KUPNÍ SMLOUVA

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

a

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
IČO: 630 79 496 DIČ: CZ63079496
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
bankovní spojení: ČSOB
číslo účtu: 8010-616133653/0300
jako **prodávající** na straně druhé (dále jen „prodávající" nebo „dodavatel")

Prodávající a kupující společně též jako „smluvní strany"

uzavírají dnešního dne, měsíce a roku na základě výsledku **veřejné zakázky malého rozsahu** s názvem „**Síťové prvky Cisco**", zadávané na elektronickém tržišti Tendermarket pod systémovým číslem T004/25V/00006876 v otevřeném řízení (dále jen „veřejná zakázka"), v souladu s ustanovením § 2079 a násl. zákona č. 89/2012 Sb., občanský zákoník, v platném znění, (dále jen „zákon č. 89/2012 Sb."), tuto

KUPNÍ SMLOUVU:

(dále též „smlouva" či „kupní smlouva")

I. Předmět plnění smlouvy

1. Předmětem plnění dle této kupní smlouvy je dodávka síťových prvků Cisco včetně podpory, která je blíže specifikována v čl. III. smlouvy (dále také „zboží" nebo „předmět plnění") dle podmínek sjednaných touto smlouvou a zadávacími podmínkami veřejné zakázky. Bližší specifikace předmětu plnění je uvedena v příloze č. 1 „Specifikace zboží", která je nedílnou součástí této smlouvy.
2. Prodávající prohlašuje, že je certifikovaným partnerem výrobce.
3. Prodávající rovněž prohlašuje, že minimálně dva jeho zaměstanaci jsou certifikováni, a to na minimální úrovni CCNP, kdy toto prokáže doložením příslušných certifikátů.
4. Prodávající se zavazuje dodat zboží kupujícímu na místo plnění specifikované v článku II. této smlouvy. Součástí předmětu plnění je rovněž poskytování bezplatného záručního servisu na dodávané zboží.
5. Nebezpečí škody na zboží a vlastnické právo k němu přechází na kupujícího okamžikem jeho řádného předání a převzetí způsobem dále uvedeným ve smlouvě.
6. Kupující se zavazuje odebrat zboží od prodávajícího za podmínek této smlouvy a zaplatit mu dohodnutou kupní cenu.
7. Prodávající se podpisem této Kupní smlouvy stává 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 (dále jen „ZKB"). To znamená, že prodávající je orgánem nebo osobou zajišťující servis a podporu podpůrného aktiva přístupových bodů podle § 3 písm. f) ZKB a provozování základní služby kupujícím podle ZKB je závislé na zajištění servisu a podpory prodávajícího.

II. Dodací podmínky

1. Prodávající se zavazuje dodat kupujícímu zboží do 60-ti kalendářních dnů od účinnosti této kupní smlouvy.
2. Místem plnění je sídlo kupujícího, konkrétně:
Odbor provozu IT, U Nemocnice 2/499, 128 00 Praha 2; kontaktním zaměstnancem je pro účely této kupní smlouvy určen pan xxxxx, tel.: xxxxx, email: xxxxx.
3. Prodávající odpovídá za dodržení přepravních podmínek po dobu přepravy ke kupujícímu, tak aby nebylo zboží znehodnoceno. Zboží bude dopraveno do místa plnění na vlastní náklady a nebezpečí prodávajícího.
4. Zboží bude prodávajícím předáno a kupujícím převzato na základě shodných prohlášení smluvních stran v zápisu o předání a převzetí zboží, kterým se pro účely této smlouvy rozumí dodací list.
5. Na daňovém dokladu bude přesná specifikace předmětu plnění. Dodávka se považuje za řádně splněnou předáním a převzetím zboží a potvrzením dodacího listu oprávněným zaměstnancem kupujícího dle čl. IV. odst. 2. smlouvy.

