SMLOUVA NA DODÁVKU ROZŠÍŘENÍ STÁVAJÍCÍCH HPE TECHNOLOGIÍ

TresTech s.r.o.
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 244853
se sídlem: Hlubočepská 1291/2, 152 00 Praha 5
IČO: 042 62 719 DIČ: CZ04262719
zastoupena: Tomášem Hauznerem, jednatelem
bankovní spojení: Raiffeisenbank a.s.
číslo účtu: 11403841/5500

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

a

Všeobecná fakultní nemocnice v Praze
se sídlem: U Nemocnice 499/2, 128 08 Praha 2
IČO: 000 64 165 DIČ: CZ00064165
zastoupena: prof. MUDr. Davidem Feltlem, Ph.D., MBA, ředitelem
bankovní spojení: ČNB
číslo účtu: 24035021/0710

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

Dodavatel a objednatel společně též jako „smluvní strany"

uzavírají dnešního dne na základě výsledku **nadlimitní veřejné zakázky** s názvem „**Rozšíření stávajících HPE technologií**", **vyhlášené otevřeným řízením** dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „z. č. 134/2016 Sb.") a zveřejněné ve Věstníku veřejných zakázek pod ev. č. Z2025-034152 ze dne 24.06.2025, ID na profilu zadavatele VZ0222665 (dále jen „veřejná zakázka"), v souladu s ustanovením § 1746 odst. 2. zákona č. 89/2012 Sb., občanský zákoník, v platném znění (dále jen „zákon č. 89/2012 Sb."), tuto

smlouvu na dodávku rozšíření stávajících HPE technologií
(dále jen „smlouva")

I. Předmět smlouvy

1. Předmětem plnění dle této smlouvy je dodání komponent pro kapacitní rozšíření stávajících diskových polí HPE Primera C650 v datových centrech objednatele včetně instalace, implementace, zprovoznění v prostředí objednatele, dodání technické a provozní dokumentace, záruky a záručního servisu (dále také „řešení" nebo „předmět plnění"), a to v souladu s požadavky definovanými v příloze č. 2 této smlouvy – Minimální technické a funkční požadavky objednatele.

   Nedílnou součástí předmětu plnění je:

   a) rozšíření stávajícího diskového pole Primera C650 primární lokalita
   - 12 ks HPE Primera 600 8TB SAS 7.2K LFF (3.5in) HDD
   - 16 ks HPE Primera 600 7.68TB SAS SFF (2.5in) FIPS Encrypted SSD
   - 1 ks HPE Service Credit
   - 1 ks HPE 3Y Service Credits 10 Per Yr SVC
   - 1 ks HPE 3Y Service Credits Qty 30 SVC
   - 1 ks HPE 3Y Tech Care Essential Service
   - 16 ks HPE Primera 600 7.68TB SFF FE SSD Supp
   - 12 ks HPE Primera 600 8TB 7.2K LFF HDD Support
   - 16 ks HPE Storage SSD Extended Replacement SVC
   - instalace a implementace kapacitního rozšíření diskového pole v prostředí objednatele

   b) rozšíření stávajícího diskového pole Primera C650 sekundární lokalita
   - 12 ks HPE Primera 600 8TB SAS 7.2K LFF (3.5in) HDD
   - 16 ks HPE Primera 600 7.68TB SAS SFF (2.5in) FIPS Encrypted SSD
   - 1 ks HPE Service Credit
   - 1 ks HPE 3Y Service Credits 10 Per Yr SVC
   - 1 ks HPE 3Y Service Credits Qty 30 SVC
   - 1 ks HPE 3Y Tech Care Essential Service
   - 16 ks HPE Primera 600 7.68TB SFF FE SSD Supp
   - 12 ks HPE Primera 600 8TB 7.2K LFF HDD Support
   - 16 ks HPE Storage SSD Extended Replacement SVC
   - instalace a implementace kapacitního rozšíření diskového pole v prostředí objednatele

c) dodání technické a provozní dokumentace
Dodavatel vypracuje a předá podrobnou dokumentaci k dodanému řešení v českém (CZ) jazyce, zahrnující popis a/nebo postupy minimálně pro tyto oblasti:

- Technická dokumentace – popis architektury, konfigurací, nastavení a integrace řešení,
- Provozní dokumentace – aktualizace stávajících návodů a postupů ke správě řešení od její údržby, záchranné mechanismy až po postupy při havárii.

d) akceptační testy
Akceptační testy budou provedeny dle objednatelem připravených testovacích scénářů. Akceptační testy pokrývají funkčnosti vyplývající z požadavků na řešení. Úspěšná akceptace je podmíněna úspěšnými HW výkonnostními testy.

e) záruku a zajištění poskytování záručního servisu

Bližší specifikace předmětu plnění je uvedena v příloze č. 1 této smlouvy. Záruka a způsob jejího poskytování je rovněž blíže řešena v čl. III. smlouvy.

2. Vzhledem k tomu, že dodávané technologie, systémy a služby budou součástí informačních systémů základní služby (poskytování zdravotních služeb) podle § 2 písm. i) bodu 5. zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „ZKB"), je dodavatel osobou, které se ukládají povinnosti v oblasti kybernetické bezpečnosti podle § 3 písm. f) ZKB.
3. Dodavatel bere na vědomí, že v době uzavření smlouvy nesmí být dodávané technické nebo programové prostředky označeny NÚKIB jako hrozba. Následně poskytované služby nesmí být provozované na technických nebo programových prostředcích označených NÚKIB jako hrozba.
4. Dodavatel je povinen neprodleně informovat objednatele prostřednictvím objednatelem určené odpovědné osoby: Manažera kybernetické bezpečnosti, e-mail:xxxxxx, o kybernetických bezpečnostních incidentech souvisejících s implementací nebo při zajištění záručního servisu dodávaného řešení.
5. Součástí předmětu plnění dle této smlouvy je rovněž zajištění záruky na dodaný předmět plnění dle podmínek uvedených v čl. III smlouvy. Dodavatel prohlašuje, že je certifikovaným partnerem výrobce, jehož produkty jsou předmětem plnění této smlouvy.
6. Dodavatel se zavazuje dodat předmět plnění specifikovaný v čl. I a příloze č. 1 této smlouvy a objednatel se zavazuje uhradit dodavateli cenu specifikovanou v čl. IV. této smlouvy.

