SMLOUVA O POSKYTOVÁNÍ SW ŘEŠENÍ A SLUŽEB PODPORY

MedText s.r.o
zapsaná v obchodním rejstříku vedenému Městského soudu v Praze, sp. zn. C 339607
se sídlem: U michelského mlýna 380/4, Michle, 140 00 Praha 4
IČO: 096 45 284 DIČ: CZ09645284
zastoupena: Ing. Bc. Lukášem Buškem, MBA, jednatelem
bankovní spojení: Komerční Banka a.s
číslo účtu: 123-2795130237/0100

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

a

Všeobecná fakultní nemocnice v Praze
se sídlem: U Nemocnice 499/2, 128 08 Praha 2
IČO: 000 64 165 DIČ: CZ00064165
zastoupená: doc. MUDr. Jánem Dudrou, PhD., MPH, ředitelem
bankovní spojení: ČNB
číslo účtu: 24035021/0710

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

Poskytovatel a objednatel společně též jako „smluvní strany"

uzavírají dnešního dne na základě výsledků veřejné zakázky malého rozsahu s názvem **„Zabezpečená komunikační platforma",** vyhlášené poptávkovým (výběrovým) řízením v otevřené výzvě dle § 6 a § 31 zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „z. č. 134/2016 Sb."), ID veřejné zakázky dle profilu zadavatele: VZ0237827 (dále jen „veřejná zakázka"), v souladu s ustanovením § 1746 odst. 2, § 2079 a násl. a § 2586 a násl. č. 89/2012 Sb., občanský zákoník, v platném znění (dále jen „zákon č. 89/2012 Sb."), tuto

smlouvu o poskytování SW řešení a služeb podpory

(dále jen „smlouva")

Preambule:

Služby budou do data 30.6.2028 pořizovány v rámci projektu „Implementace systému přednemocniční extrakorporální kardiopulmonální resuscitace pro zajištění dostupnosti vysoce specializované péče o pacienty se srdeční zástavou" (dále jen "dotační projekt"). Dotační projekt je spolufinancován Evropskou unií z Operačního programu Zaměstnanost plus. Služby budou po tomto výše uvedeném datu plně hrazeny z vlastních zdrojů objednatele.

I. Předmět plnění

1. Předmětem plnění této smlouvy je závazek poskytovatele poskytovat objednateli po dobu platnosti této smlouvy multilicenci pro neomezený počet uživatelů objednatele k SW řešení pro zabezpečenou a rychlou komunikaci pro předávání informací mezi VFN a organizacemi zdravotnické záchranné služby (dále také „ZZS") a jinými zdravotnickými organizacemi (dále také „ZZ") (externí komunikace) a mezi jednotlivými zaměstnanci a týmy uvnitř VFN (interní komunikace) MedText (dále jen „SW řešení" nebo „systém"), které je popsáno v příloze č. 1 smlouvy. Bližší specifikace předmětu plnění je uvedena v příloze č. 2 smlouvy.
2. V rámci předmětu plnění bude provedena implementace SW řešení dle bodu 8 přílohy č. 2 smlouvy v rámci které poskytovatel:
   a) zpracuje předimplementační analýzu,
   b) provede implementaci SW řešení,
   c) proškolí určené pracovníky objednatele v rozsahu kompletní dokumentace k SW řešení včetně e-learningu uživatelů objednatele v rozsahu 138 hodin,
   d) ověří kvalitu všech dodávek před jejich předáním objednateli, a to provedením funkčního testu (FAT) a uživatelského akceptačního testu (UAT).
3. Poskytnutí licence, implementace a uvedení poskytovaného SW řešení do ostrého provozu a akceptování celého řešení bez závažných výhrad pro uživatelské použití musí být provedeno nejpozději do 14 kalendářních dnů ode dne účinnosti smlouvy.
4. Poskytovatel se zavazuje poskytovat podporu SW řešení k zajišťování komplexní funkčnosti SW řešení po celou dobu trvání smlouvy, jejíž bližší specifikace je popsána v bodě č. 9 přílohy č. 2 smlouvy.
5. Objednatel se zavazuje zaplatit odměnu za poskytnutí předmětu plnění dle tohoto článku v souladu s podmínkami sjednanými touto smlouvou.
6. Veškerá data uložená nebo ukládaná objednatelem do systému jsou výhradním vlastnictvím objednatele.

II. Způsob poskytování podpory software

1. Bližší specifikace poskytování podpory je popsána v bodě 9 přílohy č. 2 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 poskytování předmětu plnění dle čl. I. a přílohy č. 1 a 2 (vyjma bodu 9.4 přílohy č. 2 smlouvy) této smlouvy je stanovena ve výši **217 900,- Kč bez DPH** za poskytování SW řešení v délce 1 rok.

2. Cena služeb na vyžádání dle bodu č. 9.4 přílohy č. 2 této smlouvy je stanovena dohodou smluvních stran na částku **1 800,-** 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 ročních platbách. Dnem uskutečnění zdanitelného plnění pro první rok plnění dle smlouvy bude den finální akceptace implementace SW řešení, tzn. den podpisu akceptačního protokolu objednatelem. Dnem uskutečnění zdanitelného plnění pro následující období bude vždy první kalendářní den následujícího příslušného roku plnění. Přílohou první faktury za první rok plnění dle smlouvy bude akceptační protokol potvrzující řádnou implementaci SW řešení, který bude podepsán oběma smluvními stranami.
4. Cena za služby na vyžádání dle čl. III. odst. 2 této smlouvy bude objednatelem hrazena po akceptaci každé jednotlivé realizace na základě objednávky. Přílohou jednotlivé faktury za jednotlivou realizaci služeb na vyžádání bude akceptační protokol příslušné fakturované realizace, který bude podepsán oběma smluvními stranami.
5. Ceny dle čl. III. této smlouvy budou hrazeny na základě faktur – daňových dokladů (dále jen „**faktura**") vystavených poskytovatelem, přičemž tyto musí obsahovat všechny údaje uvedené v § 29 odst. 1 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a dále též dle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů.
6. Poskytovatel se touto smlouvou zavazuje, že jím vystavená faktura bude obsahovat všechny náležitosti řádného daňového dokladu dle platné právní úpravy.
7. Splatnost faktury činí 60 dní ode dne doručení faktury objednateli. Faktura bude zaslána elektronicky ve formátu PDF na e-mailovou adresu: faktury@vfn.cz
8. Při fakturaci vztahující se k plnění do data 30.6.2028 musí být na faktuře uvedeny název a číslo dotačního projektu, tj. „Implementace systému přednemocniční extrakorporální kardiopulmonální resuscitace pro zajištění dostupnosti vysoce specializované péče o pacienty se srdeční zástavou", reg. č. CZ.03.02.02/00/25_102/0005580.
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. 7 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 1.1.2029. 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. Dodací podmínky

1. Kontaktní osobou a odpovědným zaměstnancem objednatele je pro účely této smlouvy určen vedoucí Odboru vývoje a správy SW, tel: xxxxx, e-mail: xxxxx. Kontaktní osobou poskytovatele je pro účely této smlouvy určen: xxxxx, tel: xxxxx, e-mail: xxxxx.
2. SW řešení bude objednateli poskytováno výhradně s využitím hardwarových prostředků objednatele Implementace SW řešení dle čl. I. odst. 2 smlouvy se považuje podle této smlouvy za splněnou, pokud byl předmět plnění řádně realizován způsobem sjednaným níže.
3. O řádné implementaci předmětu plnění dle čl. I. odst. 2 smlouvy bude sepsán akceptační protokol, který podepíší obě smluvní strany. Podpisem akceptačního protokolu dochází k předání části předmětu plnění poskytovatelem objednateli.
4. Objednatel není povinen akceptovat realizaci části předmětu plnění v případě, že předmět plnění bude vykazovat vady a nedodělky. Pokud vada nebo nedodělek nebrání převzetí předmětu plnění smlouvy, musí být vždy uveden v akceptačním protokolu s uvedením data odstranění. Nebude-li objednatelem akceptováno předání a převzetí předmětu plnění z důvodů vad a nedodělků, bude o této skutečnosti sepsán zápis s výčtem zjištěných vad nebo nedodělků, které zjistil objednatel, a to včetně způsobu a lhůt k jejich odstranění. Tento zápis bude současně podepsán zástupci obou smluvních stran.
5. Veškeré činnosti při aplikaci softwarového řešení je poskytovatel povinen provádět osobami, které mají odpovídající kvalifikaci.

V. 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 od prvního dne měsíce následujícího po doručení písemné výpovědi druhé smluvní straně,
   - 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 překračující o 90 dnů termín splatnosti.
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 odstoupení od smlouvy není dotčen nárok objednatele na náhradu škody vzniklé porušením podmínek této smlouvy, ani nárok na zaplacení smluvní pokuty.

VI. Závazky objednatele

1. Objednatel se zavazuje zaplatit poskytovateli dohodnuté ceny za služby poskytnuté dle této smlouvy.
2. Objednatel se zavazuje, že umožní poskytovateli poskytování podpory SW řešení vzdáleným přístupem.
3. Objednatel se zavazuje zajistit poskytovateli jím požadované potřebné informace věcného i systémového charakteru pro řádné 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 Hot-line (Helpdesk) závažnost dle podmínek specifikovaných v bodě 9.3.2 přílohy č. 2 této smlouvy.

