SMLOUVA O POSKYTOVÁNÍ SLUŽEB

uzavřená podle občanského zákoníku v účinném znění.
Č.smlouvy prodávajícího: RCV-220001

1. Objednatel:

název:	Nemocnice Jihlava, příspěvková organizace
sídlo:	Vrchlického 59, Jihlava, 586 33
IČO:	00090638
DIČ:	CZ00090638
bankovní spojení:	18736–681/0100, Komerční banka, a.s.
statutární orgán:	MUDr. Lukáš Velev, MHA

a

2. Poskytovatel:

název:	AUTOCONT a.s.
sídlo:	Hornopolní 3322/34, Ostrava, PSČ 702 00
IČO:	04308697
DIČ:	CZ04308697
bankovní spojení:	Česká spořitelna a.s., č.ú. 6563752/0800
statutární orgán:	Jaroslav Biolek - člen představenstva třídy A Milan Sameš – předseda představenstva, člen představenstva třídy B Martin Grigar – místopředseda představenstva, člen představenstva třídy A Michal Tománek – člen představenstva třídy B David Emr – člen představenstva třídy B Ondřej Matuštík – člen představenstva třídy B Martin Stejskal – člen představenstva třídy A
jednající:	Ing. Martin Stejskal, člen představenstva třídy A

Objednatel a poskytovatel uzavírají tuto smlouvu o poskytování služeb (dále jen „smlouva“) na základě výsledku výběru nejvhodnější nabídky pro podlimitní veřejnou zakázku s názvem **„Systém ochrany privilegovaných účtů a přístupů“**.

1. Předmět plnění

1.1. Předmětem plnění této smlouvy je závazek poskytovatele dodat objednateli řešení systému pro jednotnou správu a monitoring privilegovaných účtů objednatele (dále jen „řešení“ nebo „systém“).

1.2. Systém bude poskytnut včetně:

- poskytnutí SW licencí pro systém ochrany privilegovaných účtů a přístupů (tzv. „Privileged Identity Management – PIM“ a „Privileged Access Management – PAM“) pro **50 uživatelů** zadavatele ve specifikaci v Příloze č. 1 smlouvy,
- implementace systému dle specifikace v Příloze č. 1 smlouvy,

- poskytnutí souvisejících služeb, záručního servisu a podpory dle specifikace v Příloze č. 1 smlouvy.

1.3. Poskytovatel se zavazuje poskytnout objednateli řešení v rozsahu uvedeném v odstavci 1.1 a 1.2. a dále dle podrobné specifikace předmětu plnění uvedené v Přílohách č. 1 a 2 této smlouvy, a to vlastním jménem, na své náklady, na vlastní zodpovědnost a nebezpečí a předat a realizovat ho v rozsahu, kvalitě, podmínkách a termínech dohodnutých v této smlouvě a jejích přílohách.

1.4. Poskytovatel se zavazuje poskytnout objednateli řešení v místě plnění dle článku 3, odst. 3. 2. této smlouvy.

1.5. Objednatel se zavazuje řešení od poskytovatele řádně a včas převzít a uhradit poskytovateli cenu v souladu s podmínkami sjednanými touto smlouvou.

2. Cena

2.1. Cena za předmět plnění za 48 měsíců: **4.985.050,-** Kč bez DPH 6.031.910,50 Kč s DPH

2.2. Cena obsahuje veškeré náklady poskytovatele, spjaté s poskytnutím řešení.

2.3. Cena za předmět plnění je poskytovatelem garantována jako cena maximální, nejvýše přípustná a lze ji překročit pouze v případě, kdy dojde ke změně sazby DPH. Pokud v průběhu realizace plnění ze smlouvy dojde ke změnám sazeb DPH, bude cena upravena podle změny sazeb DPH platných v době vzniku zdanitelného plnění, a to ve výši odpovídající změně sazby DPH. Smluvní strany se dohodly, že v takovém případě nebudou uzavírat dodatek k této kupní smlouvě. Celkovou a pro účely fakturace rozhodnou cenou se rozumí cena včetně DPH.

3. Doba a místo plnění

3.1. Doba plnění

Doba plnění je sjednána na dobu neurčitou. Plnění musí být zahájeno do 1 měsíce ode dne nabytí účinnosti smlouvy.

3.2. Místo plnění

Místem plnění je sídlo objednatele Nemocnice Jihlava, p. o., na adrese Vrchlického 59, 586 33 Jihlava.

4. Platební podmínky

4.1. Zálohy nebudou poskytovány.

4.2. Poskytovatel vystaví 1 fakturu za poskytnutý předmět plnění. Splatnost faktury nesmí být stanovena na méně než 30 dní od data jejího doručení objednateli.

4.3. Objednatel v rámci platebních podmínek **požaduje odloženou platbu se splátkami dle níže uvedeného splátkového harmonogramu:**

25 % z ceny za předmět plnění bude uhrazeno **k datu splatnosti faktury**
25 % z ceny za předmět plnění bude uhrazeno **do 12 měsíců** od 1. splátky
25 % z ceny za předmět plnění bude uhrazeno **do 24 měsíců** od 1. splátky
25 % z ceny za předmět plnění bude uhrazeno **do 36 měsíců** od 1. splátky

4.4. Úhradu provede objednatel v české měně.

4.5. Poskytovatel se zavazuje, že jím vystavená faktura bude obsahovat všechny náležitosti účetního a daňového dokladu stanovené obecně závaznými právními předpisy a smluvními ujednáními. Dále uvede název a číslo veřejné zakázky.

4.6. Úhrada za plnění z této smlouvy bude realizována bezhotovostním převodem na účet poskytovatele, který je správcem daně (finančním úřadem) zveřejněn způsobem umožňujícím dálkový přístup ve smyslu ustanovení § 98 zákona č. 235/2004 Sb. o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „zákon o DPH“).

4.7. Veškeré platby mezi smluvními stranami se uskutečňují prostřednictvím bankovního spojení uvedeného v záhlaví této smlouvy. Poskytovatel prohlašuje, že uvedené číslo jeho bankovního účtu splňuje požadavky dle § 106a zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění, a jedná se o zveřejněné číslo účtu registrovaného plátce daně z přidané hodnoty.

4.8. Poskytovatel prohlašuje, že ke dni uzavření této smlouvy není veden v registru nespolehlivých plátců daně z přidané hodnoty a ani mu nejsou známy žádné skutečnosti, na základě kterých by s ním správce daně mohl zahájit řízení o prohlášení za nespolehlivého plátce daně dle § 106a zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění.