II. Dodání předmětu plnění

1. Dodavatel se zavazuje dodat objednateli předmět plnění dle čl. I. a přílohy č. 1 této smlouvy **nejpozději do 90 kalendářních dnů od účinnosti této smlouvy.**
2. Předmět plnění dle čl. I. odst. 1 a přílohy č. 1 této smlouvy bude dodán do sídla objednatele. Dodavatel bude informovat objednatele o přesném termínu dodávky předmětu plnění, a to nejméně 10 pracovních dnů před realizací dodávky. Kontaktní osobou a odpovědným zaměstnancem objednatele je pro účely této smlouvy určen xxxxx, tel.: xxxxx, email: xxxxx. Kontaktní osobou za dodavatele je xxxxx, tel.: xxxxx, e-mail: xxxxx

Kontaktní a odpovědná osoba za objednatele:
Za převzetí HW: xxxxx, xxxxx, xxxxx
Za akceptaci předmětu plnění: xxxxx, xxxxx, xxxxx
K nahlašování požadavků na záruční servis: xxxxx, xxxxx, xxxxx
Za identifikaci případného kybernetického útoku v průběhu plnění předmětu plnění dle této smlouvy: xxxxx
Za ochranu osobních údajů: xxxxx

Kontaktní a odpovědná osoba za dodavatele:
Za předání HW: xxxxx, tel.: xxxxx, e-mail: xxxxx
Za akceptaci předmětu plnění: xxxxx, tel.: xxxxx, e-mail: xxxxx
K poskytování záručního servisu: xxxxx, tel.: xxxxx, e-mail: xxxxx
Za identifikaci případného kybernetického útoku v průběhu plnění předmětu plnění dle této smlouvy: xxxxx, tel.: xxxxx, e-mail: xxxxx
Za ochranu osobních údajů: xxxxx, tel.: xxxxx, e-mail: xxxxx

3. Dodací list podepíší a opatří otisky razítek oprávnění zaměstnanci obou smluvních stran. Takto opatřený dodací list slouží jako doklad o řádném předání a převzetí HW (je nedílnou součástí akceptačního protokolu).
4. Okamžikem protokolárního předání a převzetí HW přechází na objednatele vlastnické právo HW a nebezpečí škody na HW. Objednatel není povinen převzít HW či jeho část, která je poškozena nebo která jinak nesplňuje podmínky této smlouvy, zejména pak jakost zařízení.
5. Dodavatel odpovídá za dodržení přepravních podmínek po dobu přepravy HW k objednateli, tak aby nebylo zařízení znehodnoceno. HW bude dopraven do místa plnění na vlastní náklady a nebezpečí dodavatele.
6. Dodávka předmětu plnění se považuje podle této smlouvy za řádně splněnou, pokud:
    - předmět plnění byl řádně doručen na místo plnění, vybalen, naimplementován a zprovozněn,

- bylo objednateli předáno oficiální potvrzení lokálního zastoupení výrobce dodávaného předmětu plnění o tom, že předmět plnění je nový, nepoužitý a určený pro koncového zákazníka „Všeobecná fakultní nemocnice v Praze",
- byl objednateli předán certifikát ze kterého je zřejmé, že dodavatel je certifikovaným partnerem výrobce, jehož produkty jsou předmětem plnění této smlouvy,
- byla předána veškerá potřebná dokumentace,
- byl odstraněn obalový materiál,
- byly provedeny výkonnostní HW testy v rámci akceptace,
- byla provedena akceptace řádného předání a převzetí předmětu plnění, byly splněny podmínky akceptačních testů,
- byla dodavatelem aktivována záruka výrobce dle čl. III. smlouvy, a to ke dni řádné akceptace předmětu plnění objednatelem a byla objednateli předána související dokumentace.