VII. Závazky poskytovatele

1. Poskytovatel se zavazuje plnit své povinnosti vyplývající z této smlouvy s maximální odpovědností tak, aby systém byl udržován nepřetržitě v provozuschopném, funkčním stavu, který je řádně zdokumentován. Poskytovatel je povinen zajistit nepřetržitý přístup k datům objednatele uložených v systému. Poskytovatel odpovídá za kvalitu a včasnost vykonaných prací ve smyslu výše uvedených ustanovení.
2. Poskytovatel zavede relevantní bezpečnostní, technická a organizační opatření, která zajistí podporu SW řešení včetně všech jeho vývojových úprav při dodržení důvěrnosti, integrity a dostupnosti SW řešení.
3. 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.
4. Poskytovatel je povinen identifikovat a odstraňovat technické zranitelnosti spojené s bezpečnostním nastavením nebo fungováním jím provozovaných/spravovaných zařízení nebo systémů. Odstranění uvedených zranitelností se vztahuje i na zranitelnosti identifikované výrobcem, NÚKIB, objednatelem nebo zveřejněné v mezinárodní databázi zranitelností (např. NIST - https://nvd.nist.gov/, CISA - https://www.cisa.gov/news-events/cybersecurity-advisories).
5. Poskytovatel je povinen neprodleně informovat objednatele prostřednictvím poskytovatelem určené odpovědné osoby: Manažera kybernetické bezpečnosti, e-mail: ManazerKB@vfn.cz, o kybernetických bezpečnostních incidentech souvisejících s poskytováním předmětu plnění.
6. Poskytovatel je povinen systém zabezpečit tak, aby nedošlo k přihlášení osoby, která nemá příslušné oprávnění, do systému. Za jakékoli škody, s výjimkou fyzického zabezpečení serverů, způsobené objednateli zásahem neoprávněně přihlášené osoby odpovídá poskytovatel.
7. Poskytovatel je odpovědný za škodu, která objednateli vznikne prokazatelným neplněním nebo vadným plněním jeho závazků vyplývajících z této smlouvy.
8. 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 požadovaných potřebných informací specifikuje objednateli poskytovatel, a to po nahlášení nebo potvrzení přijetí požadavku.
9. V případě ukončení této smlouvy je poskytovatel povinen bezplatně předat veškerá data v systému za dobu poskytování služby. Poskytovatel musí data předat ve strukturované podobě (xml, sql, csv, json) za požadované období tak, aby byl možný import do následnického systému objednatele. O ukončení služby a předání dat bude sepsán předávací protokol.
10. V případě ukončení této smlouvy je poskytovatel povinen poskytnout objednateli nezbytně nutnou součinnost při převodu dat objednatele do nového systému.
11. Poskytovatel dále prohlašuje, že je plně oprávněn nakládat s díly svých zaměstnanců a spolupracujících osob, která jsou využita při plnění smlouvy.
12. Minimálně do konce roku 2038 je poskytovatel povinen poskytovat požadované informace a dokumentaci související s plněním služeb v období do 30.6.2028 objednateli, zaměstnancům nebo zmocněncům pověřených orgánů (MPSV, MZ ČR, MMR ČR, MF ČR, Evropská komise, Evropský účetní dvůr, Nejvyšší kontrolní úřad, příslušné orgány finanční správy a další oprávněné orgány veřejné správy), a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci zakázky, poskytnout jim při provádění kontroly součinnost a být fyzicky přítomen kontrolám v místě plnění.

VIII. Smluvní pokuty, sankce

1. Pro případ prodlení objednatele s úhradou ceny dle čl. III. této smlouvy má poskytovatel nárok na zaplacení úroku z prodlení ze strany objednatele ve výši 0,01 % z částky, s jejíž platbou je objednatel v prodlení, za každý den takového prodlení. Smluvní strany se dohodly, že poskytovatel je oprávněn požadovat zaplacení úroku z prodlení až po uplynutí 30 dnů od sjednané lhůty splatnosti.
2. V případě nedodržení termínů uvedených v čl. I. odst. 3 je objednatel oprávněn požadovat jednorázovou smluvní pokutu ve výši 50.000 Kč za nedodržení stanoveného termínu plnění a dále je objednatel oprávněn požadovat smluvní pokutu ve výši 1.000 Kč za každý i započatý den prodlení.
3. V případě nedodržení termínu pro odstranění kritické závady dle bodu 9.3.2 přílohy č. 2 smlouvy je objednatel oprávněn požadovat smluvní pokutu ve výši 5.000,- Kč za každou i započatou hodinu prodlení za každý jednotlivý případ.
4. V případě nedodržení termínu pro odstranění chyby je objednatel oprávněn dle bodu 9.3.2 přílohy č. 2 smlouvy požadovat smluvní pokutu ve výši 1.000,- Kč za každý i započatý pracovní den prodlení za každý jednotlivý případ.
5. Na výše uvedené smluvní pokuty nemá objednatel nárok, prokáže-li se, že kritická závada nebo chyba byla způsobena jednáním objednatele, selháním nebo jinými problémy na straně objednatele.
6. V případě nedodržení některé z povinností poskytovatele stanovených v čl. VII. odst. 12 smlouvy má objednatel právo účtovat prodávajícímu smluvní pokutu ve výši sankce uložené objednateli Řídicím orgánem Operačního programu Zaměstnanost Plus za nedodržení povinností stanovených v Rozhodnutí o poskytnutí dotace nebo ve výši zkrácení dotace z téhož důvodu.
7. V případě nedodržení povinností dle čl. VII. odst. 2.- 6., IX. a X. odst. 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 povinnosti stanovené v čl. XI. odst. 3 smlouvy má objednatel právo účtovat smluvní pokutu ve výši pohledávky, která byla postoupena v rozporu s touto smlouvu. Objednatel má zároveň právo odstoupit od smlouvy.
9. 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.
10. Smluvní pokuta bude vyúčtovaná samostatným daňovým dokladem, splatnost smluvní pokuty činí 30 dní ode dne doručení vyúčtování Poskytovateli.
11. Zaplacením smluvní pokuty není dotčen nárok objednatele na náhradu škody, včetně náhrady škody, která převyšuje smluvní pokutu.

IX. Mlčenlivost

1. Poskytovatel se zavazuje zachovávat mlčenlivost ve vztahu ke všem informacím a skutečnostem, které se dozví o objednateli, jeho zaměstnancích, pacientech atd. v souvislosti s uzavřením a plněním smlouvy, pokud tyto informace mají povahu obchodního tajemství, osobních údajů nebo mají být z jiných důvodů chráněny před zveřejněním. Poskytovatel je povinen nakládat s osobními údaji a zejména s údaji o zdravotním stavu,

genetickými a biometrickými údaji (dále jen „Osobní údaje") v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 (dále jen GDPR) a příslušnými ustanoveními zákona č. 110/2019 Sb., o zpracování osobních údajů.

2. Povinnost mlčenlivosti platí rovněž o skutečnostech, na něž se vztahuje povinnost mlčenlivosti zdravotnických pracovníků, zejména podle ustanovení § 51 zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (Zákon o zdravotních službách), a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení Osobních údajů.
3. Pokud poskytovatel přijde při plnění smlouvy do styku s Osobními údaji a bude v postavení zpracovatele ve smyslu GDPR a Zákona o zpracování osobních údajů, zavazuje se nakládat s Osobními údaji pouze za účelem splnění závazků z této smlouvy a žádným jiným způsobem, a to v souladu příslušnými ustanoveními GDPR a Zákona o zpracování osobních údajů v rozsahu nezbytném pro plnění smlouvy a po dobu nezbytnou k plnění smlouvy. Zpracovávání Osobních údajů v rozsahu údajů poskytnutých objednatelem a týkajících se zdravotnické dokumentace pacientů, jimž jsou objednatelem poskytovány zdravotní služby, a dále v rozsahu Osobních údajů zaměstnanců objednatele poskytovatelem může zahrnovat odstranění potíží za účelem zabránění, vyhledávání a opravy problémů zjištěných při poskytování služeb dle této smlouvy, může také zahrnovat zlepšování funkcí informačních systémů, vyhledávání hrozeb uživatelům a ochrany uživatelů informačních systémů. Osobní údaje nebudou použity k jinému účelu, ani z nich nebudou odvozovány informace pro žádné reklamní či jiné komerční účely. Poskytovatel se zavazuje za účelem ochrany osobních údajů objednatele a jeho pacientů a zaměstnanců před neoprávněným přístupem, použitím, zveřejněním nebo zničením, resp. před jejich náhodnou ztrátou či změnou uplatňovat technická a organizační bezpečnostní opatření, interní kontroly a rutiny zabezpečení osobních údajů zajišťující splnění všech povinností dle GDPR a Zákona o ochraně osobních údajů, zejména zajistit, aby data obsažená ve zdravotnické dokumentaci byla šifrována způsobem, který znemožní nahlížení do těchto údajů neoprávněným osobám.
4. Poskytovatel se zavazuje zajistit informovanost svých pracovníků (včetně poddodavatelů) o povinnostech vyplývajících z této smlouvy. Poskytovatel se zavazuje zajistit, aby jeho pracovníci, kteří budou přicházet do styku s osobními údaji, byli smluvně vázáni povinností mlčenlivosti ve smyslu GDPR a Zákona o zpracování osobních údajů a poučeni o možných následcích porušení těchto povinností s tím, že povinnost důvěrnosti bude jimi dodržována i po skončení jejich smluvního vztahu k objednateli. Toto ujednání je sjednáno ve smyslu ustanovení čl. 28 GDPR. Poskytovatel se zavazuje informovat své poddodavatele o povinnosti mlčenlivosti dle této smlouvy. V případě porušení mlčenlivosti za strany poddodavatele, odpovídá poskytovatel objednateli za vzniklou škodu, jako kdyby povinnost porušil sám.
5. Smluvní strany se zavazují zachovat mlčenlivost též o všech ostatních skutečnostech, ve vztahu, k nimž o to budou druhou stranou písemně požádány. Smluvní strany se též zavazují nevyužít informace podle prvé věty tohoto odstavce ve svůj prospěch nebo ve prospěch třetích osob v rozporu s účelem jejich předání.
6. Smluvní strany jsou povinny zajistit, že nebudou neoprávněně pořizovány kopie informací či jiné záznamy nad rámec plnění dle této smlouvy, a nebudou zjišťovány informace, které nejsou nezbytně nutné ke splnění povinností vyplývajících z této smlouvy.
7. Smluvní strany se zavazují pro případ, že se v průběhu plnění dle této smlouvy dostanou do kontaktu s údaji druhé smluvní strany vyplývajícími z její provozní činnosti, tyto údaje v žádném případě nezneužít, nezměnit ani jinak nepoškodit, neztratit či neznehodnotit.
8. Poskytovatel se zavazuje plně respektovat bezpečnostní požadavky objednatele k zajištění ochrany Osobních údajů pacientů a zaměstnanců Objednatele.
9. Povinnost mlčenlivosti o informacích a skutečnostech obchodního charakteru trvá po dobu 5 let od ukončení této smlouvy, o informacích obsahujících Osobní údaje trvá bez časového omezení.
10. Smluvní strany vylučují povinnosti jim uložené ve smyslu čl. IX., 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**").

X. Ostatní ujednání

1. Poskytovatel bere na vědomí, že objednatel je povinen dle ustanovení § 219 odst. 1 písm. a) zákona č. 134/2016 Sb., o zadávání veřejných zakázek a dle zákona č. 340/2015 Sb., o registru smluv, uveřejnit tuto smlouvu včetně případných dodatků a objednávek vystavených na základě této smlouvy, zákonem stanoveným způsobem.
2. 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.
3. Poskytovatel se zavazuje dodržovat nařízení objednatele, kterým je zakázáno kouření ve všech prostorách i plochách areálu objednatele s výjimkou vyhrazených míst.
4. Obě smluvní strany se zavazují, že v souvislosti s plněním smlouvy učiní opatření k zajištění ochrany před šířením počítačových virů a nelegálních programů.
5. Poskytovatel prohlašuje, že zajištěním podpory systému pro objednatele neporušuje práva třetích osob ve smyslu autorského zákona a že tak činí v souladu s autorským zákonem.
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 5.000.000,- Kč.
7. Poskytovatel je povinen udržovat výše uvedené pojištění po celou dobu trvání smlouvy. V případě porušení této povinnosti je objednatel oprávněn od smlouvy, která bude uzavřena na základě výsledku tohoto zadávacího řízení odstoupit. Na žádost objednatele je poskytovatel povinen předložit objednateli dokumenty prokazující, že pojištění v požadovaném rozsahu a výši trvá. Pokud by v důsledku pojistného plnění nebo jiné události mělo dojít k zániku pojištění, k omezení rozsahu pojištěných rizik, ke snížení stanovené min. výše pojistného plnění, nebo k jiným změnám, které by znamenaly zhoršení podmínek oproti původnímu stavu, je poskytovatel povinen učinit příslušná opatření tak, aby pojištění bylo udrženo tak, jak je požadováno v tomto ustanovení.
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.