III. Poskytování podpory předmětu plnění

1. Základní formou podpory je přímý přístup k webovému portálu Cisco, popřípadě služba Hot Line na tel.: xxxxx, e-mail: xxxxx nebo elektronický systém prodávajícího v režimu 24x7 (dále jen „Helpdesk"), dostupný prostřednictvím webového přístupu na adrese xxxxx. Součástí Helpdesku je popis procesu zpracování požadavku.
2. Prodávající se zavazuje v případě potřeby poskytnout kupujícímu přímý přístup a možnost stažení aktuálního software, update software a nebo firmware přímo z oficiálních zdrojů výrobce.
3. Platnost a rozsah podpory výrobce lze zkontrolovat na webovém portálu výrobce po příhlášení se do účtu kupujícího.
4. Podpora se nevztahuje na poruchy, které byly způsobeny neodbornou obsluhou a údržbou kupujícího, živelnou pohromou, nedodržením návodu od výrobce, nedodržením provozních podmínek nebo jiným způsobem než obvyklým provozem.
5. Oprávněné osoby kupujícího a prodávajícího, které mohou pracovat s Helpdeskem prodávajícího jsou uvedeny v příloze č. 4 smlouvy.
6. Prodávající se zavazuje, že bude poskytovat služby s vynaložením veškeré odborné péče, že bude dodržovat obecně závazné předpisy a vnitřní předpisy kupujícího:
   - Používání sítě VFN externími uživateli (SM-Ul-02) uvedený v příloze č. 3 této smlouvy, který mu byl kupujícím poskytnut, a se kterým byl prokazatelným způsobem seznámen před podpisem této smlouvy.
7. Prodávající se zavazuje, že bude poskytovat servis, údržbu a podporu s vynaložením veškeré odborné péče, že bude dodržovat obecně závazné předpisy a vnitřní předpisy kupujícího, se kterými byl prokazatelným způsobem seznámen.
8. Prodávající se zavazuje provádět servis, údržbu a podporu ve shodě s bezpečnostními požadavky kupujícího, které budou písemně kupujícímu sděleny a prodávajícím písemně potvrzeny.
9. Prodávající se zavazuje splňovat/dodržovat relevantní požadavky na řízení bezpečnosti informací uvedené v příloze č. 5 této smlouvy „Požadavky systému řízení bezpečnosti informací na dodavatele" vztahující se na předmět výpůjčky a prostředí nebo činnosti prodávajícího. Pojem „dodavatel" uvedený v příloze č. 5 této smlouvy představuje pro účel této smlouvy „prodávajícího".
10. Prodávající je povinen neprodleně informovat kupujícího prostřednictvím prodávajícím určené odpovědné osoby: Manažera kybernetické bezpečnosti, e-mail: xxxxx, o kybernetických bezpečnostních incidentech souvisejících s odstraněním vad, poskytováním servisních činností, údržby a podpory.

IV. Předání a převzetí zboží

1. Předání a převzetí zboží v místě dodání lze provést v pracovních dnech od 08:00 hod. do 15:00 hod.
2. Při převzetí zboží obdrží kupující v místě plnění dodací list, který potvrdí jeho oprávněný zaměstnanec svým podpisem a otiskem příslušného razítka, dále obdrží záruční listy k dodanému zboží.
3. Kupující je oprávněn odmítnout převzetí zboží:
   a) nepředá-li prodávající, resp. jím pověřený přepravce v místě plnění kupujícímu dodací list, který musí obsahovat: datum uskutečnění dodávky, množství zboží s uvedením druhů zboží a ceny za množstevní jednotku;
   b) nepředá-li prodávající, resp. jím pověřený přepravce v místě plnění kupujícímu záruční listy ke zboží;
   c) nesouhlasí-li počet položek nebo množství zboží uvedené na dodacím listě se skutečně dodaným zbožím;
   d) neodpovídá-li kvalita dodávky specifikaci zboží, která je definována v příloze č. 1 této kupní smlouvy.
4. Prodávající se zavazuje, že dodávané technické nebo programové prostředky nesmí být prostředky, které jsou zveřejněny na stránkách Národního centra kybernetické bezpečnosti (provozované NÚKIB) jako hrozba. Veškeré poskytované služby nesmí být provozované na technických nebo programových prostředcích označených NÚKIB jako hrozba. V případě porušení této povinnosti je objednatel oprávněn od smlouvy odstoupit.

V. Kupní cena

1. Po dobu účinnosti této smlouvy se prodávající zavazuje, že nepřekročí cenu uvedenou v příloze č. 2 smlouvy, vyjma případné změny sazby DPH.
2. Cena zboží je konečná a nejvýše přípustná a zahrnuje veškeré náklady prodávajícího, jako např. rizika, zisk, finanční vlivy (inflační, kursový), dopravné, clo, balné, apod. K této ceně bude připočteno DPH ve výši platné v době dodávky zboží.