7. Po splnění a předání celého předmětu plnění vystaví dodavatel akceptační protokol, který bude obsahovat níže uvedené náležitosti:
   - označení dodacího listu a jeho číslo,
   - název a sídlo dodavatele a objednatele,
   - číslo smlouvy, označení dodaného předmětu plnění: jeho množství a výrobní čísla,
   - datum řádného předání/převzetí předmětu plnění,
   - stav předmětu plnění v okamžiku jeho předání a převzetí,
   - výsledky výkonnostních HW testů a akceptace či výhrady,
   - jiné náležitosti důležité pro předání a převzetí dodaného předmětu plnění,
   - předá oficiální potvrzení lokálního zastoupení výrobce dodávaného zařízení o tom, ze zařízení je nové, nepoužité a určené pro koncového zákazníka „Všeobecná fakultní nemocnice v Praze" a pro český trh. Dodavatel prohlašuje, že zařízení je určeno k nepřetržitému provozu 24*365 v datových centrech.
8. Dodací list podepíší a opatří otisky razítek oprávnění zaměstnanci obou smluvních stran. Takto opatřený dodací list slouží jako doklad o řádném předání a převzetí předmětu plnění (HW) (je nedílnou součástí akceptačního protokolu).
9. Objednatel není povinen akceptovat řádné předání a převzetí předmětu plnění v případě, že předmět plnění bude vykazovat vady a nedodělky. Pokud vada nebo nedodělek nebrání převzetí předmětu plnění smlouvy, musí být vždy uveden v akceptačním protokolu s uvedením data odstranění. Nebude-li objednatelem akceptováno řádné předání a převzetí předmětu plnění z důvodů vad a nedodělků, bude o této skutečnosti sepsán zápis s výčtem zjištěných vad nebo nedodělků, které zjistil objednatel včetně způsobu a lhůt k jejich odstranění. Tento zápis bude současně podepsán zástupci obou smluvních stran.
10. Dodavatel ručí za dodržení přepravních podmínek po dobu přepravy k objednateli tak, aby nebylo zařízení znehodnoceno. Předmět plnění bude dopraven do místa plnění na vlastní náklady a nebezpečí dodavatele.
11. Předmět plnění bude dodavatelem předán a objednatelem převzat na základě shodných prohlášení smluvních stran v zápisu o předání a převzetí zboží, kterým se pro účely této smlouvy rozumí akceptační protokol s dodacím listem.
12. Dodavatel je při plnění dle této smlouvy povinen postupovat v souladu s vnitřními předpisy objednatele, se kterými byl prokazatelně seznámen, zejména předpisem SM-UI-02 Používání sítě VFN externími uživateli, kdy tento dokument tvoří přílohu č. 4 smlouvy.
13. Dodavatel se zavazuje splňovat/dodržet relevantní požadavky na řízení bezpečnosti informací uvedené v příloze č. 5 této smlouvy „Požadavky systému řízení bezpečnosti informací na Dodavatele" vztahující se na prostředí a činnosti dodavatele.
14. Dodavatel se zavazuje plnit předmět plnění prostřednictvím projektového týmu, tedy za přítomnosti osob, které jsou uvedeny v příloze č. 6 této smlouvy, jejichž prostřednictvím dodavatel prokázal splnění kritérií technické kvalifikace v rámci veřejné zakázky, na jejímž základě byla uzavřena tato smlouva nebo další osoby, které budou odsouhlaseny dle čl. II odst. 15 této smlouvy.
15. V případě změny členů projektového týmu je dodavatel povinen vyžádat si předchozí písemný souhlas objednatele. Nový člen projektového týmu musí splňovat příslušné požadavky na kvalifikaci stanovené původními zadávacími podmínkami, kdy splnění je dodavatel povinen objednateli doložit odpovídajícími dokumenty.
16. Pro případ jakékoliv změny ve složení projektového týmu se smluvní strany dohodly, že není potřeba uzavírat tomu odpovídající dodatek smlouvy a že taková změna je účinná dnem doručení písemného souhlasu objednatele dodavateli.
17. Veškeré činnosti při realizaci předmětu plnění je dodavatel povinen provádět osobami, které mají odpovídající kvalifikaci.

III. Způsob poskytování záruky

1. Dodavatel se zavazuje zajistit záruku za jakost poskytovanou výrobcem předmětu plnění včetně záručního servisu u dodaného předmětu plnění dle čl. I. a přílohy č. 1 této smlouvy po dobu 36 měsíců ode dne řádného předání a převzetí celého předmětu plnění. V rámci záruky za jakost a záručního servisu se dodavatel zavazuje poskytovat reaktivní a proaktivní podporu.

   Reaktivní podporou se rozumí podpora centra technické podpory objednatele v režimu 24x7, s možností nahrání nových verzí firmware za těchto podmínek:

   - V případě kritického incidentu (výrazná degradace funkčnosti provozované infrastruktury objednatele nebo úplný výpadek) dodavatel zajistí okamžitou (do 15 minut) reakci na nahlášený servisní požadavek. To znamená, že do 15 minut od nahlášení servisního požadavku se případem začne zabývat technický expert certifikovaného servisního kanálu výrobce pro danou oblast. Kritičnost incidentu určuje objednatel.
   - V případě potřeby bude u kritického incidentu dedikovaný eskalační manažer výrobce, který bude v kontaktu s dodavatelem. Bude formálně řídit řešení případu a bude koordinovat práci vyšších úrovní podpory.
   - Záruka včetně příslušné SW záruky výrobce zaregistrované u výrobce zařízení na objednatele. V případě fyzické opravy/výměny komponent, případně upgrade firmware, je požadován servisní zásah technika v místě instalace.
   - Ohlášení závady na jedno kontaktní místo dodavatele specifikované v odst. 2 tohoto článku. Komunikace s kontaktním místem, technikem a L2 supportem (podpora 2. úrovně – technik řešící složitější technické problémy, které není schopen

vyřešit technik podpory úrovně 1, vyžaduje specializovanější a hlubší znalosti technologií a systémů) bude probíhat v české jazyce.
- Stav záruky je možné kdykoliv ověřit přímo na online portálu výrobce, nebo dotazem na oficiální zastoupení výrobce v ČR.

Proaktivní podporou se rozumí komplexní péče o dodané zařízení, kterou bude zajišťovat tým specialistů znající detailně prostředí nemocnice (objednatele) a bude vykonávat proaktivní služby, které budou mít za cíl zajistit péči o důležité prvky IT infrastruktury objednatele. V rámci proaktivní podpory bude dodavatel zajišťovat:

- Provozní porady - 2x ročně, on-site provozní porada objednatele s přiděleným týmem.
- Plán podpory – vypracování a průběžná údržba dokumentu, který bude obsahovat detaily plánovaných i dodaných činností.
- Průběžnou kontrolu HW monitoringu - funkčnost HW monitoringu bude pravidelně kontrolována, monitoring musí být schopen automaticky zaslat informaci o HW problému přímo výrobci zařízení.
- Firmware analýzu dodaného HW a implementaci nových verzí – minimálně 1x ročně, analýza aktuálního stavu a verzí firmware, kontrola doporučení a „best practices" výrobce, kontrola vydaných „advisories" výrobce, doporučení a implementace závěrů analýzy (povýšení verzí firmware).
- Analýzu příčin problémů - v případě kritického incidentu, je požadován detailní popis procesu analýzy jednoznačných příčin (root cause analysis).
- Analýzu rizik a návrhy neustálého zlepšování - bude poskytováno průběžně.
- Vzdálený přístup na portál výrobce - možnost stažení aktualizací, sledování aktuálních servisních požadavků.
- Dodavatel musí zajistit objednateli po celou dobu záruky celkem 15 dnů, ve které bude tým k dispozici objednateli pro konzultace nebo technické činnosti nad rámec výše uvedených činností. Tyto dny budou čerpány po dohodě obou stran.