4.9. Objednatel jako příjemce zdanitelného plnění je oprávněn v případě, že poskytovatel je v okamžiku uskutečnění zdanitelného plnění veden v registru nespolehlivých plátců daně z přidané hodnoty, uhradit částku odpovídající výši daně z přidané hodnoty na účet správce daně za poskytovatele. Uhrazení částky odpovídající výši daně z přidané hodnoty na účet správce daně za poskytovatele bude považováno v tomto rozsahu za splnění závazku objednatele uhradit sjednanou cenu poskytovateli.

4.10. V případě, že vystavená faktura obsahuje nesprávné cenové údaje či nesprávné náležitosti nebo chybí-li ve faktuře některé z náležitostí uvedené v předchozích odstavcích, je objednatel oprávněn fakturu vrátit poskytovateli do doby její splatnosti. V takovém případě je poskytovatel povinen vystavit fakturu novou. Lhůta splatnosti počíná běžet znovu od opětovného zaslání náležitě doplněných či opravených dokladů.

5. Dodací podmínky

5.1. Licence musí být poskytovatelem profesionálně nainstalovány a po jejich nasazení řádně otestovány, včetně prokázání, že tyto licence mají všechny požadované parametry.

5.2. Řešení musí splňovat bezpečnostní kritéria podle Zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, a nebude v rozporu s požadavky Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) pro provoz významných informačních systémů.

5.3. Objednatel je povinen dle §5 Vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů, provádět analýzu rizik a identifikovaná rizika řídit. Současně je objednatel povinen zabývat se všemi hrozbami, které prostřednictvím varování vydává NÚKIB a zohlednit je v analýze rizik. Objednatel proto provedl, s přihlédnutím k vydanému "varování" NÚKIB, analýzu rizik a v hodnocení se řídil pokyny uvedenými v dokumentu NÚKIB "Metodika k varování ze dne 17. prosince 2018". Veškerá bezpečnostní opatření, která bude nutné u dodaného řešení na základě výsledků analýzy rizik přijmout, nesmí pro objednatele znamenat žádné další náklady.

5.4. V rámci realizace řešení bude poskytovatelem zpracována a předána dokumentace řešení minimálně v tomto rozsahu:

- provozně-technická dokumentace v rozsahu požadovaném Vyhláškou č. 529/2006 Sb. §10 a §11,

- plán zálohování a obnovy včetně doporučení pravidel pro pravidelné ověřování jednotlivých postupů,
- bezpečnostní dokumentace dle zákona 181/2014 Sb. o kybernetické bezpečnosti, včetně jeho novel a jeho prováděcích právních předpisů, především pak analýza aktiv ve vazbě na interní metodiku a plán obnovy,
- integrační dokumentace popisující jednotlivá aplikační rozhraní (WS a API služby) používaná k integraci IS na jednotlivé funkce včetně funkčních prototypů volání jednotlivých funkcí.

6. Součinnost

6.1. Smluvní strany jsou povinny vyvíjet veškeré úsilí k vytvoření potřebných podmínek pro realizaci předmětu smlouvy, které vyplývají z jejich smluvního postavení. To platí i v případech, kde to není výslovně uloženo v jednotlivých ustanoveních smlouvy. Především jsou smluvní strany povinny vyvinout součinnost v rámci smlouvou upravených postupů a vyvinout potřebné úsilí, které lze na nich v souladu s pravidly poctivého obchodního styku požadovat, k řádnému splnění jejich smluvních povinností.

6.2. Pokud jsou kterékoli ze smluvních stran známy okolnosti, které jí brání, aby dostála svým smluvním povinnostem, sdělí to neprodleně písemně druhé smluvní straně. Smluvní strany se zavazují neprodleně odstranit v rámci svých možností všechny okolnosti, které jsou na jejich straně a které brání splnění jejich smluvních povinností. Pokud k odstranění těchto okolností nedojde, je druhá smluvní strana oprávněna požadovat splnění povinnosti v náhradním termínu, který stanoví s přihlédnutím k povaze záležitosti.

6.3. Poskytovatel se zavazuje oznámit termín poskytnutí plnění minimálně 3 dny před plánovaným termínem následujícím osobám na kontakty:

Jméno a příjmení	Pracoviště	Telefon	E-mail
Bc. Jiří Schimmer	ICT oddělení	731 165 516	schimmerj@nemji.cz

7. Smluvní pokuty

7.1. Smluvní strany jsou v případě porušení svých závazků povinny hradit tyto smluvní pokuty:

Název položky	Hodnota
Smluvní pokuta při nedodržení závazných termínů (minimálně % z ceny nedodaného požadovaného řešení včetně DPH) za každý den prodlení	**0,03%**
Smluvní pokuty za neodstranění reklamovaných vad v záruční lhůtě (minimálně % za každý jednotlivý případ z ceny předmětu reklamace vč. DPH) za každý den prodlení	**0,05%**

7.2. Smluvní strany se zavazují zaplatit druhé smluvní straně úrok z prodlení ve výši stanovené obecně závazným předpisem z dlužné částky za každý den prodlení se splněním svého peněžitého závazku dle této smlouvy.

7.3. Smluvní pokutou není dotčeno právo na náhradu škody.

8. Zánik závazků

8.1. Závazky smluvních stran ze smlouvy zanikají:

- jejich splněním,
- dohodou smluvních stran formou písemného dodatku ke smlouvě, takový dodatek musí být písemný a obsahovat vypořádání všech závazků, na které smluvní strany, které takový dodatek uzavírají, mohly pomyslet, jinak je neplatná,
- odstoupením od smlouvy lze pouze z důvodů stanovených ve smlouvě nebo zákonem,

- skončením účinnosti smlouvy nebo jejím zánikem zanikají všechny závazky smluvních stran ze smlouvy, skončením účinnosti smlouvy nebo jejím zánikem nezanikají nároky na náhradu škody, zaplacení smluvních pokut sjednaných pro případ porušení smluvních povinností, a ty závazky smluvních stran, které podle smlouvy nebo vzhledem ke své povaze mají trvat i nadále, nebo u kterých tak stanoví zákon.

9. Závěrečná ustanovení

9.1. Objednatel je oprávněn svá práva i povinnosti podle této smlouvy postoupit anebo převést písemnou smlouvou jakékoliv třetí osobě, a to v celku nebo jednotlivě a po částech. K tomu dává poskytovatel objednateli svůj výslovný souhlas. Poskytovatel se zavazuje poskytnout objednateli potřebnou součinnost k postoupení a/nebo převodu jeho práv a povinností podle této smlouvy na třetí osobu, a to ve formě a způsobem, které jsou k tomu případně potřebné podle příslušné právní úpravy.

