SMLOUVA O ZAJIŠTĚNÍ POSKYTOVÁNÍ SLUŽEB PODPORY PRODUKTŮ VMWARE

Data Protection Delivery Center, s.r.o.
Zapsána v obchodním rejstříku u Krajskéo soudu v Brně, sp.zn. C 83488
se sídlem: Rybkova 1016/31, PSČ: 602 00, Brno
IČO: 030 64 247 DIČ: CZ03064247
zastoupený: Ing. Petrem Klabenešem, jednatelem
bankovní spojení: [redacted]

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

a

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

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

uzavírají dnešního dne na základě výsledku **veřejné zakázky malého rozsahu** s názvem **„Zajištění podpory výrobce produktů VMware"**, zadávané v otevřeném řízení (dále jen „veřejná zakázka"), v souladu s ustanovením § 1746 odst. 2., zákona č. 89/2012 Sb., občanského zákoníku, v platném znění (dále jen „občanský zákoník."), tuto

smlouvu o zajištění poskytování služeb podpory výrobce produktů VMware

(dále jen „smlouva")

I. Předmět smlouvy

1. Poskytovatel se touto smlouvou zavazuje zajistit objednateli:

   a) poskytování služby podpory výrobce v rozsahu CoverageAcademic Production Support 24 hodin denně 7 dní v týdnu, a to na 1 rok pro 24 ks licencí VMware vSphere 7 Enterprise Plus for 1 processor objednatele pro již běžící kontrakty objednatele:

      - Contract ID: [redacted]

   b) poskytování služby podpory výrobce v rozsahu CoverageAcademic Production Support 24 hodin denně 7 dní v týdnu , a to na 1 rok pro 1 ks licence VMware vCenter Server 7 Standard for vSphere 7 (Per Instance) objednatele pro dále uvedené již běžící kontrakt objednatele:

      - Contract ID: [redacted]

   (dále též souhrnně „**předmět plnění**").

2. Dále se poskytovatel zavazuje zajistit aktivaci služeb podpory výrobce v souladu s čl. I a objednatel se zavazuje uhradit poskytovateli sjednanou odměnu, jakož i další závazky a práva smluvních stran z této smlouvy vyplývající.

3. Poskytovatel se zavazuje objednateli zpřístupnit údaje o platnosti a rozsahu podpory, kteréžto údaje bude možno kontrolovat na příslušném webovém portálu výrobce po přihlášení se již existujícím účtem objednatele.

4. Poskytovatel bere na vědomí, že se v důsledku dodávek předmětu plnění stává ve smyslu této smlouvyposkytovatelem technologií, na kterých je provozována základní služba objednatele, tedy služba "poskytování zdravotních služeb" dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „ZKB"). Objednatel je orgánem nebo osobou provozující základní službu podle § 3 písm. f) ZKB a provozování základní služby objednatelem podle ZKB je závislé na službě poskytované poskytovatelem.

II. Doba plnění, způsob poskytování podpory

1. Poskytovatel se zavazuje dodat předmět plnění objednateli ve smyslu této smlouvy, a to nejpozději do 15 kalendářních dnů ode dne nabytí účinnosti smlouvy.

2. Poskytovatel výslovně prohlašuje, že je držitelem certifikátu VMware Enterprise Partner s oprávněním poskytovat podporu produktu VMware ve všech úrovních s přístupem do všech jeho znalostních bází.

3. Dodávka se považuje podle této smlouvy za splněnou, pokud si objednatel bude moci podporu zkontrolovat na oficiálním webovém portále společnosti VMware ve svém profilu.

4. Základní formou podpory je přímý přístup k webovému portálu VMware a možnost stažení aktuálního software anebo update software přímo z oficiálních zdrojů výrobce.

5. Technologie objednatele jsou umístěny v sídle objednatele na adrese: Všeobecná fakultní nemocnice v Praze, U Nemocnice 499/2, PSČ: 128 08, Praha 2.

