Smlouva o poskytování rozšířené podpory výpočetní techniky a programového vybavení

číslo: SOAP/01-2372/2026-2, JID: SOAP266505

uzavřená podle § 1746 odst. 2 a souvisejících zákona č. 89/2012 Sb., občanský zákoník.

Smluvní strany

1. Poskytovatel:

Název:	**3S.cz, s. r. o.**
Sídlo:	Eliášova 1055/25, 616 00 Brno
Zastoupená:	Ing. Jiřím Dražilem, prokuristou
Zapsaná:	u Krajského soudu v Brně, oddíl C, vložka 51803
IČ:	27683273
DIČ:	CZ27683273
Bankovní spojení:	Komerční banka, a. s.
Číslo účtu:	35-4490910207/0100
ID datové schránky:	qwhdqm2
Telefon:	
Kontaktní osoba:	
E-mail:	

dále jen „**poskytovatel**"

a

2. Objednatel

Název:	**Státní oblastní archiv v Plzni**
Sídlo:	Sedláčkova 44, 306 12 Plzeň
Zastoupená:	doc. PhDr. Karlem Řeháčkem, Ph.D., ředitelem
IČ:	70979090
DIČ:	neplátci DPH
Bankovní spojení:	Česká národní banka
Číslo účtu:	4245881/0710
ID datové schránky:	b9xaiw4
Telefon:	
Kontaktní osoby:	
E-mail:	

dále jen „**objednatel**"

uzavírají níže uvedeného dne smlouvu o poskytování služeb rozšířené podpory výpočetní techniky a programového vybavení za níže uvedených podmínek.

Článek 1
Předmět plnění

1. Předmětem smlouvy je vzdálená údržba, konfigurační zásahy a udržování aktuálních firmware výpočetní techniky a programového vybavení dodavatelem pro potřeby objednatele a dle jeho pokynů. Jedná se o následující systémy:

   - Virtualizační software VMware pro 3 fyzické servery
   - Software pro správu virtuálního prostředí vCenter
   - Software pro správu diskových polí Hitachi – Storage Navigator Modular 2
   - Software pro dohled diskových polí do dohledového centra – Hitachi Hi-Track Monitor
   - Diskové pole Infortrend Enterprise Storage System DS1000 (Cheb)
   - Diskové pole PetaStor (2 ks – Plzeň, Klášter)
   - Network Attached Gateway HNAS4060 (Plzeň)
   - Diskové pole Hitachi VSP G600 (Plzeň)
   - Zálohovací knihovna Quantum Scalar i500 (Plzeň)
   - Zálohovací knihovna Quantum Scalar i3 (Cheb)
   - Zálohovací knihovna actiLib (Klášter)
   - Switche Edgecore (Plzeň)
   - Software pro zálohování dat Veritas Backup Exec (4x V-RAY Edition – Plzeň, 2x Server Edition – Cheb a Nepomuk, 1x NDMP Option – Plzeň)
   - Údržba aktuálnosti Firmware diskových polí Hitachi, realizace konfiguračních opatření dle potřeb objednatele
   - Údržba aktuálnosti Firmware zálohovacích knihoven Quantum Scalar i500, Quantum Scalar i3, actiLib, realizace konfiguračních opatření dle potřeb objednatele
   - Údržba aktuálnosti Firmware diskových polí PetaStor, realizace konfiguračních opatření dle potřeb objednatele
   - Údržba, řešení situací selhání zálohovacích úloh a v rámci řízení změn i rekonfigurace zálohovacích úloh zálohovacího software Backup Exec, realizace konfiguračních opatření dle potřeb objednatele
   - Zálohování do S3 úložiště a ochrana proti ransomware

2. Poskytovatel se zavazuje provádět na vyžádání objednatele, minimálně však jednou za 14 dní, průběžnou preventivní kontrolu výše uvedených systémů, logů a ověření, zda systémy jsou funkční a probíhá backup. Poskytovatel se zavazuje neprodleně o případných nedostatcích informovat objednatele.

3. Poskytovatel se zavazuje provádět změny konfigurace hardware a software na vyžádání objednatele a s tím spojené případné úpravy zálohovacích procesů.

4. Poskytovatel se zavazuje po dohodě s objednatelem provádět komplexní patch management, tj. udržování výše uvedených software a firmware v aktuálních či ve výrobcem příslušného zařízení doporučených verzí.

5. Poskytovatel se zavazuje jednou provést performance analýzu diskového pole, jejímž cílem je ověření vytížení prostředků diskového pole a kontrola, zda nedochází v některých systémech diskového pole k přetížení či jiným situacím, které by mohly mít negativní dopad na chod aplikací.