9.2. Poskytovatel není oprávněn postoupit práva, povinnosti, závazky a pohledávky z této smlouvy třetí osobě bez předchozího písemného souhlasu objednatele.

9.3. Pokud v této smlouvě není stanoveno jinak, řídí se právní vztahy z ní vzniklé právním řádem České republiky, zejména zákonem č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

9.4. Poskytovatel prohlašuje, že se před uzavřením smlouvy nedopustil v souvislosti se zadávacím řízením předcházejícím uzavření této smlouvy sám nebo prostřednictvím jiné osoby žádného jednání, jež by odporovalo zákonu nebo dobrým mravům nebo by zákon obcházelo, zejména že nenabízel žádné výhody osobám podílejícím se na zadání veřejné zakázky, na kterou s ním objednatel uzavřel smlouvu, a že se nedopustil žádného jednání narušujícího hospodářskou soutěž.

9.5. Jakákoliv ústní ujednání, která nejsou písemně potvrzena oprávněnými zástupci obou smluvních stran, jsou právně neúčinná.

9.6. Smlouvu lze měnit pouze písemnými dodatky, podepsanými oprávněnými zástupci obou smluvních stran.

9.7. Veškerá textová dokumentace, která se při plnění smlouvy předává, musí být předána či předložena v českém jazyce nebo slovenském jazyce (s výjimkou produktových listů a technických manuálů, které jsou součástí předmětu plnění).

9.8. Veškeré spory z této smlouvy se zavazují smluvní strany řešit smírnou cestou. Nedohodnou-li se strany na řešení sporu, je příslušný k jeho rozhodnutí soud. V případě soudního sporu se místní příslušnost věcně příslušného soudu I. stupně řídí obecným soudem objednatele. Písemnosti mezi stranami této smlouvy, s jejichž obsahem je spojen vznik, změna nebo zánik práv a povinností upravených touto smlouvou (zejména odstoupení od smlouvy) se doručují do vlastních rukou.

9.9. Povinnost smluvní strany doručit písemnost do vlastních rukou druhé smluvní straně je splněna při doručování poštou, jakmile pošta písemnost adresátovi do vlastních rukou doručí. Účinky doručení nastanou i tehdy, jestliže pošta písemnost smluvní straně vrátí jako nedoručitelnou a adresát svým jednáním doručení zmařil, nebo přijetí písemnosti odmítl.

9.10. Smluvní strany prohlašují, že si tuto smlouvu přečetly, že s jejím obsahem souhlasí a že vyjadřuje jejich pravou, svobodnou a vážnou vůli. Smluvní strany dále prohlašují, že tuto smlouvu neuzavřely v tísni ani za nápadně nevýhodných podmínek. Na důkaz toho připojují své vlastnoruční podpisy.

9.11. Smlouva nabývá platnosti dnem podpisu a účinnosti dnem uveřejnění v informačním systému veřejné správy – Registru smluv.

9.12. Poskytovatel výslovně souhlasí se zveřejněním celého textu této smlouvy včetně podpisů v informačním systému veřejné správy – Registru smluv.

9.13. Smluvní strany shodně a svobodně prohlašují, že se bez výhrad shodly na tom, že objednatel zveřejní tuto smlouvu a související přílohy v Registru smluv, ve lhůtě a za podmínek stanovených dle zákona č. 340/2015 Sb., o registru smluv, v platném znění, a to včetně osobních údajů.

9.14. Tato smlouva je vyhotovena ve dvou stejnopisech a každá smluvní strana obdrží její jedno vyhotovení.

Seznam příloh smlouvy:

Příloha č. 1 – Soupis prvků a specifikace předmětu plnění včetně cen

Příloha č. 2 – Bezpečnostní opatření

V Jihlavě dne dle el.podpisu

Za objednatele:

Digitally signed by MUDr. Lukáš Velev
Reason: I agree to the terms defined by the placement of my signature in this document
Location: Nemocnice Jihlava
Date: 2022.01.31 12:10:50+01'00'

.....

MUDr. Lukáš Velev, MHA
ředitel

V Brně dne dle el.podpisu

Za poskytovatele:

Digitally signed by Ing. Martin Stejskal
Date: 2022.01.27 09:38:11 +01'00'

.....

Ing. Martin Stejskal
člen představenstva třídy A

SOUPIS PRVKŮ A SPECIFIKACE PŘEDMĚTU PLNĚNÍ VČETNĚ CEN

Č. položky	Popis	Množství	Jedn.	Jedn. cena	Částka
	CyberArk Privileged Cloud - 25 users (cena za 1ks = 1 měsíc) - License includes: - Credential Protection (password & SSH Keys) - Automatic session isolation, recording and monitoring (PSM) - Just in Time Access - VPN-less Remote Access - Adaptive Multi-Factor Authentication, SSO - Ability to manage local admin credentials on the endpoint - Infrastructure Components - Vault with DR hosted in Cloud with 99.9% SLA, unlimited connection components (CPM + PSM) - Unlimited Protected Systems (if users are 50 and above), if 49 users or less - number of protected systems = 20x number of users; number of managed passwords = 100x number of users (price per user)	48,00	ks	59 975,00	2 878 800,00
	CyberArk External Vendor License - 25 users (cena za 1ks = 1 měsíc) - enforced, automatic session isolation, recording and monitoring - VPN-less Remote Access - Just in time provisioning to CyberArk PAM (price per user)	48,00	ks	21 250,00	1 020 000,00
	podpora v rozsahu 1MD pro pravidelnou aktualizaci politik privilegovaných účtů, konzultace nastavení, aktualizace a patche cloud connectoru (cena za 1ks = 1 měsíc)	48,00	ks	16 000,00	768 000,00
	CyberArk Privilege Cloud Jump Start Tier 1 Service Package includes best practices guidance on solution planning, deployment, and configuration. In addition, it provides knowledge transfer on initial use cases adoption and self-paced training options. Tier 1 includes - installation of 2 connectors, connecting 3 platforms (Windows, Unix,..), integration of Alero, Idaptive MFA, 1 training seat	1,00	ks	286 250,00	286 250,00
	vzdělávací kurz pro administrátory v rozsahu 2x 8 hodin	1,00	ks	32 000,00	32 000,00

Celkem	**4 985 050,00**
Částka DPH	1 046 860,50
Zaokrouhlení	0,00
Celkem včetně DPH	**6 031 910,50**

plnění zahrnuje :

• poskytnutí SW licencí pro systém ochrany privilegovaných účtů a přístupů (tzv. „Privileged Identity Management – PIM“ a „Privileged Access Management – PAM“) pro **50 uživatelů** zadavatele ve specifikaci v tabulce níže,
• implementace systému dle specifikace v tabulce níže,
• poskytnutí souvisejících služeb, záručního servisu a podpory ve specifikaci v tabulce níže.

