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 Krajským soudem v Hradci Králové, oddíl C,   
vložka 148

se sídlem: Pernštýnské náměstí 51, 530 02 Pardubice

IČO: DIČ: 13583531 / CZ699004728

zastoupena: Ing. Leošem Raibrem, jednatelem společnosti STAPRO s. r. o.

bankovní spojení: xxxxxx

číslo účtu: xxxxxx

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: xxxxxx

číslo účtu: xxxxxx

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 „**NIS VFN – Modernizace NIS včetně integrační platformy**“, **vyhlášené otevřeným řízením** dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších přepisů (dále jen „z. č. 134/2016 Sb.“) a zveřejněné ve Věstníku veřejných zakázek. pod ev. č. Z2023-017109 ze dne 25.4.2023 a v Úředním věstníku Evropské unie pod č 2023/S 084-258551, oznámení o zahájení zadávacího řízení ze dne 25.4.2023 (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 softwarového řešení (dále jen „SW řešení“ či „SW“), který poskytovatel objednateli dodal na základě licenční smlouvy č. PO 467/S/23 (dále jen „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 odměnu za poskytnutí podpory dle tohoto článku smlouvy v souladu s podmínkami sjednanými touto smlouvou.
4. Poskytovatel se stává plněním dle této Smlouvy Poskytovatelem systémů, technologií a služeb, na kterých je provozována základní služba: Poskytování zdravotních služeb dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „ZKB“). Objednatel je orgánem nebo osobou provozující základní službu podle ZKB § 3 písm. f) a provozování základní služby Objednatelem podle ZKB je závislé na provozování řešení poskytovaného Poskytovatelem.
5. Místem plnění je sídlo objednatele.

**II. Způsob poskytování podpory software**

1. Konkrétní specifikace podpory je blíže specifikována v příloze č. 1 této smlouvy.
2. Oprávněné osoby objednatele a poskytovatele, které mohou pracovat s Helpdeskem objednatele jsou uvedeny v příloze č. 3 smlouvy.

III. Cena a platební podmínky

1. Cena za služby poskytované objednateli dle čl. I. a Přílohy č. 1 (vyjma bodu 1.4 přílohy č. 1) této smlouvy je stanovena dohodou smluvních stran ve výši **4 254 972,-**Kč bez DPH ročně.
2. Cena služeb na vyžádání dle bodu č. 1.4 Přílohy č. 1 této smlouvy je stanovena dohodou smluvních stran na částku **2 400,-** 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 **354 581,-** 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. Ceny dle čl. III. této smlouvy budou hrazeny na základě faktur – daňových dokladů (dále jen „**faktura**“) vystavených poskytovatelem, přičemž tyto musí obsahovat všechny údaje uvedené v § 29 odst. 1 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a dále též dle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů.
6. Poskytovatel se touto smlouvou zavazuje, že jím vystavená faktura bude obsahovat všechny náležitosti řádného daňového dokladu dle platné právní úpravy.
7. Splatnost faktury činí 60 dní ode dne doručení faktury objednateli do jeho sídla, přesněji na Ekonomický úsek, Odbor účetnictví nebo elektronicky ve formátu PDF nebo ISDOC na e-mailovou adresu: xxxxxx
8. Pokud faktura nebude obsahovat všechny zákonem a touto smlouvou stanovené náležitosti, je objednatel oprávněn ji do 15 dnů ode dne doručení vrátit poskytovateli s tím, že poskytovatel je poté povinen vystavit fakturu novou. Pro odstranění jakékoliv pochybnosti smluvní strany berou na vědomí, že za předpokladu vystavení nové faktury počíná běh nové doby splatnosti ve smyslu čl. III odst. 7 této smlouvy, tedy že v tomto případě objednatel není v prodlení s úhradou faktury.
9. Úhrada faktury bude provedena formou převodu na účet druhé smluvní strany uvedený na faktuře, přičemž tento bude shodný s účtem uvedeným v záhlaví této smlouvy.
10. Smluvní strany prohlašují, že povinnost objednatele zaplatit poskytovateli s touto smlouvou řádně vyfakturovanou cenu je splněna dnem odeslání platby z účtu objednatele.
11. Smluvní strany se dohodly, že pokud průměrná roční míra inflace vyjádřená přírůstkem průměrného indexu spotřebitelských cen (CPI – Consumer Price Index) dle údajů publikovaných Českým statistickým úřadem na jeho oficiálních internetových stránkách, přesáhne v České republice za posledních 12 po sobě jdoucích měsíců kalendářního roku hodnotu 5 bodů (procent) oproti míře inflace za kalendářní rok předcházející, na možnosti zvýšení kupní ceny o výši meziročního rozdílu míry inflace v uvedeném období, a to vždy od 1. ledna následujícího kalendářního roku a maximálně jednou v každém kalendářním roce účinnosti této smlouvy, nejdříve však od 1.1.2026. Poskytovatel je povinen tento nárůst inflace objednateli prokázat, ke zvýšení ceny za plnění se vyžaduje souhlas objednatele. Zvýšení ceny je účinné až po uzavření písemného číslovaného dodatku podepsaného oběma smluvními stranami.

IV. Trvání smlouvy

1. Smlouva se uzavírá na dobu neurčitou.
2. Smlouva může být ukončena:

* písemnou dohodou smluvních stran
* písemnou výpovědí ze strany objednatele nebo poskytovatele i bez udání důvodu; výpovědní doba činí 6 měsíců a počíná běžet první den následujícího měsíce, ve kterém byla písemná výpověď druhé smluvní straně doručena.
* odstoupením od smlouvy ze strany objednatele nebo poskytovatele.

1. Kterákoliv ze smluvních stran je oprávněna odstoupit od smlouvy v případě, že druhá smluvní strana hrubě poruší nebo opakovaně porušuje své smluvní závazky vyplývající z této smlouvy a přes písemnou výzvu odmítá odstranit vady svého jednání, anebo nečiní žádné kroky k nápravě vzniklého vadného stavu nebo v případě porušení závazku mlčenlivosti druhou smluvní stranou. Za hrubé porušení smluvních závazků ze strany objednatele se považuje prodlení objednatele s úhradou faktur poskytovateli překračujícím termín splatnosti o 90 dnů a na straně poskytovatele, pokud dojde k porušení povinnosti jemu uložené ust. čl. IX odst. 6 této smlouvy
2. Smluvní strany rovněž ujednávají, že smlouva automaticky zaniká v případě zániku hlavního závazku z veřejné zakázky, jejímž je tato smlouva výsledkem, tedy za předpokladu zániku licenční smlouvy č. PO 467/S/23, nedohodnou-li se smluvní strany výslovně jinak.
3. 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.
4. 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.
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 této smlouvy.

**VI. Závazky poskytovatele**

1. Poskytovatel se zavazuje plnit své povinnosti vyplývající z této smlouvy s maximální odpovědností tak, aby systém byl udržován nepřetržitě v provozuschopném a funkčním stavu, který je řádně zdokumentován. Poskytovatel odpovídá za kvalitu a včasnost vykonaných prací ve smyslu výše uvedených ustanovení.
2. Poskytovatel je povinen systém zabezpečit tak, aby nedošlo k přihlášení nebo přístupu osoby, která nemá příslušné oprávnění do systému. Za jakékoli škody, s výjimkou fyzického zabezpečení serverů, způsobené objednateli zásahem neoprávněně přihlášené osoby odpovídá Poskytovatel.
3. Poskytovatel se zavazuje zajistit objednateli přístup a nakládání s veškerými daty objednatele uloženými v SW řešení nepřetržitě a bez omezení po celou dobu trvání této smlouvy i po skončení účinnosti této smlouvy, a to v případě nedodržení podmínek sjednaných v rámci bodu 1.6 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: xxxxxx, neprodleně informovat o kybernetických bezpečnostních incidentech souvisejících s poskytovaným řešením.
7. Poskytovatel je povinen objednatele informovat prostřednictvím manažera kybernetické bezpečnosti o způsobu řízení rizik na straně poskytovatele a o zbytkových rizicích souvisejících s plněním smlouvy v půl ročním intervalu nebo v případě zjištění nových rizik nebo změn stávajících rizik informovat bezodkladně.
8. Poskytovatel je povinen informovat manažera kybernetické bezpečnosti objednatele o významné změně v ovládání poskytovatele podle dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích ve znění pozdějších předpisů nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných Poskytovatelem k plnění podle této smlouvy.
9. Poskytovatel je povinen v případě zjištění nebo podezření na probíhající kybernetický útok v průběhu poskytování služeb Poskytovatelem, provést nezbytné kroky poskytovatelem k zdokumentování a zajištění forenzních důkazů a okamžitému nahlášení kontaktní osobě za objednatele (viz kontaktní osoby), která rozhodne, zda budou práce ukončeny nebo bude v pracích pokračováno a za jakých podmínek.
10. Poskytovatel bere na vědomí, že služby poskytované dle této smlouvy nesmí být provozované na technických nebo programových prostředcích označených NÚKIB jako hrozba.
11. Poskytovatel je povinen určit oprávněné osoby pro styk s objednatelem, které budou po dobu platnosti této smlouvy zabezpečovat nezbytnou součinnost mezi objednatelem a poskytovatelem a k zajištění potřebných informací a materiálů k plnění této smlouvy. Poskytovatel může tyto oprávněné osoby zaměnit jinými, které budou vhodné pro výkon prací, a to po předchozím písemném vyrozumění a odsouhlasení ze strany objednatele (seznam oprávněných osob tvoří Přílohu č. 3 této smlouvy).
12. 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.