6. Poskytovatel se zavazuje jednou provést technickou profylaxi vybavení dle článku 1.1 smlouvy s cílem optimalizace jejich chodu a odstranění zjištěných nekonzistencí.

7. Poskytovatel se zavazuje po dohodě s objednatelem minimálně dvakrát provést v součinnosti s objednatelem test obnovy zálohovaných dat v dohodnutém rozsahu minimálně pro tři objednatelem určené systémy a vyhotovit písemný zápis o výsledcích testu.

8. Poskytovatel se zavazuje k součinnosti s objednatelem při vytváření, úpravách a dokumentaci systému řízení bezpečnosti informací v oblasti politiky zálohování, ukládání a obnovy dat, v oblasti politiky bezpečnosti komunikační sítě a v oblasti politiky zvládání kybernetických událostí a incidentů při detekci kybernetických událostí včetně součinnosti při případném napojení nástroje pro detekci kybernetických událostí na systémy dle článku 1.1 smlouvy.

9. Předmětem smlouvy není odstraňování případných vad produktů. Odstranění vad je řešeno separátně v rámci záručních podmínek výše uvedených produktů.

10. Objednatel bere na vědomí, že poskytovatel může úspěšně provádět udržování aktuálních SW verzí (PatchManagement) jen u těch produktů, kde má objednatel na příslušnou licenci nárok. Z titulu licenčních podmínek je toto právo podmíněno platným support/subscription kontraktem objednatele s výrobcem daného produktu.

11. Poskytovatel se zavazuje předávat objednateli aktuální údaje o konfiguraci systému a přístupové údaje zajišťující maximální oprávnění všem komponentům systému. Objednatel se zavazuje, že z důvodu bezpečnosti přístupové údaje bude uchovávat v tajnosti a po dobu trvání smlouvy nebude bez dohody s poskytovatelem měnit konfiguraci jednotlivých částí systému.

Článek 2
Podmínky a způsob provádění údržby

1. Poskytovatel provádí údržbu s využitím technických prostředků vzdálené správy. Objednatel se zavazuje vyvinout nezbytnou součinnost pro řádné plnění povinností poskytovatele, zejména pak umožnění vzdáleného přístupu a případnou součinnost při úkonech, kde je vyžadována asistence v místě instalace.

2. Poskytovatel se zavazuje realizovat požadavky objednatele na konfigurační změny a údržbu na základě požadavků objednatele a po vzájemně odsouhlaseném plánu prací. Poskytovatel je poté povinen nastoupit k realizaci dohodnutých úkonů na základě výzvy objednatele, nejpozději však do tří pracovních dnů.

Článek 3
Cena

1. Cena za plnění dle této smlouvy je stanovena na základě dohody smluvních stran takto:

   Cena za poskytování služeb za jeden měsíc:

Cena bez DPH:	11 500,00 Kč / za měsíc
DPH 21 %:	2 415,00 Kč / za měsíc
Celková cena včetně DPH:	13 915,00 Kč / za měsíc

2. V případě jiné sazby DPH bude poskytovatel objednateli účtovat sazbu DPH ve výši odpovídající platným a účinným právním předpisům. Cena za plnění bez DPH tímto není dotčena.

Článek 4
Místa plnění

Místy plnění jsou:

- Státní oblastní archiv v Plzni, Sedláčkova 44, Plzeň
- Státní oblastní archiv v Plzni, pracoviště Klášter, Klášter 101, Klášter u Nepomuka
- Státní okresní archiv Cheb, Františkánské náměstí 14, Cheb

Článek 5
Platební podmínky

1. Cena plnění bude objednatelem uhrazena na základě daňového dokladu (faktury), který je poskytovatel oprávněn vystavit po podpisu této smlouvy.
2. Splatnost daňového dokladu (faktury) je stanovena na 21 dnů ode dne jejího doručení objednateli.
3. Daňový doklad bude zasílán měsíčně elektronicky na e-mailovou adresu 
4. Daňový doklad (faktura) musí obsahovat všechny náležitosti řádného účetního a daňového dokladu ve smyslu příslušných zákonných ustanovení. V případě, že faktura nebude mít odpovídající náležitosti, je objednatel oprávněn zaslat ji ve lhůtě splatnosti zpět poskytovateli k doplnění, aniž se tak dostane do prodlení se splatností; lhůta splatnosti počíná běžet znovu od opětovného doručení náležitě doplněného či opraveného dokladu.

Článek 6
Smluvní pokuty a sankce

Smluvní strany se dohodly, že:

1. V případě prodlení objednatele s plněním peněžitého závazku je poskytovatel oprávněn objednateli účtovat úroky z prodlení ve výši 0,05% z dlužné částky za každý den prodlení.