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 – Technická a funkční specifikace SW řešení_nabídka
Příloha č. 2 – Specifikace předmětu plnění včetně minimálních technických a funkčních požadavků
Příloha č. 3 – Seznam oprávněných osob
Příloha č. 4 – Používání sítě VFN externími uživateli
Příloha č. 5 – Položkový ceník

V Praze dne dle el. podpisu:

---
doc. MUDr. Ján Dudra, PhD., MPH

ředitel

V Praze dne dle el. podpisu:

Ing. Bc. Lukáš Bušek, MBA

jednatel

schválila:

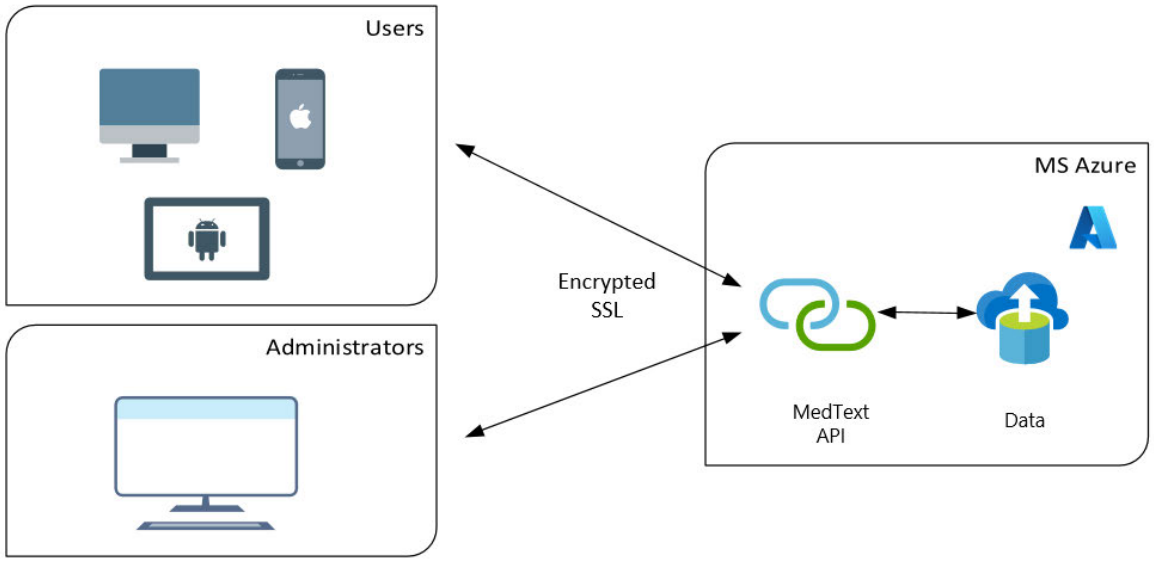
MedText – Technický přehled

1.1 Klíčové body

- **Účel MedTextu:** usnadnit komunikaci v rámci poskytování špičkové zdravotní péče
- **Bezpečná cloudová platforma:** postavená na Microsoft Azure, s dodržováním osvědčených postupů v celém životním cyklu vývoje
- **Zabezpečená platforma:** víceúrovňová bezpečnost, audity třetích stran
- **Spolehlivost a škálovatelnost:** redundance napříč několika Azure Availability Zones, horizontální i vertikální škálování

1.2 Architektura

- Mobilní aplikace pro iOS a Android (App Store, Google Play) a Windows tlustý klient
- Webová aplikace hostované MedTextem, běžící v moderních prohlížečích
- Platforma a API na infrastruktuře MS Azure
- Přístup přes HTTPS a SignalR pro API a ukládání dat



1.3 Firemní a vývojové postupy

- Dokumentované a vynucované politiky ochrany soukromí, bezpečnosti a řízení rizik
- Pravidelné měření a řízení procesů
- Prověrky zaměstnanců a každoroční školení o ochraně soukromí a bezpečnosti
- Bezpečný životní cyklus vývoje se striktní správou změn
- Certifikace:
    - ISO/IEC 9001
    - ISO/IEC 27001
    - ISO/IEC 27701
    - Cyber Essentials

1.4 Ochrana citlivých informací

1.4.1 Zabezpečení mobilních zařízení

- Žádná data nejsou trvale uložena po vypršení retenční doby
- Veškerá komunikace je šifrovaná
- Ochrana proti MITM útokům pomocí JWT tokenů
- Zamezení snímání obrazovky (Android), logování (iOS)
- Hesla dle OWASP
- Volitelné: federované přihlášení (OpenID Connect), MDM, zámek zařízení

1.4.2 Cloud a síť

- Datová centra MS Azure v souladu s GDPR
- Všechny služby jsou defaultně zakázané, povolují se jen nutné
- Porty jsou uzamčené
- Pravidelné bezpečnostní aktualizace
- Přístup pouze z IP MedTextu (VPN, firewall, klíče)
- Antivirus, HIDS
- Monitoring v Azure
- Ochrana proti DDoS

1.4.3 Šifrování a soukromí

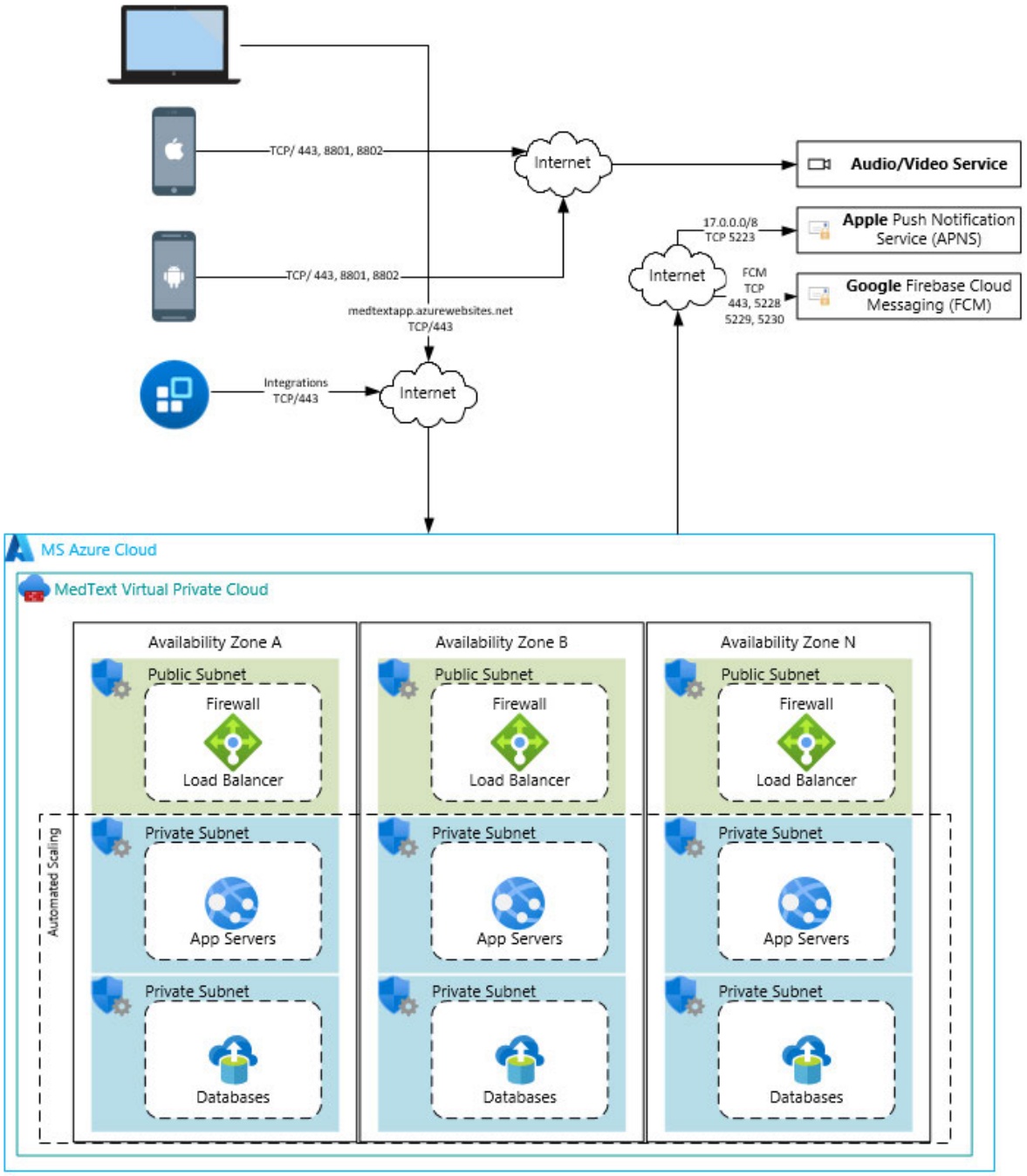
- Šifrování dat při přenosu i uložení
- TLS 1.2, SHA-256, 2048bit klíče
- Interní komunikace přes HTTPS
- Šifrování databází:
    - Sloupce: AES 128
    - Disky: AES 256
    - Zálohy: AES 256

1.4.4 Obnova po havárii

- Více Availability Zones s automatickým přepnutím

1.5 Síťová architektura

- Obecná IP adresa: `*.medtext.eu` přes SSL



1.6 Oddělená prostředí

- Samostatná prostředí pro vývoj, test a produkci
- Každé má vlastní VPC, firewall, load balancer
- Vše spravováno kódem
- Citlivá data existují **pouze v produkci**

1.7 Škálovatelnost a spolehlivost

- Automatické přidávání výpočetních zdrojů

- Redundance ve 3 zónách

1.7.1 Horizontální škálování

- Dynamické navyšování webové vrstvy
- Distribuované fronty
- Klastrovaná databáze