Položka	**Položka zahrnuje:**
CyberArk Privileged Cloud - Standard Privileged User SaaS (systém jako služba; cloudové řešení) - 25 uživateů	- bezpečná správa hesel a SSH klíčů pro privilegované účty - centrální kontrolní bod pro izolaci, řízení a sledování všech aktivit správců - přístup Just-in-Time - přístup uživatelů bez nutnosti instalace řešení VPN - adaptivní multifaktorová autentizace, jednotné přihlašování (SSO) - řízení hesel na koncových systémech - Vault s DR hostovaný v Cloudu s 99.9 % SLA, neomezený počet připojených komponent (CPM + PSM) - neomezený počet chráněných systémů (50 uživatelů a více), 49 a méně uživatelů – počet chráněných systémů = 20x počet uživatelů; počet spravovaných hesel = 100x počet uživatelů - integrace na MS Azure AD - možnost nahrávat aktuálně realizované spojení s možností zpětného přehrání a uložením do cloudu poskytovatele
CyberArk Privileged Cloud - External Vendor User SaaS (systém jako služba; cloudové řešení) - CyberArk External Vendor License - 25 uživatelů	- vynucená, automatická izolace relace, nahrávání a monitoring - přístup bez nutnosti instalace řešení VPN - Just-in-Time poskytování PAM
CyberArk Privilege Cloud Jump Start Tier 1 Service Package	- konzultace a best practices ohledně zabezpečení privilegovaných účtů a přístupů - Tier 1 zahrnuje: instalaci 2 konektorů, napojení 3 platforem (Windows, Unix, ...), integraci s Alero (nebo jeho technologickou obdobu), Idaptive MFA (nebo jeho technologickou obdobu), 1x vzdělávací kurz dodavatele pro administrátory v rozsahu minimálně 8 hodin

BEZPEČNOSTNÍ OPATŘENÍ

Účelem této přílohy je v souladu s ustanovením § 4 odst. 4 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), v platném znění (dále jen „**ZoKB**"), ve spojení v přílohou č. 7 k vyhlášce č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) (dále jen „**Vyhláška**") stanovit závazné bezpečnostní opatření, která se vztahují na Poskytovatele, jehož předmětem plnění pro Objednatele je (výhradně či jako součást předmětu plnění jiné služby) vývoj, implementace a/nebo servis software (dále také jen „**SW**"), a/nebo který v souvislosti s plněním pro Objednatele přistupuje do informačního systému Objednatele, který byl určen informačním systémem základní služby v souladu se zákonem č. 181/2014 Sb., (dále **také „ISZS"),** a/nebo který v rámci poskytovaného plnění pro Objednatele zpracovává, a/nebo přenáší a/nebo ukládá a/nebo archivuje data a provozní údaje Objednatele a/nebo jeho zákazníků (dále také jen „**Bezpečnostní opatření**").

1. OBECNÉ POŽADAVKY

1.1 Poskytovatel se při poskytování plnění pro Objednatele zavazuje plnit následující povinnosti:

1.1.1.1 postupovat v souladu s platnými právními předpisy, zejména pak v souladu s požadavky vyplývajícími pro Objednatele, jakožto správce a provozovatele informačního sytému základní služby, ze ZoKB a Vyhlášky a reflektovat případné novely uvedených právních předpisů či novou právní úpravu;

1.1.1.2 nestanoví-li dohoda stran jinak, Poskytovatel jmenuje nejpozději do 3 dnů po uzavření Smlouvy zodpovědnou kontaktní osobu pro potřeby zajištění plnění Bezpečnostních opatření vyplývajících ze Smlouvy a související komunikace mezi Smluvními stranami (dále také jen „Kontaktní osoba"). Kontaktní osobu sdělí Poskytovatel Objednateli písemně v téže lhůtě. Případnou změnu Kontaktní osoby na straně Poskytovatele je Poskytovatel povinen Objednateli nahlásit do 5 dnů od provedení změny;

1.1.1.3 zajistit, aby Kontaktní osoba Poskytovatele nejpozději do 30 dnů od uzavření Smlouvy potvrdila písemně Objednateli, že všechny osoby podílející se na poskytování plnění této Smlouvy za stranu Poskytovatele a/nebo jeho podposkytovatelé byli prokazatelně seznámeni s těmito Bezpečnostními opatřeními;

1.1.1.4 pokud při plnění předmětu smlouvy Poskytovatel zpracovává osobní údaje pro Objednatele, zavazuje se Poskytovatel uzavřít s Objednatelem smlouvu o zpracování osobních údajů v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) a zákonem č. 110/2019 o zpracování osobních údajů;

1.1.1.5 předmět plnění nesmí být nevyhovující z hlediska informační bezpečnosti, přičemž za nevyhovující je považováno jakékoli plnění, které obsahuje technologie/klíčové prvky, vůči jejichž výrobcům příslušný správní orgán vydal opatření v souladu se ZoKB, a které dle analýzy rizik představují vysoké riziko;

1.1.1.6 dodržovat příslušná ustanovení bezpečnostních politik, metodik a postupů Objednatele, resp. platné řídící dokumentace Objednatele či její části, 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 Zhotoviteli, elektronickým předáním prostřednictvím e-mailu, zřízením přístupu Zhotoviteli na sdílené úložiště aj.);

1.1.1.7 provádět analýzu a hodnocení rizik informační infrastruktury, která je součástí předmětu Smlouvy (dodávaného řešení) a na základě výsledků navrhovat a předkládat Objednateli ke schválení opatření na minimalizaci nebo odstranění zjištěných rizik. Opatření musí být navrhována a konsolidována s přihlédnutím k výsledkům posuzování rizik;

1.1.1.8 zaznamenávat podstatné okolnosti související s poskytovaným předmětem plnění dle Smlouvy (technické záznamy, organizační záznamy o školení, pověření apod.) a informovat o nich Objednatele;