2. Objednatel je oprávněn požadovat smluvní pokutu ve výši 500 Kč za každý započatý den prodlení s realizací dohodnutých prací. V případě prodlení poskytovatele po dobu delší 14 dnů má objednatel právo od smlouvy odstoupit či ji vypovědět.

3. Poskytovatel je povinen mít po celou dobu trvání smlouvy sjednáno pojištění odpovědnosti za škodu způsobenou třetí osobě, a to s limitem pojistného plnění ve výši nejméně 2 mil. Kč.

Článek 7
Doba trvání smlouvy a odstoupení od smlouvy

1. Smlouva se sjednává na období ode dne nabytí účinnosti smlouvy do 31. 5. 2027 s tříměsíční výpovědní lhůtou, kterou může uplatnit každá ze smluvních stran. Výpovědní lhůta počíná běžet vždy prvním dnem kalendářního měsíce následujícího po doručení výpovědi druhé smluvní straně.

2. Smlouvu mohou ukončit obě strany dohodou, která musí mít písemnou formu a musí být prokazatelně doručena druhé straně.

3. Smluvní strany se dohodly na možnosti odstoupení od smlouvy v případě, že druhá smluvní strana závažným způsobem porušila povinnosti pro ni vyplývající z této smlouvy nebo právních předpisů nebo za podmínek stanovených občanským zákoníkem.

4. Odstoupení od smlouvy musí být prokazatelně (prostřednictvím doporučeného dopisu nebo datové schránky) písemně oznámeno druhé smluvní straně a je účinné dnem doručení tohoto oznámení druhé smluvní straně. Dále se postupuje v souladu s ustanovením § 2001 a následujících občanského zákoníku.

Článek 8
Povinnost mlčenlivosti, ochrana osobních údajů

1. Smluvní strany se zavazují zachovávat ve vztahu ke třetím osobám mlčenlivost o informacích, které při plnění této smlouvy vzájemně získají o sobě či o svých zaměstnancích, které nejsou veřejně známé nebo známé třetí straně a které lze s přihlédnutím k okolnostem a obchodním zvyklostem označit za důvěrné, a nesmí je použít v rozporu s účelem této smlouvy ani je poskytnout bez písemného souhlasu druhé smluvní strany žádné třetí osobě (s výjimkou zákonných případů).

2. Smluvní strany jsou povinny zajistit, že nebudou neoprávněně pořizovány kopie důvěrných informací a že nebudou zjišťovány informace, které nejsou nezbytně nutné ke splnění povinností vyplývajících z této smlouvy.

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

4. Smluvní strany se zavazují chránit osobní údaje. Pokud se smluvní strany v rámci plnění této smlouvy dostanou do kontaktu s osobními údaji, jsou povinny je ochraňovat a nakládat s nimi v souladu s příslušnými právními předpisy, a to i po ukončení této smlouvy.

5. Pro účely této smlouvy je objednatel správcem osobních údajů a poskytovatel jejich zpracovatelem ve smyslu čl. 4 GDPR. Smluvní strany sjednávají rámec zpracování dle čl. 28 odst. 3 GDPR:

   a) **předmět a doba zpracování:** osobní údaje nezbytné pro poskytování služeb dle čl. 1 této smlouvy; zpracování trvá po dobu účinnosti smlouvy a nezbytnou dobu k vypořádání práv a povinností stran, nejdéle však šedesát dnů po ukončení smlouvy, nevyžaduje-li právní předpis dobu delší;

   b) **povaha a účel zpracování:** vzdálená údržba, konfigurační zásahy, zálohování, obnova a související podpora systémů dle čl. 1;

   c) **typy osobních údajů:** osobní údaje obsažené v datech zpracovávaných, zálohovaných a obnovovaných v rámci spravovaných systémů, dále systémové identifikátory, autentizační údaje a provozní a aplikační logy;

   d) **subjekty údajů:** zejména zaměstnanci, spolupracovníci a uživatelé objednatele a osoby, jejichž osobní údaje jsou obsaženy v datech objednatele;

   e) **audit:** objednatel je oprávněn ověřovat plnění povinností poskytovatele dle tohoto článku; podrobnosti kontrol a auditů upravuje příloha č. 1 bod 2.4;

   f) **součinnost:** poskytovatel přiměřeně napomáhá objednateli při plnění povinností podle čl. 32 až 36 GDPR a při vyřizování práv subjektů údajů.

6. Poskytovatel bude zpracovávat osobní údaje pouze na základě písemných pokynů objednatele. Poskytovatel nebude předávat osobní údaje do třetích zemí mimo EU/EHS bez předchozího písemného souhlasu objednatele a bez splnění požadavků kapitoly V. GDPR. Poskytovatel zajistí, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti.