6. Poskytovatel se zavazuje splňovat/dodržet relevantní požadavky na řízení bezpečnosti informací uvedené v příloze č. 3 této smlouvy „Požadavky systému řízení bezpečnosti informací na dodavatele" vztahující se na prostředí a činnosti Poskytovatele.

7. Poskytovatel musí odpovědnou osobu Objednatele, tedy manažera kybernetické bezpečnosti, e-mail: managerKB@vfn.cz, neprodleně informovat o kybernetických bezpečnostních incidentech souvisejících s poskytováním služeb. Smluvní strany sjednávají, že porušení povinnosti ve smyslu čl. II odst. 7 této smlouvy je považováno za hrubé porušení smlouvy.

III. Cena a platební podmínky

1. Objednatel se zavazuje zaplatit poskytovateli za plnění ve smyslu této smlouvy cenu stanovenou dohodou smluvních stran, jejíž výše činí celkem 542 888,00 Kč bez DPH (slovy: pět set čtyřicet dva tisíc osm set osmdesát osm korun českých). Podrobný cenový rozpis je uveden v příloze č. 1 této smlouvy.

2. Smluvní strany prohlašují, že jim je známá skutečnosti, že poskytovatel není výrobcem předmětu plnění, nýbrž pouhým zprostředkovatelem prodeje. Z takového důvodu smluvní strany prohlašují, že berou na vědomí skutečnost, že cena je stanovena jako konečná a zahrnuje cenu uhrazenou výrobci předmětu plnění za poskytnutí podpory a veškeré náklady poskytovatele na plnění dle této smlouvy.

3. Cena za plnění dle této smlouvy bude hrazena jednorázově po dodání celého předmětu plnění na základě faktury vystavené poskytovatelem.

4. Daňový doklad (faktura) bude poskytovatelem vystaven, v souladu s ustanovením § 29 zákona č. 235/2004 Sb. o dani z přidané hodnoty, ve znění pozdějších předpisů, do 15 dnů od data uskutečnění zdanitelného plnění. Splatnost faktury je stanovena na 60 dní ode dne jejího doručení objednateli. Faktura bude zaslána elektronicky ve formátu ISDOC nebo PDF na adresu [redacted] nebo bude ve dvou vyhotoveních doručena na Ekonomický úsek zájemce, odbor účetnictví.

5. Pokud faktura nebude obsahovat všechny zákonem a touto smlouvou stanovené náležitosti, je objednatel oprávněn ji do 15 dnů od doručení vrátit poskytovatel i s tím, že poskytovatel je poté povinen vystavit novou fakturu s novým termínem splatnosti. V takovém případě objednatel není v prodlení s úhradou faktury.

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

IV. Trvání smlouvy

1. Tato smlouva se uzavírá na dobu určitou, tedy na dobu 1 roku ode dne aktivace podpory ve smyslu čl. I smlouvy, pročež tato nabývá platnosti dnem podpisu smluvními stranami a účinnosti dnem uveřejnění v registru smluv.

2. Smlouva může být před uplynutím smluvními stranami sjednané doby trvaní ve smyslu čl. IV. odst. 1 této smlouvy ukončena :
   - písemnou dohodou smluvních stran bez výpovědní doby;
   - odstoupením od smlouvy ze strany objednatele nebo poskytovatele bez výpovědní doby;

3. Kterákoliv ze smluvních stran je oprávněna odstoupit od smlouvy v případě, že druhá smluvní strana hrubě poruší nebo opakovaně porušuje své smluvní závazky vyplývající z této smlouvy a přes písemnou výzvu odmítá odstranit vady svého jednání, anebo nečiní žádné kroky k nápravě vzniklého vadného stavu nebo v případě porušení závazku mlčenlivosti druhou smluvní stranou. Za hrubé porušení smluvních závazků ze strany objednatele se považuje prodlení objednatele s úhradou faktur poskytovateli překračujícím o 90 dnů termín splatnosti. Za hrubé porušení smluvních závazků ze strany poskytovatele se považuje zejména nefunkčnost nebo nedostupnost některé z klíčových aplikací v rozsahu delším než 30 dnů.