1.7.2 Geografická redundance

- Uzly v různých datových centrech
- Load balancing a automatické přepnutí

1.7.3 DNS Failover

- Klienti vždy naleznou služby
- Ochrana proti DdoS

Popis funkcionalit řešení MedText
1. Informační systém, který umožňuje pomocí svých aplikací implementovat klienty na zařízeních využívající operační systém Windows, iOS a Android (stolní počítače, tablety, mobilní telefony) a zároveň jsou tyto aplikace nativními pro daný operační systém.
2. Systém umožňuje komunikaci mezi dvěma nebo více uživateli či subjekty, a to pomocí následujících modalit: o Chat s možností prioritizace zpráv o Fotografie o Video o Audio/Video hovor s možností nahrávání o Poloha (jak statická, tak dynamická) Uživatelé mohou do vlákna přidávat další uživatele pomocí výběru jednotlivých uživatelů nebo týmů zahrnujících více uživatelů. Data pro nově přidané uživatele musí být k dispozici v nezměněné podobě, tedy i historické, tedy uživatelům přidaným do skupinové komunikace se zobrazuje celá historie chatu
3. Systém umožňuje sdílení polohy uživatele s mapovým náhledem a zobrazením vzdálenosti s reálno-časovou aktualizací.
4. Dynamické Formuláře o Systém umožňuje tvorbu uživatelských formulářů implementovaných do komunikačního vlákna, které jsou uživatelům nabízeny řízeně dle uživatelských práv administrovaných administrátorem. o Formuláře umožňují multimodální zadávání dat: textový vstup, výběr z číselníku, numerické pole, výběr data a času, skenování čárových a QR kódů. o Formuláře umožňují nastavení závislosti zobrazení a výběru dat v závislosti na jiném poli daného formuláře, či jiné proměnné o Formulář může být opakovaně editován o Dodavatel v rámci dodávky spolu s dodávaným systémem dodá i nástroj pro úpravu formátu formuláře
5. Implementace protokolů (workflow) zákazníka. Příklad: posádka ZZS společně s dispečinkem aktivuje ECMO protokol. ECMO tým organizace je informován push notifikací a zároveň je propojen jak s operačním řízením ZZS, tak i posádkou na místě. ECMO tým může jak manuálně, tak automaticky informovat (pozvat do vlákna) jiné týmy či uživatele v rámci organizace (např. radiologii …). Nově přizvaní účastníci mají k dispozici kompletní historii dané komunikace.

Systém není omezen počtem workflow zákazníka a lze je definovat pro různé případy. Příklad: Při dokumentaci ošetření pacienta je spuštěno dokumentační workflow, kde uživatel je vyzván k zadání dat do formuláře a následně dle typu klinické události musí např pořídit fotodokumentaci ošetření.
6. Informační zprávy Systém umožňuje zasílání a příjem formátovaných jednosměrných zpráv, a to včetně příjmu datasetu přes API systému. Tyto zprávy mohou být formátovány odesílatelem a cílová skupina příjemců může být pevně dána, nebo ji lze generovat dynamicky dle požadavku odesílatele. Zákazník má možnost si administrovat jednotlivé nástěnky ve kterých se tyto info zprávy zobrazují na zařízení přihlášeného uživatele. Například informace o školení jednotlivých uživatelů, důležitých oznámení organizace atd… Infozpráva umožňuje manuální spuštění akce, definované zákazníkem.
7. Další zdroje objednatele Systém v rámci aplikace umožňuje zobrazení dalších informačních zdrojů definované uživatelem – např. interní dokumenty, schválené webové stránky atd.
8. Dodané řešení informačního systému umožní vytváření komunikačních kanálů interně napříč organizací zákazníka.
9. Jednotlivé týmy jsou schopny sdílet komunikační kanál včetně celé historie komunikace s propojenými organizacemi např. ZZS, jíné CPALP
10. Veškerá komunikace (včetně VOIP a videohovorů) je zaznamenávána a nahrávána, zobrazení dat a jejich změny jsou logovány. Objednatel požaduje úroveň logování, kdy záznamy obsahují nejméně tyto informace: kdy, kdo, co, stará hodnota, nová hodnota.
11. Informace v komunikačním kanále je možné sdílet se všemi účastníky pacientského kanálu v rámci dané události = týmem, který je dynamicky měněný dle potřeb komunikace.
12. Systém umožňuje dynamicky budovat „tým“ – tedy účastníky pacientského kanálu z adresáře, který je spravován Objednatelem.
13. Systém umožňuje uživatelsky definovat texty jako rychlé volby, které může uživatel v komunikačním kanálu použít pro zrychlení zadávání dat. Toto nastavení bude spravovat zákazník v rámci správy systému.
14. Pro předdefinované texty je možno definovat typy odpovědí (například výběrem ze seznamu hodnot). Odpovědi bude definovat zákazník v rámci správy systému.
15. Komunikační kanál umožňuje přenos/sdílení textu umožňující formátování (barvy a styl písma), fotodokumentaci, PDF soubory (například EKG).
16. Po ukončení komunikace je možno kompletní komunikační kanál uložit jako přílohu k elektronickému záznamu pacienta (za pomocí integračního API)
17. Notifikace (push notifikace) pro jednotlivé klienty je schopná ignorovat/obejít nastavení mobilního telefonu v režimu „nerušit“ a vynuceně avizovat událost/změnu v komunikaci – tzv. kritické notifikace.
18. Systém obsahuje zabezpečené API pro integraci s aplikacemi třetích stran.
19. Systém a jeho aplikace bude moci užívat neomezený počet uživatelů zákazníka.
20. Správa uživatelských rolí v systému lze plně integrovat se stávajícím systémem správy identit (AD) organizace.
21. Systém umožňuje agregaci dat z uživatelských formulářů v chatech a jejich zpracování v reálném čase do maticové tabulky zobrazované v aplikaci, tato data jsou zobrazována definovaným uživatelům.

22. Systém podporuje uživatelské role, tj. atributy uživatele, které lze upravovat uživatelem v aplikaci i v administraci. Role slouží jako způsob výběru uživatelů jak ad hoc v adresáři, tak v permanentních týmech. Uživatel může mít přiřazeno více rolí najednou.
23. Systém umožňuje odeslání zprávy s aktivním požadavkem na reakci pomocí tlačítek předdefinovaných odpovědí.
24. Pro každého uživatele lze definovat z jakých zařízení může k systému, včetně jeho aplikací, přistupovat. Seznam povolených zařízení je plně řízen pověřeným správcem na straně zákazníka.
25. Veškerá komunikace je šifrována a jsou použity kryptografické algoritmy, dle doporučení NÚKIB

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

PŘÍLOHA Č. 2

SPECIFIKACE PŘEDMĚTU PLNĚNÍ VČETNĚ MINIMÁLNÍCH TECHNICKÝCH A FUNKČNÍCH POŽADAVKŮ

ZABEZPEČENÁ KOMUNIKAČNÍ PLATFORMA

Dokument obsahuje minimální technické a funkční požadavky zadavatele pro pořízení služeb k zabezpečené komunikaci dle GDPR nařízení mezi jednotlivými týmy a jednotlivci ve Všeobecné fakultní nemocnici v Praze (dále také **VFN)** a také i s organizacemi ZZ a ZZS.

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

1 Manažerské shrnutí, základní slovník/zkratky

Účelem projektu je zajištění rychlé a zabezpečené komunikační platformy pro předávání informací v rámci VFN a i s organizacemi Zdravotnické záchranné služby (dále jen **ZZS**) a jinými Zdravotnickými zařízeními (dále jen **ZZ**). Tato komunikace musí zahrnovat jak jednotlivce, tak zdravotnické týmy. Níže uvedené specifikace popisují obecné funkce, procesy, vstupy a výstupy nebo jejich názorné příklady, detailní specifikace + kompletní popisy.

Cílem je:

- Uvedení do provozu službu pro rychlou a zabezpečenou komunikaci dle GDPR
- Vytvoření komunikačních kanálů interně napříč VFN
- Vytvoření komunikačních týmů napříč VFN
- Efektivní komunikace se Zdravotnickou záchrannou službou ještě před příjezdem pacienta do VFN
- Podklady pro reporty a možnost sledování efektivity

Předmětem plnění je:

- Časově omezená užívací práva (multilicence) pro neomezený počet uživatelů zadavatele k SW řešení – zabezpečené komunikační platformě
- Zpracování předimplementační analýzy pro aktivaci služby
- Nastavení komunikační matice pro interní prostředí VFN
- Umožnění zapojení se do ECMO týmu a následnou komunikaci se ZZS
- Zpracování dokumentace a provedení školení včetně e-learningu uživatelů v rozsahu 138 hodin
- Poskytování podpory provozu
- Služby na vyžádání v maximálním rozsahu 96 -MD za období 4 let

Slovník/zkratky:

VFN – Všeobecná fakultní nemocnice v Praze
ZZ – Zdravotnické zařízení
ZZS – Zdravotnická záchranná služba
ECMO – (extrakorporální membránová oxygenace) je pokročilá podpůrná léčebná metoda, která dočasně nahrazuje funkci srdce a plic u pacientů s kritickým selháním těchto orgánů
AD - Active Directory
NIS – Nemocniční informační systém
MD – Člověkoden tj. 8 hodin

2 Popis požadovaného řešení

Předmětem řešení je nákup SW jako služby s okamžitou možností používání pro zabezpečenou a rychlou komunikaci pro předávání informací mezi:

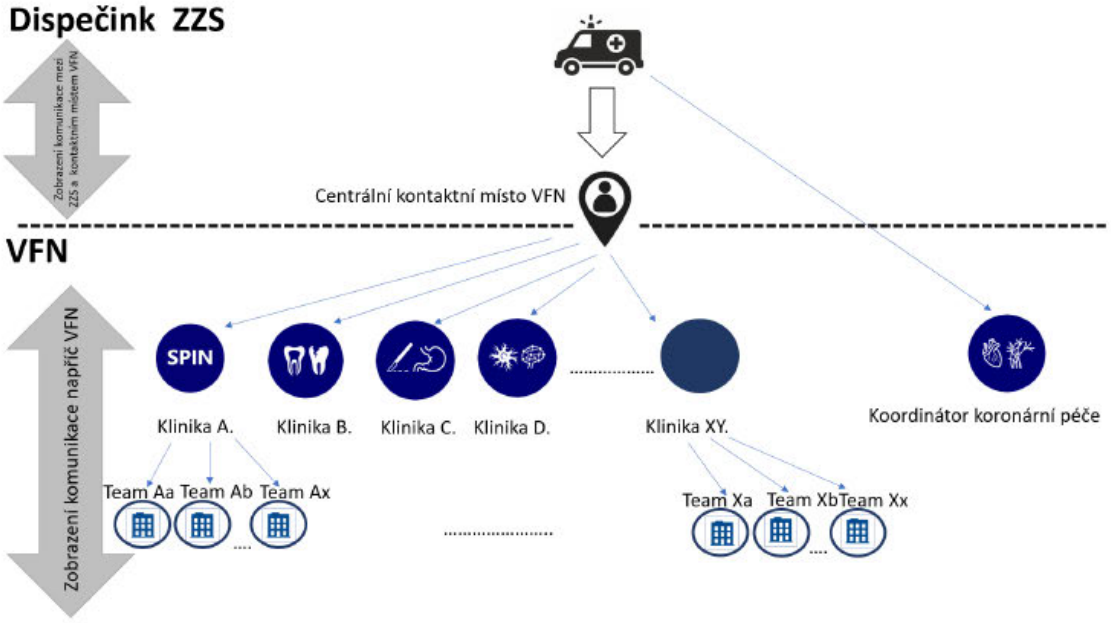
- VFN a ZZS a ZZ (Externí komunikace)
- Jednotlivými zaměstnanci a týmy uvnitř VFN (Interní komunikace)