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 u nově dodaných modulů (Operační sály, adiktologie, UA point), integrační platformy, DEA (s DocReg, MPI) v kategorii „kritická“, 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 u nově dodaných modulů (Operační sály, adiktologie, UA point), integrační platformy, DEA (s DocReg, MPI) v kategorii „vážná“, 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 u nově dodaných modulů (Operační sály, adiktologie, UA point), integrační platformy, DEA (s DocReg, MPI) v kategorii „běžná“, je objednatel oprávněn požadovat na poskytovateli smluvní pokutu ve výši 5.000,- Kč za každý započatý pracovní den prodlení za jednotlivý případ.
5. Při nedodržení termínu pro odstranění závady Portálu pacienta v kategorii „kritická“, je objednatel oprávněn požadovat na poskytovateli smluvní pokutu ve výši 5.000,- Kč za každou započatou hodinu prodlení za jednotlivý případ.
6. Při nedodržení termínu pro odstranění závady Portálu pacienta v kategorii „vážná“, je objednatel oprávněn požadovat na poskytovateli smluvní pokutu ve výši 3.000,- Kč za každou započatou hodinu prodlení za jednotlivý případ.
7. Při nedodržení termínu pro odstranění závady Portálu pacienta v kategorii „běžná“, je objednatel oprávněn požadovat na poskytovateli smluvní pokutu ve výši 5.000,- Kč za každý započatý pracovní den prodlení za jednotlivý případ.
8. Při nedodržení termínu pro odstranění závady modulu MIS v kategorii „kritická“, je objednatel oprávněn požadovat na poskytovateli smluvní pokutu ve výši 5.000,- Kč za každý započatý pracovní den prodlení za jednotlivý případ.
9. Při nedodržení termínu pro odstranění závady modulu MIS v kategorii „vážná“, je objednatel oprávněn požadovat na poskytovateli smluvní pokutu ve výši 3.000,- Kč za každý započatý pracovní den prodlení za jednotlivý případ.
10. Při nedodržení termínu pro odstranění závady modulu MIS v kategorii „běžná“, je objednatel oprávněn požadovat na poskytovateli smluvní pokutu ve výši 3.000,- Kč za každý započatý pracovní den prodlení za jednotlivý případ.
11. V případě, že nebude dodržen požadavek na dostupnost provozu nově dodaných modulů (Operační sály, adiktologie, UA point), integrační platformy, DEA (s DocReg, MPI) v režimu SLA 99,18 %, uvedený v kapitole č. 1.3.2.1 v příloze č. 1 této smlouvy, je objednatel oprávněn za nedodržení dostupnosti řešení požadovat smluvní pokutu ve výši 10.000,- Kč za každý i započatý den nedostupnosti.
12. V případě, že nebude dodržen požadavek na dostupnost provozu Portálu pacient v režimu SLA 97,14 %, uvedený v kapitole č. 1.3.2.1 v příloze č. 1 této smlouvy, je objednatel oprávněn za nedodržení dostupnosti řešení požadovat smluvní pokutu ve výši 10.000,- Kč za každý i započatý den nedostupnosti.
13. V případě, že nebude dodržen požadavek na dostupnost provozu modulu MIS v režimu SLA 95 %, uvedený v kapitole č. 1.3.2.1 v příloze č. 1 této smlouvy, je objednatel oprávněn za nedodržení dostupnosti řešení požadovat smluvní pokutu ve výši 10.000,- Kč za každý i započatý den nedostupnosti.
14. Na výše uvedené smluvní pokuty nemá objednatel nárok, prokáže-li se, že problém byl způsoben jednáním objednatele, selháním nebo jinými problémy na straně objednatele.
15. V případě nedodržení povinností poskytovatele dle čl. IX odst. 2, 6 a 7 této smlouvy, má objednatel právo účtovat poskytovateli smluvní pokutu ve výši 50 000,- Kč za každé jednotlivé porušení povinnosti.
16. V případě nedodržení povinností poskytovatele dle odst. č. 6 až 12 čl. VI a čl. VIII. této smlouvy, má objednatel právo účtovat poskytovateli smluvní pokutu ve výši 200 000,- Kč za každé jednotlivé porušení povinnosti.
17. V případě nedodržení povinnosti stanovené v čl. X. odst. 5 smlouvy má objednatel právo účtovat smluvní pokutu ve výši pohledávky, která byla postoupena v rozporu s touto smlouvou. Objednatel má zároveň právo odstoupit od smlouvy.
18. 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.
19. Smluvní pokuta bude vyúčtovaná samostatným daňovým dokladem, splatnost smluvní pokuty činí 30 dní ode dne doručení vyúčtování Poskytovateli.
20. Zaplacením smluvní pokuty není dotčen nárok objednatele na náhradu škody, včetně náhrady škody, která převyšuje smluvní pokutu.

VIII. Mlčenlivost

1. Poskytovatel se zavazuje zachovávat mlčenlivost ve vztahu ke všem informacím a skutečnostem, které se dozví o objednateli, jeho zaměstnancích, pacientech atd. v souvislosti s uzavřením a plněním smlouvy, pokud tyto informace mají povahu obchodního tajemství, osobních údajů nebo mají být z jiných důvodů chráněny před zveřejněním. Poskytovatel je povinen nakládat s osobními údaji a zejména s údaji o zdravotním stavu, genetickými a biometrickými údaji (dále jen „Osobní údaje“) v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 (dále jen GDPR) a příslušnými ustanoveními zákona č. 110/2019 Sb., o zpracování osobních údajů.
2. Povinnost mlčenlivosti platí rovněž o skutečnostech, na něž se vztahuje povinnost mlčenlivosti zdravotnických pracovníků, zejména podle ustanovení § 51 zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (Zákon o zdravotních službách), a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení Osobních údajů.
3. Pokud poskytovatel přijde při plnění Smlouvy do styku s Osobními údaji a bude v postavení zpracovatele ve smyslu GDPR a Zákona o zpracování osobních údajů, zavazuje se nakládat s Osobními údaji pouze za účelem splnění závazků z této smlouvy a žádným jiným způsobem, a to v souladu příslušnými ustanoveními GDPR a Zákona o zpracování osobních údajů v rozsahu nezbytném pro plnění smlouvy a po dobu nezbytnou k plnění smlouvy. Zpracovávání Osobních údajů v rozsahu údajů poskytnutých objednatelem a týkajících se zdravotnické dokumentace pacientů, jimž jsou objednatelem poskytovány zdravotní služby, a dále v rozsahu Osobních údajů zaměstnanců objednatele poskytovatelem může zahrnovat odstranění potíží za účelem zabránění, vyhledávání a opravy problémů zjištěných při poskytování služeb dle této smlouvy, může také zahrnovat zlepšování funkcí informačních systémů, vyhledávání hrozeb uživatelům a ochrany uživatelů informačních systémů. Osobní údaje nebudou použity k jinému účelu, ani z nich nebudou odvozovány informace pro žádné reklamní či jiné komerční účely. Poskytovatel se zavazuje za účelem ochrany osobních údajů objednatele a jeho pacientů a zaměstnanců před neoprávněným přístupem, použitím, zveřejněním nebo zničením, resp. před jejich náhodnou ztrátou či změnou uplatňovat technická a organizační bezpečnostní opatření, interní kontroly a rutiny zabezpečení osobních údajů zajišťující splnění všech povinností dle GDPR a Zákona o ochraně osobních údajů, zejména zajistit, aby data obsažená ve zdravotnické dokumentaci byla šifrována způsobem, který znemožní nahlížení do těchto údajů neoprávněným osobám.
4. Poskytovatel se zavazuje zajistit informovanost svých pracovníků (včetně poddodavatelů) o povinnostech vyplývajících z této Smlouvy. Poskytovatel se zavazuje zajistit, aby jeho pracovníci, kteří budou přicházet do styku s osobními údaji, byli smluvně vázáni povinností mlčenlivosti ve smyslu GDPR a Zákona o zpracování osobních údajů a poučeni o možných následcích porušení těchto povinností s tím, že povinnost důvěrnosti bude jimi dodržována i po skončení jejich smluvního vztahu k objednateli. Toto ujednání je sjednáno ve smyslu ustanovení čl. 28 GDPR. Poskytovatel se zavazuje informovat své poddodavatele o povinnosti mlčenlivosti dle této smlouvy. V případě porušení mlčenlivosti za strany poddodavatele, odpovídá poskytovatel objednateli za vzniklou škodu, jako kdyby povinnost porušil sám.
5. Smluvní strany se zavazují zachovat mlčenlivost též o všech ostatních skutečnostech, ve vztahu k nimž o to budou druhou stranou písemně požádány. Smluvní strany se též zavazují nevyužít informace podle prvé věty tohoto odstavce ve svůj prospěch nebo ve prospěch třetích osob v rozporu s účelem jejich předání.
6. Smluvní strany jsou povinny zajistit, že nebudou neoprávněně pořizovány kopie informací či jiné záznamy nad rámec plnění dle této smlouvy, a nebudou zjišťovány informace, které nejsou nezbytně nutné ke splnění povinností vyplývajících z této smlouvy.
7. Smluvní strany se zavazují pro případ, že se v průběhu plnění dle této smlouvy dostanou do kontaktu s údaji druhé smluvní strany vyplývajícími z její provozní činnosti, tyto údaje v žádném případě nezneužít, nezměnit ani jinak nepoškodit, neztratit či neznehodnotit.
8. Poskytovatel se zavazuje plně respektovat bezpečnostní požadavky objednatele k zajištění ochrany Osobních údajů pacientů a zaměstnanců objednatele.
9. Povinnost mlčenlivosti o informacích a skutečnostech obchodního charakteru trvá po dobu 5 let od ukončení této smlouvy, o informacích obsahujících Osobní údaje trvá bez časového omezení.
10. Smluvní strany vylučují povinnosti jim uložené ve smyslu čl. IX, a to za předpokladu plnění povinností jim uložených platnými právními předpisy, především, nikoliv však výlučně zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů (dále též „**registr smluv**“).

