezpečnosti informací ve VFN pro Dodavatele jako provozovatele, Poskytovatele služeb nebo zajišťující podporu základních služeb: zdravotních služeb dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen ZKB) jak vyplývá z přechodných ustanovení zákona č. 264/2025 Sb. (nový 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, normy 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,
- zákon č. 264/2025 Sb., o kybernetické bezpečnosti a vyhlášku č. 408/2025 Sb. o regulovaných službách a předpisy souvisejícími,
- 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,
- směrnice EU č. 2022/2555 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)
- 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.