4. Účinností odstoupení od smlouvy není dotčen nárok objednatele na náhradu škody vzniklé porušením podmínek této smlouvy, ani nárok na zaplacení smluvní pokuty.

V. Mlčenlivost

1. Poskytovatel se zavazuje zachovávat mlčenlivost ve vztahu ke všem informacím a skutečnostem, které se dozví o Objednateli, jeho zaměstnancích, pacientech atd. v souvislosti s uzavřením a plněním smlouvy, pokud tyto informace

mají povahu obchodního tajemství, osobních údajů nebo mají být z jiných důvodů chráněny před zveřejněním. Poskytovatel je povinen nakládat s osobními údaji a zejména s údaji o zdravotním stavu, genetickými a biometrickými údaji (dále jen „Osobní údaje") v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 (dále jen GDPR) a příslušnými ustanoveními zákona č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů.

2. Pokud Poskytovatel přijde při plnění Smlouvy do styku s Osobními údaji a bude v postavení zpracovatele ve smyslu GDPR a Zákona o zpracování osobních údajů, zavazuje se nakládat s Osobními údaji pouze za účelem splnění závazků z této Smlouvy a žádným jiným způsobem, a to v souladu s GDPR se Zákonem o zpracování osobních údajů a Zákonem o zdravotních službách. Zpracovávání Osobních údajů v rozsahu údajů poskytnutých Objednatelem a týkajících se zdravotnické dokumentace pacientů, jimž jsou Objednatelem poskytovány zdravotní služby, a dále v rozsahu osobních údajů zaměstnanců Objednatele, kteří jsou poskytovateli zdravotních služeb Poskytovatele, může zahrnovat odstranění potíží za účelem zabránění, vyhledávání a opravy problémů zjištěných při poskytování Služby, může také zahrnovat zlepšování funkcí informačních systémů, vyhledávání hrozeb uživatelům a ochrany uživatelů informačních systémů. Osobní údaje nebudou použity k jinému účelu, ani z nich nebudou odvozovány informace pro žádné reklamní či jiné komerční účely. Poskytovatel za účelem ochrany Osobních údajů Objednatele a jeho pacientů, zaměstnanců a klientů před neoprávněným přístupem, použitím, zveřejněním nebo zničením, resp. před jejich náhodnou ztrátou či změnou uplatňuje technická a organizační bezpečnostní opatření, interní kontroly a rutiny zabezpečení Osobních údajů zajišťující splnění všech povinností dle GDPR a Zákona o zpracování osobních údajů, zejména zajistí, aby data obsažená ve zdravotnické dokumentaci byla zabezpečena způsobem, který znemožní nahlížení do této zdravotnické dokumentace neoprávněným osobám.

3. Poskytovatel se zavazuje zajistit informovanost svých pracovníků o povinnostech vyplývajících z této Smlouvy. Poskytovatel se zavazuje zajistit, aby jeho zaměstnanci a/nebo Poddodavatelé přicházející při výkonu své práce do styku s Osobními údaji pacientů, zaměstnanců a klientů Objednatele, byli náležitě poučeni o povoleném způsobu nakládání s takovými údaji a byli seznámeni s následky jednání, které by bylo v rozporu se zákonnou úpravou a bezpečnostními směrnicemi Objednatele, s nimiž byli prokazatelně seznámeni. Poskytovatel se zavazuje informovat své poddodavatele o povinnosti mlčenlivosti dle této smlouvy. V případě porušení mlčenlivosti za strany poddodavatele, odpovídá zhotovitel objednateli za vzniklou škodu, jako kdyby povinnost porušil sám.

