SMLOUVA – DODÁVKA HW INFRASTRUKTURY

Simac Technik ČR, a.s.
zapsán: v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B., vložka 3190
se sídlem: Radlická 740/113c, 158 00 Praha 5
IČ: 63079496 DIČ: CZ63079496
zastoupen: Ing. Dušanem Bruothem, předsedou představenstva
Ing. Martinem Jirečekem, členem představenstva
Ing. Jaroslavem Šteflem, členem představenstva
Jménem společnosti jednají vždy dva členové představenstva společně.
bankovní spojení: ČSOB, hlavní pobočka Praha 2
číslo účtu: 8010-616133653/0300

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

a

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

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

uzavírají dnešního dne na základě výsledku nadlimitní veřejné zakázky s názvem „**Dodávka nezbytné HW infrastruktury pro modernizaci NIS a jeho funkcionalit**", 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. Z2021-025750 ze dne 16.07.2021 a v Úředním věstníku Evropské unie pod č. oznámení o zahájení zadávacího řízení 2021/S 139-369201 ze dne 16.07.2021 (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 (dále jen „smlouva").

Preambule

Realizace předmětu plnění je spolufinancována v rámci 26. výzvy Integrovaného regionálního operačního programu, z projektu "Zajištění celoplošné dostupnosti vybraných a zabezpečených zdravotnických dat z Všeobecné fakultní nemocnice v Praze oprávněným zdravotnickým subjektům i pacientům, spojené s technologickou připraveností vazby na další projekty eHealth", registrační číslo CZ.06.3.05/0.0/0.0/16_034/0006372. Projekt je spolufinancován Evropskou unií z Evropského fondu pro regionální rozvoj.

I. Předmět smlouvy

1. Předmětem plnění dle této smlouvy je dodávka HW infrastruktury včetně záruky výrobce a záručního servisu (dále také „zařízení" nebo „předmět plnění").

   Součástí předmětu plnění je:

   - dodání předmětu plnění do místa plnění,
   - vybalení předmětu plnění,
   - instalace do příslušných racků,
   - zapojení všech zařízení do LAN a SAN,
   - licence k souvisejícímu SW (operační SW),
   - upgrade na poslední doporučované verze firmware,
   - požadovaná instalace a zprovoznění veškerého dodaného HW a všech SW titulů a funkcí,
   - proškolení obsluhy objednatele,
   - předání dokumentace,
   - odstranění obalového materiálu,
   - akceptační testy,
   - registrace záruky u výrobce a zajištění poskytování záručního servisu.

   Bližší specifikace předmětu plnění je uvedena v příloze č. 1 této 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. Součástí předmětu plnění dle této smlouvy je rovněž zajištění záruky za jakost poskytované výrobcem zařízení dle podmínek uvedených v čl. III smlouvy. Dodavatel prohlašuje, že je certifikovaným partnerem výrobce, jehož produkty jsou předmětem plnění této smlouvy.

5. Dodavatel se zavazuje dodat zařízení specifikované 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 45 kalendářních dnů od účinnosti této smlouvy.**

2. Zařízení bude dodáno na pracoviště objednatele: Úsek informatiky, serverovna 1. patro, adresa: Na Hrádku 3, Praha 2.

3. Dodavatel bude informovat objednatele o přesném termínu dodávky zařízení, a to nejméně 10 pracovních dnů před realizací dodávky. Kontaktní osobou a odpovědným zaměstnancem objednatele je pro účely této smlouvy určen xxxxxxxx Kontaktní osobou za dodavatele je xxxxxxxxx.

4. Dodávka se považuje podle této smlouvy za splněnou, pokud:

   - předmět plnění byl řádně doručen na místo plnění a vybalen,
   - bylo objednateli předáno oficiální potvrzení lokálního zastoupení výrobce dodávaného zařízení o tom, že zařízení je nové, nepoužité a určené pro koncového zákazníka Všeobecná fakultní nemocnice v Praze,
   - předmět plnění byl nainstalován do příslušných racků a byla provedena instalace a zprovoznění veškerého dodaného HW a všech SW titulů a funkcí,
   - bylo provedeno zapojení všech zařízení do LAN a SAN,
   - byl proveden upgrade na poslední doporučovanou verzi firmware,
   - bylo provedeno proškolení obsluhy objednatele,
   - byla předána veškerá potřebná dokumentace,
   - byl odstraněn obalový materiál,
   - byly provedeny akceptační testy v souladu s podmínkami uvedenými v příloze č. 3 této smlouvy,
   - byl předán plán podpory a analýza rizik dle čl. III smlouvy,
   - předmět plnění byl řádně předán a převzat způsobem sjednaným níže,
   - byla provedena akceptace řádného předání a převzetí předmětu plnění, splněny podmínky akceptačních testů a byly odstraněny vady a nedodělky podle odst. 7. tohoto článku.
   - byla dodavatelem aktivována záruka výrobce dle čl. III. smlouvy, a to ke dni řádné akceptace předmětu plnění objednatelem a objednateli byla předána související dokumentace.

5. Po splnění dodávky předmětu plnění vystaví dodavatel dodací list, 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 zařízení v okamžiku jeho předání a převzetí,
   - jiné náležitosti důležité pro předání a převzetí dodaného předmětu plnění,

   a 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.

6. Dodací list podepíší a opatří otisky razítek oprávnění zaměstnanci obou smluvních stran. Takto opatřený dodací list slouží jako doklad o řádném předání a převzetí zboží (je nedílnou součástí akceptačního protokolu).

7. Objednatel není povinen akceptovat řádné předání a převzetí předmětu plnění v případě, že předmět plnění bude vykazovat jakékoli vady a nedodělky. Pokud se objednatel přesto rozhodne předmět plnění převzít, musí být vždy uvedeno v akceptačním protokolu datum odstranění vady či nedodělku. 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.

8. Dodavatel odpovídá 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.

9. 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.

10. Dodavatel je při plnění dle této smlouvy povinen postupovat v souladu s vnitřními předpisy objednatele se kterými byl prokazatelně seznámen, zejména SM-UI-02 Používání sítě VFN externími uživateli.

III. Způsob poskytování záruky

1. Dodavatel se zavazuje zajistit záruku za jakost poskytovanou výrobcem zařízení včetně záručního servisu zařízení po dobu 60 měsíců. 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 24x 7, 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 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 VFN. 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 každý rok 6 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 +420 239 018 793, e-mail: podpora@hpe.com nebo přístup do elektronického systému dodavatele (dále jen „Helpdesk"), dostupný prostřednictvím webového přístupu na adrese https://support.hpe.com. 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: +420 239 018 793 e-mail: podpora@hpe.com s následným písemným potvrzením na helpdesk dodavatele: https://support.hpe.com.

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: +420 239 018 793 e-mail: podpora@hpe.com s následným písemným potvrzením na helpdesk dodavatele: https://support.hpe.com.
   Dodavatel se zavazuje k vyřešení závady nejpozději do 24 hodin od nahlášení vady objednatelem dodavateli na hot-line dodavatele tel: +420 239 018 793 e-mail: podpora@hpe.com s následným písemným potvrzením na helpdesk dodavatele: https://support.hpe.com.

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 HEWLETT-PACKARD s.r.o., 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. Dodavatel musí Objednatele prostřednictvím odpovědné osoby – manažera kybernetické bezpečnosti, e-mail: managerKB@vfn.cz – neprodleně informovat o kybernetických bezpečnostních incidentech souvisejících s předmětem plnění a souvisejícími službami.

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. 4 této smlouvy „Požadavky systému řízení bezpečnosti informací".

IV. Cena a platební podmínky

1. Cena za předmět plnění dle čl. I. této smlouvy byla sjednána ve výši:
   Celková cena bez DPH **27 093 542,00 Kč**
   DPH **5 689 643,82 Kč**
   Cena vč. DPH **32 783 185,82 Kč**
   (dále jen „cena")
   Celková cena je stanovena jako konečná a zahrnuje cenu za celý předmět plnění včetně záruky za jakost, záručního servisu a veškerých dalších nákladů dodavatele a výrobce zařízení na plnění dle této smlouvy.

2. Objednatel se zavazuje zaplatit cenu na základě faktury vystavené dodavatelem. Dodavatel předá fakturu objednateli spolu s dodacím listem, popřípadě zašle objednateli do 14 dnů po řádném předání a převzetí předmětu plnění. Fakturována může být pouze celá dodávka předmětu plnění. Na faktuře budou rozepsány jednotlivé položky dle předmětu plnění.

3. 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 může být zaslána elektronicky ve formátu PDF nebo ISDOC na e-mailovou adresu: faktury@vfn.cz nebo poštou ve dvou vyhotoveních na Ekonomický úsek objednatele, odbor účetnictví. K faktuře bude přiložena kopie řádně opatřeného dodacího listu způsobem sjednaným výše v čl. II. V případě zaslání faktury elektronicky bude dodací list přiložen v neskenované podobě.

4. Faktura musí obsahovat registrační číslo projektu CZ.06.3.05/0.0/0.0/16 _034/0006372.

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, které trvá déle než 30 dnů, má dodavatel nárok na zaplacení úroku z prodlení ve výši 0,01 % z částky, s jejíž platbou je objednatel v prodlení, za každý den takového prodlení. Do 30. dne prodlení nemá dodavatel nárok na úrok z prodlení, ani na náhradu škody, která by mu prodlením mohla vzniknout.

2. V případě dodání jiného zařízení než objednaného a při nedodržení dodací lhůty je objednatel 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 celkové ceny 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 u kritického incidentu, 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, je nabyvatel 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. VII. odst. 2 - 4 smlouvy má objednatel právo účtovat smluvní pokutu ve výši 10.000,- Kč.

8. Za nedodržení povinností uvedených v čl. I. odst. 3 nebo v čl. III. odst. 7 a 8, má objednatel právo účtovat smluvní pokutu ve výši 200.000,- Kč za každé jednotlivé porušení.

9. V případě nedodržení povinnosti stanovené v čl. VII. 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.

10. V případě nedodržení některé z povinností dodavatele stanovených v čl. VII. odst. 7 a 8 smlouvy má objednatel právo účtovat dodavateli smluvní pokutu ve výši sankce uložené objednateli Řídícím orgánem IROP za nedodržení povinností stanovených v Podmínkách rozhodnutí o poskytnutí dotace nebo ve výši zkrácení dotace z téhož důvodu.

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. Ostatní ujednání

1. Dodavatel bere na vědomí, že objednatel je povinen dle ustanovení § 219 odst. 1 zákona 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 40.000.000,- 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 či zastavit 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.

