SMLOUVA č. CTU/2025_0049

uzavřená podle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník,
ve znění pozdějších předpisů (dále jen „smlouva“)

1.
Smluvní strany

1.1. Česká republika – Český telekomunikační úřad

se sídlem:	Sokolovská 219/58, 190 00 Praha 9 – Vysočany
jehož jménem jedná:	Mgr. David Krupa, ředitel sekce správy vnitřních věcí
IČO:	701 06 975
DIČ:	CZ70106975 (osoba identifikovaná k dani)
bank. spojení:	ČNB Praha
číslo účtu:	0-725001/0710

(dále jen „objednatel“)

1.2. Solutia s.r.o.

se sídlem:	Vršovická 1461/64, 101 00 Praha 10
zastoupená:	Martinem Milým, jednatelem
IČO:	271 27 982
DIČ:	CZ27127982
bank. spojení:	ČSOB a.s.
číslo účtu:	189725477/0300

zapsaný v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 98364

(dále jen „poskytovatel“)

(společně dále také jako „smluvní strany“)

uzavírají na základě výsledku výběrového řízení na veřejnou zakázku s názvem „IVANTI EM – licenční a technická podpora“ smlouvu následujícího znění:

2.
Základní pojmy

2.1. Základní pojmy jsou stanoveny pouze pro účely této smlouvy.

2.2. **Havárií** se rozumí stav technologického celku, který znemožňuje jeho používání jako celku nebo jeho části k účelu, pro který je provozován.

2.3. **Problémem** se rozumí stav technologického celku, který umožňuje pouze omezené používání technologického celku nebo jeho části k účelu, pro který je provozován. Tento stav není považován za plnohodnotný provoz. Problémem není námět na změnu funkce technologického celku.

2.4. **Vadou** se rozumí odchylka od funkce, popsané v dokumentaci.

2.5. **Dobou reakce** se rozumí doba, která uplyne od přijetí písemného, faxového nebo, e-mailového hlášení o vzniku problému nebo havárie poskytovatelem do zahájení řešení problému nebo řešení havárie.

2.6. **Řešením problému/havárie** se rozumí posloupnost činností vedoucích k:

2.6.1. identifikaci problému/havárie

2.6.2. nalezení příčin vzniku

2.6.3. odstranění problému/havárie.

Řešení problému/havárie je prováděno dle požadavku pověřeného pracovníka objednatele na pracovišti objednatele nebo na pracovišti poskytovatele. Řešení problému/havárie je ukončeno podpisem protokolu, který podepisují pověřená osoba poskytovatele a pověřená osoba uživatele.

2.7. **Odstraněním problému** se rozumí buď obnovení plného užívání technologického celku, nebo realizace funkčního náhradního řešení umožňujícího modifikované užívání technologického celku dle dokumentace. Při náhradním řešení mohou být použity aktualizované verze technologického celku na období do dohody smluvních stran. Za odstranění problému se považují i prokázaná zjištění vady součástí technologického celku, které poskytovatel nedodává, prokázaná nutnost reinstalace současné verze nebo nasazení aktualizované verze součásti technologického celku, které poskytovatel nedodává.

2.8. **Odstraněním havárie** se rozumí buď obnovení plného užívání technologického celku dle poslední platné zálohy dat nebo realizace funkčního náhradního řešení umožňujícího buď modifikované užívání technologického celku dle dokumentace, nebo převedení na problém.

2.9. **Uživatelem** se rozumí libovolná lokalita objednatele, která využívá technologický celek dle přílohy č. 1 této smlouvy.

2.10. **Hot–line** se rozumí poskytování bezprostředních telefonických rad, konzultací a telefonických asistencí pověřenému pracovníku objednatele poskytovatelem. Bude provozován na určeném telefonním čísle, popř. na určené elektronické adrese. Jeho součástí je informování uživatelů objednatele po době reakce o řešiteli, způsobu řešení, příp. o způsobu vyřešení problémů/havárií.

2.11. **Neoprávněným zásahem** se rozumí prokázaný zásah do technologického celku, který je v rozporu s dokumentací, pokud není proveden na písemný pokyn poskytovatele (včetně písemného pokynu z hot – line). Za neoprávněný zásah nejsou považovány změny provedené k řešení problému/havárie, pokud budou písemně sděleny poskytovatelem objednateli do 14 dnů po jejich zavedení do technologického celku.