VI. Platební podmínky

1. Dodávka zboží bude kupujícímu fakturována samostatnou fakturou (daňovým dokladem) k dodacímu listu. Fakturována může být pouze celá dodávka zboží. Na faktuře budou rozepsány jednotlivé položky dle předmětu plnění.
2. Faktura bude zaslána elektronicky ve formátu PDF na adresu xxxxx. Dodací list bude přiložen v nascanované podobě.
3. Vystavená faktura musí splňovat všechny náležitosti řádného daňového dokladu dle § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty v platném znění. Neobsahuje-li faktura zákonem stanovené náležitosti, je oprávněn ji kupující do 15 dnů prodávajícímu vrátit k opravě a doplnění. Dnem nového doručení faktury začíná běžet nová lhůta splatnosti faktury.
4. Lhůta splatnosti faktur se sjednávána na 60 dní ode dne jejich předání či doručení dle podmínek uvedených v odst. 2 tohoto článku.
5. Veškeré platby mezi smluvními stranami se uskutečňují prostřednictvím bankovního spojení uvedeného v záhlaví této smlouvy.

VII. Dodání zboží

1. Prodávající odpovídá za dodržení přepravních podmínek po dobu přepravy ke kupujícímu, tak aby nebylo zboží znehodnoceno. Zboží bude dopraveno do místa plnění na vlastní náklady a nebezpečí prodávajícího.
2. Zboží bude prodávajícím předáno a kupujícím převzato na základě shodných prohlášení smluvních stran v zápisu o předání a převzetí zboží, kterým se pro účely této smlouvy rozumí dodací list.
3. Na daňovém dokladu bude přesná specifikace předmětu plnění. Dodávka se považuje za splněnou předáním a převzetím zboží a potvrzením dodacího listu oprávněným zaměstnancem kupujícího dle čl. IV. odst. 2. smlouvy.

VIII. Sankce

1. V případě prodlení kupujícího s úhradou řádně fakturované ceny je prodávající oprávněn požadovat zaplacení smluvního úroku z prodlení ve výši 0,01% z nezaplacené částky za každý i započatý den prodlení. Smluvní strany se dohodly, že prodávající je oprávněn požadovat zaplacení úroku z prodlení až po uplynutí 30 dnů od sjednané lhůty splatnosti.
2. V případě, že bude prodávající v prodlení s dodávkou řádně objednaného zboží, je kupující oprávněn požadovat zaplacení smluvní pokuty ve výši 0,1% z ceny dodávky bez DPH za každý i započatý den prodlení.
3. V případě nedodržení povinnosti stanovené v čl. XII. odst. 2 smlouvy má kupující právo účtovat smluvní pokutu ve výši pohledávky, která byla postoupena v rozporu s touto smlouvou. Kupující má zároveň právo odstoupit od smlouvy.
4. Smluvní pokuta bude vyúčtovaná samostatným daňovým dokladem a její splatnost činí 30 dní ode dne doručení daňového dokladu.
5. Kupujícímu vzniká právo na náhradu škody způsobené porušením smluvních povinností v plné výši i po úhradách výše sjednaných smluvních pokut.
6. V případě sankcí nebo jiných finančních dopadů vyplývajících z porušení nebo nedodržení povinností dle čl. IV. odst. 4., čl. III. odst. 7.-10. a čl. XI. této smlouvy způsobené prodávajícím, má kupující právo účtovat prodávajícímu smluvní pokutu ve výši 100.000,- Kč za každé jednotlivé porušení povinnosti.

IX. Reklamace vadného zboží, záruční podmínky

1. Zjistí-li kupující po převzetí zboží, že je obal zboží porušen nebo množství dodaného zboží neodpovídá dodacímu listu, uplatní kupující reklamaci u prodávajícího, bez prodlení po převzetí zboží.
2. Prodávající prohlašuje, že dodávané zboží je nové, nepoužité a nerepasované a je bez vad faktických i právních. Dále prodávající prohlašuje, že dodané zboží bude mít po celou dobu záruky ode dne potvrzení dodacího listu vlastnosti odpovídající specifikacím, které jsou uvedeny v příloze č. 1 této kupní smlouvy.
3. Prodávající přejímá níže uvedenou záruku za jakost zboží dodaného podle této kupní smlouvy:
    - záruční doba na zboží činí 24 měsíců (není-li ve specifikaci zboží v příloze č. 1 této smlouvy uvedeno jinak), po tuto dobu bude zboží způsobilé k užívání a zachová si smluvené, resp. obvyklé vlastnosti,
    - záruka poskytnutá prodávajícím kupujícímu platí jen tehdy, pokud závada není zaviněna kupujícím,
    - zjistí-li kupující vadu zboží, je povinen bez prodlení písemně vadu reklamovat u prodávajícího. Písemná reklamace bude obsahovat podrobný popis vady, případně budou uvedeny všechny okolnosti, které mohou mít pro posouzení vady podstatný význam,
    - prodávající je povinen posoudit oprávněnost reklamace dle dodaného druhu zboží, a bez prodlení po obdržení písemné reklamace sdělit kupujícímu, zda reklamaci považuje za oprávněnou nebo neoprávněnou. V případě oprávněné reklamace má kupující právo na výměnu vadného zboží nebo na vrácení kupní ceny vadného zboží.
4. Záruční doba počíná běžet následujícím dnem po dni potvrzení dodacího listu oprávněným zástupcem kupujícího. Záruka se vztahuje na plnou funkčnost zboží.
5. Prodávající se zavazuje v případě záručních oprav vyměnit kupujícímu zboží za bezvadné v místě dodání dle této smlouvy, případně zajistit provedení záručního servisu zboží v místě dodání dle této smlouvy. V případě, že nebude možné provést záruční servis v místě dodání dle této smlouvy, nýbrž bude nutné provést tento záruční servis v jiném místě než je místo dodání dle této smlouvy, zavazuje se prodávající zajistit odvoz tohoto zboží k provedení záručního servisu na náklady prodávajícího.
6. Záruční lhůta se automaticky prodlužuje o dobu, která uplyne mezi nahlášením a odstraněním reklamované závady.
7. Prodávající se zavazuje ke garanci dodávky náhradních dílů zboží po dobu životnosti zboží.