7. Dodavatel je povinen uchovávat veškeré doklady související s realizací plnění předmětu smlouvy (způsobem dle zákona o účetnictví) včetně účetních dokladů minimálně do konce roku 2033 nebo po dobu nejméně 10 let ode dne poslední platby za provedené práce, přičemž závazná je lhůta, která je delší. Dále je povinen zajistit, aby také všichni jeho poddodavatelé, partneři, dodavatelé partnerů uchovávali veškeré dokumenty související s prováděním plnění předmětu této smlouvy.

8. Minimálně do konce roku 2033 resp. ve lhůtách dle předchozího odstavce je dodavatel povinen poskytovat požadované informace a dokumentaci související s realizací projektu objednateli, zaměstnancům nebo zmocněncům pověřených orgánů (CRR, MMR ČR, MF ČR, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů veřejné správy), a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu, poskytnout jim při provádění kontroly součinnost a být fyzicky přítomen kontrolám v místě plnění.

VIII. Závěrečná ujednání

1. Tato smlouva nabývá platnosti dnem podpisu oběma smluvními stranami a účinnosti dnem uveřejnění v registru smluv.

2. Veškeré právní vztahy založené, resp. vyplývající z této smlouvy, které zde nejsou výslovně upravené, včetně eventuálních řešení vzájemných sporů, se řídí ustanoveními příslušných právních předpisů České republiky. Změny a doplnění této smlouvy lze učinit pouze na základě písemné dohody smluvních stran. Takové dohody musí mít podobu datovaných, vzestupně číslovaných dodatků této smlouvy podepsanými jejich statutárními zástupci.

3. Tato smlouva včetně příloh je vyhotovena ve 2 stejnopisech, z nichž každá strana obdrží po jednom vyhotovení. Obě vyhotovení jsou rovnocenná a mají platnost originálu.

4. Autentičnost této smlouvy potvrzují smluvní strany vlastnoručními podpisy svých zástupců.

Přílohy:
Příloha č. 1 – Specifikace předmětu plnění
Příloha č. 2 – Cenová kalkulace
Příloha č. 3 – Akceptační testy
Příloha č. 4 – Požadavky systému řízení bezpečnosti informací
Příloha č. 5 - Používání sítě VFN externími uživateli

V Praze dne:

---

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

V Praze dne:

Ing. Dušan Bruoth, předseda představenstva
Ing. Jaroslav Štefl, člen představenstva
Simac Technik ČR, a.s.

Příloha č.1

Specifikace předmětu plnění

Položka č. 1 – Rack – konfigurace a parametry na rackové kabinety odpovídají požadovaným funkčním a technickým požadavkům v zadání. Doplněny jsou HPE G2 Enterprise Series Racks včetně příslušenství, PDU, Rack Baying Kit atd..

Položka č. 2 – Blade šasi - konfigurace a parametry blade šasi a interconnect modulů odpovídají požadovaným funkčním a technickým požadavkům v zadání. Doplněny jsou HPE Synergy 12000 Frames.

Položka č. 3 - Blade server - konfigurace a parametry blade serverů odpovídají požadovaným funkčním a technickým požadavkům v zadání – CPU, operační paměť atd.
V nabídce jsou doplněny HPE Synergy SY480 Gen10+ konfigurovatelné Compute moduly.

Položka č. 4 - SAN switch - konfigurace a parametry Fibre Channel přepínačů odpovídají požadovaným funkčním a technickým požadavkům v zadání. Doplněny jsou HPE StoreFabric SN3600B SAN přepínače.

Položka č. 5 - Diskové pole - konfigurace a parametry diskových subsystémů odpovídají požadované technické specifikaci na diskové pole - výkon v IOPS , využitelná kapacita, konektivita atd... .Doplněny jsou HPE Primera Storage C650.

Položka č. 6 – D2D zálohovací zařízení - konfigurace a parametry na deduplikační a zálohovací zařízení odpovídají technickým parametrům v zadání pro požadovanou funkcionalitu řešení.

Položka č. 7 – Zálohovací server - konfigurace a parametry zálohovacího serveru odpovídají požadovaným technickým požadavkům v zadávací dokumentaci. Doplněn je HPE Apollo 4200 Gen10 server.

Navrhovaná konfigurace splňuje uvedené minimální funkční a technické požadavky:

Položka č. 1 - Rack

Technická specifikace Racků	
Fyzické parametry:	Výška 42U.
	Užitečná hloubka racku 1200 mm.
	Maximální šířka 600 mm.
	Konstrukce racku umožňuje minimální zatížení 1300 kg bez dodatečných prvků pro vyztužení konstrukce racku.
	Uzamykatelné přední i zadní dveře.
	Perforace dveří je minimálně 80 %.
	Uzemňovací kit.
	Záslepky na optimální proudění vzduchu minimálně 35U per rack.
	Bočnice celkem 2 ks , neboť racky budou svázané vedle sebe.

PDU:	Každý rack musí být vybaven 6 ks napájecí lišty, která každá musí být vybavena zásuvkami minimálně 12x C13, 4x C19 s přívodním kabelem a konektorem IEC 60309. Každá napájecí lišta musí mít parametry 1phase/3Pin/230V/32A/7.3kVA.
Počet sestav/kusů:	5

Položka č. 2 - Blade šasi

Technická specifikace blade šasi	
Konstrukční provedení jednotky:	Instalace do 19" racku, nesmí zabírat více než 10U, včetně veškeré potřebné konektivity.
	Možnost osazení sestavy šasi kombinací dvou i čtyř socketových serverů s CPU poslední generace.
	Servery musí jít osadit více než 200 wattovýma CPU bez dopadů na redundanci a celkovou rozšiřitelnost konfigurace.
	Osazení minimálně 12 ks dvou socketových serverů.
	Možnost budoucího osazení blade šasi GPU kartami se specifikací full height, full length, double-wide.
Konektivita:	Možnost osazení jednotlivé části v sestavě šasi alespoň 6x I/O síťovými moduly s podporou konektivity Ethernet, FC a FCoE, SAS.
Rozšiřitelnost:	Kapacita šasi musí umožňovat rozšiřitelnost na dvojnásobnou kapacitu připojením dalšího šasi a vytvořením jednoho logického šasi, přičemž síťová propustnost mezi šasimi musí být minimálně 120Gb/s Full Duplex.
	Propojení více šasí musí být realizováno plně redundantními síťovými zařízeními při dodržení požadované síťové propustnosti. Potřebné síťové zařízení, musí být součástí konfigurace, aby bylo možné vytvořit z budoucích dvou fyzických serverových šasi, jedno šasi logické.
Certifikace:	Blade šasi se servery musí být certifikované na provoz: - VMware ESXi, - VMware vSphere - VMware vSAN ready nodes - Horizon View, Citrix Hypervisor (XenServer) - Citrix Virtual Desktops (XenDesktop) - Citrix Virtual Apps (XenApp) - Microsoft Azure Stack HCI - Microsoft Windows Server 2016 - Microsoft Windows Server 2019 - Microsoft Hyper-V Server - Red Hat Enterprise Linux - SUSE Linux Enterprise Server
Backplane:	Pasivní oddělené sběrnice (datové a napájecí) zajištující redundanci datových i napájecích okruhů pro servery i instalované I/O moduly.
Napájení a chlazení:	Integrované jednofázové a za provozu vyměnitelné napájecí zdroje.
	Redundance napájení N+N s možností připojit alespoň dva nezávislé přívody napájení tak, aby výpadek jednoho z nich neznamenal omezení výkonu serveru.
	Zařízení musí obsahovat zdroje a ventilátory, které výrobce doporučuje pro maximální obsazení dodávaného šasi z důvodu budoucí potřeby instalace dalších nových serverů.
	Dodávané zdroje musí splňovat požadavky na certifikaci energetické účinnosti minimálně 96 %.

	Šasi musí podporovat řízení výkonu napájení a chlazení dle aktuální spotřeby poptávaných serverů.
Konvergovaný LAN/SAN prvek splňující:	Integrované redundantní prvky celé sestavy pro LAN/SAN všechny vzájemně propojené do stacku s možností připojení do LAN i SAN prvků infrastruktury.
	Alespoň jeden dedikovaný 25/50Gb downlink z každého IO modulu ke všem slotům v šasi.
	Celková externí konektivita z šasi do LAN/SAN alespoň 12x QSFP28 port konfigurovatelný jako 1x100Gb/4x25Gb/1x40Gb/4x10Gb Ethernet nebo 1x32Gb/1x16Gb FC.
	Rychlost portů line-rate, full duplex s latencí přepínání maximálně 1.0 µs.
	Interní přepínání LAN v rámci sestavy šasi bez komunikace mimo sestavu šasi.
	Podpora protokolů 802.1Q (podpora VLAN), 802.1AB (LLDP), NIC teaming, Jumbo Frames.
	Podpora multi šasi linkové agregace (802.3ad) pro uplinky i downlinky.
	Funkce automatické přeprogramování MAC adresy serveru po jeho výměně v případě selhání.
	Možnost vytváření společných agregačních skupin a pravidel pro LAN a SAN konektivitu serverů.
	FC konektivita s podporou minimálně FC 32Gb, případné licence musí být součástí nabídky.
	Musí podporovat agregaci dvou šasi pro konsolidaci síťových připojení datového centra. Pro agregaci musí být podporováno minimálně 24 serverů bez jakéhokoliv negativního vlivu na rychlost downlink a uplink portů. Síťový provoz Layer2 musí být přepnut v rámci agregace police/polic (nikoliv s použitím ToR switchů).
	Požadované připojení blade šasi k infrastruktuře: - 8x 32 Gb FC kompatibilní s 16Gb FC, včetně příslušných optických kabelů - 4x 40Gb Bidi Ethernet QSFP+ - Minimálně 4 porty musí zůstat volné v každém konvergovaném prvku
Management splňující:	Management procesory/moduly musí být redundantní fyzické zařízení pro správu přímo v šasi, nebo ve více připojených šasi s plnou podporou převzetí služeb při selhání a vysokou dostupností.
	Redundantní management procesory/moduly musí umožňovat spojení dvou šasí do jednoho logického celku pro správu celého prostředí z jednoho místa.
	Každý management procesor/modul musí mít ethernet port 1/10Gbps, osazený 1Gbit RJ-45 modulem pro připojení do management linky
	Plně grafické mgmt rozhraní pro správu všech instalovaných komponent se single-sign-on pro management serverů, storage, switchů, zdrojů a ventilátorů s možností přechodu do plné grafické konzole jednotlivých serverů.
	Grafické rozhraní v HTML5 s podporou běžných prohlížečů integrovaných v desktopovém OS pro správu serverů (Firefox, Chrome, Safari, Edge) a možností řízení přístupových účtů a úrovně oprávnění prostřednictvím účtů a skupin v Active Directory.
	Kódování Advanced Encryption Standard (AES) pro zabezpečení komunikace s běžnými www prohlížeči s možností instalace vlastního certifikátu.
	Managament nesmí vyžadovat instalaci Java nebo jiného frameworku na stanici administrátora.
	Podpora měření aktuální spotřeby celého šasi a instalovaných komponent, včetně monitoringu aktuální teploty. Hodnoty jsou v zařízení ukládány pro možnost dohledání a náhledu s minimálně měsíční retencí dat.
	Podpora správy zařízení a serverů dle specifikace Redfish, s dostupnými knihovnami pro Powershell, Python a Ruby.
	Validace a certifikace managementu na FIPS 140-2 a CNSA.
	Podpora RBAC (Role-based access control) a SBAC(Scope-based access control).
	Podpora integrace s nástroji Chef, Docker, OpenStack.
	Podpora integrace managementu šasi s vCenter, pokud je funkcionalita licencována, součástí dodávky je i potřebná licence.