1.1.1.9 zavést opatření pro ochranu zálohy dat vztahujících se k plnění Smlouvy a pravidelně testovat funkčnost těchto záloh;

1.1.1.10 v případě potřeby Objednatele musí Poskytovatel garantovat schopnost zrekonstruovat funkcionalitu aktiva do stavu požadovaného dle Smlouvy;

1.1.1.11 průběžně detekovat 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;

1.1.1.12 realizovat bezpečnostní opatření pro ochranu dat souvisejících s plněním předmětu Smlouvy;

1.1.1.13 splnit všechny relevantní požadavky na bezpečnost v procesech vývoje a podpory minimálně v rozsahu požadavků dle ISO/IEC 27001 A. 14;

1.1.1.14 uchovávat data o provozu (provozní a lokalizační údaje) v souladu s planými právními předpisy a dodržovat požadavky vyplývající z Vyhlášky na obsah provozních událostí;

1.1.1.15 zabezpečit veškerý přenos dat a informací z pohledu bezpečnostních požadavků na jejich důvěrnost, integritu a dostupnost během poskytování plnění pro Objednatele;

1.1.1.16 poskytovat Objednateli v termínech stanovených Objednatelem, resp. bez zbytečného odkladu požadovanou součinnost na provedení bezpečnostního testování v průběhu vývoje SW či po jeho předání;

1.1.1.17 dodat systémové a provozní bezpečnostní dokumentace nejpozději do doby předání a převzetí SW způsobem uvedeným ve smlouvě, a to minimálně v rozsahu stanoveném Objednatelem;

1.1.1.18 že plnění bude obsahovat jen ty součásti, které jsou objektivně potřebné pro řádné provozování SW a/nebo které jsou specifikovány výslovně ve smlouvě, zejména, že SW nebude obsahovat žádné nepotřebné komponenty apod.;

1.1.1.19 pokud součástí plnění je i instalace operačního systému případně SW třetích stran, v průběhu jeho instalace budou použity nejnovější aktualizované verze těchto produktů;

1.1.1.20 veškeré důvěrné informace1 poskytnuté Objednatelem při poskytování plnění nebudou uchovávány v nešifrovaném tvaru a budou chráněny vůči neautorizovanému přístupu, pokud nebude mezi smluvními stranami v konkrétním případě dohodnuto jinak;

[1] Za důvěrné informace se ve smyslu této přílohy považují zejména identifikační údaje certifikátu, hesla, přístupová oprávnění, konfigurační soubory, systémové programy, kritické knihovny, obnovovací procedury apod.

1.1.1.21 pokud v rámci poskytovaného plnění bude instalovat SW nebo jejich upgrade bude postupovat podle hardeningových bezpečnostních politik a v souladu s bezpečnostními standardy Objednatele, pokud byl s takovými dokumenty nebo jejich částmi seznámen;

1.1.1.22 v produkčním prostředí systému ISZS bude obsažen jen kompilovaný, respektive spustitelný kód a další nezbytná data pro provozování systému ISZS;

1.1.1.23 před spuštěním SW v produkčním prostředí daného systému ISZS provede kontrolu souladu daného SW s bezpečnostními požadavky hardeningových bezpečnostních politik a v případě zjištění nesouladu zajistí bez zbytečného odkladu soulad dodávaného SW s bezpečnostními požadavky hardeningových politik, pokud byl s takovými dokumenty nebo jejich částmi seznámen.

1.1.1.24 bude instalovat nový SW nebo nové verze SW pouze na základě Objednatelem předem schválených migračních postupů2;

1.1.1.25 ověří integritu zdrojového kódu a předá zdrojový kód Objednateli bezpečnou formou zajišťující integritu zdrojového kódu, přičemž bude průběžně evidovat a bezpečné ukládat zdrojové kódy provozovaných aplikací, a to i v případě, že budou zdrojové kódy předávány Objednateli, přičemž při vývoji SW se Poskytovatel zavazuje, že

a. zdrojový kód programů vyvíjených Poskytovatelem bude předmětem procesu řízení verzí;

b. zdrojový kód programů je zálohován a uložen mimo produkční prostředí a současně je stanoven postup, jak sestavit systém ze zdrojového kódu;

c. provádění konfiguračních změn je v souladu s procesem změnového řízení Objednatele;

d. konfigurační soubory jsou pravidelně průběžně zálohovány;

e. eviduje každou změnu konfigurace;

2. POŽADAVKY NA SYSTÉMOVOU A PROVOZNÍ BEZPEČNOSTNÍ DOKUMENTACI

2.1 Nedílnou součástí poskytovaného plnění je zdokumentování všech bezpečnostních nastavení, funkcí a mechanismů formou zpracování bezpečnostní dokumentace. Poskytovatel se v rámci poskytovaného plnění pro Objednatele zavazuje předat Objednateli dokumentaci minimálně v následujícím rozsahu:

a. plány kontinuity činností a havarijní plány,

b. provozní a bezpečnostní dokumentace skutečného provedení,

c. popis autorizačního konceptu a oprávnění,

d. zálohovací a archivační postupy,

e. instalační a konfigurační postupy;

f. bezpečností nastavení.

3. FYZICKÁ OCHRANA A BEZPEČNOST PROSTŘEDÍ

3.1 Poskytovatel se zavazuje dodržovat provozní řády budov (režimová opatření) a využívaných prostor, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěny komponenty systémů ISZS anebo datové nosiče (dále také jen „**Pracoviště**“).

[2] Migrační postup – soubor kroků definující převod dat mezi dvěma nebo více systémy ISZS.

3.2 Poskytovatel se zavazuje, že na Pracovišti neponechá volně dostupná instalační, záložní nebo archivní média ani dokumentaci k systému ISZS, který je předmětem plnění dle této smlouvy.

4. ŘÍZENÍ PŘÍSTUPU

4.1 Poskytovatel bere na vědomí, že přístup k systému ISZS je možné povolit pouze fyzické identitě zaměstnance Poskytovatele (popřípadě Podposkytovatele) zaevidované v registru identit Objednatele, a to na základě požadavku Poskytovatele na přístup.

4.2 Poskytovatel bere na vědomí, že jeho zaměstnanec musí poskytnout své osobní údaje Objednateli, a to v rozsahu nutném pro zřízení přístupu, v opačném případě Objednatel není povinen přístup k systému ISZS zaměstnanci Poskytovatele povolit. Zaměstnanec Poskytovatele s přiděleným přístupem (fyzickým, logickým) k systému ISZS, bere na vědomí, že dochází ke zpracování osobních údajů během vyhodnocování údajů o pohybu a prováděných aktivitách v prostorách Objednatele (např.: monitoring pomocí řešení Security Information and Event Management).