X. Zvláštní ujednání

1. Prodávající bere na vědomí, že kupující je povinen dle ustanovení § 219 odst. 1. zákona č. 134/2016 Sb., o zadávání veřejných zakázek a dle zákona č. 340/2015 Sb., o registru smluv, uveřejnit tuto smlouvu včetně případných dodatků zákonem stanoveným způsobem.
2. Prodávající je povinen udržovat mít v platnosti a udržovat pojištění odpovědnosti za škodu způsobenou kupujícímu či třetím osobám při výkonu podnikatelské činnosti prodávajícího, která je předmětem této smlouvy, s limitem pojistného plnění v minimální výši 1.000.000,- Kč.

XI. 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 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 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. XI., 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**").

XII. Závěrečná ustanovení

1. Tato smlouva nabývá platnosti dnem podpisu oběma smluvními stranami a účinnosti uveřejněním v registru smluv.
2. Prodávající je oprávněn postoupit pohledávku vyplývající z plnění dle této smlouvy na třetí osobu pouze s předchozím písemným souhlasem kupujícího.
3. Práva a povinnosti smluvních stran, které nejsou touto smlouvou výslovně upravené, řídí se obecnými ustanoveními občanského zákoníku, v platném znění.
4. Smlouvu lze ukončit písemnou dohodou nebo výpovědí kterékoliv strany, a to i bez udání důvodu s jednoměsíční výpovědní lhůtou, která počíná běžet následujícím dnem po doručení písemné výpovědi druhé smluvní strany. Smluvní strany mohou od této smlouvy odstoupit v případech hrubého porušení smluvních povinností.
5. Kupující si vymiňuje právo odstoupit od kupní smlouvy a nepřevzít předmět plnění v případech:
   - kdy bude dodán jiný předmět plnění než vysoutěžený.
   - že předmět plnění bez vad nebude realizován v plném rozsahu nejpozději do 30 dnů od účinnosti této smlouvy z viny na straně prodávajícího.
6. Kupující si vymiňuje právo částečného odstoupení od smlouvy v případech, kdy:
   - v průběhu záruční lhůty dojde během 12ti po sobě jdoucích kalendářních měsíců k opakovanému výskytu 3 a více stejných závad na zboží,
   - odstranění závady na zboží bude delší než 30 kalendářních dnů ode dne uplatnění reklamace,
   - celková doba odstávky zboží pro záruční závadu bude za dobu 12ti po sobě jdoucích kalendářních měsíců delší než 30 kalendářních dnů, a to v té části plnění, které se týká porušení povinnosti prodávajícího. Ostatní ustanovení kupní smlouvy zůstávají v platnosti.
7. Prodávajícímu v případech odstoupení od smlouvy kupujícím dle odst. 5. a 6. tohoto článku smlouvy nevzniká nárok na úhradu jakýchkoliv nákladů spojených s přípravou realizace anebo s realizací předmětu smlouvy nebo části smlouvy. Odstoupení od smlouvy nabývá účinnosti dnem doručení jeho písemného vyhotovení druhé smluvní straně. Účinky odstoupení od smlouvy nastávají okamžikem doručení písemného projevu vůle druhé smluvní straně.
8. Veškeré změny smlouvy lze provést pouze písemným dodatkem.
9. Smlouva byla vypracována ve dvou vyhotoveních s platností originálu, po jednom vyhotovení pro každou smluvní stranu. 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.
10. Smluvní strany prohlašují, že si tuto smlouvu před jejím podpisem přečetly, že byla uzavřena podle jejich pravé a svobodné vůle, vážně, určitě a srozumitelně a na důkaz výše uvedeného připojují své vlastnoruční podpisy.