	Možnost vytváření a úpravy vzorových profilů pro deployment a životní cyklus serverů s těmito nastaveními: - nastavení verze BIOS - RAID konfigurace lokální storage - nastavení parametrů bootování - přiřazení SAN storage - nastavení sítí LAN - nastavení sítí SAN - nastavení verze firmware - nastavení verze ovladačů - vytvoření unikátního ID, které obsahuje MAC a WWN adresu
	Zadavatel požaduje, aby k profilům blade serveru bylo možno přiřadit privátní či sdílený úložný prostor z lokálního uložiště, či z nabízeného externě připojeného SAN pole a zajistit tak plně automatický provisioning a zoning diskového prostoru jednotlivým blade serverům v souladu se zvoleným profilem.
	V rámci managementu blade platformy zadavatel požaduje plnou správu přiděleného diskového prostoru z nabízené externí SAN storage zahrnující: - přímou tvorbu virtuálních disků na diskovém poli - přiřazení již vytvořených virtuálních disků - vytváření snapshotů a vytváření nových virtuálních disků ze snapshotů, jejich odebrání a mazání
	Podpora funkce vzdáleného zapnutí, vypnutí a restartu serveru s podporou připojení vzdálených médií jak pro boot, tak i instalaci OS.
	Možnost zasílání proaktivních hlášení o možných chybách a výpadcích komponent v systému pomocí SNMP v3 a na uživatelsky definovanou emailovou adresu/y prostřednictvím uživatelsky definované SMTP brány a adresy odesílatele
	Automatické zakládání událostí technické podpoře výrobce či Dodavatele při selhání HW.
	Validace a ochrana BIOS a firmware všech komponent včetně managementu s možnost rollbacku na předchozí verzi v případě detekce napadeného či jinak poškozeného firmware.
Další vlastnosti:	Z důvodu zachování jednotné správy HW, zadavatel požaduje plnou integraci s nástrojem HPE OneView, který již ve svém prostředí provozuje, zejména v podobě odesílání notifikací o HW závadě na servisní středisko výrobce, monitoring HW komponent, spotřeby energie, reporty o stavu firmware, vzdálená instalace a update firmware, správa profilů pro jednotlivé servery, jednotná inventory HW, včetně možnosti reportingu stavu spravované infrastruktury. Plnohodnotná a časově i licenčně neomezené funkce vzdálené správy. Dodávané šasi musí být plně kompatibilní s požadovanými servery v rámci položky č. 3 tohoto zadávacího řízení.
Počet sestav/kusů:	2

Položka č. 3 - Blade server

Technická specifikace blade serverů	
Konstrukční provedení:	Blade server musí zabírat maximálně jednu pozici v šasi
Typ procesoru:	x86-64

Procesor – výkon dle SPEC	Výkon dle Standard Performance Evaluation Corporation (SPEC) měřeno na 2 procesorech o 48 aktivních jádrech: CPU2017 Integer Rates Base Result 300 bodů CPU2017 Floating Point Rates Base Result 258 bodů
Počet jader jednoho procesoru:	24
Počet procesorů:	2
Paměť operační – velikost:	768 GB RAM s možností dalšího rozšíření až na 1,5TB bez nutnosti výměnu modulů Rychlost DIMM modulů 2933MT/s
Boot:	Redundantní interní připojení (RAID 1) flash pamětí, které je určené pro boot. Podpora bootování VMware. 2x Flash paměť minimálně o kapacitě 32 GB Možnost budoucího osazení minimálně 4mi interními disky – z toho minimálně 2 hot-plug
Konvergovaná síťová karta:	Konvergovaný LAN/SAN adaptér s celkovou propustností min. 100Gbit active-active a nebo 2x 50Gbit active-passive (full duplex),
	Konvergovaný LAN/SAN adaptér s možností rozdělení síťových karet na minimálně 16 oddílů (partitions) per server, bez nutnosti dodatečných investic na straně konvergovaného prvku v serverové polici či blade serveru. Z toho alespoň dva porty pro FC SAN s možností nastavení propustnosti v rozmezí 16 – 32 Gbit.
	Adaptér musí podporovat Large Send and Receive offload capability, NVMe-oF, Jumbo Frames, MSI-X, RoCE v1, RoCE v2, VMware NetQueue and Microsoft Virtual Machine Queue (VMQ), GENEVE, NVGRE
Další vlastnosti:	Server musí být schopen zajistit bezpečný provoz firmware komponent v serveru (minimálně HDD, SSD, síťové adaptéry, BIOS a vzdálenou správu) po celou dobu životnosti serveru. Server musí být schopen autonomně monitorovat autenticitu firmware na těchto komponentách. V případě zjištění neschváleného firmware musí být schopen automaticky uvést stav poškozené komponenty do bezpečného stavu. Pokud tato funkcionalita vyžaduje licenci, tak musí být součástí.
	Validace a certifikace managementu serveru na FIPS 140-2 a CNSA
	Z důvodu zachování jednotné správy HW, zadavatel požaduje plnou integraci s nástrojem HPE OneView, který již ve svém prostředí provozuje, zejména v podobě odesílání notifikací o HW závadě na servisní středisko výrobce, monitoring HW komponent, spotřeby energie, reporty o stavu firmware, vzdálená instalace a update firmware, správa profilů pro jednotlivé servery, jednotná inventory HW, včetně možnosti reportingu stavu spravované infra.
	Dodávaný server musí být plně kompatibilní a určený pro provoz v poptávaném šasi v rámci položky č. 2 tohoto zadávacího řízení.
Počet kusů:	8

Položka č. 4 - SAN switch

Technická specifikace SAN switche	
Typ:	1U, montáž do racku
Porty:	- 24 fyzických a plně aktivovaných portů - 22 fyzických osazených MMF FC32 optikou – zadavatel požaduje originální SFP28 a ne OEM - 2 fyzické osazené SMF FC32 optikou – zadavatel požaduje originální SFP28 a ne OEM - možnost automatického přepnutí na FC16 na FC8 - podpora režimu portů D_PORT (ClearLink Diagnostic Port), E_PORT, EX_PORT, F_PORT, AE_PORT
Kapacita a výkon:	minimálně 2000 Frame Buffers 768Gbps agregovaná propustnost
Integrace:	Pro zachování kompatibility se stávající infrastrukturou zadavatel požaduje technologii Brocade.
Fabric služby:	- Frame Filtering - Advanced Zoning - Web Tools - Ingress Rate Limiting - Quality of Service - Traffic Isolation Zones - Fabric Vision - Extended Fabric - ISL Trunking
Vizualizační a management SW pro SAN:	- Zobrazování topologie sítě - Vytváření reportů - Kontrolování interoperability - Automatické konfigurování SAN pravidel - Vytváření a konfigurace pomocí templatů - Monitorování aktivit a alertů - Zasílání alertů - Přehledný a uživatelsky editovatelný dashboard se základními infromacemi - Zobrazování výkonnostních parametrů - Detailní informace o komponentách (SFP)
Chlazení:	Rear-to-front
Kabeláž:	12x 15m LC-LC optický kabel OM4
	12x 5m LC-LC optický kabel OM4
Počet kusů:	4

Položka č. 5 - Diskové pole

Technická specifikace diskového pole	
Typ zařízení:	Diskové pole v provedení do 19“racku
Napájení:	Zařízení musí být zapojitelné do 1 fázového rack PDU 220-240V C13. (Celkově bude připojeno do dvou nezávislých fází.)
Výkon:	Výkon na front-end portech minimálně 50 000 IOPS při velikosti bloku 64kB, poměru čtecích a zápisových operací 50%/50% a response time nejvýše 1ms, při zapnuté inline deduplikaci a kompresi.
Kapacita:	Využitelná kapacita pole v RAID 6, po odečtení režie RAID, režie pole a spare disků/prostoru, minimálně: - 210 TB pro SSD tier - 370 TB pro HDD tier

	Pro SSD a HDD vrstvu nesmějí být použita média s kapacitou více jak 8TB. Při výpočtu kapacity nesmí být počítáno s delším RAID setem než je 10:2 a uvažováno s efekty jakékoliv technologie pro úsporu místa (jako například deduplikace, komprese, tenký provisioning, apod.).
	Veškeré disky SSD/Flash musí být v provedení dualport
	Ochrana RAID 6 nebo lepší.
	Rebuild disků musí být pro SSD kratší než 4 hodiny a pro HDD kratší než 24 hodin.
	Pole musí podporovat vytváření distribuovaných RAIDů s ochranou proti současnému výpadku 2 disků
	Při výpadku média/modulu musí být tento modul automaticky nahrazen spare diskem/prostorem.
	Pole musí obsahovat spare disky nebo spare kapacitu dle standardních doporučení výrobce. Kapacita spare se do využitelné kapacity pole nezapočítává.
	Podpora konfigurace globálních hot-spare disků nebo spare prostoru.
	Pole musí umožnit upgrade minimálně na dvojnásobek současné požadované kapacity pouze přidáním polic a disků.
	Veškerá datová média musí být pokryta zárukou proti jejich opotřebení na minimálně 5 let. Pro každé vadné či opotřebené médium je požadována jeho bezplatná výměna.
Řadiče:	Minimálně 4 diskové řadiče
	Všechny řadiče musí pracovat v režimu active-active, všechny řadiče musí být aktivní a umožňovat symetrický přístup ke všem LUNům, to znamená, že server (host) může přistupovat přes libovolný řadič a data budou čtena a zapisována přímo z datových nosičů. Režim proxy pro odbavování IO operací není povolený.
	Minimálně 1TB paměti RAM cache (nikoliv SSD cache) na pole.
	Ochrana cache v případě výpadku napájení je její obsah překopírován do dedikovaného média, které není z požadovaných datových medií a je zajištěno jeho napájení, případně je zajištěna jiná ochrana.
Redundance a odolnost:	Plně redundantní konstrukce pole s nonSPOF charakteristikou. Celé pole je bez SPOF, tzn. všechny komponenty nutné pro běh pole, musí být redundantní - komponentou nejsou míněny jednotlivé disky.
	Dopad na výkon pole při výpadku jednoho řadiče nesmí překročit 25 %.
	Každé z polí musí zcela samostatně umožňovat bezvýpadkovou realizaci následujících úkonů: - online výměna zdroje, - online výměna ventilátorů, - online výměna řadičů, - online aktualizace firmware/mikrokódu.
Konektivita:	Požadovaná konektivita minimálně 16x FC portů 32 GB/s, možno použít pro HOST konektivitu, nebo pro replikaci.
	Požadovaná konektivita minimálně 8x Ethernet port 10 GB/s, možno použít pro replikaci.
	Dedikovaný port typu 1Gbit RJ-45 pro management na každém řadiči.
	Možnost rozšíření o 25Gb Ethernet porty.
	Možnost rozšíření o další IO karty, minimálně na dvojnásobek.
Minimální požadavky na HW:	Minimální rozsah provozních teplot 10-35°C.
	Minimální rozsah provozních nekondenzujících vlhkostí 15-85%.
	Chlazení vzduchem, zpředu dozadu.

