

## LICENČNÍ SMLOUVA

### Simac Technik ČR, a.s.

zapsána v obchodním rejstříku vedeném Městským soudem v Praze oddíl B, vložka 3190

se sídlem: Radlická 740/113c, 158 00, Praha 5

zastoupena: Ing. Martin Jireček – předseda představenstva

Ing. Tomáš Kudělka – místopředseda představenstva

Ing. Jaroslav Štefl – místopředseda představenstva

Ing. Ivo Němeček – člen představenstva

Ing. Daniel Merhaut – člen představenstva

za společnost jednají dva členové představenstva společně, z nichž jeden je vždy předseda nebo místopředseda představenstva

IČO: 630 79 496 DIČ: CZ63079496

bankovní spojení: ČSOB

číslo účtu: 8010-616133653/0300

jako **poskytovatel** na straně jedné (dále jen „poskytovatel“ nebo „dodavatel“)

a

### Všeobecná fakultní nemocnice v Praze

se sídlem: U Nemocnice 499/2, 128 08 Praha 2

IČ: 000 64 165 DIČ: CZ00064165

zastoupena: prof. MUDr. Davidem Feltlem, Ph.D., MBA, ředitelem

bankovní spojení: ČNB

číslo účtu: 24035021/0710

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

Poskytovatel a objednatel společně též jako „smluvní strany“

uzavírají dnešního dne na základě výsledku **veřejné zakázky malého rozsahu** s názvem „**Zajištění podpory a licencí pro Cisco produkty – předplatné bezpečnostního řešení**“, zadávané na elektronickém tržišti Tendermarket pod systémovým číslem T004/25V/00007065 v otevřeném řízení (dále jen „veřejná zakázka“), v souladu s ustanovením § 1746 odst. 2. zákona č. 89/2012 Sb., občanský zákoník, v platném znění, (dále jen „občanský zákoník“), tuto

### smlouvu o zajištění podpory a licencí pro Cisco produkty (dále jen „smlouva“)

#### I. Předmět smlouvy

1. Předmětem plnění smlouvy je zajištění předplatného bezpečnostního řešení, tzn. zajištění podpory a licencí pro Cisco produkty (dále jen „bezpečnostní řešení“ nebo „předmět plnění“). Bližší specifikace předmětu plnění je uvedena v příloze č. 1 této smlouvy.
2. Poskytovatel prohlašuje, že je certifikovaným partnerem společnosti Cisco Systems (Czech Republic) s.r.o. (dále také „Cisco“). Objednatel se zavazuje uhradit poskytovateli sjednanou odměnu, jakož i další závazky vyplývající z této smlouvy.
3. V případě provedení úprav (patches), aktualizací (updates), vylepšení (upgrades) či jiných změn bezpečnostního řešení, které je předmětem smlouvy ze strany poskytovatele, je licence poskytnuta i k takto změněnému řešení.
4. Poskytovatel bere na vědomí, že dle zákona č. 264/2025 Sb., o kybernetické bezpečnosti jsou (dále jen „nový ZKB“) dodávané služby podpory výrobce poskytované na systémy a technologie nezbytné pro zajištění základní služby: Poskytování zdravotních služeb dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „ZKB“), a orgán nebo osoba (poskytovatel) poskytující služby podpory se stává provozovatelem základní služby podle § 3 písm. f) ZKB.
5. Poskytovatel se zavazuje, že bude poskytovat služby s vynaložením veškeré odborné péče, že bude dodržovat obecně závazné předpisy a vnitřní předpisy objednatele:
  - Používání sítě VFN externími uživateli (SM-UI-02) uvedený v příloze č. 3 této smlouvy, které mu byly objednatelem poskytnuty, a se kterými byl prokazatelným způsobem seznámen před podpisem této smlouvy.
6. Veškeré činnosti při realizaci předmětu plnění je poskytovatel povinen provádět osobami, které mají odpovídající kvalifikaci. Odpovědnou osobou ve věci plnění této smlouvy je za poskytovatele xxxxx, tel.: xxxxx, email: xxxxx a za objednatele xxxxx, tel.: xxxxx, email: xxxxx.