4. Smluvní strany se zavazují zachovat mlčenlivost též o všech ostatních skutečnostech, ve vztahu k nimž o to budou druhou stranou písemně požádány. Smluvní strany se též zavazují nevyužít informace podle prvé věty tohoto odstavce ve svůj prospěch nebo ve prospěch třetích osob v rozporu s účelem jejich předání. Povinnost mlčenlivosti o informacích a skutečnostech obchodního charakteru trvá po dobu 5 let od ukončení této smlouvy, o informacích obsahujících osobní údaje zaměstnanců objednatele trvá bez časového omezení.

5. Smluvní strany jsou povinny zajistit, že nebudou neoprávněně pořizovány kopie informací dle čl. V, odst. 1 této smlouvy, a nebudou zjišťovány informace, které nejsou nezbytně nutné ke splnění povinností vyplývajících z této smlouvy.

6. Smluvní strany se zavazují pro případ, že se v průběhu plnění dle této smlouvy dostanou do kontaktu s údaji druhé smluvní strany vyplývajícími z její provozní činnosti, tyto údaje v žádném případě nezneužít, nezměnit ani jinak nepoškodit, neztratit či neznehodnotit.

VI. Smluvní pokuty, sankce

1. Pro případ prodlení objednatele s úhradou ceny dle čl. III této smlouvy má poskytovatel nárok na zaplacení úroku z prodlení ze strany objednatele ve výši 0,01 % z částky, s jejíž platbou je objednatel v prodlení, za každý den takového prodlení. Smluvní strany se dohodly, že poskytovatel je oprávněn požadovat zaplacení úroku z prodlení až po uplynutí 30 dnů od sjednané lhůty splatnosti.

2. Poskytovatel je v případě nedodržení termínu plnění dle čl. II této smlouvy povinen uhradit objednateli smluvní pokutu ve výši 0,1% z celkové ceny za služby dle této smlouvy za každý i započatý den prodlení, jestliže se s objednatelem nedohodne jinak. Objednatel je dále v těchto případech oprávněn odstoupit od smlouvy.

3. V případě nedodržení povinnosti stanovené v čl. VII. odst. 2 smlouvy má objednatel právo účtovat smluvní pokutu ve výši pohledávky, která byla postoupena v rozporu s touto smlouvu. Objednatel má zároveň právo odstoupit od smlouvy.

4. V případě nedodržení povinnosti poskytovatele dle čl. VII. odst. 5 – 7 této smlouvy, má objednatel právo účtovat poskytovateli smluvní pokutu ve výši 10 000,- Kč za každé jednotlivé porušení.

5. V případě nedodržení povinností dle čl. V. této smlouvy má objednatel právo účtovat poskytovateli smluvní pokutu ve výši 200.000,- Kč za každé jednotlivé porušení povinnosti.

6. V případě sankcí nebo jiných finančních dopadů z poskytované podpory vyplývající z porušení nebo nedodržení povinností a náležitostí ZKB a povinností dle čl. II odst. 6 - 7 a čl. VII odst. 4 této smlouvy způsobené poskytovatelem, má objednatel právo účtovat poskytovateli smluvní pokutu ve výši 300 000,- Kč za každé jednotlivé porušení povinnosti.

7. 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. Poskytovatel bere na vědomí, že objednatel je povinen dle ustanovení § 219, odst. 1., písm. a) zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů a dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů zveřejnit tuto smlouvu včetně případných dodatků zákonem stanoveným způsobem.

2. Poskytovatel je oprávněn postoupit pohledávku vyplývající z plnění dle této smlouvy na třetí osobu pouze s předchozím písemným souhlasem objednatele.

3. Poskytovatel bere na vědomí, že objednatel je povinným subjektem podle zák. č. 106/1999 Sb., zákona o svobodném přístupu k informacím, ve znění pozdějších předpisů.

4. Poskytovatel bere na vědomí, že předmět plnění poskytovaný objednateli na základě a v souladu s touto smlouvou nesmí být provozovaný na technických nebo programových prostředcích označených Národním úřadem pro kybernetickou a informační bezpečnost jako hrozba. V případě porušení této povinnosti je objednatel oprávněn od smlouvy odstoupit.