Snapshoty:	Diskové pole musí podporovat tvorbu kopií a snapshotů LUNů. Zadavatel požaduje licenčně neomezené vytváření kopií a snapshotů je součástí dodávky.
	Pole podporuje vytvoření až 1024 read/write a nebo read-only snapshotů z jednoho zdrojového LUNu.
	Lze vytvářet skupiny LUNů, ze kterých se snapshoty vyrábí v atomicky stejném čase. Musí jít udělat skupinu ve které bude až 200 LUNů.
	Lze vytvářet snapshot ze snapshotu (kaskádování)
	Snapshoty je možné používat jak v režimu pouze ke čtení RO, tak v režimu pro plný zápis RW.
	Snapshoty musí být možné vytvářet i na replikovaných LUNech.
	Pole musí umožňovat vytváření automatických periodicky se opakujích snapshotů.
	Snapshoty lze při vytvoření označit značkou časové platnosti (expirace), po jejíž vypršení se snapshot automaticky smaže.
	U replikovaných LUNů lze nastavit jiné expirační pravidlo pro LUNy na primární a sekundární straně.
	Snapshoty lze při vytvoření označit značkou časové ochrany, po jejíž dobu nelze snapshot smazat (ochrana proti úmyslnému poškození).
	Podporována je možnost integrovat funkci snapshotů s VMware prostředím tak, aby bylo možné přímo z prostředí VMware vytvářet datově konzistentní snapshoty prostředky diskového pole.
Integrace se zálohovacím prostředím:	
	Diskové pole musí podporovat vytváření aplikačně konzistentních snapshotů včetně jejich transportu do nabízeného D2D zálohovacího zařízení vlastními prostředky diskové pole nebo dodatečným SW.
Geocluster a replikace:	Pole musí podporovat zrcadlení dat (replikace) na HW úrovni diskového pole do záložního diskového pole pro tvorbu disaster recovery řešení. Neomezené licence, které je možno využít v obousměrném režimu (tedy jak z primárního pole do záložního pole i naopak) musí být součástí dodávky.
	Pole musí podporovat jak synchronní tak asynchronní režim replikace.
	Pro replikaci musí být možné použít FC, nebo IP transportní vrstvu.
	V případě replikace se replikují pouze data, nikoli prázdné místo.
	Podpora Metro Cluster. Tedy LUN se synchronní replikací a s připojením na server z obou polí zároveň. Metro Cluster musí podporovat režim, kdy LUN bude aktivní z obou lokalit a v případě výpadku jedné lokality nedojde k automatickému failoveru a data budou odbavována z pole, které zůstane aktivní. Metro Cluster musí podporovat režim kdy LUN bude aktivní pouze z jedné lokality a v případě výpadku jedné lokality dojde k automatickému failoveru a aktivní se stane pole v druhé lokalitě. Pro split-brain detekci se použije virtuální server v třetí lokalitě (VM může být na KVM nebo VMWare). Komunikace s virtuálním serverem bude pouze po IP a případná licence na quorum SW musí být dodána s polem.
	Zadavatel požaduje funkcionalitu synchronní replikace a podporu Metro Cluster se stávajícími diskovými poli 3Par řady 8000.
LUNy:	Pole musí podporovat expanzi LUNů při provozu, tzn. bez výpadku I/O operací. Funkce musí být dostupná pro všechny typy LUNů, včetně Thin, Thick, i LUNů s aktivní deduplikací a kompresí dat.
	LUN mapping
	LUN masking

	Podpora vytváření skupin pro přidělování přístupu jednotlivých serverů k LUNům.
	Podpora expanze LUNů při provozu, tzn. bez výpadku I/O operací, jak pro běžné LUNy, tak pro replikované a Geocluster LUNy.
Deduplikace a komprese:	Inline deduplikace dat na blokové vrstvě minimálně pro SSD disky. Musí být efektivní pro všechny běžně ukládané datové struktury, nikoliv jen pro řetězce opakujících se znaků.
	Inline komprese dat na blokové vrstvě minimálně pro SSD disky. Musí být efektivní pro všechny běžně ukládané datové struktury, nikoliv jen pro řetězce opakujících se znaků.
	Podpora deduplikace a komprese i pro Geocluster/Metro Cluster LUNy.
Kompatibilita:	Windows server 2016 a vyšší včetně Hyper-V, RHEL 7.x a vyšší, ESX 6.7 a vyšší.
	Pole musí podporovat Vmware standardy VAAI (XCOPY, WRITE_SAME, ATS) a VASA v.3.
	Pole musí podporovat Vmware standardy VVOL v.2.0.
	Pole musí podporovat Vmware VADP (Vmware vStorage API for Data Protection) a vytváření konzistentních snapshotů a jejích mazání.
	Pole musí podporovat Vmware vSphere Uniform Metro Storage Cluster řešení.
	SW pro integraci s Vmware technologiemi včetně management nástrojů jako je vCenter, vRealize Operations (vROPS), vRealize Log Insight (vRLI), vRealize Orchestartion (vRO) je součástí dodávky.
	Pole musí umožňovat automatizaci pomocí nástroje Ansible.
	Podpora Microsoft VSS a ODX.
	Možnost připojení OS bez nutnosti instalace driverů výrobce (FC) multipath s použitím generických multipath driverů ve všech operačních systémech, pro které je požadována kompatibilita dle předchozích bodů této specifikace.
QoS:	QoS funkce, umožňující definovat maximální IOPS a MB/s pro daný LUN nebo pro skupinu LUNů.
	QoS funkce, umožňující definovat požadovanou latenci pro daný LUN nebo pro skupinu LUNů s vyšší prioritou, kdy pole následně pracuje tak, aby latenci prioritních LUNů dodrželo.
Jednotný nástroj pro správu musí:	Mít webové rozhraní, které umožní kompletní správu pole z webového prohlížeče Edge, Firefox, Chrome.
	Podporovat SNMP protokol verze 2c a novější.
	Pro veškerá (neagregovaná) provozní data za období nejméně 3 let zpětně musí být umožněno externí zpracování, např. s využitím exportu dat. Pokud bude vyžadován i specializovaný HW a SW, musí být kompletně součástí dodávky.
	Umožňovat predikci zaplnění daty v horizontu minimálně rok.
	Umožňovat online zobrazení zdravotního stavu pole.
	Umožňovat reporty dat z pole automatizovaně i adhoc, s možností customizace.
	Umožňovat automatické generovaní reportů ve zvoleném čase s granularitou minimálně jedna hodina a s automatickým zasíláním formou SMTP zvoleným příjemcům.
	Umožňovat online zobrazení stavů diskového pole a jeho součástí.
	Umožňovat zobrazování informací o výkonosti diskového pole v reálném i historickém čase.
	Minimální granularita pro odesílání dat z pole do nástroje pro pole je 5 minut formou přírůstku.
	Umožňovat minimálně zobrazení na úrovni pole i LUN poskytovat informace o Read IOPS, Write IOPS, Total IOPS (Read+Write), Read MB, Write MB, LUN response time (latence) ms, Total transfer MB, Random IOPS a Sequential IOPS maximální i průměrné hodnoty.

	Umožňovat minimálně zobrazení na úrovni RAID groups utilizace v % nebo například v Transefer MB/s, IOPS počet, Latence ms.
	Umožňovat minimálně zobrazení na úrovni kontrolérů utilizace procesorů v %.
	Umožňovat minimálně zobrazení na úrovni FiberChanel interface IOPS za port, MB za port.
	Umožňovat on-premise řešení management nástroje.
	Poskytovat informace minimálně o Read IOPS, Write IOPS, Read MB/s, Write MB/s, Latenci, výkonové utilizaci hardwaru.
	Podporovat správu a skriptování pomocí RestAPI.
	Mít standardní update verzí, kdy veškeré aktualizace verzí SW a FW musí být přímo od výrobce. Použití firmwaru nebo nástrojů pro správu vyvinutých speciálně pro konkrétního zákazníka není povoleno.
Jednotný nástroj pro cloud monitorovací a analytické služby, poskytující:	Informace o konfiguraci, aktuální i historické.
	Informaci o výkonu, aktuální i historické.
	Informace o využití kapacity, aktuální i historické včetně informací o úsporách díky redukčním technologiím.
	Informace o změnách konfigurace, výkonu, kapacity po celou dobu životnosti pole.
	Informace o incidentech a jejich řešení (provozní deník).
	Přehledný dashboard sumarizující hlavní informace s možností uživatelského upravení.
	Informace o úrovni a čase expirace servisních smluv x Informace o servisních událostech, jejich řešení a jejich historie.
	Možnost vytváření reportů o výkonu, o konfiguraci a kapacitě.
	Odhady trendů výkonu, využití kapacity, utilizace pole.
	Odhady a doporučení pro navyšování výkonu a kapacity.
	Doporučení pro změny konfigurace vedoucí ke zvýšení dostupnosti, výkonu, utilizace pole.
	Informace o propojené infrastruktuře Vmware ve vztahu k diskovému poli.
	Informace o konfiguraci a výkonu VM v návaznosti na diskové LUNy a jejich výkonu.
	Informace o zastoupení jednotlivých komponent VM, host, pole na celkové latenci systému.
Zasílání eventů:	Podpora logování pro účely SIEM (Syslog).
	Email notifikace na danou adresu.
	Alerty výpadku fyzické nebo logické komponenty pole minimálně pro indikaci HW problému přes SMTP a případně SNMP nebo Syslog.
Řízení práv:	Součástí nabízeného řešení musí být podpora vytváření logických skupin pro administraci. Nástroj musí umožňovat přiřadit operátorům různé úrovně správy pro různé skupiny objektů - Role Based Access Control.
	Musí umožňovat logování přístupu i administrátorských zásahů.
Licence:	Všechny požadované funkce a konfigurace musí být s legálně dodanými a kalkulovanými licencemi. Pokud jsou některé požadované funkce nebo konfigurace podmíněny licencemi, nebo licence jsou vázané na kapacitu (nebo i jinak omezené), zadavatel požaduje dodání neomezené licence nebo licence na maximální možnou/plnou kapacitu pole. Zadavatel nepřipouští použití časově omezených licencí (např. trial) pro požadované funkce, pokud je použito pro nepovinné požadavky nebo nad rámce požadavků zadavatele, tak musí být výslovně uvedeno a popsáno.
Počet kusů:	2