7. Pokud bude vzdálená údržba poskytována mimo území České republiky, zajistí poskytovatel její provádění způsobem, který bude minimalizovat rizika týkající se ochrany osobních údajů a zájmů objednatele. Úmysl poskytovat vzdálenou údržbu mimo území České republiky oznámí poskytovatel objednateli před započetím poskytování vzdálené údržby mimo území České republiky a uvede z jakého státu (nebo států) bude vzdálená údržba poskytována a jaká technická opatření k zabezpečení přenosu dat budou učiněna.

8. Poskytovatel nesmí zapojovat do svých činností pro objednatele kromě svých zaměstnanců žádné další osoby bez předchozího písemného povolení objednatele.

9. Zjistí-li poskytovatel porušení zabezpečení osobních údajů, ohlásí je bez zbytečného odkladu objednateli.

10. Poskytovatel odpovídá objednateli v plné míře za škodu, kterou mu způsobí porušením povinnosti mlčenlivosti nebo povinnosti vztahující se k ochraně osobních údajů nebo povinnosti vztahující se k bezpečnostním opatřením vyplývající z této smlouvy.

11. Poruší-li poskytovatel povinnost mlčenlivosti nebo povinnost vztahující se k ochraně osobních údajů nebo povinnost vztahující se k bezpečnostním opatřením vyplývající z této smlouvy, je povinen zaplatit objednateli smluvní pokutu ve výši 50 000 Kč za každé nikoli nepodstatné porušení takové povinnosti.

12. Účinnost ustanovení tohoto článku přetrvá i po ukončení účinnosti této smlouvy z jakéhokoliv důvodu.

Článek 9
Závěrečná ustanovení

1. Tato smlouva nabývá platnosti podpisem obou smluvních stran a účinnosti od 1. 6. 2026, nejdříve však dnem uveřejnění prostřednictvím registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, ve znění pozdějších předpisů. Poskytovatel se zavazuje realizovat zveřejnění této smlouvy v předmětném registru v souladu s uvedeným zákonem.

2. Smlouvu lze měnit či doplňovat pouze vzestupně očíslovanými písemnými dodatky, které se stanou nedílnou součástí této smlouvy. Dodatky musí být podepsané oprávněnými zástupci obou smluvních stran.

3. Tato smlouva je vyhotovena v elektronické podobě, smlouvu podepsanou oběma smluvními stranami obdrží obě smluvní strany.

4. Záležitosti v této smlouvě výslovně neupravené se řídí příslušnými ustanoveními občanského zákoníku v účinném znění.

5. Objednatel i poskytovatel se zavazují vzájemně informovat o všech organizačních změnách (název, sídlo, telefon apod.).

6. Smluvní strany se zavazují, že veškeré spory vzniklé v souvislosti s realizací smlouvy budou řešeny smírnou cestou – dohodou. Nedojde-li k dohodě, budou spory řešeny před příslušnými obecnými soudy České republiky.

7. Vzhledem k veřejnoprávnímu charakteru objednatele poskytovatel bezvýhradně souhlasí se zveřejněním jakékoli části i plného znění této smlouvy včetně dodatků za podmínek vyplývajících z příslušných právních předpisů (zejména zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů a zákona číslo 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, ve znění pozdějších předpisů). Text této smlouvy, dodatků ani příloh této smlouvy se nepovažuje za obchodní tajemství.

8. Obě smluvní strany prohlašují, že si tuto smlouvu před podpisem přečetly, smlouvu uzavřely svobodně a vážně, že považují obsah této smlouvy za srozumitelný, že jsou jim známy veškeré skutečnosti, jež jsou pro uzavření této smlouvy rozhodující, že se na ustanoveních této smlouvy dohodly jasně a určitě tak, aby kvůli nim nedošlo ke sporům, a že smlouva nebyla uzavřena v tísni, ani za jednostranně nevýhodných podmínek, na důkaz čehož připojují smluvní strany k této smlouvě své podpisy.

9. Nedílnou součástí této smlouvy je následující příloha:

    - Příloha č. 1 – Bezpečnostní opatření

Za objednatele elektronicky podepsáno

doc. PhDr. Karel Řeháček, Ph.D.
v zastoupení Ing. Danuše Dostálová

Za poskytovatele elektronicky podepsáno

Ing. Jiří Dražil

Příloha č. 1 – Bezpečnostní opatření

1. Úvod

Tato příloha smlouvy stanovuje bezpečnostní opatření zejména pro naplnění požadavků vyplývajících ze zákona č. 264/2025 Sb., o kybernetické bezpečnosti, (dále jen „ZoKB"), a prováděcích vyhlášek č. 408/2025 Sb., o regulovaných službách, a č. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností (dále jen „VyKB").