2. K přijetí požadavků stran záruky a záručního servisu (hlášení incidentů, vad zařízení apod.) se dodavatel zavazuje zajistit objednateli přímý a nepřetržitý přístup k webovému portálu výrobce dodaného zařízení, popřípadě zajistit nepřetržitě službu Hot Line na tel. čísle xxxxx nebo přístup do elektronického systému dodavatele (dále jen „Helpdesk"), dostupný prostřednictvím webového přístupu na adrese xxxxx. Součástí Helpdesku je popis procesu zpracování požadavku.
3. Objednatel si nárokuje zahájení činností vedoucích k odstranění vad předmětu plnění do 4 hodin v režimu 24x7 od nahlášení vady objednatelem dodavateli na hot-line dodavatele tel: xxxxx, e-mail: xxxxx s následným písemným potvrzením na helpdesk dodavatele: xxxxx.
4. U kritického incidentu si objednatel nárokuje zahájení činností vedoucích k odstranění vad předmětu plnění do 15 minut v režimu 24x7 od nahlášení vady objednatelem dodavateli na hot-line dodavatele tel: xxxxx, e-mail: xxxxx s následným písemným potvrzením na helpdesk dodavatele: xxxxx.
   Dodavatel se zavazuje k vyřešení závady nejpozději do 24 hodin od nahlášení vady objednatelem dodavateli na hot-line dodavatele tel: xxxxx, e-mail: xxxxx s následným písemným potvrzením na helpdesk dodavatele: xxxxx.
5. Záruka 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.
6. Po záruční dobu (poskytování záruky výrobce) je objednatel povinen využívat dodaná zařízení dle pokynů dodavatele, popřípadě dle pokynů výrobce zařízení, výlučně v souladu s jejich určením a příslušnými technickými podmínkami. Případná technická zlepšení nebo úpravy může vykonat jen na základě písemného souhlasu dodavatele nebo výrobce.
7. V případě zjištění nebo podezření na probíhající kybernetický útok v průběhu poskytování služeb (záruky) dodavatele, musí být provedeny nezbytné kroky dodavatelem k zdokumentování a zajištění forenzních důkazů a okamžitému nahlášení kontaktní osobě za objednatele (viz kontaktní osoby uvedené v čl. II. odst. 2), která rozhodne, zda budou práce ukončeny nebo bude v pracích pokračováno a za jakých podmínek.
8. Dodavatel se zavazuje splňovat/dodržet relevantní „Požadavky ISMS na dodavatele" vztahující se na dodání předmětu plnění a poskytování záruky, které jsou uvedené v příloze č. 5 této smlouvy „Požadavky systému řízení bezpečnosti informací na Dodavatele".

IV. Cena a platební podmínky

1. Cena za předmět plnění dle čl. I. odst. 1 této smlouvy byla sjednána ve výši:
   Celková cena bez DPH **4 924 400,00 Kč**
   DPH **1 034 124,00 Kč**
   Cena vč. DPH **5 958 524,00 Kč**
   (dále jen „cena") skládající se z dílčích položek uvedených v příloze č. 3 – Položkový ceník, této smlouvy.
2. Celková cena je stanovena jako konečná a zahrnuje cenu za celý předmět plnění včetně záruky za jakost, záručního servisu a veškerých nákladů dodavatele a výrobce předmětu plnění dle této smlouvy.
3. Objednatel se zavazuje zaplatit cenu uvedenou v čl. IV. odst. 1 této smlouvy na základě faktury vystavené dodavatelem. Dodavatel předá fakturu objednateli spolu s akceptačním protokolem, jehož součástí bude dodací list, popřípadě zašle objednateli do 14 dnů po řádném předání a převzetí předmětu plnění. Fakturována může být pouze celá dodávka předmětu plnění, dílčí fakturace není povolena. Na faktuře budou rozepsány jednotlivé položky dle předmětu plnění.
4. Faktura musí dále obsahovat všechny údaje uvedené v § 29 odst. 1 zákona č. 235/2004 Sb., o dani z přidané hodnoty a dle zákona č. 563/1991 Sb., o účetnictví. Splatnost faktury činí 60 dnů od jejího doručení objednateli. Faktura bude zaslána elektronicky ve formátu PDF na e-mailovou adresu: xxxxx. Akceptační protokol, jehož součástí bude kopie dodacího listu, bude v nascanované podobě přiložen k faktuře.
5. V případě, že dodavatelem vystavená faktura bude obsahovat nesprávné či neúplné údaje, je právem objednatele takovou fakturu do 15 dnů od jejího převzetí vrátit dodavateli. Ten podle charakteru nedostatků fakturu opraví anebo vystaví novou. U opravené nebo nové faktury běží nová lhůta splatnosti.
6. Platby budou probíhat výhradně v CZK a rovněž veškeré cenové údaje budou v této měně.

7. Faktury se platí bankovním převodem na účet druhé smluvní strany uvedený na faktuře. Povinnost objednatele zaplatit dodavateli vyúčtovanou dohodnutou cenu je splněna dnem odeslání platby z účtu objednatele.

V. Odstoupení od smlouvy

1. 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, přestože byl dodavatelem na neplnění této smlouvy písemně upozorněn,
   - na straně dodavatele zejména jednání uvedená v čl. VI. odst. 2 této smlouvy, tj. jestliže nedodá řádně a včas předmět plnění, pokud dodavatel nezjednal nápravu, přestože byl objednatelem na neplnění této smlouvy písemně upozorněn.
2. 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.