Položka č. 6 – D2D zálohovací zařízení

Technická specifikace D2D (disk to disk) zálohovacího zařízení	
Provedení:	K montáži do „racku“ vč. rack-mount-kitu, maximální výška 12U.
Kapacita:	Zálohovací systém s kapacitou minimálně 430 TB čisté využitelné kapacity s dvojitou paritou a bez započítání deduplikace.
	Řešení musí na úrovni uzlu chránit data minimálně RAID-6 ochranou.
	Rozšiřitelnost minimálně na dvojnásobek.
	Výkon minimálně 2,8 GB/s.
Vlastnosti:	Možnost vytvořit alespoň 64 VTL/NAS/akcelerovaných zařízení.
	Možnost vytvořit v každé VTL alespoň 64 emulovaných LTO mechanik.
	Možnost vytvořit v každé VTL alespoň 800 emulovaných LTO pásek
	Možnost přijímat a zpracovávat alespoň 512 souběžných datových zdrojů
	D2D zálohovací zařízení musí umožňovat inline deduplikaci.
	D2D zálohovací zařízení musí podporovat REST API.
	D2D zálohovací zařízení musí umožňovat kopírování do objektového úložiště včetně S3 protokolu.
	D2D zálohovací zařízení musí poskytovat souborové služby SMB/NFS.
	D2D zálohovací zařízení musí umožňovat odlévání dat do cloudových služeb.
	D2D zálohovací zařízení musí umožňovat obousměrné kopírování obsahu do/z cloudových služeb Microsoft Azure, AWS, případně další. Případné licence nejsou požadovány.
	Akcelerační protokol musí podporovat přenos po FC i po IP vrstvě.
	Akcelerační protokol musí podporovat i operace typu copy job.
	Akcelerační protokol musí podporovat režim WORM.
	Akcelerační protokol musí podporovat další úroveň autentizace (uživatel – heslo).
Bezpečnost:	D2D zálohovací zařízení musí umožňovat administraci v režimu RBAC.
	D2D zálohovací zařízení musí umožňovat ověřování uživatelů proti externí autoritě AD/LDAP.
	D2D zálohovací zařízení musí umožňovat inline šifrování (data at rest).
	D2D zálohovací zařízení musí umožňovat šifrování AES-256 bit nebo lepší.
	D2D zálohovací zařízení musí mít certifikaci FIPS 140-2 CAVP/CMVP.
	D2D zálohovací zařízení musí mít možnost integrace do externích Key management nástrojů.
	D2D zálohovací zařízení podporuje pro zálohování po LAN protokolo IPSec.
	D2D zálohovací zařízení umožňuje bezpečné smazání dat splňující standardy NIST SP800-88 nebo lepší.
	D2D zálohovací zařízení podporuje vytváření needitovatelných/nesmazatelných záloh (WORM), s časovou expirací.
Redundance:	D2D zálohovací zařízení musí mít redundantní zdroje.
	D2D zálohovací zařízení musí mít redundantní ventilátory.
Konektivita:	Připojení do SAN 4x 32Gb včetně transceiverů.
	Připojení do LAN 2x 25Gb včetně transceiverů.
Počet kusů:	1

Položka č. 7 – Zálohovací server

Technická specifikace zálohovacího serveru	
Provedení:	K montáži do „racku“ vč. rack-mount-kitu, maximální výška serveru 2U

Počet instalovaných CPU:	2
Min. počet procesorových patic:	2
Počet Core jednoho procesoru:	Minimálně 12 s podporou Hyper-threading
Pracovní kmitočet procesoru:	Minimálně 2.4 GHz
Velikost L3 cache:	Minimálně 16MB
Minimální velikost operační paměti RAM:	384 GB; paměťové moduly @ 2933 MT/s; registered, podpora Advanced ECC (nebo obdobná technologie opravy více bitové chyby paměti); podpora zrcadlení paměti a online spare
Min. rozšiřitelnost operační paměti:	1TB
Konektivita LAN:	Minimálně 2x 25GbE porty, včetně SFP28 transceiverů typu multimode
Konektivita FC:	Minimálně 4x 32Gb FC porty, včetně SFP28 transceiverů typu multimode
Napájení:	redundantní napájecí zdroje s účinností 94% a vyšší; zdroje s podporou řízení výkonu (nabízená konfigurace napájecích zdrojů musí být schopná zajistit provoz plně osazeného serveru)
Kompatibilita:	Nabízený server musí být kompatibilní s OS: MS Windows Server (min. 2019, 2016) včetně Hyper-V Linux (min. RHES, SLES) VMware (min. v6.7, v7.0)
Osazení pevnými disky:	2x SSD min. 1,92TB (DWPD≥3)
	32x HDD min. 2.4TB/10k rpm
Rozšiřitelnost:	Minimální rozšiřitelnost na 52 hotswap 2,5“ disků v rámci 2U.
Diskový řadič:	HW SAS 12Gbit/s RAID řadič s podporou RAID 1, 1+0, 5, 5+0,6, 6+0; 4 GB cache zálohovaná kapacitorem
Redundantní prvky:	Ventilátory a zdroje a HDD - vše vyměnitelné za provozu
Prediktivní analýza poruch:	Pevné disky, procesory, paměť
Rozhraní:	seriový port; USB. 1x SD/microSD slot
PCI sloty:	Podpora až 5x PCIe 3.0
Bezpečnost:	Systém musí umožňovat šifrování dat na interních pevných discích s podporou lokální i centrální správy šifrovacích klíčů
	Systém musí být schopen zajistit bezpečný provoz firmware komponent v serveru (minimálně HDD, SSD, síťové adaptéry, BIOS a vzdálenou správu) po celou dobu životnosti serveru. Server musí být schopen autonomně monitorovat autenticitu firmware na těchto komponentách. V případě zjištění neschváleného firmware musí být schopen automaticky uvést stav poškozené komponenty do bezpečného stavu. Pokud tato funkcionalita vyžaduje licenci, tak musí být součástí. Systém disponuje úložištěm firmwaru a driverů pro případ nutného rollbacku.
Dálková správa serveru:	Vzdálený „agentless“ přístup přes dedikované ethernet rozhraní.
	Řízení přístupových práv k centrální části SW a k management nástrojům na serverech pomocí účtů Active Directory domény.
	Ochrana heslem.
	Zabezpečení komunikace TLS 1.2 a vyšší; SSH.

	Zabezpečení serveru s podporou CNSA a FIPS 140-2.
	Vzdálený přístup umožňuje provést tyto operace se serverem: power on/off, reset, remote control, update BIOS, výběr bootovacího zařízení.
	GUI v HTML5 interface s možností využití běžných www prohlížečů integrovaných v desktopovém OS pro správu serverů (Firefox, Chrome atd.)
	Encryption Standard (3DES) pro zabezpečení komunikace s běžnými www prohlížeči.
	Kódování Advanced Encryption Standard (AES)
	Podpora monitoringu a záznamu změn v konfiguraci pro efektivnější diagnostiku a řešení případných problémů
	Podpora integrace managementu HW serveru do konzole Hypervizoru (MSSC, vCenter)
	Podpora automatického založení servisního případu v servisního střediska dodavatele/výrobce
	RESTful API rozhraní pro skriptování
	Podpora UEFI Secure Boot.
Další vlastnosti:	Z důvodu zachování jednotné správy HW, zadavatel požaduje plnou integraci s nástrojem HPE OneView, který již ve svém prostředí provozuje, zejména v podobě odesílání notifikací o HW závadě na servisní středisko výrobce, monitoring HW komponent, spotřeby energie, reporty o stavu firmware, vzdálená instalace a update firmware, jednotná inventory HW, včetně možnosti reportingu stavu spravované infrastruktury. Plnohodnotná a časově i licenčně neomezené funkce vzdálené správy.
Počet kusů:	1

Simac Technik ČR, a.s.
Sídlo
Radlická 740/113c
158 00 Praha 5 - Jinonice, ČR
Tel.: +(420) 283 061 281
Fax: +(420) 283 061 280

Provozovna Brno
Traťová 574/1
619 00 Brno
Tel.: +(420) 545 423 571
Fax: +(420) 545 423 570

IČ: 63079496
DIČ: CZ63079496
B. 3190 vedená u M. s. v Praze
http://www.simac.cz
e-mail: info@simac.cz

CENOVÁ KALKULACE

Zakázka č.: **VŠEOB747**

Číslo cenové nabídky: VŠEOB747-01

Dodávka nezbytné HW infrastruktury pro modernizaci NIS a jeho funkcionalit

Obchodník: Jílková Martina

Technický konzultant:

Datum vystavení: 06.08.2021

Poznámky:

Odběratel:

Všeobecná fakultní nemocnice v Praze
U nemocnice 499/2
128 00 Praha - Nové Město
Česká republika
IČ: 00064165 **DIČ: CZ00064165**

ID	Kód	Popis	Množství	Kusová cena	Sleva %	Cena / jedn. po slevě	Částka	DPH %	Částka DPH	Částka vč. DPH
		5x HPE Rack s příslušenstvím								
1	P9K39A	HPE 42U 600x1200 Ent G2 Pallet Rack	5,00 ks	50 347,95	56	22 153,10	110 765,50	21	23 260,76	134 026,26
2	P9L11A	HPE G2 Rack Grounding Kit	5,00 ks	2 168,00	55	975,60	4 878,00	21	1 024,38	5 902,38
3	P9L15A	HPE G2 Rack 42U 1075mm Side Panel Kit	1,00 ks	9 832,88	48	5 113,10	5 113,10	21	1 073,75	6 186,85
4	BW929A	HPE 1U 100-pack Black Universal Filler Panel	2,00 ks	10 927,92	52	5 245,40	10 490,80	21	2 203,07	12 693,87
5	P9L12A	HPE G2 Rack Baying Kit	4,00 ks	1 292,00	69	400,52	1 602,08	21	336,44	1 938,52
6	P9Q46A	HPE G2 Basic 7.3kVA/C13 C19 INTL PDU	20,00 ks	7 642,96	46	4 127,20	82 544,00	21	17 334,24	99 878,24
		Instalace								
7	HA113A1	HP CP Installation	1,00 ks	0,00	0	0,00	0,00	21	0,00	0,00
8	HA113A15BY	HPE Rack and Rack Options Install SVC	5,00 ks	9 948,00	45	5 471,40	27 357,00	21	5 744,97	33 101,97
		2x HPE Synergy 12000 Frame								
9	P06011-B21	HPE Synergy 12000 CTO Frame 10x Fan	2,00 ks	129 209,82	72	36 178,75	72 357,50	21	15 195,08	87 552,58
10	867796-B21	HPE VC SE 100Gb F32 Module	4,00 ks	416 077,98	58	174 752,75	699 011,00	21	146 792,31	845 803,31
11	841716-B21	HPE QSFP+ 40Gb Bi-Directional XCVR	8,00 ks	23 849,00	70	7 154,70	57 237,60	21	12 019,90	69 257,50