2. Bezpečnostní požadavky

2.1. Účel

1. Tato příloha smlouvy stanoví způsoby a úrovně realizace bezpečnostních opatření pro poskytovatele a určuje vzájemný vztah odpovědnosti za zavedení a kontrolu bezpečnostních opatření mezi objednatelem a poskytovatelem. Požadavky na poskytovatele jsou definovány dle platné právní úpravy, především pak dle ZoKB a VyKB pro poskytování služeb v režimu nižších povinností.
2. Smluvní strany se dohodly, že pokud to bude potřebné ke splnění požadavků ZoKB, VyKB, či souvisejících právních předpisů z oblasti bezpečnosti informací, uzavřou bez zbytečného odkladu po výzvě kterékoli smluvní strany písemný dodatek smlouvy zohledňující takové požadavky.

2.2. Obecné bezpečnostně provozní požadavky

Poskytovatel se při poskytování plnění pro objednatele zavazuje plnit následující povinnosti:

1. postupovat v souladu s účinnými právními předpisy, zejména pak požadavky vyplývajícími pro poskytovatele, jakožto významného dodavatele významného informačního systému, ze ZoKB a VyKB a reflektovat případné novely dotčených právních předpisů či novou právní úpravu, a bezpečnostními politikami stanovenými systémem řízení bezpečnosti informací (ISMS) objednatele dle specifikace předmětu veřejné zakázky;
2. kontaktní osoba poskytovatele uvedená ve smlouvě je zodpovědnou kontaktní osobou pro potřeby zajištění plnění bezpečnostních požadavků vyplývajících ze smlouvy a této přílohy a související komunikace mezi smluvními stranami (dále také jen „kontaktní osoba pro bezpečnost na straně poskytovatele");
3. prokazatelně seznámit všechny osoby podílející se na poskytování plnění této smlouvy za stranu poskytovatele a/nebo jeho poddodavatelů s těmito bezpečnostními požadavky;
4. minimálně 1x ročně poskytnout součinnost objednateli při identifikaci a hodnocení aktiv a rizik souvisejících s předmětem plnění a na základě výsledků navrhnout a předložit objednateli ke schválení opatření na minimalizaci nebo odstranění zjištěných rizik s přihlédnutím k výsledkům posuzování rizik i z hlediska dopadu na práva a svobody subjektů údajů;

5. dodržovat příslušná ustanovení bezpečnostních politik, metodik a postupů předaných poskytovateli objednatelem, k jejímuž dodržování se poskytovatel zavázal, pokud byl poskytovatel s takovými dokumenty nebo jejich částmi seznámen, a to bez ohledu na způsob, jakým byl s takovou dokumentací objednatele seznámen (např. školením, protokolárním předáním příslušné dokumentace poskytovateli, elektronickým předáním prostřednictvím e-mailu či datovou schránkou, zřízením přístupu poskytovateli na sdílené úložiště aj.);

6. rozvíjet bezpečnostní povědomí svých zaměstnanců a příp. dalších osob, které se podílejí na plnění smlouvy a průběžně je seznamovat s prováděnými nebo plánovanými změnami; zaměstnanci a další osoby na straně poskytovatele podílející se na plnění smlouvy musí být prokazatelně seznámeni s platnými předpisy a bezpečnostními požadavky objednatele, a to ještě před zahájením jakékoli činnosti ze strany těchto osob pro objednatele v souvislosti s plněním této smlouvy;

7. zaznamenávat a na vyžádání objednateli poskytnout veškeré podstatné okolnosti související s poskytovaným předmětem plnění dle smlouvy (technické záznamy, organizační záznamy o školení, pověření apod.);

8. přidělovat svým jednotlivým pracovníkům oprávnění k výkonu činností a přísně při tom dodržovat bezpečnostní zásadu tzv. „potřeba vědět" (need-to-know principle), tedy zejména dbát o to, aby byla minimalizována rizika nežádoucího přístupu k aktivům objednatele;

9. garantovat dostupnost, důvěrnost plnění a integritu předávaných dat s tím, že dodávané služby musí být v souladu s uzavřeným smluvním vztahem provozně monitorovány a vyhodnocovány;

10. průběžně dokumentovat, kontrolovat a vyhodnocovat oprávněnost přístupu, jak fyzického, tak i logického, u všech osob na straně poskytovatele, které přistupují k předmětu plnění dle této smlouvy;

11. zavést opatření pro ochranu zálohy dat vztahujících se k plnění smlouvy a pravidelně (alespoň 1x za čtvrtletí, vždy ale s minimálně dvouměsíčním odstupem) testovat funkčnost těchto záloh;

12. průběžně detekovat, minimálně však jednou za 3 měsíce, technické zranitelnosti a konfigurační nesoulady předmětu plnění smlouvy a o zjištěných skutečnostech bez zbytečného odkladu informovat objednatele; detekované technické zranitelnosti musí být vyhodnoceny s ohledem na související riziko a musí podle povahy předmětu plnění dojít k nápravným opatřením ze strany poskytovatele, nápravná opatření musí být schválena objednatelem;

13. v případě napojení objednatele na dohledová centra zajistit rozhraní pro napojení a součinnost při zvládání kybernetických bezpečnostních událostí a incidentů;

14. uchovávat data o provozu (provozní a lokalizační údaje) v souladu s požadavky účinné legislativy ČR a dodržovat požadavky VyKB na obsah provozních událostí.