3.
Předmět smlouvy

3.1. Předmětem smlouvy je na straně jedné závazek poskytovatele poskytnout objednateli licenční podporu 755 ks produktu IVANTI Endpoint Manager pro koncové stanice objednatele na dobu 24 měsíců.

3.2. Předmětem smlouvy je dále závazek poskytovatele poskytovat objednateli po dobu 24 měsíců technickou podporu k 755 ks produktu IVANTI Endpoint Manager pro koncové stanice objednatele v rozsahu uvedeném v bodech 2 až 7 Přílohy č. 1 této smlouvy spojené se správou systémů uvedených v bodu 1 Přílohy č. 1 této smlouvy.

3.3. Předmětem smlouvy je na straně druhé závazek objednatele uhradit poskytovateli za služby poskytnuté v souladu s touto smlouvou cenu dle čl. 6 této smlouvy.

4.
Místo a doba plnění

4.1. Místem plnění je sídlo objednatele a další lokality dle přílohy č. 2 této smlouvy.

4.2. Poskytovatel se zavazuje, že plnění podle čl. 3.1 a čl. 3.2. této smlouvy bude poskytovat objednateli počínaje dnem 1. 7. 2025, přičemž toto bude navazovat na stávající licenční podporu, která končí ke dni 30. 6. 2025.

5.
Oprávněné osoby

Objednatel do sedmi dnů ode dne účinnosti této smlouvy předá poskytovateli seznam osob oprávněných vyžádat služby dle čl. 3.2 této smlouvy.

6.
Cena a platební podmínky

6.1. Cena za poskytnutí licenční podpory 755 ks produktu IVANTI Endpoint Manager dle čl. 3.1 této smlouvy činí 875.750 Kč/rok bez DPH.

6.2. Cena za poskytnutí technické podpory 755 ks produktu IVANTI Endpoint Manager a souvisejících služeb dle č. 3.2 této smlouvy činí 21.900 Kč/měsíc bez DPH.

6.3. Cena je stanovena jako pevná a lze ji měnit, pouze pokud dojde ke změně sazby DPH. K ceně bude při její fakturaci připočtena DPH v aktuální výši ke dni uskutečněného zdanitelného plnění.

6.4. Veškeré náklady poskytovatele nezbytné pro plnění smlouvy, tj. zejména cestovní, ubytovací, komunikace, zajištění jednání s pracovníky objednatele, jsou součástí uvedených cen.

6.5. Cenu bude objednatel hradit postupně na základě daňových dokladů – faktury (dále jen „faktura“), následujícím způsobem:

a) cenu dle čl. 6.1 této smlouvy na základě faktury vystavené poskytovatelem po poskytnutí plnění dle čl. 3.1 této smlouvy,
b) cenu dle čl. 6.2 této smlouvy na základě faktury vystavené poskytovatelem vždy k 10. dni daného měsíce.

6.6. Podkladem pro úhradu ceny podle této smlouvy bude daňový doklad – faktura (dále jen „faktura“) se splatností 30 dnů od jejího doručení objednateli, která musí obsahovat veškeré náležitosti účetního dokladu předepsané příslušnými právními předpisy (zejména § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a § 435 občanského zákoníku) a číslo této smlouvy.

6.7. V případě faktury doručené objednateli mezi 15. prosincem a 10. lednem je taková faktura splatná nejdříve následujícího 1. února.

6.8. Povinnost úhrady se považuje za splněnou okamžikem odepsání příslušné částky z účtu objednatele ve prospěch bankovního účtu poskytovatele uvedeného v záhlaví této smlouvy.

6.9. V případě, že faktura nebude obsahovat některou z předepsaných náležitostí či bude obsahovat chyby v psaní či počtech, je objednatel oprávněn vrátit takovéto faktury dodavateli k doplnění či opravě. Lhůta splatnosti se v takovém případě přerušuje a počíná znovu běžet od vystavení opravené či doplněné faktury.

7.
Smluvní pokuty

7.1. Je-li objednatel v prodlení s uhrazením faktury, poskytovatel má právo účtovat zákonný úrok z prodlení z dlužné částky za každý i započatý den prodlení.

7.2. Objednatel má právo uplatnit vůči poskytovateli smluvní pokutu v případě prodlení poskytovatele s řešením problému oproti stanovené době reakce, a to v každém jednotlivém případě ve výši 5.000 Kč za každých i započatých 24 hodin prodlení.