VI. Sankce

1. Pro případ prodlení objednatele s úhradou ceny dle čl. IV. této smlouvy má dodavatel 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 dodavatel je oprávněn požadovat zaplacení úroku z prodlení až po uplynutí 30 dnů od sjednané lhůty splatnosti.
2. V případě dodání jiného předmětu plnění než objednaného a při nedodržení dodací lhůty je kupující oprávněn požadovat zaplacení jednorázové smluvní pokuty ve výši 50.000,- Kč. Dále je objednatel oprávněn požadovat zaplacení další smluvní pokuty ve výši 0,1 % z ceny plnění dle čl. IV. odst. 1 smlouvy bez DPH za každý započatý den prodlení s dodáním předmětu plnění, jestliže se s objednatelem nedohodne jinak. Objednatel je dále v těchto případech oprávněn odstoupit od smlouvy.
3. Za nedodržení termínu uvedeného ve čl. III. odst. 3 smlouvy, tzn. nástupu na opravu/výměnu vadného zařízení, má objednatel právo účtovat smluvní pokutu ve výši 1.000,- Kč za každou započatou hodinu prodlení.
4. Za nedodržení termínu uvedeného ve čl. III. odst. 4 smlouvy, tzn. nástupu na opravu/výměnu vadného zařízení, má objednatel právo účtovat smluvní pokutu ve výši 1.000,- Kč za každou započatou čtvrthodinu prodlení.
5. Za nedodržení termínu odstranění závady uvedeného ve čl. III. odst. 4, má objednatel právo účtovat smluvní pokutu ve výši 10.000,- Kč za každý započatý den prodlení.
6. V případě prodlení dodavatele s dodržením termínů odstranění vad předmětu plnění, jsou-li uvedeny v akceptačním protokolu o předání a převzetí předmětu plnění dle čl. II. odst. 9 smlouvy, je objednatel oprávněn požadovat zaplacení smluvní pokuty ve výši 0,1% z celkové ceny předmětu plnění bez DPH za každý i započatý den prodlení.
7. V případě nedodržení některé z povinností dodavatele stanovených v čl. VIII. odst. 2-4 smlouvy má objednatel právo účtovat smluvní pokutu ve výši 50.000,- Kč.
8. V případě nedodržení povinnosti stanovené v čl. VIII. odst. 6, má objednatel právo účtovat smluvní pokutu ve výši 10.000,- Kč za každé jednotlivé porušení povinnosti.
9. Za nedodržení povinností uvedených v čl. I. odst. 3 a 4 nebo v čl. III. odst. 7 a 8 nebo čl. VII., má objednatel právo účtovat smluvní pokutu ve výši 200.000,- Kč za každé jednotlivé porušení povinnosti.
10. V případě nedodržení povinnosti stanovené v čl. VIII. odst. 5 smlouvy má objednatel právo účtovat smluvní pokutu ve výši pohledávky, která byla postoupena v rozporu s touto smlouvu. Objednatel má zároveň právo odstoupit od smlouvy.
11. Smluvní pokuta bude vyúčtovaná 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.

VII. Mlčenlivost

1. Dodavatel 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. Dodavatel 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 dodavatel 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 dodavatelem 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. Dodavatel se zavazuje za účelem ochrany osobních údajů objednatele a jeho pacientů a zaměstnanců před neoprávněným přístupem, použitím, zveřejněním nebo zničením, resp. před jejich náhodnou ztrátou či změnou uplatňovat technická a organizační bezpečnostní opatření, interní kontroly a rutiny zabezpečení osobních údajů zajišťující splnění všech povinností dle GDPR a Zákona o ochraně osobních údajů, zejména zajistit, aby data obsažená ve zdravotnické dokumentaci byla šifrována způsobem, který znemožní nahlížení do těchto údajů neoprávněným osobám.

4. Dodavatel se zavazuje zajistit informovanost svých pracovníků (včetně poddodavatelů) o povinnostech vyplývajících z této smlouvy. Dodavatel 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. Dodavatel se zavazuje informovat své poddodavatele o povinnosti mlčenlivosti dle této smlouvy. V případě porušení mlčenlivosti za strany poddodavatele, odpovídá dodavatel 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. Dodavatel 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. VII, 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**").

VIII. Ostatní ujednání

1. Dodavatel bere na vědomí, že objednatel je povinen dle ustanovení § 219 odst. 1 z. č. 134/2016 Sb., a dle zákona č. 340/2015 Sb., o registru smluv, uveřejnit tuto smlouvu včetně případných dodatků, zákonem stanoveným způsobem.
2. Dodavatel je povinen v souladu s ustanovením § 105 z. č. 134/2016 Sb. předložit do 10 pracovních dnů od doručení oznámení o výběru dodavatele objednateli seznam, ve kterém uvede, jaké části předmětu plnění a v jakém rozsahu bude plnit prostřednictvím poddodavatele, spolu s identifikací poddodavatele a uvedením rozsahu jeho plnění, pokud mu jsou známi. Poddodavatelé, kteří nebyli tímto způsobem identifikováni a kteří se následně zapojí do plnění veřejné zakázky, musí být identifikováni dodatečně, a to nejpozději před zahájením plnění veřejné zakázky tímto poddodavatelem.
3. Dodavatel 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.
4. Dodavatel 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 dodavatel 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 dodavatel povinen učinit příslušná opatření tak, aby pojištění bylo udrženo tak, jak je požadováno v tomto ustanovení.
5. Dodavatel je oprávněn postoupit pohledávku vyplývající z plnění dle této smlouvy na třetí osobu pouze s předchozím písemným souhlasem objednatele.
6. Dodavatel se zavazuje dodržovat nařízení objednatele, kterým je zakázáno kouření ve všech prostorách i plochách areálu objednatele s výjimkou vyhrazených míst.

IX. Závěrečná ujednání

1. Tato smlouva nabývá platnosti dnem podpisu 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.

Přílohy:
Příloha č. 1 – Technická a funkční specifikace předmětu plnění
Příloha č. 2 – Minimální technické a funkční požadavky objednatele
Příloha č. 3 – Položkový ceník
Příloha č. 4 - Používání sítě VFN externími uživateli
Příloha č. 5 – Požadavky systému řízení bezpečnosti informací na Dodavatele
Příloha č. 6 – Seznam členů projektového týmu

V Praze dne dle el. podpisu:

---

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

V Praze dne dle el. podpisu:

Tomáš Hauzner
jednatel TresTech s.r.o.