IX. Ostatní ujednání

1. Poskytovatel bere na vědomí, že objednatel je povinen dle ustanovení § 219 odst. 1 zákona č. 134/2016 Sb., a dle zákona o registru smluv uveřejnit tuto smlouvu včetně případných dodatků, příloh a objednávek vystavených na základě této smlouvy, zákonem stanoveným způsobem.
2. Poskytovatel je povinen v souladu s ustanovením § 105 z. č. 134/2016 Sb. předložit do 10 pracovních dnů od doručení oznámení o výběru dodavatele objednateli seznam, ve kterém uvede, jaké části předmětu plnění a v jakém rozsahu bude plnit prostřednictvím poddodavatele, spolu s identifikací poddodavatele a uvedením rozsahu jeho plnění, pokud mu jsou známi. Poddodavatelé, kteří nebyli tímto způsobem identifikováni a kteří se následně zapojí do plnění veřejné zakázky, musí být identifikováni dodatečně, a to nejpozději před zahájením plnění veřejné zakázky tímto poddodavatelem.
3. Poskytovatel bere na vědomí, že objednatel je povinným subjektem podle zák. č. 106/1999 Sb., zákona o svobodném přístupu k informacím, ve znění pozdějších předpisů.
4. Poskytovatel se zavazuje dodržovat nařízení objednatele, kterým je zakázáno kouření ve všech prostorách i plochách areálu objednatele s výjimkou vyhrazených míst.
5. Obě strany se zavazují, že v souvislosti s plněním smlouvy učiní opatření k zajištění ochrany před šířením počítačových virů a nelegálních programů.
6. Poskytovatel je povinen mít v platnosti a udržovat pojištění odpovědnosti za škodu způsobenou objednateli či třetím osobám při výkonu podnikatelské činnosti, která je předmětem této smlouvy, s limitem pojistného plnění v minimální výši 40.000.000,- 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. Poskytovatel je oprávněn postoupit pohledávku vyplývající z plnění dle této smlouvy na třetí osobu pouze s předchozím písemným souhlasem objednatele.

X. Závěrečná ujednání

1. Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem finální akceptace předmětu plnění dle licenční smlouvy ze dne PO 467/S/23 po uveřejnění v registru smluv.
2. Tato smlouva se řídí právním řádem České republiky a případné spory z ní, které nebudou urovnány smírnou cestou, budou rozhodovány věcně a místně příslušným soudem ČR, za kterýžto pro účely této smlouvy smluvní strany označují obecný soud objednatele.
3. Právní vztahy touto smlouvou neupravené, jakož i právní poměry z ní vznikající a vyplývající, se řídí příslušnými ustanoveními občanského zákoníku v platném znění a předpisy souvisejícími.
4. Jakékoliv změny této smlouvy mohou být prováděny pouze formou písemných dodatků k této smlouvě a musí být podepsány oprávněnými zástupci smluvních stran. Tyto případné dodatky budou tvořit nedílnou součást této smlouvy.
5. Poskytovatel je oprávněn postoupit pohledávku vyplývající z plnění dle této smlouvy na třetí osobu pouze s předchozím písemným souhlasem objednatele.
6. 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.
7. Práva a závazky, které pro smluvní strany ze smlouvy vyplývají, přecházejí na jejich případné právní nástupce.
8. Smluvní strany prohlašují, že si tuto smlouvu přečetly, a že byla ujednána po vzájemném projednání podle jejich svobodné vůle, určitě, vážně a srozumitelně, nikoliv v tísni za nápadně nevýhodných podmínek.

**Přílohy:**

Příloha č. 1 - Specifikace podpory SW řešení

Příloha č. 2 – 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 V Pardubicích dne

------------------------------------------------------------------ -----------------------------------------------------

prof. MUDr. David Feltl, Ph.D., MBA Ing. Leoš Raibr

ředitel Všeobecné fakultní nemocnice v Praze jednatel společnosti STAPRO s. r. o.

**Příloha č. 1 Smlouvy – Specifikace podpory SW řešení**

# Servis a podpora

Dodavatel poskytuje servis a podporu v těchto oblastech:

1. Údržba software.
2. Systémová podpora.
3. Uživatelská podpora.
4. Řešení závad.
5. Reporting.
6. Exitová součinnost.

Objednatel poskytne poskytovateli ke splnění tohoto závazku nezbytnou součinnost.

## Údržba software

Poskytovatel se zavazuje udržovat „systémový SW na integrační platformě 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. Dodavatel musí zajistit aktuálnost ASW na všech aktivních i neaktivních nodech použité virtualizace.
* Proaktivní řešení bezpečnostních chyb a zranitelnosti ASW.
* Odstraňuje zranitelnosti identifikované nezávislými subjekty (např. NIST), NÚKIB a z penetračních testů objednatele (provádí smluvní dodavatel objednatele).
* Aktualizaci ASW tak, aby byl v souladu s relevantními platnými právními předpisy ČR a EU.

## 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.

## Uživatelská podpora

Poskytovatel se zavazuje poskytovat uživatelskou podporu softwarového řešení druhé a vyšší úrovně.

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

**Služby spojené s uživatelskou podporou**

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

1. Uvedené služby jsou součástí dodávky a nejsou zpoplatněny vysoutěženou hodinovou sazbou.
2. Jsou to služby poskytované zpravidla v místě objednatele, služby mohou být poskytnuty i vzdáleně. O poskytnutých službách je vždy zapsán řešitelem záznam do příslušného Ticketu v ServiceDesku VFN, resp. integrované aplikaci Helpdesku poskytovatele.
3. Služby spojené s podporou zahrnují:

* Dílčí konzultační činnost pro uživatele a správce systému,
* zaškolení uživatelů při rutinním provozu na pracovišti objednatele,
* zaškolení správce systému při implementaci nových verzí,
* metodická podpora při rutinním používání systému,
* sledování využití systému a vypracování návrhů na jeho zlepšení (proškolení uživatelů ASW, organizační opatření, posílení, doplnění nebo přesuny techniky apod.),
* metodická podpora pro konfigurace systému a pro přípravy číselníků ASW,
* vytváření databázových view na základě požadavků objednatele,
* průběžná aktualizace veškeré dokumentace systému.

### 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 **xxxxxx.** Tato komunikace má z hlediska úrovně služeb stejnou váhu jako komunikace v ServiceDesku objednatele.

Pro operativní komunikaci mezi objednatelem a poskytovatelem bude zřízena telefonní Hot Line poskytovatele na určeném telefonním čísle, které **bude sděleno po podpisu smlouvy.**

### 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.

### Definice kategorií dostupnosti

1. Nově dodávané moduly (operační sály, adiktologie, UA point), Integrační platforma a DEA (současně s DocReg, MPI) jsou v režimu 24 hodin denně x 7 dní v týdnu (dále též „24x7“) při dostupnosti 99,18%.
2. Portál pacienta je v režimu 24 x 7 při dostupnosti 97,14%.
3. MIS je v režimu 24 x 7 při dostupnosti 95%.

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.

### Řešení incidentů pro nově dodávané moduly (operační sály, adiktologie, UA point), integrační platformu, DEA (s DocReg, MPI)

Provoz řešení je v režimu 24x7 při roční dostupnosti dle definované kategorie dostupnosti (viz kap 1.3.2.1 tohoto dokumentu - Definice kategorií dostupnosti) garantovaná podpora je uvedena v následující tabulce podle příslušné úrovně SLA.

*Tabulka 1: Řešení incidentů pro nově dodávané moduly, integrační platformu, DEA*

|  |  |  |  |
| --- | --- | --- | --- |
| Úroveň poskytování služeb | Příjem hlášení | Reakční doba (doba od nahlášení do zahájení řešení) | Maximální doba od nahlášení do odstranění závady |
| 1 – KRITICKÁ | Telefonicky HelpDesk  7:00 – 16:00  \* (9,5x5)  Telefonicky Hotline – 24x7 | Do 1 hodiny | Do 2 hodin |
| 2 – VÁŽNÁ | Telefonicky HelpDesk  7:00 – 16:00 (9,5x5)  Telefonicky Hotline – 24x7 | Do 24 hodin | Do 72 hodin |
| 3 – BĚŽNÁ | Telefonicky HelpDesk  7:00 – 16:00  Aplikace HelpDesk – 24x7 | Do 1 pracovního dne | Do 15 pracovních dnů |

\*(9,5 hodin denně v pracovní dny (PO až PÁ) – dříve a dále též jako „(9,5x5)“

Řešení závad není omezeno počtem hodin / měsíc.