2.3. Oprávnění užívat data

1. Poskytovatel je při poskytování plnění pro objednatele oprávněn nakládat s daty předanými poskytovateli objednatelem výhradně za účelem plnění předmětu smlouvy, avšak vždy pouze v rozsahu nezbytném ke splnění předmětu smlouvy.
2. Poskytovatel se při poskytování plnění pro objednatele zavazuje nakládat s daty pouze v souladu se smlouvou a příslušnými právními předpisy, zejména ZoKB, VyKB a dalšími souvisejícími právními předpisy.

2.4. Kontrola souladu s požadavky bezpečnosti

1. Poskytovatel je srozuměn s prováděním hodnocení rizik, kontrolou a auditem zavedených bezpečnostních opatření ze strany objednatele v souvislosti s poskytovanou službou poskytovatelem.
2. Hodnocení, kontrola a audit probíhají v intervalech stanovených objednatelem nebo v případě vzniku kybernetického bezpečnostního incidentu v rámci poskytované služby nebo v případě, že se vznik bezpečnostního incidentu jeví jako pravděpodobný. Kontrola nebo audit mohou být provedeny v prostorách poskytovatele nebo jeho poddodavatele a poskytovatel má povinnost tyto kontroly a audity objednateli či objednatelem pověřené osobě umožnit či možnost jejich provedení v prostorách poddodavatele zajistit, přispět k nim a poskytnout objednateli či objednatelem pověřené osobě k jejich provedení maximální možnou součinnost, kterou lze po poskytovateli rozumně požadovat. Počet a frekvence kontrol ani auditů nejsou nijak omezeny.
3. Poskytovatel je povinen po zavedení opatření provést také vlastní hodnocení rizik a kontrolu zavedených bezpečnostních opatření. Tato kontrola probíhá v pravidelných intervalech stanovených objednatelem, na žádost objednatele nebo v případě vzniku kybernetického bezpečnostního incidentu v rámci poskytované služby nebo v případě, že se vznik bezpečnostního incidentu jeví jako pravděpodobný. O výsledku kontroly podá poskytovatel objednateli bez zbytečného odkladu písemnou kontrolní zprávu.

2.5. Řetězení a řízení dodavatelů

Poskytovatel se při poskytování plnění pro objednatele zavazuje plnit následující povinnosti:

1. Poskytovatel nezapojí do poskytování plnění dle této smlouvy žádného dalšího poddodavatele bez předchozího konkrétního písemného povolení objednatele;
2. Poskytovatel se zavazuje, že se bude řídit požadavky objednatele na řízení bezpečnosti informací a poskytne objednateli veškerou nezbytnou součinnost v otázkách řízení bezpečnosti informací a pokud využívá při poskytování plnění poddodavatele, zajistí, že bude objednateli poskytnuta veškerá nezbytná součinnost v otázkách řízení bezpečnosti informací také od těchto poddodavatelů;
3. Poskytovatel je povinen předat objednateli kontaktní údaje všech osob dodávajících systémovou a technickou podporu pro řešení;
4. Pokud poskytovatel využívá při poskytování plnění poddodavatele, zavazuje se, že budou dodržovat bezpečnostní požadavky vč. požadavků na ochranu osobních údajů vyplývající

z této smlouvy. Poskytovatel se zavazuje bezodkladně doložit objednateli na základě jeho výzvy smluvní dokumenty se svými poddodavateli, ze kterých bude vyplývat závazek poddodavatele poskytovat plnění v souladu s bezpečnostními požadavky vyplývajícími z této smlouvy;

5. Poskytovatel odpovídá za to, že jeho poddodavatelé nebudou jednat v rozporu s bezpečnostními požadavky vyplývajícími z této smlouvy; v případě, že dojde k nedodržení těchto požadavků ze strany poddodavatele poskytovatele, považuje se každé takové nedodržení požadavků za porušení povinnosti poskytovatele dle této smlouvy.