2.1 VFN a ZZS a ZZ (Externí komunikace)

a. Koordinovaný příjezd složek ZZS s pacientem

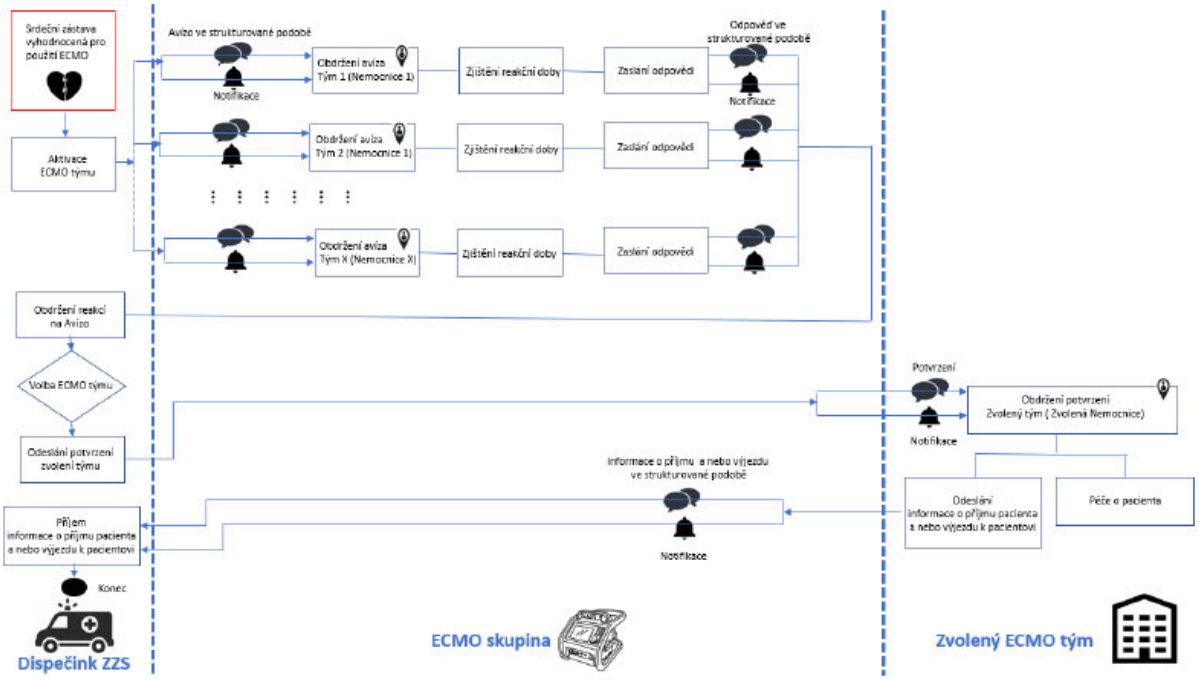
Služba umožní vytvoření interní komunikační matice pro včasné avízo pacienta přiváženého vozy ZZS.

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



b. Zapojení do ECMO týmu

Služba umožní zapojení do ECMO týmu a rychlou reakci na avizované možné pacienty pro léčbu přístrojem ECMO dle následujícího schémata.



2.2 Jednotlivými zaměstnanci a týmy uvnitř VFN (Interní komunikace)

Služba umožní zabezpečenou komunikaci uvnitř VFN a to:

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

- Individuální – umožní komunikaci mezi jednotlivými uživateli služby
- Skupinovou – umožní každému uživateli založení vlastní komunikační skupiny
- Komunitní – umožní každému uživateli komunikaci v rámci předefinovaných skupin ve VFN

3 Funkční požadavky

V kapitole jsou uvedené funkční požadavky na řešení.

Detailní specifikace (např. přesná komunikační schémata, procesní mapy atd.) – na úroveň potřebných detailů bude dodefinováno v rámci předimplementační analýzy.

Obecné funkční požadavky	• Komunikace mezi:
	  ○ Jednotlivci
	  ○ Týmy
	  ○ Celými organizacemi
	• Komunikace mezi osobami a organizačními jednotkami:
	  ○ Ve VFN
	  ○ Mimo VFN
	  ▪ Zdravotnickou záchrannou službu hl. m. Praha
	  ▪ Zdravotnickou záchrannou službu Středočeského kraje
	  ▪ ECMO týmy
	• Synchronní komunikace:
	  ○ Individuální audio/video hovor
	  ○ Skupinový audio/video hovor
	• Asynchronní komunikace
	  ○ Obousměrné textové zprávy
	  ▪ Individuální chat
	  ▪ Skupinový chat
	• Sdílení media formátů
	  ○ Fotodokumentace (JPEG, PNG, TIFF)
	  ○ Video (MP4, MKV, MOV)
	  ○ Audio (MP3, AAC)
	  ○ PDF
	• Klasifikace zpráv
	  ○ Normální
	  ○ Prioritní
	• Zvukové a vizuální upozornění na prioritní zprávy
	• Push notifikace
	• Formátování textu v konverzacích
	  ○ Barva písma
	  ○ Styl písma
	• Dynamické formuláře
	• Předdefinované odpovědi
	• Rychlé volby
	• Neomezený počet zasílaných strukturovaných informací
	• Tvorba eskalačních pravidel
	• Tvorba týmů
	• Komunikační historie i pro přidané účastníky konverzace
	• Sdílení polohy
	• Aktivace ECMO

4 Nefunkční požadavky

V kapitole jsou uvedené nefunkční požadavky na řešení.

4.1 Technologie

Řešení musí být přístupné z následujících platforem: Linux, Android, Windows, iOS.

Dané řešení musí být postaveno na podporovaných technologiích, které mají garantovaný vývojový cyklus minimálně na příštích 5 let. Tyto technologie musí být pravidelně aktualizovány dodavatelem. Jestliže bude řešení realizováno jako webová aplikace, musí podporovat základní webové prohlížeče (MS Edge, Google Chrome, Mozilla Firefox, Opera) a zároveň být responzivní pro mobilní zařízení a různá rozlišení obrazovek.

Řešení může být instalováno i jako tlustý klient na lokální stanice s Windows 11 spolu s instalovatelnou mobilní aplikací skrze interní nástroj Intune.

4.2 Řízení přístupů

Přihlašování do služby musí umožňovat využití integrace na Active Directory zadavatele. Řešení řídí možnosti a přístupné funkcionality všech rolí, z Active Directory zadavatele je přebírána příslušnost uživatele do určené role.

4.3 Monitoring

Monitoring musí zahrnovat nepřetržitý dohled nad důležitými prvky řešení a jejich funkcemi včetně průběžného vyhodnocování tak, aby bylo možné předejít většině hrozících výpadků a selhání.

Monitoring musí zahrnovat zejména prvky jako servery, aplikace, databáze, a integrační prvky se souvisejícími systémy.

4.4 Logování

Systém logování řešení musí zahrnovat logy transakční, aplikační a specifikace bezpečnostního logování je upřesněno v kap. 7.6 a 7.7.

V rámci systému pro logování musí být zajištěno:

- Logování všech aktivních transakcí během procesů.
- Správně nastavené časové značky na všech zdrojích (tj. synchronizovaný čas, jeho jednotný formát).
- Zajištění dostatečné kapacity pro logování a jejich uchovávání po dobu min. 6 měsíců.
- Zajištění bezpečnosti a integrity log záznamů (ochrana před zneužitím, změněním nebo vymazáním) napříč celým log management systémem (dle možné závažnosti zneužití).
- Dostupnost logů i v případě poruchy systému (zálohování).

4.5 Zálohování dat

Zálohovací plány předepisují, jak ochránit data při neočekávané události, pádem systému počínaje a fyzickým zničením zařízení konče. Zálohovací plán řeší, jaká data, jakým způsobem a jak často se mají zálohovat, aby byly splněny požadavky uživatelů na přijatelnou lhůtu obnovení dat ze zálohy.

Zálohovací plán musí obsahovat:

- Způsob zálohování (metoda, scope atp.),
- Stanovení četnosti a cyklů záloh pro technologie, systémy a data.

Způsob zálohování a rozsah zodpovědností mezi dodavatelem a zadavatelem bude upřesněn v rámci Předimplementační analýzy.

4.6 Obnova po havárii

Plány obnovy provozu řešení po rozsáhlém výpadku musí být zpracovány pro nejpravděpodobnější havárie s největším dopadem na činnost zadavatele tak, aby snížily na minimum dobu zásahu, chybovost a riziko ze zanedbání důležitých souvislostí.

Plány obnovy musí obsahovat:

- Umístění a popis záloh.
- Pořadí a způsob obnovy jednotlivých komponent systémů.

5 Integrační požadavky

V kapitole jsou uvedené integrační požadavky na řešení, konkrétní návrh řešení bude proveden v rámci **Předimplementační analýzy**.

Předimplementační analýza bude provedena dodavatelem tak, aby implementace řešení proběhla řádně v plánovaném termínu, požadované kvalitě a rozsahu a výstupem předimplementační analýzy bude dokument ve formátu MS Office. Předimplementační analýza bude schválená Zadavatelem na základě akceptačního protokolu.

5.1 Nemocniční informační systém

Zadavatel nepožaduje provedení plné integrace s NIS. Pacientská data z NIS budou stahována přes API:

1. Získávání informací o pacientovi v rozsahu, nutném pro identifikaci pacienta (číslo pojištěnce, , jméno a příjmení, adresa (primárně kontaktní adresa, pokud je jiná než trvalá; ulice a číslo, město, PSČ), kontaktní údaje = mobilní telefon, email)

5.2 AD / Entra ID

Řízení uživatelů musí být možné integrovat s AD zadavatele, tedy systém musí umožňovat ověřit uživatele oproti AD.

Zadavatel provozuje doménu ve verzi 2016.

1. Zadavatel požaduje pro ověření identity (autentizace) interních uživatelů v systému prostřednictvím ověření (AD/Entra ID).
2. Z pohledu autorizace požaduje Zadavatel využití claim-based mechanismů. Identitním providerem a nastavení identitního systému bude včetně podpory Single Sign On s on-premise prostředím Active Directory. Nastavení pravidel pro hesla a podmíněné přístupy (komplexita hesla apod.) poskytuje Zadavatel.
3. Z pohledu autorizace musí řešení podporovat hierarchizovatelné nastavení přístupových práv se stanovením rozsahu přístupu i stupně oprávnění manipulace se záznamem. Princip nastavování přístupových práv k jednotlivým uživatelům musí vycházet z definice libovolného množství

uživatelských rolí a skupin, do kterých jsou jednotliví uživatelé přiřazováni v rámci identitního systému Zadavatele.