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

### Řešení incidentů pro Portál pacienta

Provoz řešení je v režimu 24x7 při roční dostupnosti dle definované kategorie dostupnosti (viz kap 1.3.2.1 tohoto dokumentu - Definice kategorií dostupnosti), garantovaná podpora je uvedena v následující tabulce podle příslušné úrovně SLA.

|  |  |  |  |
| --- | --- | --- | --- |
| Úroveň poskytování služeb | Příjem hlášení | Reakční doba (doba od nahlášení do zahájení řešení) | Maximální doba od nahlášení do odstranění závady |
| 1 – KRITICKÁ | Telefonicky HelpDesk  7:00 – 16:00 (9,5x5)  Telefonicky Hotline – 24x7 | Do 24 hodin | Do 48 hodin |
| 2 – VÁŽNÁ | Telefonicky HelpDesk  7:00 – 16:00 (9,5x5)  Telefonicky Hotline – 24x7 | Do 24 hodin | Do 120 hodin |
| 3 – BĚŽNÁ | Telefonicky HelpDesk  7:00 – 16:00  Aplikace HelpDesk – 24x7 | Do 120 hodin | Do 20 pracovních dnů |

*Tabulka 2: Řešení incidentů pro Portál pacienta*

Řešení závad není omezeno počtem hodin / měsíc.

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

### Řešení incidentů pro modernizovaný modul MIS

Provoz řešení je v režimu 24x7 při roční dostupnosti dle definované kategorie dostupnosti (viz kap 1.3.2.1 tohoto dokumentu - Definice kategorií dostupnosti), garantovaná podpora je uvedena v následující tabulce podle příslušné úrovně SLA.

|  |  |  |  |
| --- | --- | --- | --- |
| Úroveň poskytování služeb | Příjem hlášení | Reakční doba (doba od nahlášení do zahájení řešení) | Maximální doba od nahlášení do odstranění závady |
| 1 – KRITICKÁ | Telefonicky HelpDesk  7:00 – 16:00 (9,5x5)  Telefonicky Hotline – 24x7 | Následující pracovní den | Do 2 pracovních dnů |
| 2 – VÁŽNÁ | Telefonicky HelpDesk  7:00 – 16:00 (9,5x5)  Telefonicky Hotline – 24x7 | Do druhého pracovní ho dne | Do 5 pracovních dnů |
| 3 – BĚŽNÁ | Telefonicky HelpDesk  7:00 – 16:00  Aplikace HelpDesk – 24x7 | Do pátého pracovního dne | Do 20 pracovních dnů |

*Tabulka 3: Řešení incidentů pro modernizovaný modul MIS*

Řešení závad není omezeno počtem hodin / měsíc.

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

### Definice kategorie incidentu

|  |  |  |
| --- | --- | --- |
| Kategorie incidentu | Závažnost incidentu | Příklad |
| Kritická - 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. * Nefunkční zpracování Výkaznictví v období vykazování. |
| Vážná - 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. |
| Běžná – 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. |

*Tabulka 4: Definice kategorie incidentu*

## 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.

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:
5. Konzultační a analytické služby zaměřené na požadovanou oblast,
6. poskytování systémových, programátorských a vývojových prací,
7. realizace požadavků na novou funkcionalitu nad rámec dodaného řešení v rámci licenční smlouvy PO (bude doplněno).

## 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 v řešení,
* soupis poskytnutých a poskytovaných Služeb spojených s uživatelskou podporou,
* soupis poskytnutých a poskytovaných Služeb na vyžádání,
* přehled splněných a nesplněných SLA.

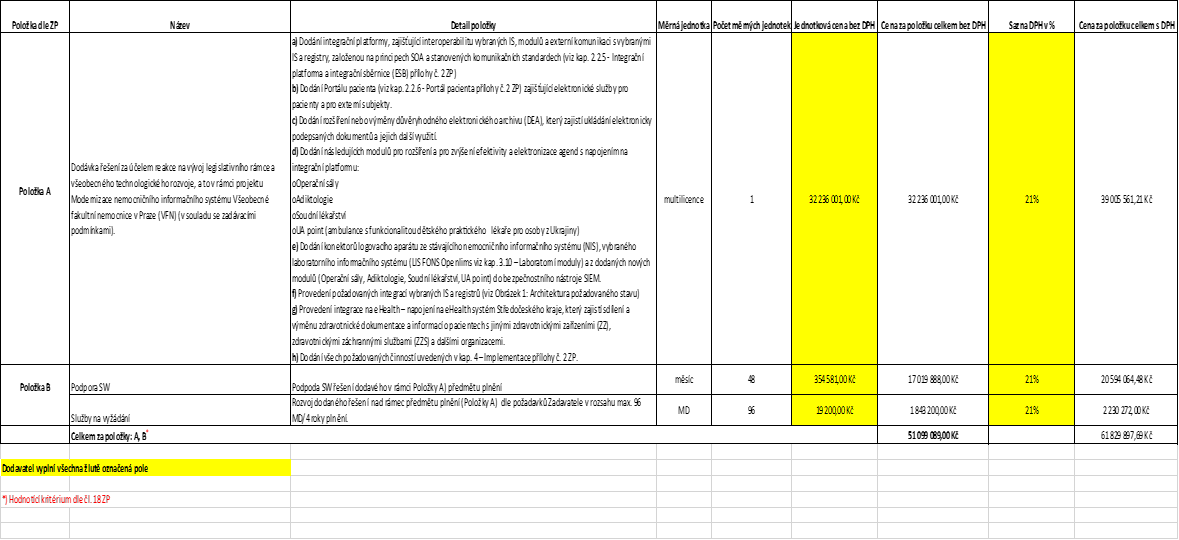
Tento report se dodavatel zavazuje poskytovat objednateli jednou měsíčně vždy za uplynulý měsíc, k poslednímu dni v měsíci. Reporting může být nahrazen on-line přístupem objednatele do HelpDesku dodavatele, pokud jsou požadované informace uvedeny u jednotlivých záznamů nebo takový reporting aplikace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

## Exitová součinnost

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

* Poskytne náležitou a nezbytnou součinnost pro takové převedení,
* poskytne veškeré nezbytné informace a dokumentaci,
* předá objednateli data způsobem a ve formátu stanoveném v Předimplementační analýze.

**Příloha č. 2 – Položkový ceník cenová kalkulace**

****

**Příloha č. 3 Smlouvy – Seznam oprávněných osob**

A. Seznam kontaktních osob poskytovatele oprávněných poskytovat podporu

|  |  |  |
| --- | --- | --- |
| **Jméno** | **Funkce** | **Telefonní číslo** |
| xxxxxx | Manažer podpory | xxxxxx |
| xxxxxx | Vedoucí oddělení HD | xxxxxx |

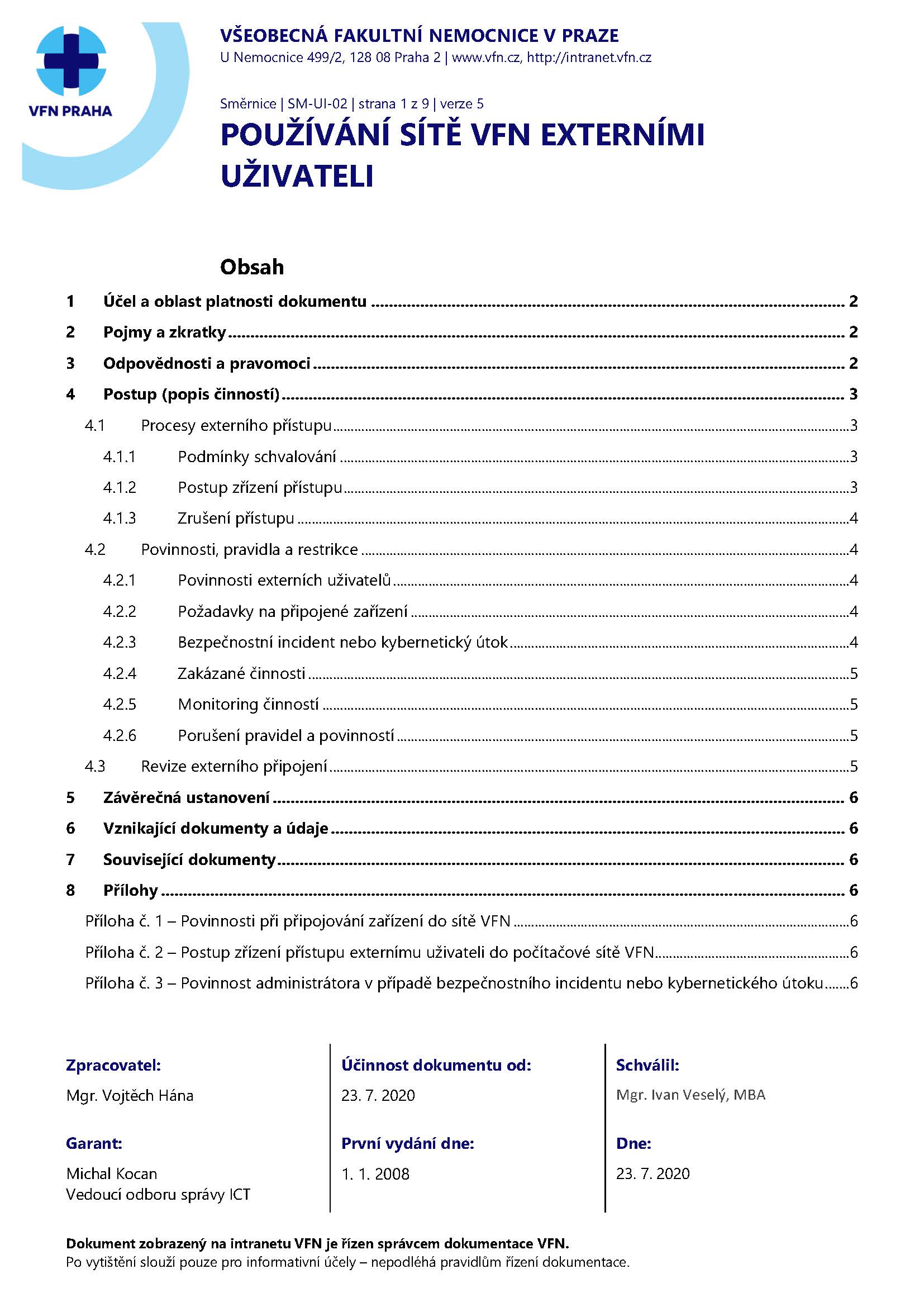
B. Seznam kontaktních osob objednatele oprávněných k hlášení požadavků na poskytování podpory