2.6. Povinnosti v řízení změn dle ZoKB a VyKB

1. Poskytovatel se zavazuje v rozsahu předmětu plnění aktivně podílet na splnění povinností v oblasti řízení změn dle ZoKB a VyKB, zejména při analýze souvisejících rizik, přijímání opatření za účelem snížení všech nepříznivých dopadů spojených se změnami, aktualizaci bezpečnostní dokumentace, souvisejícím testováním a zajištění možnosti navrácení do původního stavu.
2. Poskytovatel se minimálně zavazuje v rozsahu předmětu plnění na své straně přiměřeně reagovat na změny na a upravit na své straně technická a organizační opatření tak, aby odpovídala novému stavu po provedení změny.
3. Poskytovatel se zavazuje aktivně spolupracovat při testování významné změny.

2.7. Zvládání bezpečnostních událostí a incidentů

Poskytovatel se při poskytování plnění pro objednatele zavazuje, že:

1. stanoví činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání bezpečnostních událostí a incidentů, podle takto stanovených a popsaných pravidel bude postupovat, a bude hlásit všechny bezpečnostní události a incidenty neprodleně po jejich detekci objednateli prostřednictvím ohlašovacích kanálů objednatele, v případech, kdy situace nestrpí odklad telefonicky; dále se zavazuje vyhodnotit informace o bezpečnostních událostech a incidentech a o těchto informacích, vzniklých bezpečnostních incidentech, vč. krátkodobých a dlouhodobých nápravných opatřeních nad všemi částmi řešení, které jsou ve správě poskytovatele, a rizicích souvisejících s ohrožením kontinuity činností vést záznamy a tyto uchovat pro jejich budoucí použití s ohledem na požadavky objednatele a legislativy České republiky; nastavená pravidla a postupy podléhají schválení objednatelem;
2. nastavená pravidla pro zvládání bezpečnostních incidentů budou respektovat požadavek na legalitu zajištění stop, tj. jejich původ a oprávněnost jejich získaní musí být v souladu s platnými zákony a standardy tak, aby bylo možné jejich následné využití v rámci forenzní analýzy a eventuální použití jako důkazní materiál;
3. navrhne řešení tak, aby byl systém detekce a zvládání bezpečnostních událostí a incidentů začleněn do procesů a systémů a realizuje opatření pro zvýšení odolnosti informačního a komunikačního systému vůči kybernetickým bezpečnostním incidentům a omezením dostupnosti;

4. v případě napojení objednatele na dohledová centra pro zvládání kybernetických bezpečnostních událostí a incidentů zajistí rozhraní pro napojení, zajistí součinnost a bude se řídit jeho pokyny;

5. provede analýzu příčin bezpečnostního incidentu a navrhne opatření s cílem zamezit jeho opakování v případě, že poskytovatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

2.8. Informační povinnost a povinnosti při výměně informací

1. Poskytovatel se během poskytování plnění pro objednatele zavazuje objednatele informovat o:

   a) způsobu řízení rizik, zbytkových rizicích souvisejících s plněním smlouvy a bez zbytečného odkladu také o změnách ve způsobu řízení rizik;

   b) významné změně ovládání poskytovatele podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných poskytovatelem k plnění na základě smluvního vztahu s objednatelem.

2. Poskytovatel se během poskytování plnění pro objednatele zavazuje dostatečně zabezpečit veškerý přenos dat a informací z pohledu bezpečnostních požadavků na jejich důvěrnost, integritu a dostupnost před hrozbami v kybernetické bezpečnosti v souladu se ZoKB a VyKB.

2.9. Specifikace podmínek pro řízení kontinuity činností a zálohování a obnovu dat z pohledu ZoKB a VyKB

1. Poskytovatel se zavazuje poskytnout součinnost při zpracování plánu řízení KBI a plánu kontinuity a obnovy činností informačních systémů objednatele, které souvisí s předmětem plnění, včetně všech jejich komponent na základě zhodnocení a výsledků analýzy dopadů (Business Impact Analysis) vypracované v součinnosti s objednatelem.

2. Poskytovatel se zavazuje dodržovat požadavky objednatele na řízení kontinuity činností v souladu se ZoKB, VyKB a ustanoveními bezpečnostní politik, metodik a postupů předaných poskytovateli objednatelem.

3. Poskytovatel vypracuje a předá objednateli metodiku zálohování a obnovy dat (ve smyslu primárních aktiv) i systémů (resp. technických aktiv) ve formě zálohovacího plánu, testovacího scénáře obnovy dat, systému evidence, zajištění integrity a autenticity zálohovacího média. V případě požadavku objednatele poskytovatel zajistí, že záloha jako taková bude šifrována. Poskytovatel jako součást dodávky dále dodá a nasadí odpovídající technologické řešení, na kterém bude záloha a obnova dat prováděna.

2.10. Bezpečnost lidských zdrojů

1. Poskytovatel připraví poučení a zajistí poučení všech stran podílejících se na poskytování předmětu plnění o bezpečnostních pravidlech, jež se musí v průběhu dodávky dodržovat a zajistí jejich dodržování nasazením kontrolních a vynucovacích mechanismů.