## II. Způsob poskytování podpory, záruky

1. Poskytovatel se zavazuje zajistit licence a podporu Cisco produktům specifikovaných v článku I. a příloze č. 1 této smlouvy po období, které je uvedené u jednotlivých položek v příloze č. 1 této smlouvy.
2. Základní formou podpory je přímý přístup k webovému portálu Cisco, popřípadě služba Hot-Line na tel. čísle: xxxxx, e-mail: xxxxx nebo elektronický systém poskytovatele v režimu 24x7 (dále jen „Helpdesk“), dostupný prostřednictvím webového přístupu na adrese <https://hd.simac.cz>. Součástí Helpdesku je popis procesu zpracování požadavku.
3. Objednatel si nárokuje zahájení činností vedoucích k odstranění vad bezpečnostního řešení do 4 hodin v režimu 24x7 od nahlášení vady objednatelem poskytovateli na Hot-line poskytovatele s následným písemným potvrzením na Helpdesk poskytovatele, popř. přímo na webový portál společnosti Cisco.
4. Poskytovatel se zavazuje k vyřešení závady nejpozději do 48 hodin od nahlášení vady objednatelem poskytovateli na Hot-line poskytovatele tel: xxxxx, s následným písemným potvrzením na Helpdesk poskytovatele: xxxxx.
5. V rámci podpory je:
  - bezplatná výměna dílů dotčených síťových prvků v místě plnění,
  - spolupráce techniků poskytovatele s IT specialisty objednatele při řešení provozních problémů,
  - pomoc při diagnostice a řešení HW problémů.
6. Případné změny v konfiguraci dotčených síťových prvků či licencí je možno provádět jen se souhlasem obou smluvních stran.
7. Poskytovatel zajistí přímý přístup a možnost stažení aktuálního software, update software, anebo firmware přímo z oficiálních zdrojů výrobce.
8. Poskytovatel se zavazuje, že po dobu platnosti této smlouvy minimálně dva jeho pracovníci mají certifikaci minimálně na úrovni CCNP.
9. Platnost a rozsah podpory lze zkontrolovat na příslušném webovém portálu Cisco po přihlášení se již existujícím účtem objednatele.
10. Technologie objednatele jsou umístěny v sídle objednatele na adrese: Všeobecná fakultní nemocnice v Praze, **U Nemocnice 499/2, 128 08 Praha 2**.
11. Podpora se nevztahuje na poruchy, které byly způsobeny neodbornou obsluhou a údržbou, živelnou pohromou, nedodržením návodu od výrobce, nedodržením provozních podmínek nebo jiným způsobem než obvyklým provozem.
12. Po dobu podpory je objednatel povinen využívat dodané licence dle pokynů poskytovatele, popřípadě dle pokynů Cisco, výlučně v souladu s jejich určením a příslušnými technickými podmínkami. Případná technická zlepšení nebo úpravy může objednatel vykonat jen na základě písemného souhlasu poskytovatele.
13. Veškeré poskytované služby nesmí být provozované na technických nebo programových prostředcích označených Národním centrem kybernetické bezpečnosti za hrozbu (provozovaný NÚKIB). Poskytovatel služeb a jeho poddodavatel nebo výrobce technického nebo programového prostředku nesmí být z území či oblastí označených Národním centrem kybernetické bezpečnosti za hrozbu.  
V případě porušení této povinnosti je objednatel oprávněn od smlouvy odstoupit.
14. Poskytovatel je povinen neprodleně informovat objednatele prostřednictvím poskytovatelem určené odpovědné osoby: Manažera kybernetické bezpečnosti, e-mail: xxxxx, o kybernetických bezpečnostních incidentech souvisejících s poskytováním služeb podpory.
15. Poskytovatel je povinen objednatele informovat prostřednictvím Manažera kybernetické bezpečnosti o způsobu řízení rizik na straně poskytovatele a o zbytkových rizicích souvisejících s plněním smlouvy v ročním intervalu nebo v případě zjištění nových rizik nebo změn stávajících rizik informuje bezodkladně.
16. Poskytovatel je povinen objednatele informovat prostřednictvím Manažera kybernetické bezpečnosti o významné změně tohoto poskytovatele 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, využívaných tímto poskytovatelem služeb podpory.
17. Poskytovatel se zavazuje splňovat/dodržet relevantní požadavky na řízení bezpečnosti informací uvedené v příloze č. 4 této smlouvy „Požadavky systému řízení bezpečnosti informací na dodavatele“ vztahující se na prostředí a činnosti poskytovatele.
18. Oprávněné osoby objednatele a poskytovatele, které mohou pracovat s Helpdeskem objednatele jsou uvedeny v příloze č. 2 smlouvy.

## III. Cena a platební podmínky

1. Cena za předmět plnění byla sjednána ve výši:  
**Celková cena bez DPH 2 144 415,13 Kč**

**DPH 450 327,17 Kč****Cena vč. DPH 2 594 742,30 Kč (dále jen „cena“)**

Celková cena je stanovena jako konečná a zahrnuje cenu za celý předmět plnění a veškeré náklady dodavatele na plnění dle této smlouvy.