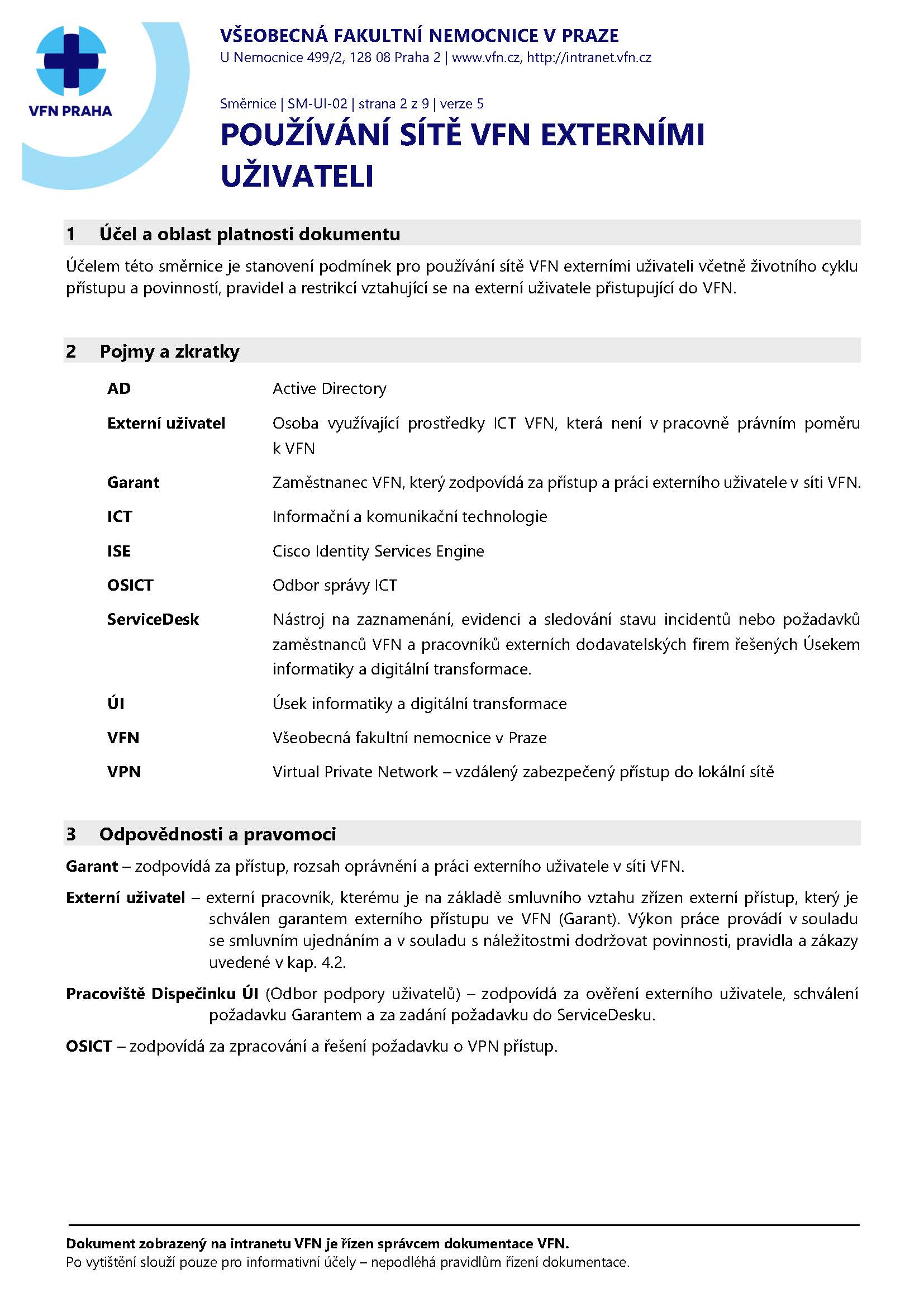
|  |  |  |
| --- | --- | --- |
| **Jméno** | **Funkce** | **Telefonní číslo** |
| Hlášení požadavků na poskytování podpory je přes Service Desk Zadavatele: xxxxxx. | | |
| xxxxxx | Vedoucí oddělení – odbor podpory uživatelů | xxxxxx |
| xxxxxx | Operátor ICT | xxxxxx |

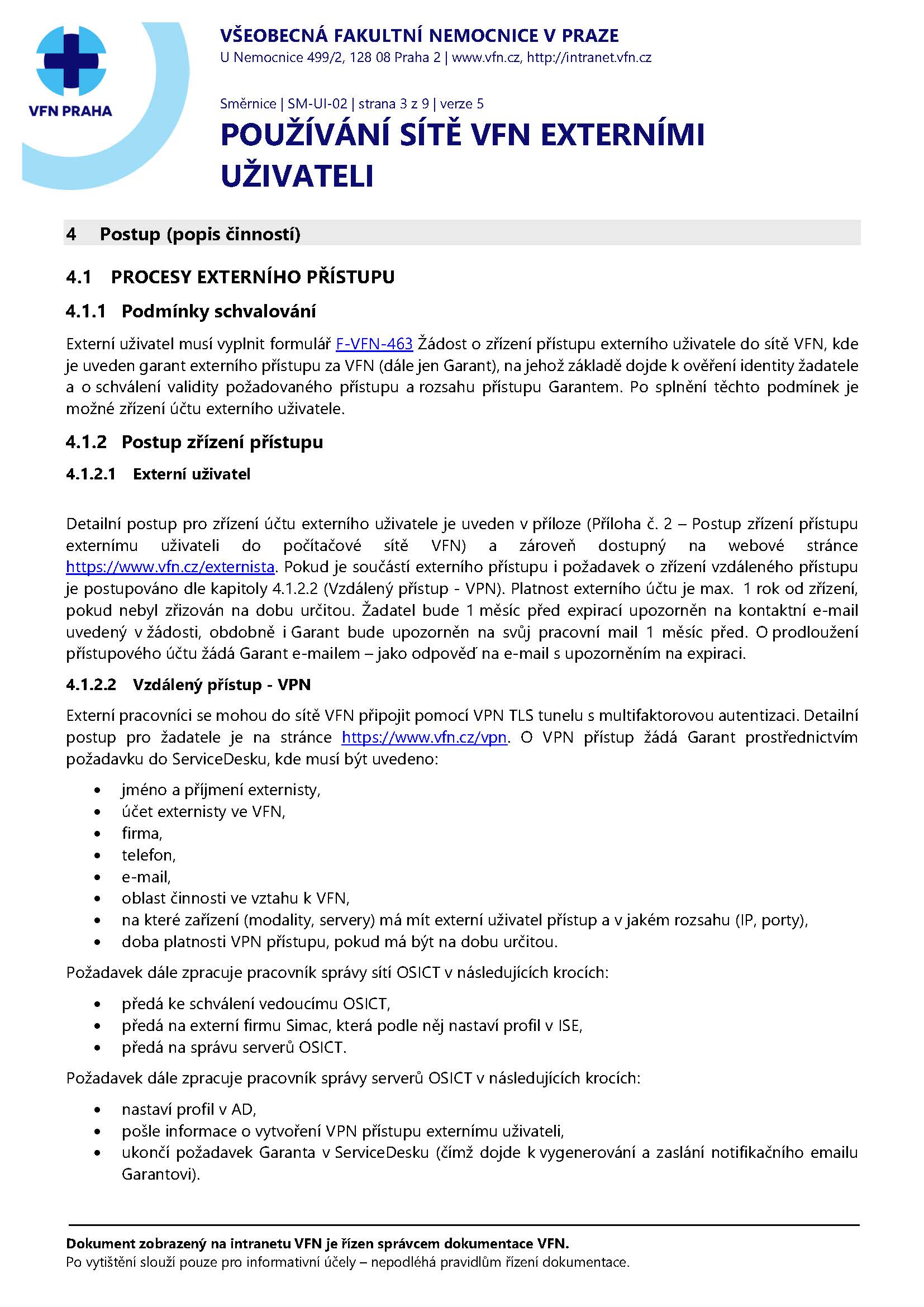
C. Seznam kontaktních osob objednatele určených k hlášení oznámení, požadavků, událostí nebo incidentů poskytovatele ve vztahu k ochraně osobních údajů nebo bezpečnosti informací nebo kybernetické bezpečnosti