Vystavil:

Simac Technik ČR, a.s.
Sídlo
Radlická 740/113c
158 00 Praha 5 - Jinonice, ČR
Tel.: +(420) 283 061 281
Fax: +(420) 283 061 280

Provozovna Brno
Traťová 574/1
619 00 Brno
Tel.: +(420) 545 423 571
Fax: +(420) 545 423 570

IČ: 63079496
DIČ: CZ63079496
B. 3190 vedená u M. s. v Praze
http://www.simac.cz
e-mail: info@simac.cz

ID Kód	Popis	Množství	Kusová cena	Sleva %	Cena / jedn. po slevě	Částka	DPH %	Částka DPH	Částka vč. DPH
12 882251-B21	HPE SY 100GE/4x25GE/4x32GFC QSFP28 XCVR	8,00 ks	89 548,78	59	36 715,00	293 720,00	21	61 681,20	355 401,20
13 R3P67A	HPE Synergy 32Gb FC Upgrade FIO LTU	4,00 ks	65 677,78	55	29 555,00	118 220,00	21	24 826,20	143 046,20
14 876852-B21	HPE Synergy 4-port Frame Link Module	4,00 ks	27 375,00	72	7 665,00	30 660,00	21	6 438,60	37 098,60
15 453154-B21	HP BLc VC 1Gb RJ-45 SFP Opt Kit	4,00 ks	7 205,00	66	2 449,70	9 798,80	21	2 057,75	11 856,55
16 798096-B21	HPE Synergy 12000F 6x 2650W AC Ti FIO PS	2,00 ks	70 058,04	72	19 616,25	39 232,50	21	8 238,83	47 471,33
17 804938-B21	HPE Synergy 12000 Frame Rack Rail Option	2,00 ks	3 262,50	72	913,50	1 827,00	21	383,67	2 210,67
18 804943-B21	HPE Synergy 12000 Frame 4x Lift Handle	2,00 ks	2 387,00	72	668,36	1 336,72	21	280,71	1 617,43
19 872957-B21	HPE Synergy Composer2 Appliance	4,00 ks	109 390,18	72	30 629,25	122 517,00	21	25 728,57	148 245,57
20 845406-B21	HPE 100Gb QSFP28 to QSFP28 3m DAC	4,00 ks	10 927,94	66	3 715,50	14 862,00	21	3 121,02	17 983,02
21 487655-B21	HP BLc SFP+ 3m 10GbE Copper Cable	2,00 ks	5 036,76	66	1 712,50	3 425,00	21	719,25	4 144,25
	Instalace								
22 HA124A15ZQ	HPE Technical Installation Startup SVC	1,00 ks	69 711,00	45	38 341,05	38 341,05	21	8 051,62	46 392,67
23 HA124A15ZM	HPE Technical Installation Startup SVC	1,00 ks	327 916,13	69	101 654,00	101 654,00	21	21 347,34	123 001,34
	8x HPE Synergy 480 Gen10+								
24 P22139-B21	HPE Synergy 480 Gen10 Plus Base Chassis Configure-to-order Compute Module	8,00 ks	69 677,75	72	19 649,13	157 193,00	21	33 010,53	190 203,53
25 P36936-B21	Intel Xeon-Gold 6342 Processor	16,00 ks	99 578,95	66	33 856,84	541 709,50	21	113 759,00	655 468,50
26 P06035-B21	HPE 64GB 2Rx4 PC4-3200AA-R Smart Kit	96,00 ks	57 797,99	71	16 761,42	1 609 096,00	21	337 910,16	1 947 006,16
27 P36676-B21	HPE Synergy 480 Gen10 Plus without Drive Front Cage Kit	8,00 ks	5 475,00	72	1 533,00	12 264,00	21	2 575,44	14 839,44
28 P02054-B21	HPE Synergy 6820C 25/50Gb CNA	8,00 ks	32 827,68	72	9 191,75	73 534,00	21	15 442,14	88 976,14
29 P21868-B21	HPE 32GB microSD RAID 1 USB Boot Drive	8,00 ks	10 927,94	66	3 715,50	29 724,00	21	6 242,04	35 966,04
30 P37274-B21	HPE Synergy 480 Gen10 Plus CPU Front Heat Sink Kit	8,00 ks	8 321,88	72	2 330,13	18 641,00	21	3 914,61	22 555,61
31 P37275-B21	HPE Synergy 480 Gen10 Plus CPU Rear Heat Sink Kit	8,00 ks	9 307,59	72	2 606,13	20 849,00	21	4 378,29	25 227,29

Vystavil:

Simac Technik ČR, a.s.
Sídlo
Radlická 740/113c
158 00 Praha 5 - Jinonice, ČR
Tel.: +(420) 283 061 281
Fax: +(420) 283 061 280

Provozovna Brno
Traťová 574/1
619 00 Brno
Tel.: +(420) 545 423 571
Fax: +(420) 545 423 570

IČ: 63079496
DIČ: CZ63079496
B. 3190 vedená u M. s. v Praze
http://www.simac.cz
e-mail: info@simac.cz

ID Kód	Popis	Množství	Kusová cena	Sleva %	Cena / jedn. po slevě	Částka	DPH %	Částka DPH	Částka vč. DPH
	4xHPE SN3600B SAN switch								
32 Q1H72B	HPE SN3600B 32Gb 24/24 Power Pack+ Fibre Channel Switch	4,00 ks	694 034,82	72	194 329,75	777 319,00	21	163 236,99	940 555,99
33 P9H32A	HPE B-series 32Gb SFP28 Short Wave 1-pack Transceiver	88,00 ks	48 158,00	72	13 484,24	1 186 613,12	21	249 188,76	1 435 801,88
34 R6B13A	HPE B-series 32Gb SFP28 LW 1pk Sec XCVR	8,00 ks	158 161,61	72	44 285,25	354 282,00	21	74 399,22	428 681,22
35 Q9Y41AAE	HPE Network Orchestrator SW-6 E-LTU	4,00 ks	28 362,00	67	9 359,46	37 437,84	21	7 861,95	45 299,79
	Instalace								
36 HA113A15GA	HPE LowEnd SAN/Edge Switch/HAFM Inst SVC	4,00 ks	11 885,96	43	6 775,00	27 100,00	21	5 691,00	32 791,00
37 QK734A	HP Premier Flex LC/LC OM4 2f 5m Cbl	48,00 ks	2 496,94	68	799,02	38 353,00	21	8 054,13	46 407,13
38 QK735A	HPE Premier Flex LC/LC OM4 2f 15m Cbl	48,00 ks	3 548,00	67	1 170,84	56 200,32	21	11 802,07	68 002,39
	2xHPE Primera 600								
	Diskové pole								
39 N9Z47A	HPE Primera 600 4-way Storage Base	2,00 ks	76 678,85	74	19 936,50	39 873,00	21	8 373,33	48 246,33
40 581817-B21	HPE Configurator Defined Build Instruction Option	2,00 ks	22,00	90	2,20	4,40	21	0,92	5,32
41 N9Z63A	HPE Primera C650 4N Controller	2,00 ks	5 187 669,23	87	674 397,00	1 348 794,00	21	283 246,74	1 632 040,74
42 R0Q00A	HPE Primera 600 7.68TB SAS SFF (2.5in) FIPS Encrypted SSD	72,00 ks	705 332,94	86	98 746,61	7 109 756,00	21	1 493 048,76	8 602 804,76
43 N9Z39A	HPE Primera 600 32Gb 4p FC HBA	8,00 ks	307 080,36	86	42 991,25	343 930,00	21	72 225,30	416 155,30
44 716195-B21	HPE Ext 1.0m MiniSAS HD-MiniSAS HD Cbl	24,00 ks	2 386,89	66	811,54	19 477,00	21	4 090,17	23 567,17
45 N9Z51A	HPE Primera 600 2U 12d LFF Drv Encl	12,00 ks	88 015,98	73	24 010,76	288 129,10	21	60 507,11	348 636,21
46 R0Q04A	HPE Primera 600 8TB SAS 7.2K LFF FE HDD	120,00 ks	79 190,00	82	14 254,20	1 710 504,00	21	359 205,84	2 069 709,84
	Instalace								
47 HA124A15SY	HPE Technical Installation Startup SVC	2,00 ks	117 221,00	43	66 815,97	133 631,94	21	28 062,71	161 694,65
48 HA124A15Q3	HPE Technical Installation Startup SVC	12,00 ks	20 178,00	43	11 501,46	138 017,52	21	28 983,68	167 001,20
49 HA124A15R5	HPE Technical Installation Startup SVC	2,00 ks	156 280,74	43	89 080,02	178 160,04	21	37 413,61	215 573,65

Vystavil:

Simac Technik ČR, a.s.
Sídlo
Radlická 740/113c
158 00 Praha 5 - Jinonice, ČR
Tel.: +(420) 283 061 281
Fax: +(420) 283 061 280

Provozovna Brno
Traťová 574/1
619 00 Brno
Tel.: +(420) 545 423 571
Fax: +(420) 545 423 570

IČ: 63079496
DIČ: CZ63079496
B. 3190 vedená u M. s. v Praze
http://www.simac.cz
e-mail: info@simac.cz