Přílohy: Příloha č. 1 – Specifikace zboží
Příloha č. 2 – Položkový ceník

Příloha č. 3 – Používání sítě VFN externími uživateli
Příloha č. 4 – Seznam oprávněných osob
Příloha č. 5 – Požadavky systému řízení bezpečnosti informací na dodavatele

V Praze dne dle el. podpisu:

Simac Technik ČR, a.s.

V Praze dne dle el. podpisu:

---

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

Příloha č. 1 – Specifikace zboží

Položka č. 1
Přepínač Catalyst C9200-48T-E s moduly **1 kus**
Typ: Catalyst 9200 48-port
PN: C9200-48T-E
Podpora 5 let SNTC-8X5XNBD Catalyst 9200 48-port data only, Network, PN: CON-SNT-C920048E
C9200 Cisco DNA Essentials, 48-Port Term Licenses, PN: C9200-DNA-E-48
C9200 Cisco DNA Essentials, 48-Port, 5 Year Term License, PN: C9200-DNA-E-48-5Y
Config 5 Power Supply Blank, PN: PWR-C5-BLANK
C9200 Network Essentials, 48-port license, PN: C9200-NW-E-48
Europe AC Type A Power Cable, PN: CAB-TA-EU
RUBBER FEET FOR TABLE TOP SETUP 9200 and 9300, PN:C9K-ACC-RBFT
12-24 and 10-32 SCREWS FOR RACK INSTALLATION, QTY 4, PN: C9K-ACC-SCR-4
1RU CABLE MANAGEMENT GUIDES 9200 and 9300, PN: CAB-GUIDE-1RU
Network Plug-n-Play Connect for zero-touch device deployment, PN: NETWORK-PNP-LIC
Catalyst 9200 4 x 10G Network Module, PN: C9200-NM-4X
Cisco Catalyst 9200 Stack Module, PN: C9200-STACK-KIT
2 ks Catalyst 9200 Stack Module, PN: C9200-STACK
50CM Type 4 Stacking Cable, PN: STACK-T4-50CM

Položka č. 2
Přepínač Catalyst C9200-24P-E **1 kus**
Typ: Catalyst 9200 24-port
PN: C9200-24P-E
Podpora 5 let SNTC-8X5XNBD Catalyst 9200 24-port PoE+, Network Esse, PN: CON-SNT-C920024P
C9200 Cisco DNA Essentials, 24-Port Term Licenses, PN: C9200-DNA-E-24
C9200 Cisco DNA Essentials, 24-Port, 5 Year Term License, PN: C9200-DNA-E-24-5Y
Config 5 Power Supply Blank, PN: PWR-C5-BLANK
C9200 Network Essentials, 24-port license, PN: C9200-NW-E-24
No Network Module Selected, PN: C9200-NM-NONE
Europe AC Type A Power Cable, PN: CAB-TA-EU
RUBBER FEET FOR TABLE TOP SETUP 9200 and 9300, PN: C9K-ACC-RBFT
12-24 and 10-32 SCREWS FOR RACK INSTALLATION, QTY 4, PN: C9K-ACC-SCR-4
1RU CABLE MANAGEMENT GUIDES 9200 and 9300, PN: CAB-GUIDE-1RU
Network Plug-n-Play Connect for zero-touch device deployment, PN: NETWORK-PNP-LIC
Cisco Catalyst 9200 Stack Module, PN: C9200-STACK-KIT
2 ks Catalyst 9200 Stack Module, PN: C9200-STACK
50CM Type 4 Stacking Cable, PN: STACK-T4-50CM

Položka č. 3
Vnitřní přístupový bod Cisco CW9162I-E **9 kusů**
Typ: Wireless 9162I AP
PN: CW9162I-E
Podpora 5 let SNTC-8X5XNBD CAT WLS 9162I AP W6E tri-band 2x2 Reg E, PN:CON-SNT-CW9162IE
Capwap software for Catalyst 9162I, PN:SW9162-CAPWAP-K9
Ceiling Grid Clip for APs & Cellular Gateways-Recessed, PN:AIR-AP-T-RAIL-R
802.11 AP Low Profile Mounting Bracket (Default), PN:AIR-AP-BRACKET-1
Network Plug-n-Play Connect for zero-touch device deployment, PN:NETWORK-PNP-LIC
SINGLE PACK OPTION, PN:CW9162I-SINGLE
C9162I OVER OPTION, PN:CW9162I-OVER
Wireless Cisco DNA On-Prem Essential, 9162 Tracking, PN:CDNA-E-C9162
Wireless Cisco DNA On-Prem Essential, Spare Lic, PN:AIR-DNA-E
Wireless Cisco DNA On-Prem Essential, 5Y Term Lic, PN:AIR-DNA-E-5Y
Wireless Cisco DNA On-Prem Essential, Term, Tracker Lic, PN:IR-DNA-E-T
Wireless Cisco DNA On-Prem Essential, 5Y Term, Tracker Lic, PN:AIR-DNA-E-T-5Y
Wireless DNA Perpetual Network Stack - Essentials, PN:AIR-DNA-NWSTACK-E