4.3 Poskytovatel bere na vědomí, že přidělení oprávnění zaměstnanci Poskytovatele musí být řízeno principem nezbytného minima a není nárokové.

4.4 Poskytovatel se zavazuje, že udělený přístup nesmí být sdílen více zaměstnanci Poskytovatele nebo Podposkytovatele.

4.5 Poskytovatel se zavazuje, že vzdálený přístup do systému ISZS bude vždy uskutečněn pouze prostřednictvím zabezpečeného připojení definovaným Objednatelem.

4.6 Poskytovatel se zavazuje, že před připojením koncového zařízení, mobilní koncového zařízení nebo aktivního síťového prvku jako síťové switche, WiFi access pointy, routery či huby do počítačové sítě zažádá o schválení připojení kontaktní osobu na straně Objednatele.

4.7 Poskytovatel se zavazuje, že bez zbytečného odkladu deaktivuje všechny nevyužívané zakončení sítě anebo nepoužívané porty aktivního síťového prvku.

4.8 Poskytovatel se zavazuje, že nebude instalovat a používat zejména typy nástrojů Keylogger, Sniffer, Analyzátor zranitelností a Port Scanner, Backdoor, rootkit a trojský kůň nebo jinou podobu malware.

4.9 Poskytovatel se zavazuje, že všechny jeho informační systémy, které se připojují do síťové infrastruktury Objednatele, jsou a budou chráněny proti malware.

4.10 Poskytovatel se zavazuje, že nebude vyvíjet, kompilovat a šířit v jakékoliv části systému ISZS programový kód, který má za cíl nelegální ovládnutí, narušení, nebo diskreditaci systému ISZS nebo nelegální získání dat a informací.

4.11 Poskytovatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednateli v ISZS:

a. neukládali, nesdíleli, data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno Objednatele;

b. nestahovali, nesdíleli, neukládali, nearchivovali a/nebo neinstalovali datové a spustitelné soubory v rozporu s licenčními podmínkami nebo autorským zákonem;

c. nezasílali řetězové emaily.

4.12 Poskytovatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednateli, kteří přistupují do interní sítě nebo ISZS Objednatele, měli v externím zařízení typu notebook/počítač aplikovány bezpečnostní záplaty a nainstalovanou, spuštěnou a aktualizovanou antivirovou ochranu;

4.13 Poskytovatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednateli, kteří přistupují do interní sítě a/nebo systému ISZS Objednatele chránili autentizační prostředky a údaje k systémům ISZS Objednatele. Poskytovatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet zablokován a řešen jako kybernetická bezpečnostní událost ve smyslu příslušné řídící dokumentace a mohou být uplatněny příslušné postupy zvládání kybernetické bezpečnostní události (např. okamžité zrušení přístupu k informačním aktivům fyzických osob externího

subjektu). Poskytovatel bere na vědomí, že postup zvládáním kybernetické bezpečnostní události či jiný důsledek porušení Bezpečnostních opatření 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 Objednatele.

5. MONITOROVÁNÍ ČINNOSTÍ

5.1 Poskytovatel bere na vědomí, že veškerá jeho aktivita a jeho plnění realizované v systémovém prostředí Objednatele budou Objednatelem průběžně a pravidelně monitorovány a vyhodnocovány s ohledem na obsah smlouvy a interních dokumentů Objednatele, se kterými byl Poskytovatel seznámen.

5.2 Poskytovatel se zavazuje, že bude průběžně monitorovat a zaznamenávat veškerou svoji aktivitu a plnění realizované v rámci plnění předmětu Smlouvy nebo s ním úzce související. Poskytovatel se zavazuje, poskytnout záznamy/logy obsahující výsledky monitorování, úspěšná a neúspěšná přihlášení do ISZS systému a záznamy o správě uživatelů, v případě že jimi disponuje, na vyžádání a bez zbytečného odkladu Objednateli, a to po celou dobu trvání smlouvy i o jejím ukončení.

6. PŘEDÁNÍ A PŘEVZETÍ PLNĚNÍ

6.1 Poskytovatel bere na vědomí, že nedodržení Bezpečnostních opatření Objednatele včetně požadavku na předání kompletní systémové a provozní dokumentace je vadou bránící převzetí předmětu Smlouvy, přičemž Objednatel není do doby odstranění příslušné vady plnění povinen plnění převzít.

6.2 Poskytovatel odpovídá za to, že systémy dodávané do ISZS budou obsahovat nejnovější bezpečnostní aktualizace (patche)3.

7. VÝMĚNA INFORMACÍ

7.1 Pokud je předmětem Smlouvy výměna informací mezi smluvními stranami, musí být mezi smluvními stranami uzavřena dohoda o ochraně předmětných informací, zejména při jejich výměně, uložení, archivaci a ukončení smlouvy.

7.2 Poskytovatel se zavazuje, že veškerý přenos dat a informací musí být dostatečně zabezpečen pomocí aktuálně odolných kryptografických algoritmů a kryptografických klíčů.

7.3 Poskytovatel se zavazuje, že on-line transakce realizované prostřednictvím webových technologií budou chráněny SSL certifikáty.

7.4 Poskytovatel má povinnost na základě výzvy Objednatele, předat Objednateli všechna vyžádaná data, provozní údaje a informace bez zbytečného odkladu, a to v systematizované podobě a ve strojově čitelném formátu.

8. ZVLÁDÁNÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH INCIDENTŮ

8.1 Poskytovatel se zavazuje, že při poskytování plnění pro Objednatele stanoví činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání kybernetických bezpečnostních událostí a incidentů, podle takto stanovených a popsaných pravidel bude postupovat, a bude hlásit všechny kybernetické bezpečnostní události a incidenty včetně případů porušení zabezpečení osobních údajů neprodleně po jejich detekci Objednateli. Dále se zavazuje vyhodnotit informace o kybernetických bezpečnostních událostech a incidentech a o těchto informacích, vzniklých kybernetických 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 přiměřené záznamy a tyto uchovat pro jejich budoucí použití s ohledem na požadavky Objednatele;

[3] Aktualizace software na vyšší vývojovou verzi.