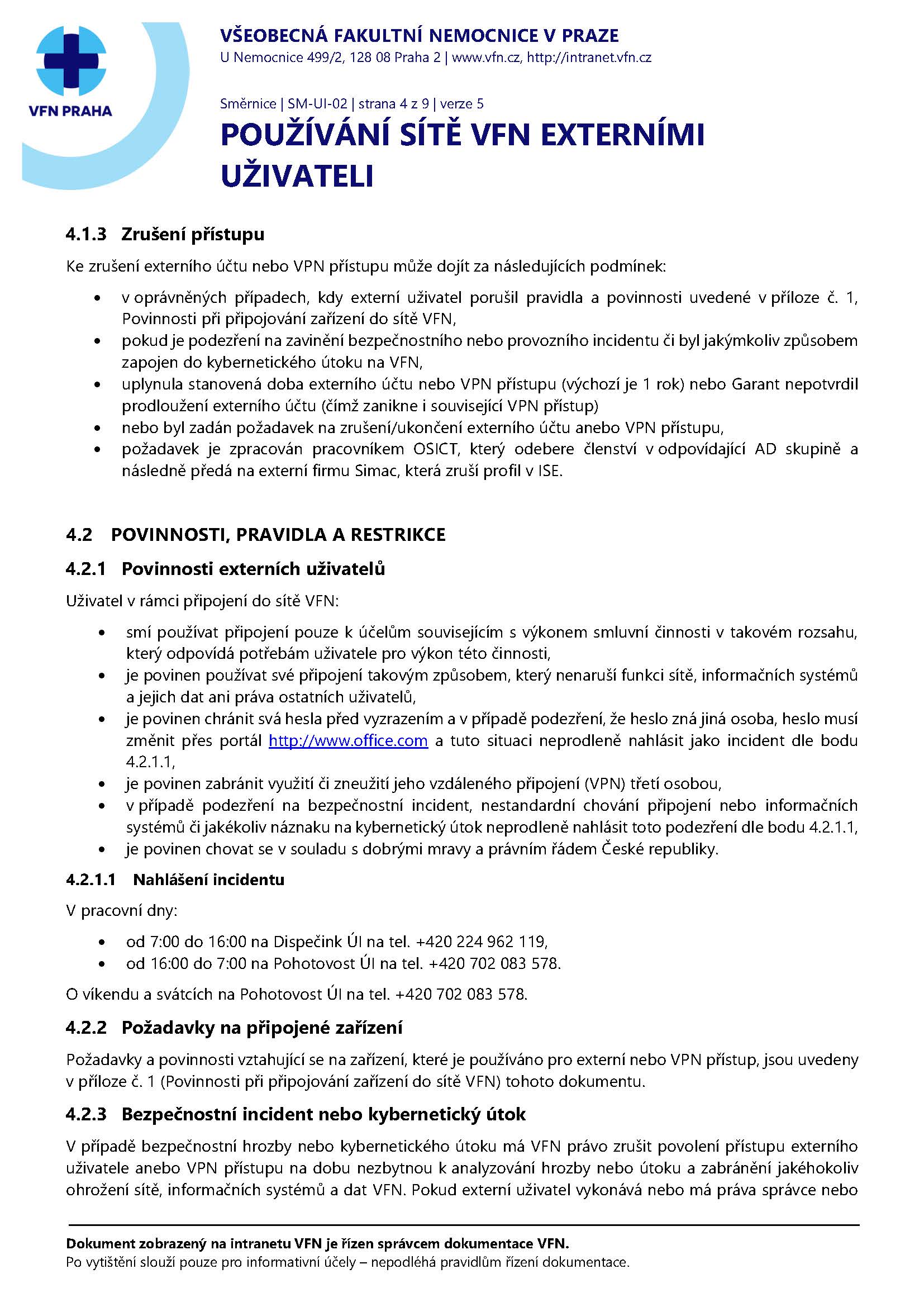
|  |  |  |
| --- | --- | --- |
| **Oblast** | **Funkce** | **Kontakt** |
| Ochrana osobních údajů | Pověřenec pro ochranu osobních údajů | xxxxxx |
| Bezpečnosti informací, kybernetické bezpečnost | Manažer bezpečnosti informací / kybernetické bezpečnosti | xxxxxx |

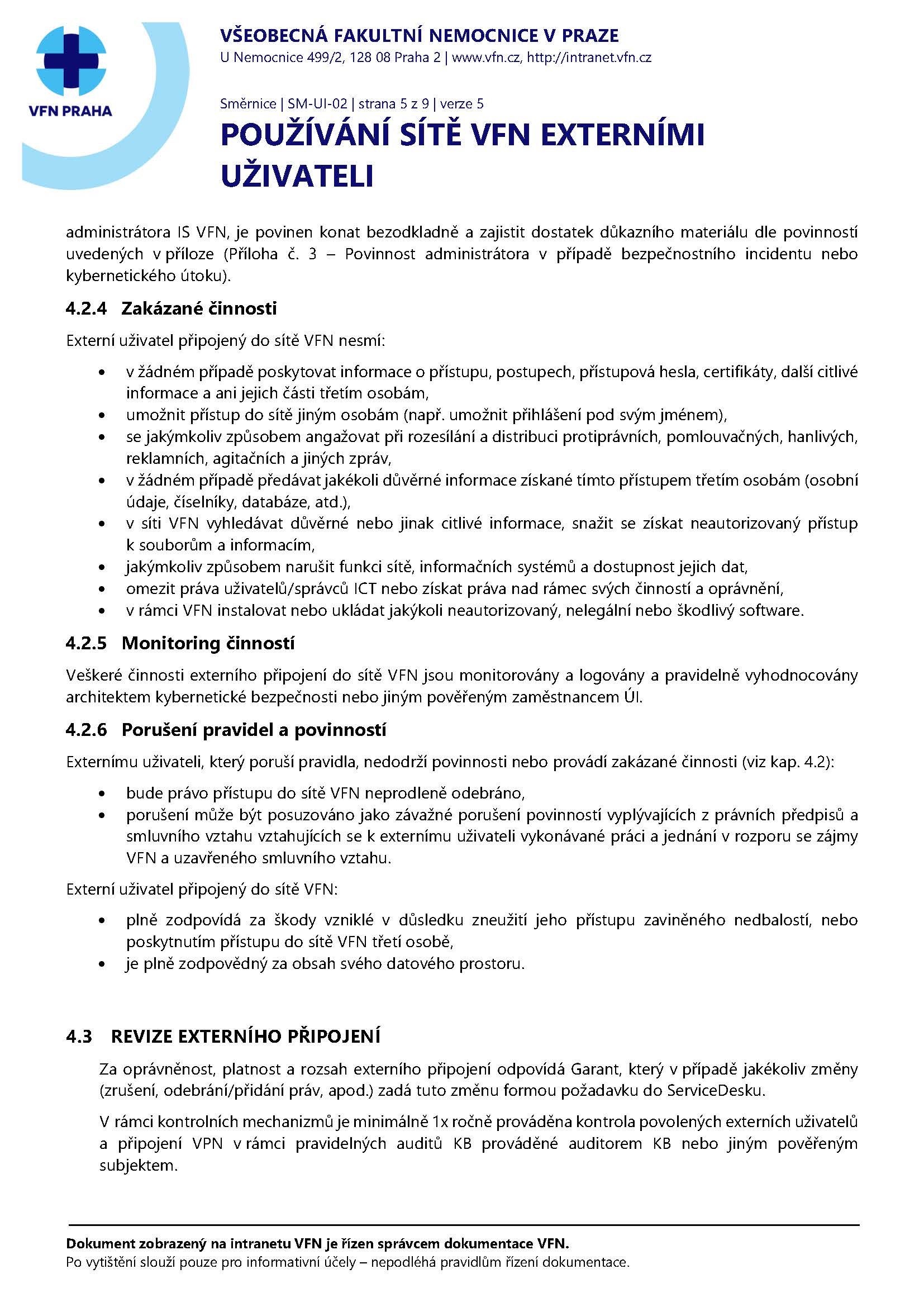
**Příloha č. 4 – Používání sítě VFN externími uživateli**