Příloha č. 2 – Položkový ceník

Položka číslo	Položka	Specifikace položky	Ks	Jednotková cena bez DPH (Kč)	Celková cena bez DPH (Kč)
1	Přepínač C9200-48T-E s moduly	Catalyst 9200 48-port data only, Network Essentials, PN:C9200-48T-E	1	131 465,96 Kč	131 465,96 Kč
2	Přepínač C9200-24P-E	Catalyst 9200 24-port PoE+, Network Essentials, PN:C9200-24P-E	1	80 460,34 Kč	80 460,34 Kč
3	Vnitřní přístupový bod Cisco CW9162I-E	Catalyst Wireless 9162I AP (W6E, tri-band 2x2) w/Reg, PN:CW9162I-E	9	17 474,08 Kč	157 266,72 Kč
					369 193,02 Kč

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

POUŽÍVÁNÍ SÍTĚ VFN EXTERNÍMI UŽIVATELI

Obsah

Dokument je nově vytvořen, změny nejsou vyznačeny.

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

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

POUŽÍVÁNÍ SÍTĚ VFN EXTERNÍMI UŽIVATELI

1 Účel a oblast platnosti dokumentu

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

2 Pojmy a zkratky

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

3 Odpovědnosti a pravomoci

Garant – zodpovídá za přístup, rozsah oprávnění a práci externího uživatele v síti VFN.

Externí uživatel – externí pracovník, kterému je na základě smluvního vztahu zřízen externí přístup, který je schválen garantem externího přístupu ve VFN (Garant). Výkon práce provádí v souladu se smluvním ujednáním a v souladu s náležitostmi dodržovat povinnosti, pravidla a zákazy uvedené v kap. 4.2.

Pracoviště Dispečinku ÚI (Odbor podpory uživatelů) – zodpovídá za ověření externího uživatele, schválení požadavku Garantem a za zadání požadavku do ServiceDesku.

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

POUŽÍVÁNÍ SÍTĚ VFN EXTERNÍMI UŽIVATELI

4 Postup (popis činností)

4.1 PROCESY EXTERNÍHO PŘÍSTUPU

4.1.1 Podmínky schvalování

Externí uživatel musí vyplnit formulář F-VFN-463 Žádost o zřízení přístupu externího uživatele do sítě VFN, kde je uveden garant externího přístupu za VFN (dále jen Garant), na jehož základě dojde k ověření identity žadatele a o schválení validity požadovaného přístupu a rozsahu přístupu Garantem. Po splnění těchto podmínek je možné zřízení účtu externího uživatele.

4.1.2 Postup zřízení přístupu

4.1.2.1 Externí uživatel

Detailní postup pro zřízení účtu externího uživatele je uveden v příloze (Příloha č. 2 – Postup zřízení přístupu externímu uživateli do počítačové sítě VFN) a zároveň dostupný na webové stránce https://www.vfn.cz/externista. Pokud je součástí externího přístupu i požadavek o zřízení vzdáleného přístupu je postupováno dle kapitoly 4.1.2.2 (Vzdálený přístup - VPN). Platnost externího účtu je max. 1 rok od zřízení, pokud nebyl zřizován na dobu určitou. Žadatel bude 1 měsíc před expirací upozorněn na kontaktní e-mail uvedený v žádosti, obdobně i Garant bude upozorněn na svůj pracovní mail 1 měsíc před. O prodloužení přístupového účtu žádá Garant e-mailem – jako odpověď na e-mail s upozorněním na expiraci.

4.1.2.2 Vzdálený přístup - VPN

Externí pracovníci se mohou do sítě VFN připojit pomocí VPN TLS tunelu s multifaktorovou autentizaci. Detailní postup pro žadatele je na stránce https://www.vfn.cz/vpn. O VPN přístup žádá Garant prostřednictvím požadavku do ServiceDesku, kde musí být uvedeno:

- jméno a příjmení externisty,
- účet externisty ve VFN,
- firma,
- telefon,
- e-mail,
- oblast činnosti ve vztahu k VFN,
- na které zařízení (modality, servery) má mít externí uživatel přístup a v jakém rozsahu (IP, porty),
- doba platnosti VPN přístupu, pokud má být na dobu určitou.