- Objednatel nebude poskytovat zálohy.
- Cena za předmět plnění dle této smlouvy bude uhrazena jednorázově po dodání celého předmětu plnění, tzn. po zajištění aktivace celého předmětu plnění (všech licencí a podpory) u výrobce, na základě faktury vystavené poskytovatelem.
- Objednatel se zavazuje zaplatit cenu na základě faktury vystavené dodavatelem do 14 dnů po řádném předání a převzetí celého předmětu plnění specifikovaného v čl. I. smlouvy. Daňový doklad (faktura) bude poskytovatelem vystaven, v souladu s ustanovením § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty ve znění pozdějších předpisů. Splatnost faktury činí 60 dnů od jejího doručení objednateli. Faktura bude zaslána elektronicky ve formátu PDF na e-mailovou adresu: xxxxx. K faktuře bude přiložena kopie potvrzení od výrobce Cisco o zakoupení a aktivaci předmětu plnění pro objednatele dle této smlouvy.
- Pokud faktura nebude obsahovat všechny zákonem a touto smlouvou stanovené náležitosti, je objednatel oprávněn ji do 15 dnů od doručení vrátit poskytovateli s tím, že poskytovatel je poté povinen vystavit novou fakturu s novým termínem splatnosti. V takovém případě objednatel není v prodlení s úhradou faktury.
- Platba proběhne výhradně v CZK (česká koruna) a rovněž veškeré cenové údaje budou uváděny v této měně.
- Faktura se platí bankovním převodem na účet druhé smluvní strany uvedený na faktuře. Povinnost objednatele zaplatit poskytovateli vyúčtovanou stanovenou cenu je splněna dnem odeslání platby z bankovního účtu objednatele.

**IV. Odstoupení od smlouvy**

- Kterákoliv ze smluvních stran je oprávněna od této smlouvy odstoupit v případě jejího podstatného porušení druhou smluvní stranou. Pro účely této smlouvy se za podstatné porušení smluvních povinností považuje takové porušení, u kterého strana porušující smlouvu měla nebo mohla předpokládat, že při takovémto porušení smlouvy, s přihlédnutím ke všem okolnostem, by druhá smluvní strana neměla zájem smlouvu uzavřít, zejména:
  - na straně objednatele nezaplacení ceny plnění podle této smlouvy ve lhůtě delší 60 dní po dni splatnosti příslušné faktury,
  - na straně poskytovatele, jestliže nedodá řádně a včas předmět plnění a pokud nezjednal nápravu, přestože byl objednatelem na neplnění této smlouvy písemně upozorněn.
- Odstoupení od smlouvy musí být provedeno písemným oznámením o odstoupení, které musí obsahovat důvod odstoupení a musí být doručeno druhé smluvní straně. Účinky odstoupení nastanou okamžikem doručení písemného vyhotovení odstoupení druhé smluvní straně.

**V. Smluvní pokuty, sankce**

- 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 od 31. dne od sjednané lhůty splatnosti.
- Poskytovatel je v případě nedodržení termínu plnění dle čl. II. odst. 1 této smlouvy povinen uhradit objednateli smluvní pokutu ve výši 0,1 % z celkové ceny za předmět plnění dle této smlouvy za každý i započatý den prodlení, jestliže se s objednatelem nedohodne jinak. Objednatel je dále v těchto případech oprávněn odstoupit od smlouvy.
- V případě nedodržení povinnosti stanovené v čl. VII. odst. 2 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.
- V případě nedodržení povinnosti poskytovatele dle čl. VII. odst. 5 - 7 této smlouvy, má objednatel právo účtovat poskytovateli smluvní pokutu ve výši 10.000,- Kč za každé jednotlivé porušení povinnosti.
- V případě nedodržení povinností poskytovatele dle čl. II. odst. 13 - 17 a dle čl. VI. této smlouvy, má objednatel právo účtovat poskytovateli smluvní pokutu ve výši 100.000,- Kč za každé jednotlivé porušení povinnosti.
- Smluvní pokuta bude vyúčtována samostatným daňovým dokladem a její splatnost činí 30 dní ode dne doručení daňového dokladu. Zaplacením smluvní pokuty není dotčeno právo na náhradu škody vzniklé smluvní straně požadující zaplacení smluvní pokuty.

**VI. Mlčenlivost**

- 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 zpracování 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 poučení 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 první 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. VI., 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**“).

## VII. Ostatní ujednání

1. Poskytovatel bere na vědomí, že objednatel je povinen dle zákona č. 340/2015 Sb., o registru smluv, uveřejnit tuto smlouvu včetně případných dodatků zákonem stanoveným způsobem.
2. Poskytovatel je oprávněn postoupit pohledávku vyplývající z plnění dle této smlouvy na třetí osobu pouze s předchozím písemným souhlasem objednatele.
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. 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 10.000.000,- Kč.
6. 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.
7. Poskytovatel se zavazuje, že při poskytování předmětu plnění této smlouvy, nedojde k žádnému porušení licenčních podmínek výrobce Cisco nebo objednatele.

### VIII. 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. 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.
4. Autentičnost této smlouvy potvrzují smluvní strany svými podpisy.

V Praze dne dle el. podpisu:

V Praze dne dle el podpisu:

-----  
prof. MUDr. David Feltl, Ph.D., MBA  
ředitel

-----  
Simac Technik ČR, a.s.