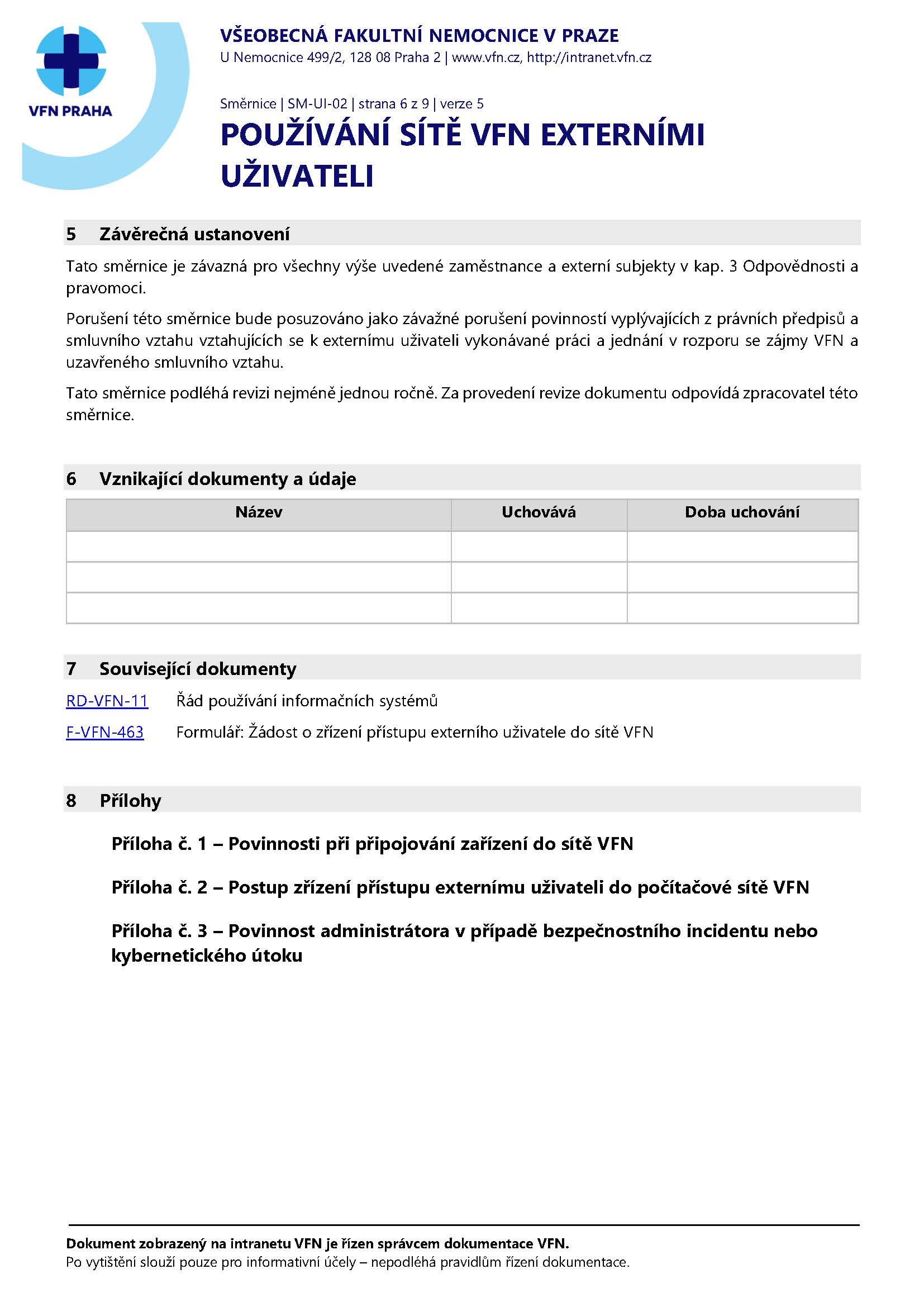


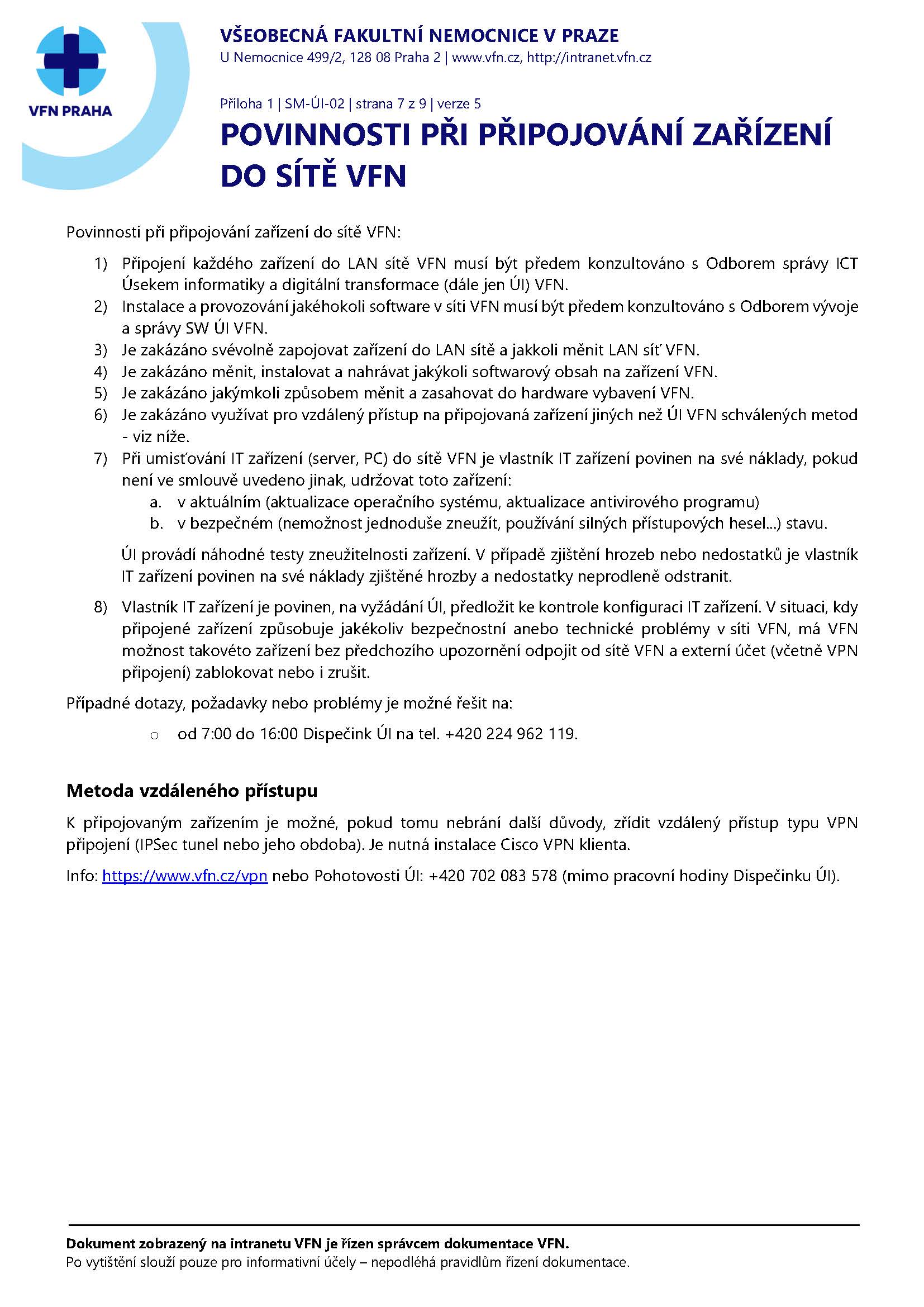


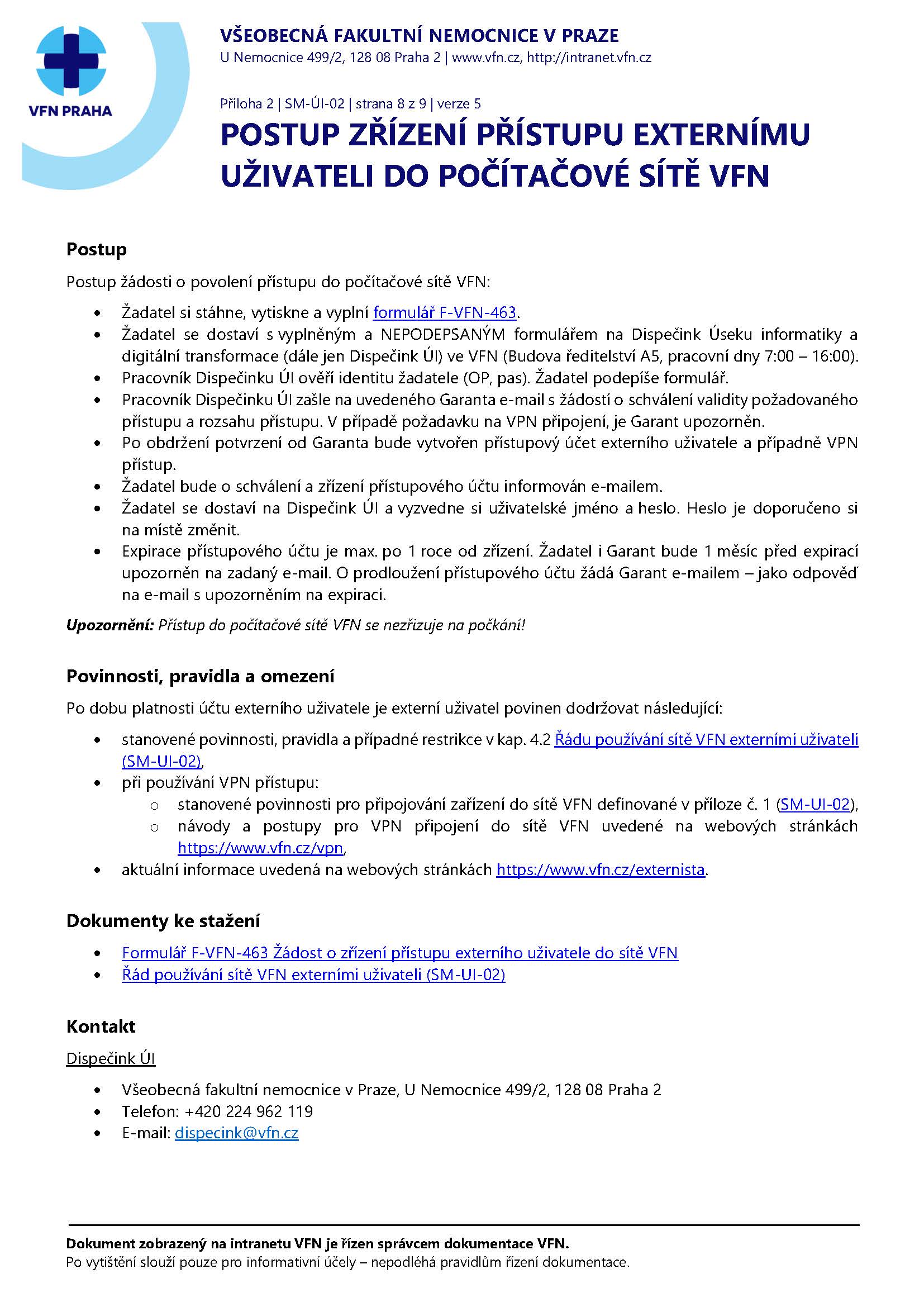


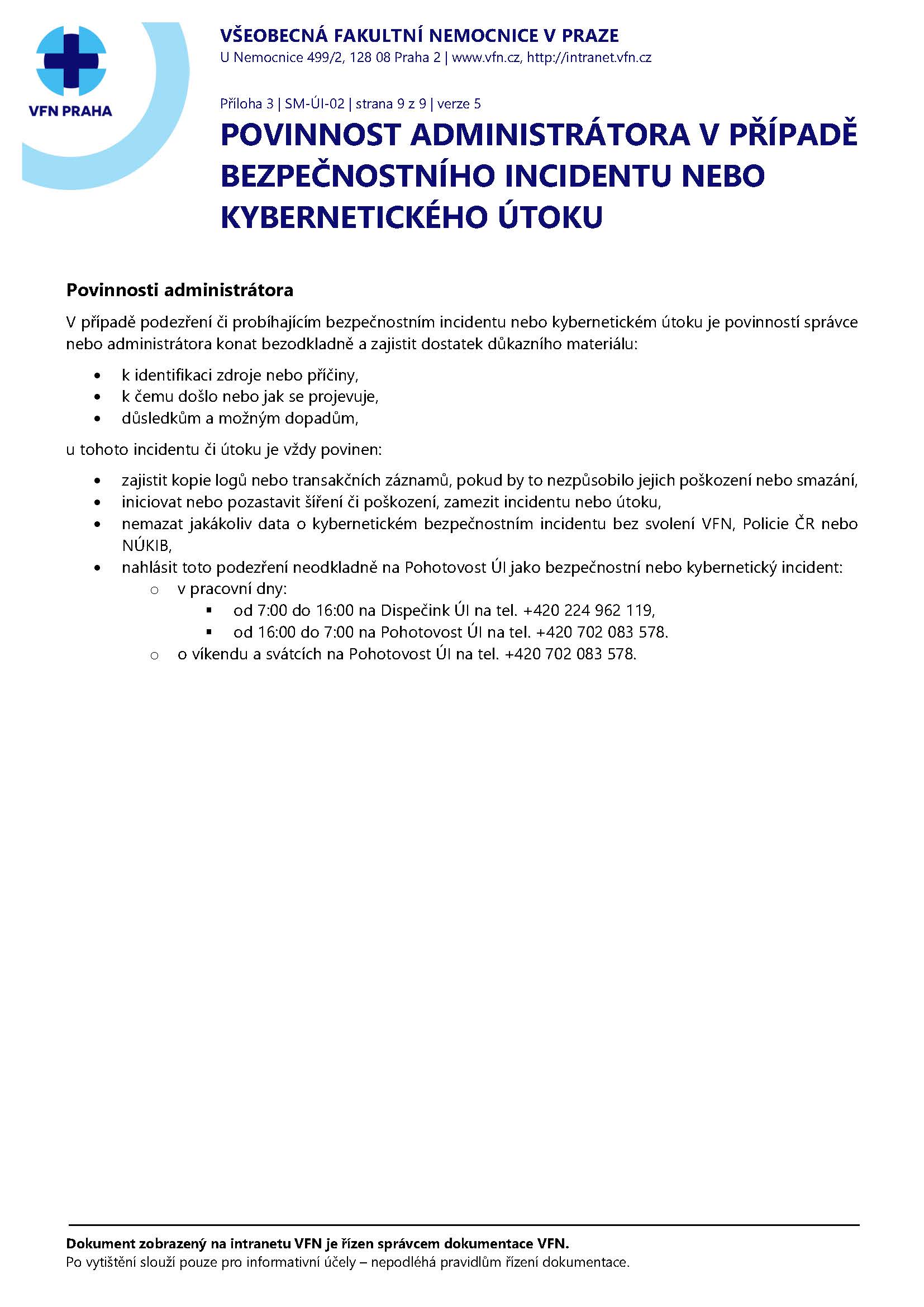












**Příloha č. 5 - Požadavky systému řízení bezpečnosti informací na Dodavatele**

# Účel

Účelem toho dokumentu je stanovit požadavky vyplývající ze systému řízení bezpečnosti informací ve VFN pro Dodavatele jako provozovatele, Poskytovatele služeb nebo zajištující podporu základních služeb: zdravotních služeb dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen ZKB).

Příloha vymezuje obecná pravidla a zásady kybernetické bezpečnosti vztahující se na smluvní plnění Dodavatele, pokud nejsou detailně specifikovány Smlouvou. Tato příloha nerozšiřuje předmět plnění Dodavatele vymezený smlouvou, ale pouze specifikuje relevantní požadavky systému řízení bezpečnosti informací ve VFN, které musí Dodavatel při plnění dodržovat.

Dodavatel je povinen prokazatelně seznámit všechny své zainteresované zaměstnance s obsahem tohoto dokumentu.

1. **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.

* 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.
  1. **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.
  1. **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.
  1. **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.
  1. **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.).
  1. **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](https://www.vfn.cz/externista/)“, zde uvedených povinností a směrnice Používání sítě VFN externími uživateli ([SM-UI-02](https://www.vfn.cz/files/ext-vpn/SM-UI-02.pdf)). 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.
  1. **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.

* 1. **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.
  1. **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.
  1. **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.
  1. **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.