4. Dodavatel musí do dokumentace uvést detailní popis úrovně privilegovaných i neprivilegovaných přístupových oprávnění, resp. jednotlivých uživatelských rolí.
5. Přístup do systému (zařazení do relevantní role) je poskytován s využitím aplikace pro správu přístupů na základě přiřazení do příslušné skupiny v Active Directory Přiřazení do skupin bude řízeno požadavkem přes ServiceDesk, případně administrátory dané platformy.

5.3 Monitory životních funkcí / defibrilátory

Řešení umožní přenos dat z monitorů životních funkcí a defibrilátorů od výrobců Stryker, Tempus a Corpus, případně dalších zařízení obdobné třídy po schválení Zadavatelem.

5.4 REST API

Řešení poskytne REST API pro případnou možnou integraci dalších systémů Zadavatele

6 Standardní technologické prostředí Zadavatele

Kapitola obsahuje popis standardního technologického prostředí zadavatele, ve kterém bude dodavatel realizovat požadované řešení. Předběžné požadavky na architekturu a parametry komponent uvede dodavatel v nabídce, zpřesnění požadavků bude provedeno v Předimplementační analýze.

6.1 Obecné standardy

Prostředí VFN je v převážné většině postaveno na produktech společnosti Microsoft. Zadavatel využívá následující technologie, které v některých případech definují prostředí, pro které je dodávka řešení požadována:

Oblast	Technologie	Doplňující informace
Virtualizační platforma	VMware	VFN požaduje, aby dodávané řešení bylo provozuschopné v tomto prostředí.
Dohled	PRTG Network Monitor	Dodavatel poskytne Zadavateli vstupy pro dohled nad během systému jako celku.
Vzdálený přístup	VPN Cisco AnyConnect s vícefaktorovým ověřením	Přístup pro management prostředí bude realizován přes VPN Zadavatele.
Zálohovací systém	Veeam	Zadavatel požaduje zálohování skrz tento zálohovací systém

VFN disponuje dvěma geograficky oddělenými datovými centry. V těchto datových centrech VFN provozuje virtualizované prostředí založené na VMware 8.0. Část infrastruktury VFN může být poskytnuta k využití pro dodávané řešení. Poskytovaná virtualizovaná serverová infrastruktura v rozsahu minimální/maximální konfigurace serveru:

- 4 vCPU / 8 vCPU
- 8GB RAM / 32GB RAM

- OS – disk C: (40GB / 80GB)
- Data/SW - disk D: 100GB / 500GB

Pro operační systémy jsou používány:

- Windows Server 2025 a Linuxová distribuce Debian 13.

Z databázových systémů je standardně využíván Microsoft SQL Server 2022 a vyšší.

V případě, že není uvedena konkrétní technologie nebo oblast, Zadavatel ji nespecifikuje a připouští využití jiného řešení po schválení v rámci předimplementační analýzy.

Zálohu a obnovu aplikačního prostředí provádí Zadavatel dle specifikací a postupů dodaných Dodavatelem v rámci dokumentace řešení.

6.2 Vzdálený přístup pro dodavatele

- Vzdálené přístupy dodavatele budou realizovány standardní formou VPN ve VFN
- Přidělení přístupu a přistupování do sítě VFN z důvodu nutných oprav nebo potřebných změn je definováno směrnicí SM-UI-02

7 Požadavky na bezpečnost řešení

Dodávané řešení musí být navržené, vyvíjené, konfigurované, implementované, nastavené, testované, zdokumentované, udržované a provozované v souladu s požadavky, specifikacemi a zásadami definované v mezinárodní normě ISO/IEC 27001:2022 (resp. 2023), ISO 27799:2019 (doporučení a požadavky na řízení bezpečnosti informací ve zdravotnických zařízeních), NIST SP 800 řady, metodice OWASP a 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 vše v níže uvedeném rozsahu (kap. 7.1 až 7.10).

7.1 Analýza rizik navrhovaného řešení

Dodavatel musí provést v rámci předimplementační analýzy analýzu rizik navrhovaného řešení. Zejména pro technické vybavení, komunikační prostředky, programové vybavení, zpracování dat a objekty dodávaného řešení se zaměřením na následující hrozby:

1. poškození nebo selhání hardwaru nebo softwaru,
2. škodlivý kód (např. viry, spyware, trojské koně),
3. zneužití nebo modifikace údajů,
4. zneužití nebo prolomení přístupových oprávnění,
5. selhání nebo nefungování kontrolních mechanismů nebo bezpečnostních funkcí,
6. zajištění kontinuity provozu.

Dodavatel zpracuje na základě bezpečnostních potřeb a výsledků hodnocení rizik prohlášení o aplikovatelnosti, které obsahuje přehled vybraných a zavedených bezpečnostních opatření a popis vazeb mezi identifikovanými riziky a příslušnými bezpečnostními opatřeními. Součástí bude i úroveň pokrytí rizika (např. %) navrženými opatřeními a možné dopady těchto zbytkových rizik.

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

7.2 Dokumentace

Dodavatel musí v rámci dodávky zpracovat dokumentaci, která musí zahrnovat tyto provozní postupy, bezpečnostní specifikace a skutečnosti:

1. spuštění a ukončení chodu systému,
2. instalace a konfigurace systému,
3. bezpečnostní dokumentaci:
    i. implementované kontrolní mechanismy a bezpečnostní funkce, bezpečnostní nastavení ochrany DB a dat,
    ii. bezpečnostní logy,
    iii. řízení přístupu,
    iv. komunikační bezpečnost, použité kryptografické nástroje, funkce a klíče,
    v. popis datových rozhraní pro napojení na systémy 3. stran,
4. administrátorská a uživatelská dokumentace,
5. zpracování a nakládání s informacemi,
6. vzájemné vztahy a vazby na jiné systémy,
7. postupy zálohování a obnova systému a dat ze záloh v souladu s kap. 4.5 a 4.6.
8. restart nebo obnovení chodu systému po selhání, ošetření chybových stavů anebo mimořádných jevů,
9. podpora a eskalační kontakty v případě neočekávaných provozních nebo technických obtíží či bezpečnostních incidentů.

7.3 Požadavky provoz dodávaného řešení

1. Dodavatel musí zajistit z pohledu zajištění bezpečnosti prostředí:
    a. Testovací a produkční prostředí musí být zcela oddělena v sítích a musí být podporována oddělenými stroji.
    b. Produkční servery nesmí obsahovat překladače a systémové utility, které nejsou nezbytné pro jejich správu nebo provoz.
    c. Testování a vývoj nových verzí systémů, aplikací i zařízení se nesmí provádět v produkčním prostředí.
2. Pro potřebu školení uživatelů a testování nově nasazovaných verzí informačních systémů musí dodavatel vytvořit testovací prostředí v dostatečném předstihu před pilotním provozem – duplicitní provoz.
3. Dodavatel musí zajistit potřebné služby pro testování informačních systémů. Dodavatel musí testovací prostředí naplnit daty tak, aby bylo možné systém řádně otestovat. V rámci instalace nových verzí informačního systému bude zajištěna možnost pravidelně upgradovat provozovaná data a aplikace.

7.4 Postup ověření identity uživatelů

1. Zadavatel požaduje ověření identity (autentizace) v souladu s požadavky uvedenými v kapitole 5.2 AD / Entra ID.

7.5 Ochrana před škodlivým kódem

V rámci dodávaného řešení musí být zajištěna a popsána ochrana:

1. komunikace ve vnitřní sítí,

2. ochrana serverů a sdílených datových úložišť.

7.6 Požadavky na logovací aparát

Všechny logovací aparáty musí obsahovat dle relevance minimálně tyto údaje:

- OS/DB/aplikace,
- druh záznamu/transakce/operace,
- u nových, změn nebo odstranění i zadanou/změněnou hodnotu,
- stav záznamu (dokončený/nedokončený/selhání),
- uživatel, datum a čas,

pro následující operace logování v systému (viz kap. 7.7).

7.7 Zaznamenávání událostí a jejich vyhodnocování

V rámci dodávaného řešení musí být realizováno zaznamenání minimálně následujících událostí:

1. přihlášení a odhlášení uživatelů,
2. činnosti vedoucí ke změně přístupových oprávnění (standardních i privilegovaných),
3. neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů,
4. zahájení a ukončení činností (včetně „pádů" nebo selhání) jednotlivých komponent systému,
5. činnosti spojené s přijímáním/odesíláním ze/do SW třetích stran (integrační logy),
6. automatická varovná nebo chybová hlášení komponent systému,
7. v případě ukládání logů do aplikační vrstvy: přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností,
8. použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení,
9. založení, změna a výmaz datových záznamů včetně času, uživatele a identifikace pracovní stanice, ze které byl úkon proveden (transakční protokol).

Takto zaznamenané události musí být zpracovatelné (strukturované, strojově čitelné) nezávislým prostředkem pro ochranu získaných informací před neoprávněným čtením nebo změnou a pro další vyhodnocování (standardní rozhraní SIEM).

7.8 Aplikační bezpečnost

Dodavatel zajistí v rámci dodávaného řešení:

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.

7.9 Ochrana dat

Dodavatel zajistí v rámci dodávaného řešení:

1. Nastavení ochrany dat zpracovaných nebo uchovávaných v řešení, a to především osobních údajů nebo citlivých údajů, kdy bude kladen důraz na data dostupná z vnější sítě. Budou zohledněna rizika:
    a. neoprávněného přístupu,
    b. nedovolených činností nad rámec svých práv,
    c. popření provedených činností,
    d. kompromitace,
    e. porušení integrity dat,
    f. nedostupnosti dat,
    g. neautorizované změny.
2. Ochranu prováděných transakcí nebo změn dat:
    a. před jejich nedokončením,
    b. nesprávným směrováním,
    c. neautorizovanou změnou předávaného datového obsahu,
    d. kompromitací,
    e. neautorizovaným duplikováním nebo opakováním, a to v souladu s legislativními nebo normativními požadavky, např. daňové, účetní, na ochranu dat.

7.10 Zabezpečení síťových služeb

Realizace a dokumentace způsobu zabezpečení síťových služeb:

- Virtuální servery v prostředí zadavatele budou umístěny ve Virtuální síti, která bude propojena s on-premise s datovým centrem zadavatele. Hybridní propojení zajistí zadavatel.
- Komunikace mezi jednotlivými funkčními celky bude řízená na úrovni síťových služeb a protokolů s pomocí network security groups. Povolena bude pouze vzájemná komunikace, která je nezbytná pro funkci systému.
- Vstupní, výstupní i vzájemná síťová komunikace mezi jednotlivými částmi systému bude monitorována viz kapitola Monitoring (kap. 4.3).