#### Přílohy:

- Příloha č. 1 – Položkový ceník – Cenová kalkulace  
Příloha č. 2 – Seznam oprávněných osob  
Příloha č. 3 – Používání sítě VFN externími uživateli  
Příloha č. 4 – Požadavky systému řízení bezpečnosti informací na poskytovatele

## Příloha č. 1 Položkový ceník – cenová kalkulace

| Položka číslo | Název položky     | Popis položky                                                | Délka požadovaného prodloužení podpory/licence |            | Počet | Jednotková cena bez DPH (Kč) | Celková cena bez DPH (Kč) |
|---------------|-------------------|--------------------------------------------------------------|------------------------------------------------|------------|-------|------------------------------|---------------------------|
|               |                   |                                                              | OD                                             | DO         |       |                              |                           |
| 1             | L-FPR4110T-TMC=   | Cisco FPR4110 Threat Defense Threat, Malware and URL License | 26.11.2025                                     | 25.11.2026 | 2     | 144 306,24 Kč                | 288 612,48 Kč             |
| 2             | L-FPR4110T-TMC-1Y | Cisco FPR4110 Threat Defense Threat, Malware and URL 1Y Subs | 26.11.2025                                     | 25.11.2026 | 2     | 746 462,77 Kč                | 1 492 925,54 Kč           |
| 3             | L-AC-PLS-LIC=     | Cisco AnyConnect Plus Term License, Total Authorized Users   | 25.10.2025                                     | 24.10.2026 | 200   | 0,58 Kč                      | 116,00 Kč                 |
| 4             | L-AC-PLS-1Y-S2    | Cisco AnyConnect Plus License, 1YR, 100-249 Users            | 25.10.2025                                     | 24.10.2026 | 200   | 68,36 Kč                     | 13 672,00 Kč              |
| 5             | C9200CX-DNA-E-8   | C9200CX Cisco DNA Essentials, 8-Port Term Licenses           | 13.09.2025                                     | 31.12.2026 | 14    | 278,15 Kč                    | 3 894,10 Kč               |
| 6             | C9300L-DNA-E-24   | C9300L Cisco DNA Essentials, 24-port license                 | 01.01.2026                                     | 31.12.2026 | 1     | 591,76 Kč                    | 591,76 Kč                 |
| 7             | C9300-DNA-E-24    | C9300 DNA Essentials, 24-Port Term Licenses                  | 01.01.2026                                     | 31.12.2026 | 4     | 591,76 Kč                    | 2 367,04 Kč               |
| 8             | C9300X-DNA-24Y-E  | C9300 DNA Essentials, Term License                           | 13.09.2025                                     | 31.12.2026 | 1     | 770,14 Kč                    | 770,14 Kč                 |
| 9             | C9200-DNA-E-48    | C9200 Cisco DNA Essentials, 48-Port Term Licenses            | 01.01.2026                                     | 31.12.2026 | 60    | 1 232,82 Kč                  | 73 969,20 Kč              |
| 10            | C9200-DNA-E-24    | C9200 Cisco DNA Essentials, 24-Port Term Licenses            | 01.01.2026                                     | 31.12.2026 | 4     | 673,95 Kč                    | 2 695,80 Kč               |
| 11            | C9200-DNA-E-48    | C9200 Cisco DNA Essentials, 48-Port Term Licenses            | 01.01.2026                                     | 31.12.2026 | 8     | 1 232,83 Kč                  | 9 862,64 Kč               |
| 12            | C9300-DNA-E-24    | C9300 DNA Essentials, 24-Port Term Licenses                  | 13.09.2025                                     | 31.12.2026 | 1     | 770,14 Kč                    | 770,14 Kč                 |
| 13            | C9200-DNA-E-48    | C9200 Cisco DNA Essentials, 48-Port Term Licenses            | 13.09.2025                                     | 31.12.2026 | 10    | 1 604,32 Kč                  | 16 043,20 Kč              |
| 14            | C9200-DNA-E-24    | C9200 Cisco DNA Essentials, 24-Port Term Licenses            | 01.01.2026                                     | 31.12.2026 | 8     | 673,94 Kč                    | 5 391,52 Kč               |
| 15            | C9200-DNA-E-48    | C9200 Cisco DNA Essentials, 48-Port Term Licenses            | 01.01.2026                                     | 31.12.2026 | 30    | 1 232,82 Kč                  | 36 984,60 Kč              |
| 16            | C9300-DNA-E-24    | C9300 DNA Essentials, 24-Port Term Licenses                  | 13.09.2025                                     | 31.12.2026 | 1     | 770,14 Kč                    | 770,14 Kč                 |
| 17            | C9300-DNA-E-48    | C9300 DNA Essentials, 48-Port Term Licenses                  | 01.01.2026                                     | 31.12.2026 | 3     | 1 084,89 Kč                  | 3 254,67 Kč               |
| 18            | C9200-DNA-E-24    | C9200 Cisco DNA Essentials, 24-Port Term Licenses            | 01.01.2026                                     | 31.12.2026 | 39    | 673,94 Kč                    | 26 283,66 Kč              |
| 19            | C9300L-DNA-E-48   | C9300L Cisco DNA Essentials, 48-port license                 | 13.09.2025                                     | 31.12.2026 | 1     | 1 411,78 Kč                  | 1 411,78 Kč               |
| 20            | C9200-DNA-E-48    | C9200 Cisco DNA Essentials, 48-Port Term Licenses            | 13.09.2025                                     | 31.12.2026 | 4     | 1 604,32 Kč                  | 6 417,28 Kč               |
| 21            | C9300-DNA-E-24    | C9300 DNA Essentials, 24-Port Term Licenses                  | 01.01.2026                                     | 31.12.2026 | 7     | 591,76 Kč                    | 4 142,32 Kč               |
| 22            | C9300-DNA-E-48    | C9300 DNA Essentials, 48-Port Term Licenses                  | 01.01.2026                                     | 31.12.2026 | 12    | 1 084,89 Kč                  | 13 018,68 Kč              |
| 23            | C9200-DNA-E-24    | C9200 Cisco DNA Essentials, 24-Port Term Licenses            | 13.09.2025                                     | 31.12.2026 | 4     | 877,06 Kč                    | 3 508,24 Kč               |
| 24            | C9200-DNA-E-48    | C9200 Cisco DNA Essentials, 48-Port Term Licenses            | 13.09.2025                                     | 31.12.2026 | 31    | 1 604,32 Kč                  | 49 733,92 Kč              |
| 25            | C9200-DNA-E-24    | C9200 Cisco DNA Essentials, 24-Port Term Licenses            | 13.09.2025                                     | 31.12.2026 | 4     | 877,06 Kč                    | 3 508,24 Kč               |
| 26            | C9300X-DNA-12Y-E  | C9300 DNA Essentials, Term License                           | 13.09.2025                                     | 31.12.2026 | 1     | 770,14 Kč                    | 770,14 Kč                 |
| 27            | C9500-DNA-24Y4C-A | C9500 DNA Advantage, Term License                            | 13.09.2025                                     | 31.12.2026 | 4     | 8 941,66 Kč                  | 35 766,64 Kč              |
| 28            | C9300L-DNA-E-24   | C9300L Cisco DNA Essentials, 24-port license                 | 01.01.2026                                     | 31.12.2026 | 2     | 591,76 Kč                    | 1 183,52 Kč               |
| 29            | C9300-DNA-E-48    | C9300 DNA Essentials, 48-Port Term Licenses                  | 13.09.2025                                     | 31.12.2026 | 4     | 1 411,78 Kč                  | 5 647,12 Kč               |
| 30            | C9300L-DNA-E-48   | C9300L Cisco DNA Essentials, 48-port license                 | 01.01.2026                                     | 31.12.2026 | 4     | 1 084,89 Kč                  | 4 339,56 Kč               |
| 31            | C9400-DNA-A       | Cisco Catalyst 9400 DNA Advantage Term License               | 13.09.2025                                     | 31.12.2026 | 2     | 16 171,95 Kč                 | 32 343,90 Kč              |
| 32            | C9300L-DNA-A-48   | C9300L Cisco DNA Advantage, 48-port license                  | 01.01.2026                                     | 31.12.2026 | 1     | 3 649,16 Kč                  | 3 649,16 Kč               |
|               |                   |                                                              |                                                |            |       |                              | <b>2 144 415,13 Kč</b>    |