HPE Primera 600 upgrade 1

POČET	KÓD PRODUKTU	POPIS PRODUKTU	PODROBNÝ POPIS PRODUKTU
Pevné disky			
12	R0Q03A	HPE Primera 600 8TB SAS 7.2K LFF HDD	8 TB SAS SSD LFF (3,5") pevný disk pro Primera 600
16	R0Q00A	HPE Primera 600 7.68TB SAS SFF FE SSD	7,68 TB SAS SSD SFF (2,5") FIPS-Encrypted pevný disk pro Primera 600
Instalace a startup			
3	HA124A1 5Q4	HPE Storage System Startup Drive Fld SVC	služba instalace a startup
16	H0JD6A1	HPE Storage SSD Extended Replacement SVC	služba SSD Extended Replacement

HPE Primera 600 upgrade 2

POČET	KÓD PRODUKTU	POPIS PRODUKTU	PODROBNÝ POPIS PRODUKTU
Pevné disky			
12	R0Q03A	HPE Primera 600 8TB SAS 7.2K LFF HDD	8 TB SAS SSD LFF (3,5") pevný disk pro Primera 600
16	R0Q00A	HPE Primera 600 7.68TB SAS SFF FE SSD	7,68 TB SAS SSD SFF (2,5") FIPS-Encrypted pevný disk pro Primera 600
Instalace a startup			
3	HA124A1 5Q4	HPE Storage System Startup Drive Fld SVC	služba instalace a startup
16	H0JD6A1	HPE Storage SSD Extended Replacement SVC	služba SSD Extended Replacement

HPE servisní podpora

POČET	SAID	SAR	PODROBNÝ POPIS PRODUKTU
Servisní podpora			
1	2002100617	CZ-C1297-LL165	3Y, 24CTR, 24x7 + DMR Support pro 24x 8TB SAS 7.2K LFF HDD
1	2002100617	CZ-C1297-LL165	3Y, 24CTR, 24x7 + DMR Support pro 32x 7.68TB SAS SFF FE SSD
Support Credits			
1	2002402400	CZ-C1297-L002	Support Credits 20 per year

Příloha č. 2 – Minimální technické a funkční požadavky objednatele

1. Pojmy a zkratky

- DC1 – Datové centrum 1, Budova A5
- DC2 – Datové centrum 2, Budova Fakultní nemocnice
- HW – hardware
- NÚKIB - Národní úřad pro kybernetickou a informační bezpečnost
- On-Premise - řešení představuje software či hardware, který je uložen v interní infrastruktuře a prostoru společnosti
- ÚIDT - Úsek informatiky a digitální transformace
- VFN – Všeobecná fakultní nemocnice v Praze

2. Technologické prostředí objednatele

Kapitola obsahuje popis technologického prostředí objednatele, ve kterém bude dodavatel realizovat požadované řešení.

2.1 Obecné standardy

- Produkční prostředí je realizováno v On-Premise prostředí objednatele.
- Objednatel provozuje dvě datová centra, která jsou geograficky oddělená a pracující v režimu HA clustrovém řešení.

2.2 Virtualizační standardy

- VMWare vSphere 7 Enterprise Plus (8.0.3).

2.3 Popis stávajících HPE technologií

Aktuální HPE vybavení pro zajištění provozu virtualizačního VMware prostředí (servery, úložiště), zálohování a SAN propojení zahrnuje následující HW ve dvou datových centrech

- DC1
  - HPE Synergy 12000 Frame + 4x server HPE SY480 Gen10+
  - diskové pole HPE Primera 600 (4 kontrolery, 4 SFF police s SSD disky + 8 LFF diskových polic pro velkokapacitní NL disky)
  - SAN switch HPE SN3600B 32Gb 24port
  - úložiště pro backup HPE StoreOnce 5250
- DC2
  - HPE Synergy 12000 Frame + 4x server HPE SY480 Gen10+
  - diskové pole HPE Primera 600 (4 kontrolery, 4 SFF police s SSD disky + 8 LFF diskových polic pro velkokapacitní NL disky)
  - zálohovací server s interním úložištěm HPE Apollo 4200 Gen10 48SFF
  - SAN switch HPE SN3600B 32Gb 24port

3. Funkční požadavky

Rozšíření stávajícího diskového pole Primera C650 primární lokalita

- 12 ks HPE Primera 600 8TB SAS 7.2K LFF (3.5in) HDD
- 16 ks HPE Primera 600 7.68TB SAS SFF (2.5in) FIPS Encrypted SSD
- 1 ks HPE Service Credit
- 1 ks HPE 3Y Service Credits 10 Per Yr SVC
- 1 ks HPE 3Y Service Credits Qty 30 SVC
- 1 ks HPE 3Y Tech Care Essential Service
- 16 ks HPE Primera 600 7.68TB SFF FE SSD Supp
- 12 ks HPE Primera 600 8TB 7.2K LFF HDD Support
- 16 ks HPE Storage SSD Extended Replacement SVC
- instalace a implementace kapacitního rozšíření diskového pole v prostředí objednatele

Rozšíření stávajícího diskového pole Primera C650 sekundární lokalita

- 12 ks HPE Primera 600 8TB SAS 7.2K LFF (3.5in) HDD
- 16 ks HPE Primera 600 7.68TB SAS SFF (2.5in) FIPS Encrypted SSD
- 1 ks HPE Service Credit
- 1 ks HPE 3Y Service Credits 10 Per Yr SVC
- 1 ks HPE 3Y Service Credits Qty 30 SVC
- 1 ks HPE 3Y Tech Care Essential Service
- 16 ks HPE Primera 600 7.68TB SFF FE SSD Supp
- 12 ks HPE Primera 600 8TB 7.2K LFF HDD Support
- 16 ks HPE Storage SSD Extended Replacement SVC
- instalace a implementace kapacitního rozšíření diskového pole v prostředí objednatele

4. Požadavky na bezpečnost řešení

Dodávané technické nebo programové prostředky nesmí být prostředky, které jsou zveřejněny na stránkách Národního centra kybernetické bezpečnosti (provozované NÚKIB) jako hrozba.