5. Poskytovatel se zavazuje dodržovat nařízení objednatele, kterým je zakázáno kouření ve všech prostorách i plochách areálu nabyvatele s výjimkou vyhrazených míst.

6. Poskytovatel je povinen mít v platnosti a udržovat pojištění odpovědnosti za škodu způsobenou zadavateli či třetím osobám při výkonu podnikatelské činnosti, která je předmětem této smlouvy, s limitem pojistného plnění v minimální výši 1.000.000,- Kč.

7. Poskytovatel je povinen udržovat výše uvedené pojištění po celou dobu trvání smlouvy. V případě porušení této povinnosti je objednatel oprávněn od smlouvy, která je uzavřena na základě výsledku zadávacího řízení odstoupit. Na žádost objednatele je poskytovatel povinen předložit objednateli dokumenty prokazující, že pojištění v požadovaném rozsahu a výši trvá. Pokud by v důsledku pojistného plnění nebo jiné události mělo dojít k zániku pojištění, k omezení rozsahu pojištěných rizik, ke snížení stanovené min. výše pojistného plnění, nebo k jiným změnám, které by znamenaly zhoršení podmínek oproti původnímu stavu, je poskytovatel povinen učinit příslušná opatření tak, aby pojištění bylo udrženo tak, jak je požadováno v tomto ustanovení.

VIII. Závěrečná ujednání

1. 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.

2. Tato smlouva nabývá platnosti podpisem zástupců obou smluvních stran a účinnosti v souladu se zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv).

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 svými vlastnoručními podpisy.

V Praze dne:

V Brně dne:

Prof. MUDr. David Feltl, Ph.D., MBA
ředitel

Ing. Petr Klabeneš
jednatel

Přílohy:
Příloha č. 1 – Položkový ceník nabídka
Příloha č. 2 – Seznam oprávněných osob
Příloha č. 3 – Požadavky sytému řízení bezpečnosti informací na dodavatele

Příloha č. 1 smlouvy

Předmět plnění VZ	Popis	Množství	Jednotka	Nabídková cena/jednotka		Nabídková cena celkem		
				(bez DPH)	(s DPH)	(bez DPH)	Samostatně DPH (základní sazba)	(s DPH)
Zajištění poskytování podpory výrobce VMware v souladu se zadávacími podmínkami.	[redacted]	24	různé	21 122,00 Kč	25 557,62 Kč	506 928,00 Kč	106 454,88 Kč	613 382,88 Kč
	[redacted]	1	různé	35 960,00 Kč	43 511,60 Kč	35 960,00 Kč	7 551,60 Kč	43 511,60 Kč
Celková nabídková cena za celý předmět plnění bez DPH						542 888,00 Kč		

Příloha č. 2 smlouvy PO 744/S/22

Seznam oprávněných osob

A. Seznam kontaktních osob poskytovatele

Jméno	Funkce	e-mail - Telefonní číslo
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

B. Seznam kontaktních osob objednatele

Jméno	Funkce	Telefonní číslo/e-mail

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

Oblast	Funkce	Kontakt
Ochrana osobních údajů	[redacted]	[redacted]
Bezpečnosti informací, kybernetické bezpečnost	[redacted]	[redacted]

Požadavky systému řízení bezpečnosti informací na dodavatele

1 Účel

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

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

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

2 Bezpečnostní požadavky

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

Obecná pravidla bezpečnosti informací

Dodavatel je povinen:

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

Fyzická bezpečnost

Dodavatel je povinen:

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

Bezpečnost lidských zdrojů

Dodavatel je povinen:

- prokazatelně seznámit zaměstnance dodavatele s dodržováním bezpečnostních pravidel a zásad požadovaných VFN,
- dodržovat ochranu aktiv VFN před neautorizovaným přístupem, vyzrazením, modifikací, zničením nebo narušením,
- zachovávat mlčenlivost o důvěrných údajích nebo sděleních VFN a o jejich ochraně,
- stanovit odpovědnosti zaměstnanců dodavatele pro nakládání s informacemi,
- poučit zaměstnance dodavatele hlásit zjištěné bezpečnostní události nebo jiná bezpečnostní rizika odpovědné osobě dodavatele,
- provádět pravidelné školení zaměstnanců dodavatele v souvislosti s bezpečností informací,
- při porušení pracovních povinnosti zaměstnance dodavatele ve vztahu k bezpečnosti informací nebo způsobení bezpečnostního incidentu, musí být zahájeno formální disciplinární řízení. Způsob řízení odpovídá povaze porušení nebo incidentu a jeho dopadu na VFN.

Řízení přístupu

Dodavatel je povinen:

- dodržovat princip minimálních oprávnění: přidělovat oprávnění na nejnižší možné úrovni, která umožní jejich správnou funkci,
- dodržovat požadavky na řízení přístupu:
    - definovat procesy přidělování, správy oprávnění, pravidelně provádět audit přidělených oprávnění a odstraňovat účty při odchodu zaměstnance nebo změně jeho zařazení,

- přidělovat privilegovaná oprávnění takovým způsobem, aby byla zajištěna jednoznačná auditovatelnost všech kroků provedených pod těmito účty ve vztahu ke konkrétním osobám.

Bezpečné chování uživatelů

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

Zaměstnanec dodavatele:

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

Bezpečnost mobilních zařízení a vzdáleného přístupu

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

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

Ochrana před škodlivým kódem

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

Zálohování a obnova dat

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

Zálohovaná data musí splňovat požadavky:

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

Technické zranitelnosti

Dodavatel je povinen:

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

Bezpečnost komunikační sítě

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

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

Bezpečnostní zásady pro práci s daty

Dodavatel je povinen:

- dodržovat stanovená pravidla ochrany dat zahrnující speciální nakládání s tajnými, důvěrnými, osobními a citlivými údaji dle jednotlivých zákonů (např. nařízení č. 2016/679 - GDPR, zákona č. 110/2019 Sb., zákon č. 412/2005 Sb. apod.),

- zajistit řízení přístupu k datům s využitím principu minimálních oprávnění,
- ochránit data při přenosu, předání a v datovém úložišti,
- plnit povinnosti ochrany osobních údajů, a to především technická nebo organizační opatření, hlášení úniku osobních údajů, spolupráce na řešení incidentů nebo auditu ochrany osobních údajů apod.,
- dodržet závazek dodavatele (a subdodavatele) neporušovat integritu a dostupnost aktiv,
- stanovit omezení platná pro kopírování a šíření informací,
- přijmout opatření zajišťující vrácení či zničení informací po ukončení smluvního vztahu nebo v jeho průběhu,
- definovat postupy bezpečné likvidace dat.

Používání kryptografické ochrany

Dodavatel je povinen:

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

Akvizice, vývoj a údržba informačních systémů

Dodavatel je povinen:

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

Zvládání bezpečnostních incidentů

Dodavatel je povinen:

- mít ve svém prostředí zavedený systém hlášení, upozorňování a vyšetřování bezpečnostních nebo kybernetických incidentů a případů prolomení bezpečnosti,

- neprodleně oznámit objednateli bezpečnostní nebo kybernetický incidenty a prolomení bezpečnosti v prostředí dodavatele nebo objednatele,
- spolupracovat s objednatelem na vyšetření, vyhodnocení a přijetí opatření z bezpečnostního nebo kybernetického incidentu v prostředí objednatele.

Řízení kontinuity činností

Dodavatel je povinen:

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

Legislativní a normativní požadavky

Dodavatel je povinen splnit legislativní a normativní požadavky:

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

Kontroly zavedení bezpečnostních opatření

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

Audity plnění bezpečnostních požadavků

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