Dodavatel stanoví nabídkovou cenu vyplněním této přílohy (dodavatel doplní žlutě zvýrazněné buňky). Vyplněný položkový ceník dodavatel předloží jako přílohu č. 1 smlouvy.

**Příloha č. 2** Seznam oprávněných osob

## A. Seznam kontaktních osob poskytovatele

| <b>Jméno</b> | <b>Funkce</b>   | <b>Telefonní číslo</b> |
|--------------|-----------------|------------------------|
| xxxxx        | Account manager | xxxxx                  |
|              |                 |                        |

## B. Seznam kontaktních osob objednatele

| <b>Jméno</b> | <b>Funkce</b>                | <b>Telefonní číslo</b> | <b>e-mail</b> |
|--------------|------------------------------|------------------------|---------------|
| xxxxx        | Vedoucí odboru provozu IT    | xxxxx                  | xxxxx         |
| xxxxx        | Vedoucí oddělení správy sítí | xxxxx                  | 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

| <b>Oblast</b>                                     | <b>Funkce</b>                        | <b>Kontakt</b> |
|---------------------------------------------------|--------------------------------------|----------------|
| Ochrana osobních údajů                            | Pověřenec pro ochranu osobních údajů | xxxxx          |
| Bezpečnosti informací,<br>kybernetické bezpečnost | Manažer kybernetické bezpečnosti     | xxxxx          |