Příloha č. 3 – Položkový ceník

Položka	Předmět plnění VZ	Popis	Množství	Jednotka	Nabídková cena/jednotka		Nabídková cena celkem		
					(bez DPH)	(s DPH)	(bez DPH)	Samostatně DPH (základní sazba)	(s DPH)
Rozšíření stávajících HPE technologií v souladu se zadávacími podmínkami a s návrhem smlouvy na dodávku řešení rozšíření stávajících HPE technologií + přílohy									
č. 1	**Rozšíření stávajícího diskového pole Primera C650 primární lokalita** dle čl. I., odst. 1 a) návrhu smlouvy včetně instalace, implementace, dokumentace dle čl. I., odst. 1 c) návrhu smlouvy, záruky a záručního servisu **(36 měsíců)**	HPE Primera 600 8TB SAS 7.2K LFF (3.5in) HDD	12	ks	9 850,00 Kč	11 918,50 Kč	118 200,00 Kč	24 822,00 Kč	143 022,00 Kč
		HPE Primera 600 7.68TB SAS SFF (2.5in) FIPS Encrypted SSD	16	ks	146 500,00 Kč	177 265,00 Kč	2 344 000,00 Kč	492 240,00 Kč	2 836 240,00 Kč
						Cena celkem za položku č. 1	**2 462 200,00 Kč**	**517 062,00 Kč**	**2 979 262,00 Kč**
č. 2	**Rozšíření stávajícího diskového pole Primera C650 sekundární lokalita** dle čl. I., odst. 1 b) návrhu smlouvy včetně instalace, implementace, dokumentace dle čl. I., odst. 1 c) návrhu smlouvy, záruky a záručního servisu **(36 měsíců)**	HPE Primera 600 8TB SAS 7.2K LFF (3.5in) HDD	12	ks	9 850,00 Kč	11 918,50 Kč	118 200,00 Kč	24 822,00 Kč	143 022,00 Kč
		HPE Primera 600 7.68TB SAS SFF (2.5in) FIPS Encrypted SSD	16	ks	146 500,00 Kč	177 265,00 Kč	2 344 000,00 Kč	492 240,00 Kč	2 836 240,00 Kč
						Cena celkem za položku č. 2	**2 462 200,00 Kč**	**517 062,00 Kč**	**2 979 262,00 Kč**
		Celková nabídková cena za celý předmět plnění bez DPH *					**4 924 400,00 Kč**		

*) Hodnotící kritérium dle bodu 8 ZP

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

POUŽÍVÁNÍ SÍTĚ VFN EXTERNÍMI UŽIVATELI

Obsah

Zpracovatel: [redacted]	**Účinnost dokumentu od:** 23. 7. 2020	**Schválil:** [redacted]
Garant: [redacted] Vedoucí odboru správy ICT	**První vydání dne:** 1. 1. 2008	**Dne:** 23. 7. 2020

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 ICT 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
OSICT	Odbor správy ICT
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.

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

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 OSICT v následujících krocích:

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

Požadavek dále zpracuje pracovník správy serverů OSICT 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 OSICT, 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. [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.

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

    ÚI provádí náhodné testy zneužitelnosti zařízení. V případě zjištění hrozeb nebo nedostatků je vlastník IT zařízení povinen na své náklady zjištěné hrozby a nedostatky neprodleně odstranit.
8) Vlastník IT zařízení je povinen, na vyžádání ÚI, předložit ke kontrole konfiguraci IT zařízení. V situaci, kdy připojené zařízení způsobuje jakékoliv bezpečnostní anebo technické problémy v síti VFN, má VFN možnost takovéto zařízení bez předchozího upozornění odpojit od sítě VFN a externí účet (včetně VPN připojení) zablokovat nebo i zrušit.

Případné dotazy, požadavky nebo problémy je možné řešit na:

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

Metoda vzdáleného přístupu

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

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

POSTUP ZŘÍZENÍ PŘÍSTUPU EXTERNÍMU UŽIVATELI DO POČÍTAČOVÉ SÍTĚ VFN

Postup

Postup žádosti o povolení přístupu do počítačové sítě VFN:

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

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

Povinnosti, pravidla a omezení

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

- stanovené povinnosti, pravidla a případné restrikce v kap. 4.2 Řádu používání sítě VFN externími uživateli (SM-UI-02),
- při 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: [redacted]
- E-mail: [redacted]

POVINNOST ADMINISTRÁTORA V PŘÍPADĚ BEZPEČNOSTNÍHO INCIDENTU NEBO KYBERNETICKÉHO ÚTOKU

Povinnosti administrátora

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

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

u tohoto incidentu či útoku je vždy povinen:

- zajistit kopie logů nebo transakčních záznamů, pokud by to nezpůsobilo jejich poškození nebo smazání,
- iniciovat nebo pozastavit šíření či poškození, zamezit incidentu nebo útoku,
- nemazat jakákoliv data o kybernetickém bezpečnostním incidentu bez svolení VFN, Policie ČR nebo NÚKIB,
- nahlásit toto podezření neodkladně na Pohotovost ÚI jako bezpečnostní nebo kybernetický incident:
  - v pracovní dny:
    - od 7:00 do 16:00 na Dispečink ÚI na [redacted]
    - od 16:00 do 7:00 na Pohotovost ÚI n
  - o víkendu a svátcích na Pohotovost ÚI na te

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

Účel

Účelem toho dokumentu je stanovit požadavky vyplývající ze systému řízení bezpečnosti informací ve Všeobecné fakultní nemocnici v Praze (dále jen „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.