Požadavek dále zpracuje pracovník správy sítí OPIT v následujících krocích:

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

Požadavek dále zpracuje pracovník správy serverů OPIT v následujících krocích:

- nastaví profil v AD,
- pošle informace o vytvoření VPN přístupu externímu uživateli,

- ukončí požadavek Garanta v ServiceDesku (čímž dojde k vygenerování a zaslání notifikačního emailu Garantovi).

4.1.3 Zrušení přístupu

Ke zrušení externího účtu nebo VPN přístupu může dojít za následujících podmínek:

- v oprávněných případech, kdy externí uživatel porušil pravidla a povinnosti uvedené v příloze č. 1, Povinnosti při připojování zařízení do sítě VFN,
- pokud je podezření na zavinění bezpečnostního nebo provozního incidentu či byl jakýmkoliv způsobem zapojen do kybernetického útoku na VFN,
- uplynula stanovená doba externího účtu nebo VPN přístupu (výchozí je 1 rok) nebo Garant nepotvrdil prodloužení externího účtu (čímž zanikne i související VPN přístup)
- nebo byl zadán požadavek na zrušení/ukončení externího účtu anebo VPN přístupu,
- požadavek je zpracován pracovníkem OPIT, který odebere členství v odpovídající AD skupině a následně předá na externí firmu Simac, která zruší profil v ISE.

4.2 POVINNOSTI, PRAVIDLA A RESTRIKCE

4.2.1 Povinnosti externích uživatelů

Uživatel v rámci připojení do sítě VFN:

- smí používat připojení pouze k účelům souvisejícím s výkonem smluvní činnosti v takovém rozsahu, který odpovídá potřebám uživatele pro výkon této činnosti,
- je povinen používat své připojení takovým způsobem, který nenaruší funkci sítě, informačních systémů a jejich dat ani práva ostatních uživatelů,
- je povinen chránit svá hesla před vyzrazením a v případě podezření, že heslo zná jiná osoba, heslo musí změnit přes portál http://www.office.com a tuto situaci neprodleně nahlásit jako incident dle bodu 4.2.1.1,
- je povinen zabránit využití či zneužití jeho vzdáleného připojení (VPN) třetí osobou,
- v případě podezření na bezpečnostní incident, nestandardní chování připojení nebo informačních systémů či jakékoliv náznaku na kybernetický útok neprodleně nahlásit toto podezření dle bodu 4.2.1.1,
- je povinen chovat se v souladu s dobrými mravy a právním řádem České republiky.

4.2.1.1 Nahlášení incidentu

V pracovní dny:

- od 7:00 do 16:00 na Dispečink ÚI na tel
- od 16:00 do 7:00 na Pohotovost ÚI na t

O víkendu a svátcích na Pohotovost ÚI na tel. +

4.2.2 Požadavky na připojené zařízení

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

4.2.3 Bezpečnostní incident nebo kybernetický útok

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

4.2.4 Zakázané činnosti

Externí uživatel připojený do sítě VFN nesmí:

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

4.2.5 Monitoring činností

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

4.2.6 Porušení pravidel a povinností

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

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

Externí uživatel připojený do sítě VFN:

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

4.3 REVIZE EXTERNÍHO PŘIPOJENÍ

Za oprávněnost, platnost a rozsah externího připojení odpovídá Garant, který v případě jakékoliv změny (zrušení, odebrání/přidání práv, apod.) zadá tuto změnu formou požadavku do ServiceDesku.
V rámci kontrolních mechanizmů je minimálně 1x ročně prováděna kontrola povolených externích uživatelů a připojení VPN v rámci pravidelných auditů KB prováděné auditorem KB nebo jiným pověřeným subjektem.

5 Závěrečná ustanovení

Tato směrnice je závazná pro všechny výše uvedené zaměstnance a externí subjekty v kap. 3 Odpovědnosti a pravomoci.
Porušení této směrnice bude posuzováno jako závažné porušení povinností vyplývajících z právních předpisů a smluvního vztahu vztahujících se k externímu uživateli vykonávané práci a jednání v rozporu se zájmy VFN a uzavřeného smluvního vztahu.
Tato směrnice podléhá revizi nejméně jednou ročně. Za provedení revize dokumentu odpovídá zpracovatel této směrnice.