## Příloha č. 3 - Používání sítě VFN externími uživateli



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

Směrnice | SM-UI-02 | strana 1 z 9 | verze 6

## POUŽÍVÁNÍ SÍTĚ VFN EXTERNÍMI UŽIVATELI

### Obsah

|       |                                                    |   |
|-------|----------------------------------------------------|---|
| 1     | Účel a oblast platnosti dokumentu .....            | 2 |
| 2     | Pojmy a zkratky.....                               | 2 |
| 3     | Odpovědnosti a pravomoci .....                     | 2 |
| 4     | Postup (popis činností) .....                      | 3 |
| 4.1   | PROCESY EXTERNÍHO PŘÍSTUPU.....                    | 3 |
| 4.1.1 | Podmínky schvalování .....                         | 3 |
| 4.1.2 | Postup zřízení přístupu.....                       | 3 |
| 4.1.3 | Zrušení přístupu.....                              | 4 |
| 4.2   | POVINNOSTI, PRAVIDLA A RESTRIKCE.....              | 4 |
| 4.2.1 | Povinnosti externích uživatelů .....               | 4 |
| 4.2.2 | Požadavky na připojené zařízení .....              | 4 |
| 4.2.3 | Bezpečnostní incident nebo kybernetický útok ..... | 5 |
| 4.2.4 | Zakázané činnosti .....                            | 5 |
| 4.2.5 | Monitoring činností .....                          | 5 |
| 4.2.6 | Porušení pravidel a povinností .....               | 5 |
| 4.3   | REVIZE EXTERNÍHO PŘIPOJENÍ.....                    | 6 |
| 5     | Závěrečná ustanovení .....                         | 6 |
| 6     | Vznikající dokumenty a údaje .....                 | 6 |
| 7     | Související dokumenty .....                        | 6 |
| 8     | Přílohy .....                                      | 6 |

Dokument je nově vytvořen, změny nejsou vyznačeny.

Zpracovatel:



Účinnost dokumentu od:

1.8.2025

Schválil:



Garant:

Vedoucí odboru provozu IT

První vydání dne:

1.1.2008

Dne:

1.8.2025

Dokument zobrazený na intranetu VFN je řízen správcem dokumentace pracoviště.

Po vytištění slouží pouze pro informativní účely – nepodléhá pravidlům řízení dokumentace.





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

Směrnice | SM-UI-02 | strana 2 z 9 | verze 6

## 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

|                         |                                                                                                                                                                                                                  |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>AD</b>               | Active Directory                                                                                                                                                                                                 |
| <b>Externí uživatel</b> | Osoba využívající prostředky IT VFN, která není v pracovně právním poměru k VFN                                                                                                                                  |
| <b>Garant</b>           | Zaměstnanec VFN, který zodpovídá za přístup a práci externího uživatele v síti VFN.                                                                                                                              |
| <b>ICT</b>              | Informační a komunikační technologie                                                                                                                                                                             |
| <b>ISE</b>              | Cisco Identity Services Engine                                                                                                                                                                                   |
| <b>OPIT</b>             | Odbor provozu IT                                                                                                                                                                                                 |
|                         | <b>ServiceDesk</b> Nástroj na zaznamenání, evidenci a sledování stavu incidentů nebo požadavků zaměstnanců VFN a pracovníků externích dodavatelských firem řešených Úsekem informatiky a digitální transformace. |
| <b>ÚI</b>               | Úsek informatiky a digitální transformace                                                                                                                                                                        |
| <b>VFN</b>              | Všeobecná fakultní nemocnice v Praze                                                                                                                                                                             |
| <b>VPN</b>              | 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.

---

Dokument zobrazený na intranetu VFN je řízen správcem dokumentace pracoviště.

Po vytištění slouží pouze pro informativní účely – nepodléhá pravidlům řízení dokumentace.



**Usek informatiky a digitální transformace |**  
U Nemocnice 499/2, 128 08 Praha 2 | [www.vfn.cz](http://www.vfn.cz), <http://intranet.vfn.cz>

Směrnice | SM-UI-02 | strana 3 z 9 | verze 6

## **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 autentizací. 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,

---

**Dokument zobrazený na intranetu VFN je řízen správcem dokumentace pracoviště.**

Po vytištění slouží pouze pro informativní účely – nepodléhá pravidlům řízení dokumentace.



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

Směrnice | SM-UI-02 | strana 4 z 9 | verze 6

## POUŽÍVÁNÍ SÍTĚ VFN EXTERNÍMI 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 Símac, 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 vyražením a v případě podezření, že heslo zná jiná osoba, heslo musí změnit přes portál <http://www.office.com> a tuto situaci neprodleně nahlásit jako incident dle bodu 4.2.1.1,
- je povinen zabránit využití či zneužití jeho vzdáleného připojení (VPN) třetí osobou,
- v případě podezření na bezpečnostní incident, nestandardní chování připojení nebo informačních systémů či jakékoliv náznaku na kybernetický útok neprodleně nahlásit toto podezření dle bodu 4.2.1.1,
- je povinen chovat se v souladu s dobrými mravy a právním řádem České republiky.