  1. **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.
  1. **Akvizice, vývoj a údržba informačních systémů**

Dodavatel je povinen:

* dodržovat bezpečnostní pravidla, noremy a best practices (např. OWASP - Open Web Application Security Project) v rámci celého životního cyklu nákupu a vývoje SW od zadání, návrhu, přes vývoj a testování až po nasazení do provozu,
* zavést oddělení rolí vývoje, testu a provozu; vytvářet a provozovat vývojové, integrační, testovací a provozní prostředí tak, aby byla zcela oddělena v sítích a byla podporována oddělenými stroji,
* zohlednit bezpečnostní požadavky VFN na dodávaný nebo vyvíjený SW, a to především:
  + podporované frameworky a platformy v prostředí VFN,
  + nefunkční bezpečnostní požadavky,
  + provádět ověření codereview v jednotlivých fázích vývoje a testování,
  + spolupracovat na bezpečnostním testování včetně penetračních testů,
  + dodávat systémové a provozní bezpečnostní dokumentace,
* stanovit způsob převzetí, akceptace a instalaci do produkčního prostředí,
* používat jasný a specifikovaný proces řízení změn.
  1. **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.
  1. **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).
  1. **Legislativní a normativní požadavky**

Dodavatel je povinen splnit legislativní a normativní požadavky:

* zákon č. 181/2014 Sb., o kybernetické bezpečnosti a vyhlášku č. 82/2018Sb., o kybernetické bezpečnosti,
* nařízení EU č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR),
* zákon č. 110/2019 Sb., zpracování osobních údajů,
* směrnici EU č. 2016/1148, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů (NIS),
* nařízení EU č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (eIDAS),
* standardy systému řízení bezpečnosti řady ISO/IEC 27000 – Information Security Management System (ISMS), především ISO/IEC 27001, ISO/IEC 27002 a ISO/IEC 27799,
* a související normy nebo best-practice.
  1. **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.

* 1. **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.