2. Poskytovatel se zaváže zajistit dostatečnou míru zastupitelnosti pro technické aspekty řešení (zajištění kontinuity dodávky, zastupitelnost pracovníků, zejména kontaktní osoby pro bezpečnost na straně poskytovatele).

2.11. Požadavky na systémovou a provozní bezpečnostní dokumentaci

1. Nedílnou součástí poskytovaného plnění je součinnost při zdokumentování všech bezpečnostních nastavení, funkcí a mechanismů formou zpracování bezpečnostní dokumentace a zpracování provozní dokumentace v souladu se ZoKB a VyKB.
2. V rámci součinnosti se poskytovatel zavazuje objednateli předat potřebné informace včetně identifikovaných datových toků, protokolů, architektonického nákresu systémů a jejich spolupráce, diagramu logického a fyzického zapojení a další dokumentaci předmětu plnění dle požadavku objednatele.

2.12. Fyzická ochrana a bezpečnost prostředí

1. Poskytovatel se zavazuje v budovách objednatele dodržovat režim návštěv v neveřejných prostorách a bezpečnostní požadavky na řízený přístup do bezpečnostních zón, kde jsou umístěny komponenty technologických a komunikačních systémů, anebo datové nosiče.
2. Poskytovatel se zavazuje, že v budovách objednatele neponechá volně dostupná instalační, záložní nebo archivní média ani dokumentaci k předmětu plnění této smlouvy.

2.13. Požadavky na Řízení přístupu

1. Poskytovatel bere na vědomí, že přístup k datům, informacím či zařízením souvisejícím s předmětem smlouvy je možné povolit pouze konkrétním fyzickým osobám (zaměstnancům poskytovatele) na základě požadavku poskytovatele.
2. Poskytovatel bere na vědomí, že přidělení oprávnění zaměstnanci poskytovatele musí být řízeno zásadou tzv. „potřeba vědět" (need-to-know principle) a není nárokové.
3. Poskytovatel se zavazuje, že nebude instalovat a používat žádné nástroje, které nebyly předem písemně odsouhlaseny objednatelem.
4. Poskytovatel se zavazuje, že nebude vyvíjet, kompilovat a šířit v jakékoliv části technologického nebo komunikačního systému programový kód, který má za cíl nelegální ovládnutí, narušení, nebo diskreditaci technologického nebo komunikačního systému nebo nelegální získání dat a informací.
5. Poskytovatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění objednateli chránily autentizační prostředky a údaje k systémům objednatele.
6. Poskytovatel bere na vědomí, že postup zvládání bezpečnostního incidentu či skutečnosti vzniklé v důsledku porušení bezpečnostních požadavků nebude posuzován jako okolnost vylučující odpovědnost poskytovatele za prodlení s řádným a včasným plněním předmětu smlouvy a nebude důvodem k jakékoli náhradě případné újmy poskytovateli či jiné osobě ze strany poskytovatele. Ostatní ustanovení ohledně odpovědnosti poskytovatele za prodlení obsažená ve smlouvě nejsou tímto ustanovením dotčena.

2.14. Monitorování činností

Poskytovatel bere na vědomí, že plnění realizovaná v rámci plnění předmětu smlouvy nebo s ním úzce související mohou být objednatelem monitorovány a vyhodnocovány s ohledem na obsah smlouvy a interních dokumentů objednatele.

2.15. Likvidace dat

Poskytovatel se zavazuje při likvidaci dat a datových nosičů postupovat v souladu s pokyny objednatele a požadavky ZoKB a VyKB. Při ukončení smlouvy bezpečně zlikviduje data a přístupové údaje objednatele, které má uložené na vlastních technických prostředcích (např. servisní notebook, lokální kopie), ledaže je povinen je uchovávat na základě právních předpisů, a na žádost objednatele provedení této likvidace písemně potvrdí. Tímto nejsou dotčena data a zálohy uložené na technických prostředcích objednatele nebo v úložištích zajišťovaných pro objednatele, která zůstávají objednateli.

2.16. Sankce

Sankce za porušení povinností plynoucích ze ZoKB, VyKB a této přílohy se řídí článkem 6 a článkem 8 smlouvy.

2.17. Způsob distribuce dokumentů poskytovateli

Poskytovatel má právo vyžádat si od objednatele bezpečnostní politiky a interní dokumenty ISMS relevantní k předmětu smlouvy. Tyto dokumenty představují důvěrné informace ve smyslu článku 8 smlouvy a poskytovatel je povinen je po ukončení smlouvy vrátit nebo prokazatelně bezpečně zlikvidovat.