8.2 Nastavená pravidla pro zvládání kybernetických bezpečnostních incidentů budou respektovat požadavek na legalitu zajištění stop, tj. jejich původ a oprávněnost jejich získaní musí být v souladu s platnými právními předpisy tak, aby bylo možné jejich následné využití v rámci forenzní analýzy a eventuální použití jako důkazní materiál;

8.3 Poskytovatel navrhne řešení tak, aby byl systém detekce a zvládání kybernetických bezpečnostních událostí a incidentů začleněn do procesů a systémů Objednatele (mj. aby byly reflektovány požadavky Objednatele na krizové řízení) a realizuje opatření pro zvýšení odolnosti informačního systému vůči kybernetickým bezpečnostním incidentům a omezením dostupnosti a vychází při tom zejména z požadavků stanovených Vyhláškou;

8.4 Poskytovatel má povinnost neprodleně informovat Objednatele o kybernetických bezpečnostních incidentech souvisejících s plněním předmětu Smlouvy. Součástí oznámení musí být popis povahy případu kybernetického bezpečnostního incidentu.

8.5 Pokud dojde ke kybernetické bezpečnostní události popřípadě ke kybernetickému bezpečnostnímu incidentu a následnému zvládání a vyhodnocování kybernetického bezpečnostního incidentu na bezpečnostní incident na straně Objednatele, poskytne Poskytovatel požadovanou součinnost např.: poskytne logy a identifikační údaje (např. IP adresa, MAC adresa, sériové číslo případně IMEI) dotyčného koncového zařízení nebo mobilního koncového zařízení, k analýze obsahu, případně bez zbytečného odkladu zrealizuje opatření požadovaná Objednatelem).

8.6 Poskytovatel má povinnost provést analýzu příčin kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu a navrhne opatření s cílem zamezit jeho opakování v případě, že Poskytovatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

9. AUTORSTVÍ

9.1 Poskytovatel se při poskytování plnění pro Objednatele zavazuje zajistit, aby při plnění Smlouvy dodržel podmínky stanovené zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

9.2 Další požadavky mohou být stanovené ve Smlouvě.

10. OPRÁVNĚNÍ UŽÍVAT DATA

10.1 Poskytovatel je při poskytování plnění pro Objednatele oprávněn užívat data předaná Poskytovateli Objednatelem za účelem plnění předmětu Smlouvy, avšak vždy pouze v rozsahu nezbytném ke splnění předmětu Smlouvy.

10.2 Poskytovatel se při poskytování plnění pro Objednatele zavazuje nakládat s daty pouze v souladu se Smlouvou a příslušnými právními předpisy, zejména ZoKB a Vyhláškou a dalšími souvisejícími právními předpisy.

11. ŘÍZENÍ ZMĚN

11.1 Objednatel v rámci řízení změn v ISZS přezkoumává možné dopady změn a určuje významné změny dle Vyhlášky.

11.2 Objednatel u významných změn dokumentuje jejich řízení, provádí analýzu rizik, přijímá opatření za účelem snížení všech nepříznivých dopadů spojených s významnými změnami, aktualizuje bezpečnostní politiku a bezpečnostní dokumentaci, zajistí testování ISZS a zajistí možnost navrácení do původního stavu.

11.3 Objednatel má povinnost informovat Poskytovatele o výsledcích řízení změn, které mají dopady na plnění předmětu Smlouvy ze strany Poskytovatele.

11.4 Poskytovatel má povinnost přijmout účinná opatření ke snížení nepříznivých dopadů v souladu s výsledky řízení změn uvedených v čl. 11.3.

11.5 Poskytovatel se zavazuje poskytnout Objednateli veškerou nezbytnou součinnost 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.

11.6 V případě realizace penetračního testování nebo testování zranitelnosti řešení poskytne Poskytovatel Objednateli veškerou potřebnou součinnost.

12. ŘÍZENÍ KONTINUITY ČINNOSTÍ

12.1 Objednatel má oprávnění zapojit Poskytovatele do řízení kontinuity činností, a to zejména oprávnění k zahrnutí Poskytovatele do plánu kontinuity činností, který souvisí s ISZS a souvisejících služeb a/nebo zahrnutí Poskytovatele do havarijního plánu Objednatele.

12.2 Objednatel má povinnost informovat Poskytovatele o způsobu zapojení dle čl. 12.1.

12.3 Poskytovatel předloží Objednateli metodiku zálohování a obnovy dat ve formě zálohovacího plánu, testovacího scénáře obnovy dat, systému evidence, zajištění integrity a autenticity zálohovacího média. Záloha jako taková musí být šifrována. Poskytovatel jako součást dodávky dále dodá a nasadí odpovídající technologické řešení, na kterém bude záloha a obnova dat prováděna.

13. INFORMAČNÍ POVINNOST POSKYTOVATELE

13.1 Poskytovatel má povinnost bez zbytečného odkladu informovat Objednatele o významné změně ovládání Poskytovatele podle zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích) nebo změně vlastnictví základních aktiv, jakož i změně v oprávnění Poskytovatele nakládat s aktivy, které jsou využívány k plnění předmětu Smlouvy.

13.2 Poskytovatel má povinnost informovat Objednatele o způsobu řízení rizik, jakož i o zbytkových rizicích souvisejících s plněním předmětu Smlouvy, a to na základě písemné výzvy Objednatele.

14. PODPOSKYTOVATELÉ

14.1 Poskytovatel nezapojí do poskytování plnění dle této Smlouvy žádného dalšího Podposkytovatele bez předchozího konkrétního nebo obecného povolení Objednatele.

14.2 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 Podposkytovatele, zajistí, že bude Objednateli poskytnuta veškerá nezbytná součinnost v otázkách řízení bezpečnosti informací také od těchto Podposkytovatelů.

14.3 Poskytovatel je povinen předat Objednateli kontaktní údaje všech osob dodávajících systémovou a technickou podporu pro řešení.

14.4 Pokud Poskytovatel využívá za účelem plnění předmětu Smlouvy Podposkytovatele, musí být tomuto Podposkytovateli uloženy na základě smlouvy s Poskytovatelem stejné povinnosti k dodržování smluvních ujednání, jaká jsou sjednaná touto Přílohou mezi Objednatelem a Poskytovatelem.

14.5 Poskytovatel se zavazuje předložit Objednateli, na základě jeho písemného vyzvání, příslušnou smlouvu s Podposkytovatelem.

14.6 Poskytovatel má povinnost zajistit, že Podposkytovatel bude v souladu s požadavky, které Objednatel ukládá na základě této Přílohy Poskytovateli.