8 Požadavky na implementaci

8.1 Zpracování předimplementační analýzy

1. Zadavatel požaduje po dodavateli zpracování Předimplementační analýzy, tak aby implementace řešení proběhla řádně v plánovaném termínu, požadované kvalitě a rozsahu, a to minimálně v těchto oblastech:
    - Pravidla a postupy pro řízení projektu a plán realizace, vč. zaškolení (uživatelské, administrátorské) příslušných zaměstnanců zadavatele.
    - Popis komunikační matice včetně návrhu týmů na jednotlivých pracovištích zadavatele
    - Popis síťové datové komunikační matice včetně konkrétních síťových portů
    - Analýza požadavků na integraci stávajících systémů a popis systému pro monitorování, logování, zálohování a obnovu řešení po havárii, vč. podpory.
    - Analýza rizik navrhovaného řešení dle požadavků uvedených v kap. 7.1 tohoto dokumentu.
2. Práce dodavatele na vytvoření předimplementační analýzy budou zahájeny bez odkladu po podpisu smlouvy.

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

3. Předimplementační analýza upřesní, případně doplní požadavky požadované zadavatelem v rámci zadávacího řízení.
4. Předimplementační analýza (resp. komunikace se zadavatelem, výstupy, dokumenty atd.) bude realizována v českém jazyce.
5. Pro zpracování předimplementační analýzy zadavatel poskytne dodavateli součinnost v zajištění odborných konzultací. Součástí nabídky Dodavatele musí být i minimální specifikace požadavků na zadavatele z pohledu nezbytné součinnosti pro zpracování předimplementační analýzy.
6. Procesní diagramy a infrastrukturní prostředí dodavatel zpracuje v prostředí standardně používaném pro popis procesů a infrastruktury jako je např. Archimate 3.1, Enterprise Architekt apod.
7. Předimplementační analýza musí být schválena objednatelem na základě akceptačního protokolu předimplementační analýzy.

8.2 Provedení implementace

Na základě provedené předimplementační analýzy bude implementace provedena v následujícím pořadí:

1. Provedení instalace a konfigurace nástroje k užívání služby.
2. Zpracování a předání dokumentace.
3. Proškolení uživatelů a správců systému.
4. Pilotní provoz, vyhodnocení pilotního provozu – incidenty, jejich řešení, následné kroky a doporučení.
5. Akceptace pilotního provozu.
6. Uvedení do ostrého provozu a poskytování zvýšeného dohledu.
7. Finální akceptace.

   V souladu s požadavky na bezpečnost řešení uvedené v kap. 7.3 až 7.10 tohoto dokumentu.

   Výsledek implementace SW řešení bude schválen objednatelem na základě akceptačního protokolu.

8.3 Dokumentace a školení

1) Zadavatel požaduje dodání kompletní dokumentace k systému. Jedná se o:
   a) Bezpečnostní dokumentaci dle specifikací uvedených v kap 7.2,
   b) Administrátorskou a provozní dokumentaci vč. technické části, popisující architekturu systému a integrační vazby rozhraní.
2) Kompletní a aktuální dokumentace bude dle předchozího bodu dodána před zahájením uživatelských akceptačních testů.
3) Dodavatel je povinen tyto dokumenty udržovat aktuální bezodkladně po výskytu změny na produkčním prostředí systému.
4) Dodavatel s každou novou verzí předá zadavateli v elektronické podobě odpovídající uživatelské příručky i technologické postupy a popisy rozhraní na ostatní informační systémy.

5) Dokumentace musí být verzovaná včetně popisu změn vůči verzím předchozím.
6) Podle dokumentace provede dodavatel školení pracovníků zadavatele včetně e-learningu uživatelů v rozsahu 138 hodin.

8.4 Zajištění kvality dodávek

8.4.1 Funkční test

Dodavatel se zavazuje ověřit kvalitu všech dodávek před jejich předáním Zadavateli provedením funkčního testu (FAT), který bude zaměřen na dodržení souladu s metodikou vedení implementačního projektu, se standardy vývoje SW a poskytování služeb údržby SW, s obecně závaznými právními předpisy, a to nejméně v tomto rozsahu:

1. Testování funkčnosti nových a modifikovaných modulů,
2. Ověření funkčnosti těchto modulů v kontextu návazných aplikačních procesů,
3. Integrační testy – ověření funkčnosti komunikace s externími systémy.
4. Ověření instalační sady včetně kontroly správnosti a úplnosti sestavení dodávky,
5. Ověření dodržení bezpečnostních standardů použitých pro webové služby a SW aplikace.
6. Ověření dodržení požadavků zadavatele na výkonnost systému.

Výstupem funkčního testu je předání řešení dodavatelem do uživatelského akceptačního testu zadavateli s následujícím předmětem dodání:

1. Protokol o provedení funkčního testu a jeho výsledky v elektronické podobě,

8.4.2 Uživatelský akceptační test

Uživatelský akceptační test (UAT) provádí zadavatel za podpory dodavatele. Tento test se provádí v testovacím prostředí zadavatele.

1. Všechny chyby zaznamenané v průběhu UAT budou dokumentovány, kategorizovány podle jejich závažnosti a předány dodavateli k řešení, opravy chyb budou jednoznačným a pro zadavatele dostupným způsobem evidovány a dokumentovány, např. samostatnými položkami v helpdesku zadavatele,
2. Dodavatel dodá opravenou (aktualizovanou) dokumentaci dle specifikací uvedených v bodě 1. kap. 8.3 po zapracování chyb a oprav z UAT testů,
3. Dodavatel umožní zadavateli ověřit řešení/modifikaci pilotním provozem na vybraných pracovištích či si k uživatelskému akceptačnímu testu přizvat externího konzultanta.
4. Součástí UAT v průběhu implementačního projektu bude zátěžový test, který ověří dodržení požadavků Zadavatele na výkonnost systému. Výstupem UAT je akceptační protokol, který odpovídá podmínkám stanoveným v Předimplementační analýze.

9 Požadavky na servis a podporu

Dodavatel musí poskytovat servis a podporu v těchto oblastech:

1. Údržba softwaru.
2. Systémová podpora.

3. Uživatelská podpora.
4. Služby na vyžádání.
5. Reporting
6. Exitová součinnost.

Zadavatel poskytne dodavateli ke splnění tohoto závazku nezbytnou součinnost.

9.1 Údržba softwaru

Dodavatel se zavazuje udržovat Aplikační software (dále jen „ASW") aktuální, správně licencovaný, splňující veškeré požadavky kladené na bezpečnost, ochranu osobních údajů a legislativu.

Dodavatel 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. Dodavatel musí zajistit aktuálnost ASW na všech aktivních i neaktivních nodech.
- Je povinen identifikovat a odstraňovat technické zranitelnosti spojené s bezpečnostním nastavením nebo fungováním jím udržovaných systémů. Odstranění uvedených zranitelností se vztahuje i na zranitelnosti identifikované výrobcem, NÚKIB, objednatelem nebo zveřejněné v mezinárodní databázi zranitelností (např. NIST - https://nvd.nist.gov/, CISA - https://www.cisa.gov/news-events/cybersecurity-advisories)
- Proaktivní řešení bezpečnostních chyb a zranitelnosti ASW.
- Aktualizaci ASW tak, aby byl v souladu s relevantními platnými právními předpisy ČR a EU.

9.2 Systémová podpora

Dodavatel se zavazuje udržovat realizované řešení včetně virtuálních serverů v aktuálním stavu, splňující veškeré požadavky kladené na funkčnost, bezpečnost a ochranu osobních údajů. Správa virtuálních serverů po úroveň operačního systému je v gesci oddělení správy serverů Zadavatele.

Dodavatel se zavazuje po dobu platnosti tohoto závazku dále poskytovat zejména:

- Řešit bezpečnostní chyby, hackerské/kybernetické útoky a zjištěné zranitelnosti řešení.
- Služby migrace řešení – převod řešení na vyšší verzi databázového prostředí a operačního systému.
- Služby zahrnující monitoring, zálohování a logování v souladu s nefunkčními požadavky uvedenými v kapitole „4 Nefunkční požadavky" a specifikovanými v předimplementační analýze.
- Součinnost při správě operačního systému.

9.3 Uživatelská podpora

Dodavatel se zavazuje poskytovat uživatelskou podporu softwarového řešení.

Zadavatel bude mít podporu systému první úrovně plně ve své kompetenci, s řízenou distribucí na interní podporu nebo podporu dodavatele. Pro řádné poskytování služeb dodavatel zajistí zadavatel součinnost interního servisního týmu technických specialistů pro řešení poruch a požadavků s týmem dodavatele.

9.3.1 Komunikační cesty

K zajištění elektronické komunikace mezi zadavatelem a dodavatelem je určen helpdeskový nástroj zadavatele ServiceDesk VFN. V tomto nástroji budou probíhat hlášení událostí, které bude dodavatel řešit podle kategorie, závažnosti a úrovni dostupnosti služeb (SLA). Za tímto účelem bude určeným pracovníkům dodavatele zřízen přístup do ServiceDesk VFN. Pokud má dodavatel k dispozici svůj interní helpdeskový nástroj, je také možné provést jeho integraci s nástrojem zadavatele.

V případě technických potíží, které zabraňují zadavateli komunikovat s dodavatelem prostřednictvím ServiceDesku VFN dle předchozího odstavce, lze požadavky odeslat formou elektronické pošty na určenou emailovou adresu dodavatele. Tato komunikace má z hlediska úrovně služeb stejnou váhu jako komunikace v ServiceDesku VFN.

Pro operativní komunikaci mezi zadavatelem a dodavatelem bude zřízena telefonní Hot Line dodavatele na určeném telefonním čísle.

9.3.2 Řešení závad

Závadou se rozumí nefunkčnost jakékoli funkcionality systému, která bude dodavatelem řešena v rámci sjednané úrovně poskytování služeb (SLA).

U dané závady určuje příslušnou úroveň poskytování služeb vždy zadavatel. Dodavatel má právo se proti určené úrovni odvolat, pokud byla průkazně určena chybně.

Provoz řešení je v režimu 24 x 7 při dostupnosti 98,7 %, garantovaná podpora je uvedena v následující tabulce podle příslušné úrovně SLA.

Předem naplánované a oboustranně odsouhlasené servisní úkony/odstávky nejsou považovány za nedostupnost řešení.

Úroveň poskytování služeb	Příjem hlášení	Reakční doba (doba od nahlášení do zahájení řešení)	Maximální doba od nahlášení do odstranění závady
KRITICKÁ	7:00 – 19:00 HotLine – 12x7 HelpDesk – 12x7	2 hodiny	24 hodin
CHYBA	7:00 – 16:00 HotLine – 8x5 HelpDesk – 8x5	1 den	5 pracovních dnů

SLA podpora 12x7 znamená, že technická podpora dodavatele je dostupná 12 hodin denně po dobu 7 dnů v týdnu. SLA podpora 8x5 znamená, že technická podpora dodavatele je dostupná 8 hodin denně po dobu 5 pracovních dnů v týdnu. Reakční doba na odstranění závady se počítá od okamžiku zadání hlášení závady objednatelem do systému ServiceDesku objednatele, anebo nahlášení pomocí Hot Line.