6 Vznikající dokumenty a údaje

Název	Uchovává	Doba uchování

7 Související dokumenty

RD-VFN-11 Řád používání informačních systémů

F-VFN-463 Formulář: Žádost o zřízení přístupu externího uživatele do sítě VFN

8 Přílohy

Příloha č. 1 – Povinnosti při připojování zařízení do sítě VFN

Příloha č. 2 – Postup zřízení přístupu externímu uživateli do počítačové sítě VFN

Příloha č. 3 – Povinnost administrátora v případě bezpečnostního incidentu nebo kybernetického útoku

POVINNOSTI PŘI PŘIPOJOVÁNÍ ZAŘÍZENÍ DO SÍTĚ VFN

Povinnosti při připojování zařízení do sítě VFN:

1) Připojení každého zařízení do LAN sítě VFN musí být předem konzultováno s Odborem provozu IT Úsekem informatiky a digitální transformace (dále jen ÚI) VFN.
2) Instalace a provozování jakéhokoli software v síti VFN musí být předem konzultováno s Odborem vývoje a správy SW ÚI VFN.
3) Je zakázáno svévolně zapojovat zařízení do LAN sítě a jakkoli měnit LAN síť VFN.
4) Je zakázáno měnit, instalovat a nahrávat jakýkoli softwarový obsah na zařízení VFN.
5) Je zakázáno jakýmkoli způsobem měnit a zasahovat do hardware vybavení VFN.
6) Je zakázáno využívat pro vzdálený přístup na připojovaná zařízení jiných než ÚI VFN schválených metod - viz níže.
7) Při umisťování IT zařízení (server, PC) do sítě VFN je vlastník IT zařízení povinen na své náklady, pokud není ve smlouvě uvedeno jinak, udržovat toto zařízení:
    a. v aktuálním (aktualizace operačního systému, aktualizace antivirového programu)
    b. v bezpečném (nemožnost jednoduše zneužít, používání silných přístupových hesel...) stavu.

    ÚI provádí náhodné testy zneužitelnosti zařízení. V případě zjištění hrozeb nebo nedostatků je vlastník IT zařízení povinen na své náklady zjištěné hrozby a nedostatky neprodleně odstranit.

8) Vlastník IT zařízení je povinen, na vyžádání ÚI, předložit ke kontrole konfiguraci IT zařízení. V situaci, kdy připojené zařízení způsobuje jakékoliv bezpečnostní anebo technické problémy v síti VFN, má VFN možnost takovéto zařízení bez předchozího upozornění odpojit od sítě VFN a externí účet (včetně VPN připojení) zablokovat nebo i zrušit.

Případné dotazy, požadavky nebo problémy je možné řešit na:
od 7:00 do 16:00 Dispečink ÚI na tel. [redacted]

Metoda vzdáleného přístupu

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

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

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

POSTUP ZŘÍZENÍ PŘÍSTUPU EXTERNÍMU UŽIVATELI DO POČÍTAČOVÉ SÍTĚ VFN

Postup

Postup žádosti o povolení přístupu do počítačové sítě VFN:

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

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

Povinnosti, pravidla a omezení

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

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

Dokumenty ke stažení

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

Kontakt

Dispečink ÚI

- Všeobecná fakultní nemocnice v Praze, U Nemocnice 499/2, 128 08 Praha 2
- Telefon [redacted]
  E-mail

POVINNOST ADMINISTRÁTORA V PŘÍPADĚ BEZPEČNOSTNÍHO INCIDENTU NEBO KYBERNETICKÉHO ÚTOKU

Povinnosti administrátora

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

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

u tohoto incidentu či útoku je vždy povinen:

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

  v pracovní dny

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

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

Příloha č. 4 - Seznam oprávněných osob

A. Seznam kontaktních osob prodávajícího

Jméno	**Funkce**	**Telefonní číslo**
[redacted]	[redacted]	[redacted]

B. Seznam kontaktních osob kupujícího

Jméno	**Funkce**	**Telefonní číslo**	**e-mail**
[redacted]	Vedoucí odboru IT	[redacted]	[redacted]
[redacted]	Vedoucí oddělení správy sítí	[redacted]	[redacted]

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

Oblast	**Funkce**	**Kontakt**
Ochrana osobních údajů	Pověřenec pro ochranu osobních údajů	[redacted]
Bezpečnosti informací, kybernetické bezpečnost	Manažer kybernetické bezpečnosti	[redacted]

Příloha č. 5 – Požadavky systému řízení bezpečnosti informací na dodavatele

1. Účel

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

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.

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.

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.

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.

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.

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.).

Bezpečnost mobilních zařízení a vzdáleného přístupu

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

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

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.

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.

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.

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.

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.

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.

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.

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.

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).

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.

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.

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.