14.7 Poskytovatel odpovídá za to, že jeho Podposkytovatelé nebudou jednat v rozporu s bezpečnostními opatřeními vyplývajícími z této Přílohy; v případě, že dojde k nedodržení těchto požadavků ze strany Podposkytovatele Poskytovatele, považuje se každé takové nedodržení požadavků za porušení povinnosti Poskytovatele dle Smlouvy.

15. LIKVIDACE DAT

15.1 Pokud v rámci plnění předmětu Smlouvy má Poskytovatel povinnost k mazání dat a k likvidaci technických nosičů a/nebo provozních údajů a/nebo informací a jejich kopií, postupuje vždy v souladu s pravidly pro mazání dat a v souladu se způsoby likvidace technických nosičů informace, provozních údajů, informací a jejich kopií stanovených Objednatelem.

15.2 Objednatel se zavazuje stanovit pravidla pro mazání dat a likvidaci technických nosičů a/nebo provozních údajů a/nebo informací a jejich kopií přiměřeně hodnotě a důležitosti aktiv.

15.3 Objednatel stanovuje, že příslušným způsobem likvidace technických nosičů a/nebo provozních údajů a/nebo informací a jejich kopií v rámci plnění předmětu Smlouvy může být, v souladu s Vyhláškou, odstranění, přepsání či fyzická likvidace nosiče informace.

16. KONTROLA A AUDIT POSKYTOVATELE

16.1 Poskytovatel se zavazuje poskytnout Objednateli veškeré informace potřebné k doložení toho, že byly splněny povinnosti vyplývající z této Přílohy, jakož i ze ZoKB a Vyhlášky, a za tímto účelem se zavazuje umožnit Objednateli provedení kontrol, včetně auditů prováděných Objednatelem či auditorem, kterého Objednatel k auditu pověří, a poskytne k těmto kontrolám a auditům veškerou potřebnou součinnost.

16.2 Poskytovatel je povinen Objednateli zpřístupnit veškerou potřebnou dokumentaci pro účely kontroly či auditu, zejména výčet technických a organizačních opatření.

16.3 Poskytovatel má povinnost určit svého zástupce (případně své zástupce), který bude po dobu provádění kontroly či auditu přítomen.

16.4 Kontrola nebo audit mohou být provedeny v prostorách Poskytovatele nebo jeho Podposkytovatele a Poskytovatel má povinnost tyto kontroly nebo audity Objednateli či Objednateli pověřené osobě umožnit či možnost jejich provedení v prostorách podposkytovatele zajistit, přispět k nim a poskytnout Objednateli či Objednateli pověřené osobě k jejich provedení maximální možnou součinnost, kterou lze po Poskytovateli rozumně požadovat. Počet a frekvence kontrol ani auditů nejsou nijak omezeny.

16.5 Objednatel má povinnost písmeně oznámit Poskytovateli provedení kontroly či auditu, a to nejméně 14 dnů před provedením kontroly či auditu. Součástí oznámení bude i seznam osob, které jsou pověřeni ze strany Objednatele k provedení kontroly či auditu.

16.6 Výstupem v provedené kontroly či auditu může být auditní zpráva; s jejími výsledky bude Poskytovatel seznámen a může se k nim vyjádřit.

16.7 Poskytovatel je dále povinen umožnit provedení kontroly či auditu i ze strany dozorových orgánů.

16.8 Poskytovatel je povinen pravidelně provádět 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.

17. OCHRANA DŮVĚRNÝCH INFORMACÍ

17.1 Strany se zavazují zachovat mlčenlivost o veškerých informacích, osobních údajích, datech či zprávách, o nichž se dozvěděly v souvislosti s přípravou či plněním této Smlouvy (dále jen „důvěrné informace“), a to včetně předmětu Smlouvy, vlastní spolupráce a vnitřních záležitostí Stran.

17.2 Důvěrné informace ve smyslu této Smlouvy nepředstavují utajované informace klasifikované stupněm „důvěrné“ ve smyslu zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

17.3 Strany se zavazují, že zajistí, aby se všechny osoby oprávněné zpracovávat důvěrné informace zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti. Závazek mlčenlivosti a ochrany důvěrných informací zůstává v platnosti i po ukončení této Smlouvy.

18. POVINNOSTI PŘI UKONČENÍ SMLOUVY

18.1 Poskytovatel se zavazuje poskytnout Objednateli veškerou potřebnou součinnost, dokumentaci a informace, účastnit se jednání s Objednatelem a popřípadě třetími osobami za účelem plynulého a řádného převedení všech činností spojených s provozem, maintenance a rozvojem předmětu Smlouvy na Objednatele a/nebo nového poskytovatele, ke kterému dojde po skončení účinnosti této Smlouvy, a to vše dle pokynů Objednatele (dále jen „Ukončení smlouvy“).

18.2 Poskytovatel se zavazuje za tímto účelem vypracovat a nejpozději spolu s provozní dokumentací ke každému předávanému dílčímu plnění předat Objednateli dokumentaci, která bude stanovovat postup při Ukončení smlouvy (dále jen „Plán“). Poskytovatel se zavazuje Plán po dobu trvání této Smlouvy průběžně aktualizovat a Objednateli vždy při změně jakékoliv skutečnosti uvedené v Plánu předat aktualizovanou verzi Plánu zohledňující tuto změnu.

18.3 Poskytovatel je povinen poskytnout plnění nezbytná k realizaci tohoto Plánu za přiměřeného použití vhodných ustanovení této Smlouvy. Závazek dle tohoto ustanovení platí i po ukončení této Smlouvy.

18.4 Strany se dohodly, že cena za vypracování Plánu a poskytnutí plnění nezbytného k realizaci Plánu je součástí ceny dle této Smlouvy.

19. USTANOVENÍ SPOLEČNÁ A ZÁVĚREČNÁ

19.1 Tato Příloha je v souladu s platnými právními předpisy České republiky. Pokud se jakékoli ustanovení této Přílohy stane neplatným či nevymahatelným, nebude to mít vliv na platnost a vymahatelnost ostatních ustanovení této Přílohy a rovněž Smlouvy. Strany se zavazují nahradit neplatné nebo nevymahatelné ustanovení novým ustanovením, jehož znění bude odpovídat úmyslu vyjádřenému původním ustanovením a touto Přílohou jako celkem.

19.2 Tato Příloha může být měněna a doplňována pouze prostřednictvím písemných průběžně číslovaných dodatků podepsaných oběma Stranami.