ID	Kód	Popis	Množství	Kusová cena	Sleva %	Cena / jedn. po slevě	Částka	DPH %	Částka DPH	Částka vč. DPH
50	HU7C5A1	HPE Storage DM 40 Hours Phone Supp SVC	1,00 ks	29,00	0	29,00	29,00	21	6,09	35,09
51	H0JD6A1	HPE 3PAR SSD Extended Replacement SVC	72,00 ks	0,00	0	0,00	0,00	21	0,00	0,00
52	R1P29AAE	HPE Data Encryption E-LTU	2,00 ks	22,00	81	4,18	8,36	21	1,76	10,12
		1x HPE StoreOnce 5250								
53	BB958A	HPE StoreOnce 5250 Base System	1,00 ks	1 314 000,00	84	210 240,00	210 240,00	21	44 150,40	254 390,40
54	P19450-B21	HPE High Density Stor Encl 1U Suppt Tray	2,00 ks	10 512,00	23	8 094,24	16 188,48	21	3 399,58	19 588,06
55	BB968A	HPE StoreOnce 52/5650 120TB Drwr Upg Kit	1,00 ks	1 752 000,00	83	297 840,00	297 840,00	21	62 546,40	360 386,40
56	BB968A	HPE StoreOnce 52/5650 120TB Drwr Upg Kit	1,00 ks	1 752 000,00	84	280 320,00	280 320,00	21	58 867,20	339 187,20
57	BB976A	HPE StoreOnce 52/5650 88TB Cap Upg Kit	5,00 ks	1 423 500,00	88	170 820,00	854 100,00	21	179 361,00	1 033 461,00
58	BB982A	HPE StoreOnce Gen4 10/25Gb SFP Network Card	1,00 ks	54 750,00	85	8 212,50	8 212,50	21	1 724,63	9 937,13
59	BB990A	HPE StoreOnce Gen4 32Gb FC Network Card	2,00 ks	153 300,00	84	24 528,00	49 056,00	21	10 301,76	59 357,76
60	BB969A	HPE StoreOnce 52/5650 120TB Drwr Upg LTU	2,00 ks	22,00	84	3,52	7,04	21	1,48	8,52
61	BB977A	HPE StoreOnce 52/5650 88TB Cap Upg LTU	5,00 ks	22,00	84	3,52	17,60	21	3,70	21,30
62	BB983A	HPE StoreOnce Gen4 10/25Gb SFP Network Card LTU	1,00 ks	25,00	75	6,25	6,25	21	1,31	7,56
63	BB991A	HPE StoreOnce Gen4 32Gb FC Card LTU	2,00 ks	25,00	79	5,18	10,35	21	2,17	12,52
64	BB994AAE	HPE StoreOnce Encryption E-LTU	1,00 ks	22,00	83	3,65	3,65	21	0,77	4,42
		Instalace								
65	HA124A1	HP Technical Installation Startup SVC	1,00 ks	0,00	0	0,00	0,00	21	0,00	0,00
66	HA124A15T7	HPE StoreOnce Sing N Catalys Startup SVC	1,00 ks	89 712,98	43	51 136,40	51 136,40	21	10 738,64	61 875,04
67	HA124A15WQ	HPE StoreOnce 52/5650 Stup SVC	1,00 ks	66 659,00	43	37 995,63	37 995,63	21	7 979,08	45 974,71
		1x HPE Apollo 4200 Gen10								
68	P07246-B21	HPE Apollo 4200 Gen10 48SFF Configure-to-order Server	1,00 ks	91 980,00	55	41 391,00	41 391,00	21	8 692,11	50 083,11

Vystavil:

Simac Technik ČR, a.s.
Sídlo
Radlická 740/113c
158 00 Praha 5 - Jinonice, ČR
Tel.: +(420) 283 061 281
Fax: +(420) 283 061 280

Provozovna Brno
Traťová 574/1
619 00 Brno
Tel.: +(420) 545 423 571
Fax: +(420) 545 423 570

IČ: 63079496
DIČ: CZ63079496
B. 3190 vedená u M. s. v Praze
http://www.simac.cz
e-mail: info@simac.cz

ID	Kód	Popis	Množství	Kusová cena	Sleva %	Cena / jedn. po slevě	Částka	DPH %	Částka DPH	Částka vč. DPH
69	P19701-L21	Intel Xeon-Silver 4214R (2.4GHz/12-core/100W) FIO Processor Kit for HPE Apollo 4	1,00 ks	25 601,00	55	11 520,45	11 520,45	21	2 419,29	13 939,74
70	P19701-B21	Intel Xeon-Silver 4214R (2.4GHz/12-core/100W) Processor Kit for HPE Apollo 4200	1,00 ks	25 601,00	55	11 520,45	11 520,45	21	2 419,29	13 939,74
71	P00930-K21	HPE 64GB 2Rx4 PC4-2933Y-R Smart Kit	6,00 ks	57 798,00	77	13 293,54	79 761,24	21	16 749,86	96 511,10
72	P14010-B21	HPE Apollo 4200 6SFF SAS/SATA Rear Kit	1,00 ks	10 238,00	54	4 709,48	4 709,48	21	988,99	5 698,47
73	881457-K21	HPE 2.4TB SAS 12G Enterprise 10K SFF (2.5in) SC 3yr Wty 512e Digitally Signed Fi	32,00 ks	25 995,00	72	7 278,60	232 915,20	21	48 912,19	281 827,39
74	P09722-K21	HPE 1.92TB SATA MU SFF SC SM883 SSD	2,00 ks	79 858,00	77	18 367,34	36 734,68	21	7 714,28	44 448,96
75	P01367-B21	HPE 96W Smart Storage Battery 260mm Cbl	1,00 ks	3 373,00	66	1 146,82	1 146,82	21	240,83	1 387,65
76	830824-B21	Smart Array P408i/2 GB FBWC – 2x x4 interně Mini-SAS, 12 Gbit/s SAS RAID kontro	1,00 ks	16 403,00	66	5 577,02	5 577,02	21	1 171,17	6 748,19
77	869083-B21	HPE Smart Array P816i-a SR G10 LH Ctrlr	1,00 ks	28 229,00	66	9 597,86	9 597,86	21	2 015,55	11 613,41
78	P9M76A	HPE SN1600Q 32Gb Dual Port Fibre Channel Host Bus Adapter	2,00 ks	90 009,00	67	29 702,97	59 405,94	21	12 475,25	71 881,19
79	817718-B21	HPE 10/25GbE 2p SFP28 BCM57414 Adptr	1,00 ks	17 060,00	66	5 800,40	5 800,40	21	1 218,08	7 018,48
80	845398-B21	HPE 25Gb SFP28 SR 100m Transceiver	2,00 ks	37 208,00	66	12 650,72	25 301,44	21	5 313,30	30 614,74
81	830272-B21	HPE 1600W FS Plat Ht Plg LH Pwr Sply Kit	2,00 ks	10 841,00	66	3 685,94	7 371,88	21	1 548,09	8 919,97
82	BD505A	HPE iLO Adv incl 3yr TSU 1-Svr Lic	1,00 ks	10 650,00	55	4 845,75	4 845,75	21	1 017,61	5 863,36
83	P8B31A	HPE OV w/o iLO 3yr 24x7 FIO Phys 1 LTU	1,00 ks	9 837,00	55	4 475,84	4 475,84	21	939,93	5 415,77
84	P05045-B21	HPE DL325 Gen10 Serial Port Enable Kit	1,00 ks	767,00	35	498,55	498,55	21	104,70	603,25
85	822731-B21	HPE 2U Shelf-Mount Adjustable Rail Kit	1,00 ks	2 409,00	77	554,07	554,07	21	116,35	670,42
86	P09656-B21	HPE SA E/P FIO Ctlr for Rear Strg	1,00 ks	22,00	54	10,12	10,12	21	2,13	12,25
		Instalace								

Vystavil:

Simac Technik ČR, a.s.
Sídlo
Radlická 740/113c
158 00 Praha 5 - Jinonice, ČR
Tel.: +(420) 283 061 281
Fax: +(420) 283 061 280

Provozovna Brno
Traťová 574/1
619 00 Brno
Tel.: +(420) 545 423 571
Fax: +(420) 545 423 570

IČ: 63079496
DIČ: CZ63079496
B. 3190 vedená u M. s. v Praze
http://www.simac.cz
e-mail: info@simac.cz

ID	Kód	Popis	Množství	Kusová cena	Sleva %	Cena / jedn. po slevě	Částka	DPH %	Částka DPH	Částka vč. DPH
87	HA113A158Y	HPE Apollo 2000/4200 Install Service	1,00 ks	7 518,00	43	4 285,26	4 285,26	21	899,90	5 185,16
		HPE servisní podpora								
88		5-year service contract for products on offer	1,00 sl	5 438 003,86	0	5 438 003,86	5 438 003,86	21	1 141 980,81	6 579 984,67
89		Datecenter Care Contract	1,00 sl	1 157 000,00	0	1 157 000,00	1 157 000,00	21	242 970,00	1 399 970,00
90		Řízení projektu	22,00 hod	2 200,00	0	2 200,00	48 400,00	21	10 164,00	58 564,00
							27 093 542,00		**5 689 643,84**	**32 783 185,84**

Celkem CZK včetně DPH **32 783 185,84**

Vystavil:

Akceptační testy

Parametry akceptačních testů pro diskové pole:	Výkon diskového pole na front-end portech musí být minimálně 50 000 IOPS při velikosti bloku 64kB, poměru čtecích a zápisových operací 50%/50% a response time nejvýše 1ms, při zapnuté inline deduplikaci a kompresi.
	Součet testovacích LUNů musí být o velikosti minimálně čtyřnásobku cache diskového pole.
	Test musí běžet do celého objemu testovaných LUNů.
	Test musí běžet minimálně takovou dobu, aby se po dobu testu minimálně 2x přepsala cache diskového pole.
	Testovací servery, které budou gererovat zátěž pro tento test, tak zapůjčí dodavatel.
	Test musí proběhnout minimálně 3x a jako výsledek bude brán aritmetický průměr z těchto tří běhů.
	V případě neúspěchu je povoleno opakovat testy s novým nastavením maximálně 2x.
	Výkonnost bude ověřena pomocí nástroje vdbench nebo fio.
Parametry akceptačních testů pro blade servery:	Možnost vytváření a úpravy vzorových profilů pro deployment a životní cyklus serverů s těmito nastaveními: - nastavení verze BIOS - RAID konfigurace lokální storage - nastavení parametrů bootování - přiřazení SAN storage - nastavení sítí LAN - nastavení sítí SAN - nastavení verze firmware - nastavení verze ovladačů - vytvoření unikátního ID, které obsahuje MAC a WWN adresu
	Objednatel požaduje, aby k profilům blade serveru bylo možno přiřadit privátní či sdílený úložný prostor z lokálního uložiště, či z nabízeného externě připojeného SAN pole a zajistit tak plně automatický provisioning a zoning diskového prostoru jednotlivým blade serverům v souladu se zvoleným profilem.
	V rámci managementu blade platformy objednatel požaduje plnou správu přiděleného diskového prostoru z nabízené externí SAN storage zahrnující: - přímou tvorbu virtuálních disků na diskovém poli - přiřazení již vytvořených virtuálních disků - vytváření snapshotů a vytváření nových virtuálních disků ze snapshotů, jejich odebrání a mazání
Parametry akceptačních testů pro D2D zálohovací zařízení:	Provedení úspěšné instalace, konfigurace a otestování funkčnosti zálohovacího řešení objednatele.