#### 4.2.1.1 Nahlášení incidentu

V pracovní dny:

- od 7:00 do 16:00 na Dispečink ÚI na tel. [REDACTED]
- od 16:00 do 7:00 na Pohotovost ÚI na tel. [REDACTED]

O víkendu a svátcích na Pohotovost ÚI na tel. [REDACTED]

### 4.2.2 Požadavky na připojené zařízení

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

---

Dokument zobrazený na intranetu VFN je řízen správcem dokumentace pracoviště.

Po vytištění slouží pouze pro informativní účely – nepodléhá pravidlům řízení dokumentace.



## POUŽÍVÁNÍ SÍTĚ VFN EXTERNÍMI UŽIVATELI

### 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 analýze hrozby nebo útoku a zabránění jakékoliv 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 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.

---

Dokument zobrazený na intranetu VFN je řízen správcem dokumentace pracoviště.

Po vytištění slouží pouze pro informativní účely – nepodléhá pravidlům řízení dokumentace.



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

Směrnice | SM-UI-02 | strana 6 z 9 | verze 6

## 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 mechanismů 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**

Dokument zobrazený na intranetu VFN je řízen správcem dokumentace pracoviště.

Po vytištění slouží pouze pro informativní účely – nepodléhá pravidlům řízení dokumentace.



VŠEOBECNÁ FAKULTNÍ NEMOCNICE V PRAZE

Název pracoviště | U Nemocnice 499/2, 128 08 Praha 2 | [www.vfn.cz](http://www.vfn.cz), <http://intranet.vfn.cz>

Příloha 1 | SM-ÚI-02 | strana 7 z 9 | verze 6

## 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 umísťování 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 takového zařízení bez předchozího upozornění odpojit od sítě VFN a externí účet (včetně VPN připojení) zablokovat nebo i zrušit.

Případné dotazy, požadavky nebo problémy je možné řešit na:

od 7:00 do 16:00 Dispečink ÚI na tel. [REDACTED]

### Metoda vzdáleného přístupu

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

Info: <https://www.vfn.cz/vpn> nebo Pohotovosti ÚI: [REDACTED] (mimo pracovní hodiny Dispečinku ÚI)

Dokument zobrazený na intranetu VFN je řízen správcem dokumentace pracoviště.

Po vytištění slouží pouze pro informativní účely – nepodléhá pravidlům řízení dokumentace.





## VŠEOBECNÁ FAKULTNÍ NEMOCNICE V PRAZE

Název pracoviště | U Nemocnice 499/2, 128 08 Praha 2 | [www.vfn.cz](http://www.vfn.cz), <http://intranet.vfn.cz>

Příloha 3 | SM-ÚI-02 | strana 8 z 9 | verze 6

# POSTUP ZŘÍZENÍ PŘÍSTUPU EXTERNÍMU UŽIVATELI DO POČÍTAČOVÉ SÍTĚ VFN

### Postup

Postup žádosti o povolení přístupu do počítačové sítě VFN:

- Žadatel si stáhne, vytiskne a vyplní formulář F-VFN-463.
- Žadatel se dostaví s vyplněným a NEPODEPSANÝM formulářem na Dispečink Úseku informatiky a digitální transformace (dále jen Dispečink ÚI) ve VFN (Budova ředitelství A5, pracovní dny 7:00 – 16:00).
- Pracovník Dispečinku ÚI ověří identitu žadatele (OP, pas). Žadatel podepíše formulář.
- Pracovník Dispečinku ÚI zašle na uvedeného Garanta e-mail s žádostí o schválení validity požadovaného přístupu a rozsahu přístupu. V případě požadavku na VPN připojení, je Garant upozorněn.
- Po obdržení potvrzení od Garanta bude vytvořen přístupový účet externího uživatele a případně VPN přístup.
- Žadatel bude o schválení a zřízení přístupového účtu informován e-mailem.
- Žadatel se dostaví na Dispečink ÚI a vyzvedne si uživatelské jméno a heslo. Heslo je doporučeno si na místě změnit.
- Expirace přístupového účtu je max. po 1 roce od zřízení. Žadatel i Garant bude 1 měsíc před expirací upozorněn na zadaný e-mail. O prodloužení přístupového účtu žádá Garant e-mailem – jako odpověď na e-mail s upozorněním na expiraci.