Kritická: je stav, kdy dodané SW řešení dle předmětu smlouvy není funkční, tzn. SW neumožňuje náhradní ani dočasné řešení.

Chyba: je stav, kdy dodané SW řešení neplní některou dílčí funkci uvedenou v provozní nebo uživatelské dokumentaci, a lze ji nahradit využitím náhradního nebo dočasného řešení (workaround).

Odstávky systému je nezbytné plánovat s odpovědnými pracovníky Zadavatele. Maximální doba neplánované odstávky jsou 2 hodiny. Neplánovaná odstávka SW řešení musí být schválená zadavatelem. Není omezeno počtem odpracovaných hodin. Maximální doba na odstranění závady se počítá od okamžiku

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

zadání hlášení závady do helpdesku nebo telefonického nahlášení na určené kontakty Dodavatele, se zajištěním zpětné vazby o jejím přijetí.

Do doby na odstranění závady se nezapočítává doba, po kterou jsou dodávány doplňující či upřesňující informace nutné pro řešení.

Reakční doba je součástí doby na odstranění závady.

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

9.3.3 Služby spojené s uživatelskou podporou

Dodavatel se zavazuje po dobu platnosti této podpory zajistit pro zadavatele služby spojené s podporou řešení.

1. Uvedené služby jsou součástí dodávky a nejsou zpoplatněny vysoutěženou hodinovou sazbou.
1. Jsou to služby poskytované zpravidla v místě zadavatele, služby mohou být po dohodě poskytnuty i vzdáleně. Z poskytnutých služeb je vždy vypracována zpráva.
2. Služby spojené s podporou zahrnují:
   - Dílčí konzultační činnost pro uživatele a správce systému,
   - zaškolení uživatelů při rutinním provozu na pracovišti zadavatele,
   - zaškolení správce systému při implementaci nových verzí,
   - metodická podpora při rutinním používání systému,
   - metodická podpora konfigurace systému a přípravy číselníků ASW,
   - průběžná aktualizace veškeré dokumentace systému,

9.4 Služby na vyžádání

Dodavatel se zavazuje po dobu platnosti této podpory zajistit pro zadavatele služby na vyžádání nad rámec předmětu plnění. Předpokládaný rozsah je maximálně 96 MD za období 4 let.

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 zadavatele, služby mohou být po dohodě poskytnuty i vzdáleně. Z poskytnutých služeb je vždy vypracována zpráva o realizaci.
3. Forma akceptace poskytnutých služeb je realizována oboustranně potvrzeným akceptačním protokolem.
4. Služby na vyžádání zahrnují zejména:
   Konzultační a analytické služby zaměřené na požadovanou oblast,
   poskytování systémových, programátorských a vývojových prací,
   realizace požadavků na novou funkcionalitu nad rámec poptávaného řešení.

9.5 Reporting

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

- vyřešené závady a závady v řešení,
- vyřešené požadavky a požadavky v řešení,

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

- soupis poskytnutých a poskytovaných Služeb spojených s uživatelskou podporou,
- soupis poskytnutých a poskytovaných Služeb na vyžádání,
- přehled splněných a nesplněných SLA.

Tento report se dodavatel zavazuje poskytovat zadavateli jednou měsíčně vždy za uplynulý měsíc, k poslednímu dni v měsíci.

9.6 Exitová součinnost

Dodavatel za účelem řádného a plynulého převedení v případě ukončení smlouvy všech činností spojených se servisem a podporou SW řešení především:

- poskytne náležitou a nezbytnou součinnost pro takové převedení,
- poskytne veškeré nezbytné informace a dokumentaci,
- data ve stávajícím formátu budou Zadavateli předána bezúplatně, pokud bude Zadavatel požadovat jiný formát dat, mohou být práce související s převodem dat do požadovaného formátu zpoplatněny,
- na žádost Zadavatele provede protokolární likvidaci dat a provozních údajů souvisejících s poskytováním údržby SW řešení a tímto zanikne možnost vedení jakéhokoliv i budoucího sporu.

Příloha č. 3 Smlouvy – Seznam oprávněných osob

A. Seznam kontaktních osob poskytovatele oprávněných poskytovat podporu

Jméno	**Funkce**	**Telefonní číslo**
xxxxx	Jednatel	xxxxx
xxxxx	Vedoucí vývoje	xxxxx
xxxxx	Vedoucí podpory	xxxxx

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

Jméno	**Funkce**	**Telefonní číslo**
xxxxx	Vedoucí vývoje a správy SW	xxxxx
xxxxx	Vedoucí aplikační podpory	xxxxx
	Dispečink ÚIDT	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	Poverenec@vfn.cz
Bezpečnosti informací, kybernetické bezpečnost	Manažer bezpečnosti informací / kybernetické bezpečnosti	ManazerKB@vfn.cz

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

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

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

4.2.2 Požadavky na připojené zařízení

Požadavky a povinnosti vztahující se na zařízení, které je používáno pro externí nebo VPN přístup, jsou uvedeny v příloze č. 1 (Povinnosti při připojování zařízení do sítě VFN) tohoto dokumentu.

4.2.3 Bezpečnostní incident nebo kybernetický útok

V případě bezpečnostní hrozby nebo kybernetického útoku má VFN právo zrušit povolení přístupu externího uživatele anebo VPN přístupu na dobu nezbytnou k analyzování hrozby nebo útoku a zabránění jakéhokoliv ohrožení sítě, informačních systémů a dat VFN. Pokud externí uživatel vykonává nebo má práva správce nebo administrátora IS VFN, je povinen konat bezodkladně a zajistit dostatek důkazního materiálu dle povinností uvedených v příloze (Příloha č. 3 – Povinnost administrátora v případě bezpečnostního incidentu nebo kybernetického útoku).

4.2.4 Zakázané činnosti

Externí uživatel připojený do sítě VFN nesmí:

- v žádném případě poskytovat informace o přístupu, postupech, přístupová hesla, certifikáty, další citlivé informace a ani jejich části třetím osobám,
- umožnit přístup do sítě jiným osobám (např. umožnit přihlášení pod svým jménem),
- se jakýmkoliv způsobem angažovat při rozesílání a distribuci protiprávních, pomlouvačných, hanlivých, reklamních, agitačních a jiných zpráv,
- v žádném případě předávat jakékoli důvěrné informace získané tímto přístupem třetím osobám (osobní údaje, číselníky, databáze, atd.),
- v síti VFN vyhledávat důvěrné nebo jinak citlivé informace, snažit se získat neautorizovaný přístup k souborům a informacím,
- jakýmkoliv způsobem narušit funkci sítě, informačních systémů a dostupnost jejich dat,
- omezit práva uživatelů/správců ICT nebo získat práva nad rámec svých činností a oprávnění,
- v rámci VFN instalovat nebo ukládat jakýkoli neautorizovaný, nelegální nebo škodlivý software.

4.2.5 Monitoring činností

Veškeré činnosti externího připojení do sítě VFN jsou monitorovány a logovány a pravidelně vyhodnocovány architektem kybernetické bezpečnosti nebo jiným pověřeným zaměstnancem ÚI.

4.2.6 Porušení pravidel a povinností

Externímu uživateli, který poruší pravidla, nedodrží povinnosti nebo provádí zakázané činnosti (viz kap. 4.2):

- bude právo přístupu do sítě VFN neprodleně odebráno,
- porušení může být posuzováno jako závažné porušení povinností vyplývajících z právních předpisů a smluvního vztahu vztahujících se k externímu uživateli vykonávané práci a jednání v rozporu se zájmy VFN a uzavřeného smluvního vztahu.

Externí uživatel připojený do sítě VFN:

- plně zodpovídá za škody vzniklé v důsledku zneužití jeho přístupu zaviněného nedbalostí, nebo poskytnutím přístupu do sítě VFN třetí osobě,
- je plně zodpovědný za obsah svého datového prostoru.

POUŽÍVÁNÍ SÍTĚ VFN EXTERNÍMI UŽIVATELI

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. +420 224 962 119.

Metoda vzdáleného přístupu

K připojovaným zařízením je možné, pokud tomu nebrání další důvody, zřídit vzdálený přístup typu VPN připojení (IPSec tunel nebo jeho obdoba). Je nutná instalace Cisco VPN klienta.

Info: https://www.vfn.cz/vpn nebo Pohotovosti ÚI: +420 702 083 578 (mimo pracovní hodiny Dispečinku ÚI)

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: +420 224 962 119
  E-mail: dispecink@vfn.cz

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

POVINNOST ADMINISTRÁTORA V PŘÍPADĚ BEZPEČNOSTNÍHO INCIDENTU NEBO KYBERNETICKÉHO ÚTOKU

Povinnosti administrátora

V případě podezření či probíhajícím bezpečnostním incidentu nebo kybernetickém útoku je povinností správce nebo administrátora konat bezodkladně a zajistit dostatek důkazního materiálu:

- k identifikaci zdroje nebo příčiny,
- k čemu došlo nebo jak se projevuje,
- důsledkům a možným dopadům,

u tohoto incidentu či útoku je vždy povinen:

- zajistit kopie logů nebo transakčních záznamů, pokud by to nezpůsobilo jejich poškození nebo smazání,
- iniciovat nebo pozastavit šíření či poškození, zamezit incidentu nebo útoku,
- nemazat jakákoliv data o kybernetickém bezpečnostním incidentu bez svolení VFN, Policie ČR nebo NÚKIB,
- nahlásit toto podezření neodkladně na Pohotovost ÚI jako bezpečnostní nebo kybernetický incident:

  v pracovní dny

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

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

Příloha č. 5 smlouvy - Položkový ceník

Předmět plnění VZ	Množství	Jednotka	Nabídková cena/jednotka		Nabídková cena celkem		
			(bez DPH)	(s DPH)	(bez DPH)	Samostatně DPH (základní sazba)	(s DPH)
Poskytování SW řešení pro zabezpečenou komunikační platformu (v souladu se zadávacími podmínkami a návrhem smlouvy o poskytování SW řešení a služeb podpory vč. příloh).	48	měsíc	18,158.33 Kč	21,971.58 Kč	871,600.00 Kč	183,036.00 Kč	1,054,636.00 Kč
Služby dalšího rozvoje na vyžádání	96	MD (Manday)	14,400.00 Kč	17,424.00 Kč	1,382,400.00 Kč	290,304.00 Kč	1,672,704.00 Kč
Celková nabídková cena za celý předmět plnění bez DPH *					2,254,000.00 Kč		