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 plnění smlouvy musí definovat v interních předpisech, konfiguračních a instalačních manuálech, postupech nebo jiných dokumentech sloužících k předmětu dodávané služby či musí provádět:

2.1 Obecná pravidla bezpečnosti informací

- vydefinovaní rozsahu prací/služeb/podpory v kompetenci dodavatele a podmínky spolupráce mezi smluvními stranami,
- specifikovat popis používání každé služby provozované nebo spravované dodavatelem,
- stanovení 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 uživatelů a správců v metodách, postupech a v bezpečnosti,
- upřesnit podmínky spolupráce dodavatele se subdodavateli (třetí stranou),
- informovat o způsobu řízení rizik a o zbytkových rizicích,
- informovat o významné změně dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, či ekvivalentním postavení, nebo o změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy,
- provést neprodlené nahlášení identifikovaných bezpečnostních událostí a slabin kontaktní osobě za VFN,

2.2 Fyzická bezpečnost

- nastavení komplexních 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,
- dodržování režimových nebo organizační opatření VFN při vjezdu do objektů nebo vstupu do prostor nebo překonávání fyzických/logických zábran těchto objektů nebo prostor VFN,
- dobrovolně se podrobit případným kontrolám vnášených/vynášených osobních věcí nebo jakýchkoliv předmětů při vstupu nebo odchodu z objektů nebo prostor VFN prováděné oprávněnými zaměstnanci VFN (ostraha, vrátný, recepce apod.),
- neprovádět fotografování, video/audio záznam nebo kopírování/scanování dokumentů bez souhlasu oprávněného zaměstnance VFN. V prostorách kategorie zóny „C" (např. serverovna) pouze na základě písemného povolení vedení VFN,

2.3 Bezpečnost lidských zdrojů

- prokazatelné seznámení zaměstnanců dodavatele s dodržováním bezpečnostních pravidel a zásad požadovaných VFN,
- dodržovaní ochrany aktiv VFN před neautorizovaným přístupem, vyzrazením, modifikací, zničením nebo narušením,
- povinnost zachovávat mlčenlivost o důvěrných údajích nebo sděleních VFN a o jejich ochraně,
- stanovení odpovědností zaměstnanců dodavatele pro nakládání s informacemi,
- hlášení zjištěných bezpečnostních událostí nebo jiných bezpečnostních rizik,
- 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,

2.4 Řízení přístupu

- dodržován princip minimálních oprávnění: přidělována oprávnění na nejnižší možné úrovni, která umožní jejich správnou funkci,
- požadavky na řízení přístupu:
    - definovány procesy přidělování, správy oprávnění, pravidelné provádění auditu přidělených oprávnění a odstraňovány účty při odchodu zaměstnance nebo změně jeho zařazení,
    - privilegovaná oprávnění musí být přidělovány takovým způsobem, aby byla zajištěna jednoznačná auditovatelnost všech kroků provedených pod těmito účty ve vztahu ke konkrétním osobám,

2.5 Bezpečného chování uživatelů

Vztahuje se na prostředí VFN nebo zařízení používané ke správě nebo administraci předmětu smlouvy.

- 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,
- používat počítačové prostředky a SW vybavení VFN jen v rámci smluvního ujednání a jemu stanovené kompetence,
- je povinen respektovat VFN definovaná pravidla tvorby a nakládání s přístupovými hesly, zachování důvěrnosti 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 dbát předepsaným opatřením (aktualizace systému, spuštěný FW a antivir, využití veřejných sítí apod.) pro užití prostředků pro vzdálený přístup,

2.6 Bezpečnost mobilních zařízení a vzdáleného přístupu

- přístup externích zařízení je 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,

2.7 Ochrana před škodlivým kódem

- musí být zajištěna ochrana vnějšího perimetru dodavatele, komunikace, IS, úložišť a koncových stanic nebo mobilních zařízení před škodlivým kódem ve vztahu k dodavatelským pracím a službám zajišťující provoz a fungování základních služeb VFN,

2.8 Zálohování a obnova dat

- 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,

2.9 Technické zranitelnosti

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

2.10 Bezpečnost komunikační sítě

- omezit riziko napadení systémů nebo služeb prostřednictvím počítačové sítě, např.:
    - šifrováním,
    - řízená kontrola přístupu,
    - zamezení napadení aktivním útočníkem,
    - řízení zátěže,
    - zajištění integrity dat,
    - samostatné lokální sítě,
    - víceúrovňová bezpečnost,
    - využití vhodné sítě,

2.11 Bezpečnostní zásady pro práci s daty

- 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.),
- řízení přístupu k datům s využitím principu minimálních oprávnění,
- ochrana dat při přenosu, předání a v datovém úložišti,
- povinnost ochrany osobních údajů, a to především splnění technických nebo organizačních opatření, hlášení úniku osobních údajů, spolupráce na řešení incidentů nebo auditu ochrany osobních údajů apod.,

- dodržet závazek dodavatele (a subdodavatele) neporušovat integritu a dostupnost aktiv,
- stanovit omezení platná pro kopírování a šíření informací,
- přijmout opatření zajišťující vrácení či zničení informací po ukončení smluvního vztahu nebo v jeho průběhu,
- definovat postupy bezpečné likvidace dat,

2.12 Používání kryptografické ochrany

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

2.13 Akvizice, vývoj a údržba informačních systémů

- dodržování bezpečnostních pravidel, norem a best practices (např. OWASP - Open Web Application Security Project) v rámci celého životního cyklu nákupu a vývoje SW od zadání, návrhu, přes vývoj a testování až po nasazení do provozu,
- zavedení oddělení rolí vývoje, testu a provozu,
- vývojové, integrační, testovací a provozní prostředí musí být zcela oddělena v sítích a musí být podporována oddělenými stroji,
- zohlednění bezpečnostních požadavků VFN na dodávaný nebo vyvíjený SW, a to především:
    - podporované frameworky a platformy v prostředí VFN,
    - nefunkční bezpečnostní požadavky,
    - provedení ověření codereview v jednotlivých fázích vývoje a testování,
    - spolupráce na bezpečnostním testování včetně penetračních testů,
    - dodání systémové a provozní bezpečnostní dokumentace,
- vyjasnění vlastnictví a licenčních podmínek dodávaného nebo vyvíjeného kódu a jeho dat,
- stanoven způsob převzetí, akceptace a instalaci do produkčního prostředí,
- jasný a specifikovaný proces řízení změn,

2.14 Zvládání bezpečnostních incidentů

- mít zavedený systém hlášení, upozorňování a vyšetřování bezpečnostních nebo kybernetických incidentů a případů prolomení bezpečnosti,
- neprodlené oznámení bezpečnostním nebo kybernetickém incidentu a prolomení bezpečnosti,

- spolupráce na vyšetření, vyhodnocení a přijetí opatření z bezpečnostního nebo kybernetického incidentu,

2.15 Řízení kontinuity činností

- vytvoření takových postupů a fungujícího 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,
- provádění pravidelného testování, vyhodnocování a případně aktualizování havarijních plánů obnovy (DRP),

2.16 Legislativní a normativní požadavky

- splnění legislativních a normativních požadavků:
    - zákon č. 181/2014 Sb., o kybernetické bezpečnosti
        - vyhlášky 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),
        - zákona č. 110/2019 Sb., zpracování osobních údajů,
    - směrnice 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 souvisejících norem nebo best-practice,

2.17 Kontroly zavedení bezpečnostních opatření

- provádění kontroly zavedených bezpečnostních opatření dodavatelem v pravidelných intervalech a následné přijímání odpovídajících preventivních nebo systémových nebo organizačních opatření na zjištěné nedostatky nebo zranitelnosti,
- umožnit VFN ověření provádění kontrol a aplikaci následných opatření,

2.18 Audity plnění bezpečnostních požadavků

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

POUŽÍVÁNÍ SÍTĚ VFN EXTERNÍMI UŽIVATELI

Obsah

Zpracovatel:	Účinnost dokumentu od:	Schválil:
Mgr. Vojtěch Hána	23. 7. 2020	Mgr. Ivan Veselý, MBA
Garant:	**První vydání dne:**	**Dne:**
Michal Kocan Vedoucí odboru správy ICT	1. 1. 2008	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. +420 224 962 119,
- od 16:00 do 7:00 na Pohotovost ÚI na tel. +420 702 083 578.

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

4.2.2 Požadavky na připojené zařízení

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

4.2.3 Bezpečnostní incident nebo kybernetický útok

V případě bezpečnostní hrozby nebo kybernetického útoku má VFN právo zrušit povolení přístupu externího uživatele anebo VPN přístupu na dobu nezbytnou k analyzování hrozby nebo útoku a zabránění jakéhokoliv ohrožení sítě, informačních systémů a dat VFN. Pokud externí uživatel vykonává nebo má práva správce nebo

administrátora IS VFN, je povinen konat bezodkladně a zajistit dostatek důkazního materiálu dle povinností uvedených v příloze (Příloha č. 3 – Povinnost administrátora v případě bezpečnostního incidentu nebo kybernetického útoku).

4.2.4 Zakázané činnosti

Externí uživatel připojený do sítě VFN nesmí:

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

4.2.5 Monitoring činností

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

4.2.6 Porušení pravidel a povinností

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

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

Externí uživatel připojený do sítě VFN:

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

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. +420 224 962 119.

Metoda vzdáleného přístupu

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

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

POSTUP ZŘÍZENÍ PŘÍSTUPU EXTERNÍMU UŽIVATELI DO POČÍTAČOVÉ SÍTĚ VFN

Postup

Postup žádosti o povolení přístupu do počítačové sítě VFN:

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

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

Povinnosti, pravidla a omezení

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

- stanovené povinnosti, pravidla a případné restrikce v kap. 4.2 Řádu používání sítě VFN externími uživateli (SM-UI-02),
- při 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: +420 224 962 119
- E-mail: dispecink@vfn.cz

POVINNOST ADMINISTRÁTORA V PŘÍPADĚ BEZPEČNOSTNÍHO INCIDENTU NEBO KYBERNETICKÉHO ÚTOKU

Povinnosti administrátora

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

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

u tohoto incidentu či útoku je vždy povinen:

- zajistit kopie logů nebo transakčních záznamů, pokud by to nezpůsobilo jejich poškození nebo smazání,
- iniciovat nebo pozastavit šíření či poškození, zamezit incidentu nebo útoku,
- nemazat jakákoliv data o kybernetickém bezpečnostním incidentu bez svolení VFN, Policie ČR nebo NÚKIB,
- nahlásit toto podezření neodkladně na Pohotovost ÚI jako bezpečnostní nebo kybernetický incident:
    - v pracovní dny:
        - od 7:00 do 16:00 na Dispečink ÚI na tel. +420 224 962 119,
        - od 16:00 do 7:00 na Pohotovost ÚI na tel. +420 702 083 578.
    - o víkendu a svátcích na Pohotovost ÚI na tel. +420 702 083 578.