**Upozornění:** Přístup do počítačové sítě VFN se nezřizuje na počkání!

### Povinnosti, pravidla a omezení

Po dobu platnosti účtu externího uživatele je externí uživatel povinen dodržovat následující:

- stanovené povinnosti, pravidla a případné restrikce v kap. 4.2 Řádu používání sítě VFN externími uživateli ([SM-UI-02](#))
- při používání VPN přístupu
  - stanovené povinnosti pro připojování zařízení do sítě VFN definované v příloze č. 1 ([SM-UI-02](#)),
  - návody a postupy pro VPN připojení do sítě VFN uvedené na webových stránkách <https://www.vfn.cz/vpn>,
- aktuální informace uvedená na webových stránkách <https://www.vfn.cz/externista>

### Dokumenty ke stažení

- Formulář [F-VFN-463](#) Žádost o zřízení přístupu externího uživatele do sítě VFN
- Řád používání sítě VFN externími uživateli ([SM-UI-02](#))

### Kontakt

Dispečink ÚI

- Všeobecná fakultní nemocnice v Praze, U Nemocnice 499/2, 128 08 Praha 2
- Telefon: XXXXXXXXXX
- E-mail: XXXXXXXXXX

---

Dokument zobrazený na intranetu VFN je řízen správcem dokumentace pracoviště.

Po vytištění slouží pouze pro informativní účely – nepodléhá pravidlům řízení dokumentace.



VŠEOBECNÁ FAKULTNÍ NEMOCNICE V PRAZE

Název pracoviště | U Nemocnice 499/2, 128 08 Praha 2 | www.vfn.cz, http://intranet.vfn.cz

Příloha 3 | SM-ÚI-02 | strana 9 z 9 | verze 6

## POVINNOST ADMINISTRÁTORA V PŘÍPADĚ BEZPEČNOSTNÍHO INCIDENTU NEBO KYBERNETICKÉHO ÚTOKU

### Povinnosti administrátora

V případě podezření či probíhajícím bezpečnostním incidentu nebo kybernetickým 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
- od 16:00 do 7:00 na Pohotovost

víkendu a svátcích na Pohotovost ÚI na tel.

---

Dokument zobrazený na intranetu VFN je řízen správcem dokumentace pracoviště.

Po vytištění slouží pouze pro informativní účely – nepodléhá pravidlům řízení dokumentace.



## Příloha č. 4 - Požadavky systému řízení bezpečnosti informací na poskytovatele

### 1 Účel

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

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

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

### 2 Bezpečnostní požadavky

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

#### 2.1 Obecná pravidla bezpečnosti informací

Dodavatel je povinen:

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

#### 2.2 Fyzická bezpečnost

Dodavatel je povinen:

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

#### 2.3 Bezpečnost lidských zdrojů

Dodavatel je povinen:

- prokazatelně seznámit zaměstnance Dodavatele s dodržováním bezpečnostních pravidel a zásad požadovaných VFN,
- dodržovat ochranu aktiv VFN před neautorizovaným přístupem, vyrazením, 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 povinností zaměstnance Dodavatele ve vztahu k bezpečnosti informací nebo způsobení bezpečnostního incidentu, musí být zahájeno formální disciplinární řízení. Způsob řízení odpovídá povaze porušení nebo incidentu a jeho dopadu na VFN.

## 2.4 Řízení přístupu

Dodavatel je povinen:

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

## 2.5 Bezpečné chování uživatelů

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

Zaměstnanec Dodavatele:

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

## 2.6 Bezpečnost mobilních zařízení a vzdáleného přístupu

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

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

## 2.7 Ochrana před škodlivým kódem

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

## 2.8 Zálohování a obnova dat

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

Zálohovaná data musí splňovat požadavky:

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

## 2.9 Technické zranitelnosti

Dodavatel je povinen:

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

## 2.10 Bezpečnost komunikační sítě

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

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

## 2.11 Bezpečnostní zásady pro práci s daty

Dodavatel je povinen:

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

## 2.12 Používání kryptografické ochrany

Dodavatel je povinen:

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

## 2.13 Akvizice, vývoj a údržba informačních systémů

Dodavatel je povinen:

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

## 2.14 Zvládání bezpečnostních incidentů

Dodavatel je povinen:

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

## 2.15 Řízení kontinuity činností

Dodavatel je povinen:

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

## 2.16 Legislativní a normativní požadavky

Dodavatel je povinen splnit legislativní a normativní požadavky:

- zákon č. 181/2014 Sb., o kybernetické bezpečnosti a vyhlášku č. 82/2018Sb., o kybernetické bezpečnosti,
- zákon č. 264/2025 Sb., o kybernetické bezpečnosti
- nařízení EU č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR),
- zákon č. 110/2019 Sb., zpracování osobních údajů,
- směrnici EU č. 2016/1148, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů (NIS),
- nařízení EU č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (eIDAS),
- standardy systému řízení bezpečnosti řady ISO/IEC 27000 – Information Security Management System (ISMS), především ISO/IEC 27001, ISO/IEC 27002 a ISO/IEC 27799,
- a související normy nebo best-practice.

## 2.17 Kontroly zavedení bezpečnostních opatření

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

## 2.18 Audity plnění bezpečnostních požadavků

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