1 Bezpečnostní požadavky

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

1.1 Obecná pravidla bezpečnosti informací

Dodavatel je povinen:

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

1.2 Fyzická bezpečnost

Dodavatel je povinen:

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

1.3 Bezpečnost lidských zdrojů

Dodavatel je povinen:

- prokazatelně seznámit zaměstnance dodavatele s dodržováním bezpečnostních pravidel a zásad požadovaných VFN,
- dodržovat ochranu aktiv VFN před neautorizovaným přístupem, vyzrazením, modifikací, zničením nebo narušením,

- zachovávat mlčenlivost o důvěrných údajích nebo sděleních VFN a o jejich ochraně,
- stanovit odpovědnosti zaměstnanců dodavatele pro nakládání s informacemi,
- poučit zaměstnance dodavatele hlásit zjištěné bezpečnostní události nebo jiná bezpečnostní rizika odpovědné osobě dodavatele,
- provádět pravidelné školení zaměstnanců dodavatele v souvislosti s bezpečností informací,
- při porušení pracovních povinnosti zaměstnance dodavatele ve vztahu k bezpečnosti informací nebo způsobení bezpečnostního incidentu, musí být zahájeno formální disciplinární řízení. Způsob řízení odpovídá povaze porušení nebo incidentu a jeho dopadu na VFN.

1.4 Řízení přístupu

Dodavatel je povinen:

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

1.5 Bezpečné chování uživatelů

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

Zaměstnanec dodavatele:

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

1.6 Bezpečnost mobilních zařízení a vzdáleného přístupu

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

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

1.7 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.

1.8 Zálohování a obnova dat

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

Zálohovaná data musí splňovat požadavky:

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

1.9 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.

1.10 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.

1.11 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.

1.12 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.

1.13 Akvizice, vývoj a údržba informačních systémů

Dodavatel je povinen:

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

1.14 Zvládání bezpečnostních incidentů

Dodavatel je povinen:

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

1.15 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).

1.16 Legislativní a normativní požadavky

Dodavatel je povinen splnit legislativní a normativní požadavky:

- zákon č. 181/2014 Sb., o kybernetické bezpečnosti a vyhlášku č. 82/2018 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., o zpracování osobních údajů,
- směrnici EU č. 2016/1148, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů (NIS),
- nařízení EU č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (eIDAS),

- standardy systému řízení bezpečnosti řady ISO/IEC 27000 – Information Security Management System (ISMS), především ISO/IEC 27001, ISO/IEC 27002 a ISO/IEC 27799,
- a související normy nebo best-practice.

1.17 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.

1.18 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.

Příloha č. 6 – Seznam členů projektového týmu

Role	Zodpovědnost (náplň práce)	Jméno a příjmení	Vzdělání, praxe, certifikace	Referenční zakázka	Vztah k dodavateli
Specialista pro oblast Storage	Aktivity definované zadávací dokumentací pro roli Specialista pro oblast Storage	xxxxx	Vzdělání: Vysoké učení technické v Brně, fakulta elektrotechniky, obor automatizace. Praxe: od 2002 dosud technický konzultant (HPE). Dodávky služeb podpory pro Škoda Auto a další významné zákazníky. Implementační HW a SW projekty, primární zaměření HPE storage. Certifikace: HPE Alletra 9000 and HPE Primera - Installation and Service.	VFN Praha, 2022, instalace, implementace, migrace a podpora HW infrastruktury (HPE Synergy vč. ISS serverů, HPE Primera, HPE SAN switche, HPE StoreOnce, HPE Apollo).	Kmenový zaměstnanec subdodavatele.
Specialista pro oblast SAN	Aktivity definované zadávací dokumentací pro roli Specialista pro oblast SAN	xxxxx	Vzdělání: Gymnázium, U Libeňského zámku 1 Praha 8. Praxe: od 1998 dosud technický kounzultant (HPE). Dodávky služeb podpory pro významné zákazníky HPE. Implementační HW a SW projekty, primární zaměření HPE SAN a storage. Certifikace: Brocade Gen 7 SAN Specialist exam.	Česká Spořitelna a.s., 2002 - 2020, Člen dedikovaného týmu podpory pro oblast SAN a storage - technické konzultace, proaktivní podpora a správa v oblastech HPE storage XP12000, P9500, 3PAR a SAN. Replikace, HW monitoring a analýza performance.	Kmenový zaměstnanec subdodavatele.

Specialista pro oblast Blade serverů	Aktivity definované zadávací dokumentací pro roli Specialista pro oblast Blade serverů	xxxxx	Vzdělání: SPŠE V Úžlabině 320. Praxe: od 2014 dosud technický kvalifikátor a technický konzultant (HPE). Kvalifikace HW a SW incidentů, analýzy, dodávky služeb podpory pro významné zákazníky HPE, implementační HW a SW projekty, zaměření HPE ISS servery, HPE bladová řešení, HPE storage, SAN, LAN, zálohování, OS VMware, Linux. Certifikace: HPE Accredited Technical Professional - Hybrid IT Solution V2.	VFN Praha, 2023-2024, člen dedikovaného týmu podpory, technické konzultace, analýzy, FW upgrades, zaměření na HPE Apollo, HPE Synergy.	Kmenový zaměstnanec subdodavatele.
Projektový manažer	Aktivity definované zadávací dokumentací pro roli Projektový manažer	xxxxx	Vzdělání: vysokoškolské ČZU Praha Praxe: více než 10 let v oblasti poskytování služeb informačních technologií, více než 10 let na pozici projektového manažera Certifikace: PRINCE2 Practitioner, ITIL Foundation	Be a Future s.r.o. pro koncového zákazníka Ministerstvo vnitra ČR Poskytování podpory systému Integrace bezpečnostních systémů a systému pro automatickou biometrickou detekci obličejů 04/2023 až současnost Koordinace a projektové řízení všech aktivit dle rámcove dohody	Kmenový zaměstnanec subdodavatele.