7.3. Objednatel má právo uplatnit vůči poskytovateli smluvní pokutu v případě prodlení poskytovatele s řešením havárie oproti stanovené době reakce, a to v každém jednotlivém případě ve výši 5.000 Kč za každých i započatých 24 hodin prodlení.

7.4. Objednatel má právo uplatnit vůči poskytovateli smluvní pokutu v případě porušení povinnosti poskytovatele vyplývající z čl. 8 této smlouvy, a to v každém jednotlivém případě ve výši 50.000 Kč.

7.5. Objednatel nemá právo uplatnit smluvní pokutu, jestliže poskytovatel prokáže, že objednatel neposkytl poskytovateli spolupůsobení nutné k tomu, aby poskytovatel mohl splnit svůj závazek.

7.6. Objednatel má právo uplatnit vůči poskytovateli smluvní pokutu za nedodržení čl. 10.1 této smlouvy ve výši 2.000.000 Kč. Toto ustanovení platí 5 let po ukončení účinnosti této smlouvy.

7.7. Smluvní pokuta je splatná ve lhůtě 10 dnů ode dne, kdy poskytovatel obdrží písemnou výzvu k její úhradě.

7.8. Zaplacením smluvní pokuty dle této smlouvy není dotčen nárok smluvní strany na náhradu skutečné škody v celém rozsahu způsobené škody. Žádná ze smluvních stran neodpovídá za škodu vzniklou jako následek vyšší moci.

8.
Kybernetická bezpečnost

8.1. Poskytovatel je povinen zajistit dostatečnou bezpečnost jím provozovaných aktiv a souvisejících dat, jež využívá za účelem plnění předmětu smlouvy, a to zejména s vědomím toho, že objednatel je osoba povinná, spadající pod působnost zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále také jen „ZoKB“) a dodané plnění nesmí být v rozporu s požadavky Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) pro provoz významných informačních systémů. Dodané plnění musí proto splňovat všechny související požadavky a nařízení a musí umožňovat objednateli řádné plnění povinností podle ZoKB.

8.2. Poskytovatel se zavazuje poskytnout objednateli veškerou součinnost nezbytnou k tomu, aby objednatel řádně naplňoval právní povinnosti stanovené ZoKB a prováděcí 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; dále také jen „VoKB“). Jestliže Zhotovitel při plnění Smlouvy zjistí rozpor postupů objednatele se ZoKB nebo VoKB, je povinen takový rozpor objednateli neprodleně ohlásit a poskytnout objednateli potřebnou součinnost k jeho odstranění.

8.3. Poskytovatel se zavazuje, že bude respektovat požadavky vyplývající ze ZoKB a VoKB a bude postupovat v souladu s přílohou č. 3 této smlouvy (Specifikace plnění požadavků v oblasti kybernetické bezpečnosti).

8.4. Smluvní strany spolu v průběhu plnění smlouvy vzájemně komunikují za účelem dosažení požadované úrovně bezpečnosti. V případě ohrožení anebo porušení kybernetické bezpečnosti, zejména pak v případě výskytu kybernetické bezpečností události anebo incidentu, jejichž charakter má přímý vztah s předmětem plnění smlouvy, jsou smluvní strany povinny ihned po zjištění takových skutečností hlásit jejich výskyt druhé smluvní straně a společně podnikat potřebné kroky k zajištění obnovení požadované úrovně bezpečnosti.

8.5. V případě potřeby objednatele zajistí poskytovatel potřebnou součinnost pro účely testování plánů kontinuity činností, obnovy a procesů spojených se zvládáním kybernetických bezpečnostních incidentů.

8.6. Poskytovatel je povinen informovat objednatele o významné změně ovládání poskytovatele (ve smyslu § 71 a násl. zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů (např. případy, kdy dojde k významné změně kontroly nad poskytovatelem,

přičemž kontrolou se zde rozumí vliv, ovládání či řízení či ekvivalentní postavení) nebo změně vlastnictví zásadních aktiv, popř. změně oprávnění nakládat s těmito aktivy, využívanými poskytovatelem k plnění dle této smlouvy. Pokud bude tato změna vyhodnocena objednatelem jako bezpečnostní riziko ve smyslu ZoKB, je objednatel oprávněn odstoupit od smlouvy.

9.
Ukončení smlouvy

9.1. Tato smlouva může být ukončena písemnou dohodou obou smluvních stran.

9.2. Smluvní strany jsou oprávněny od této smlouvy odstoupit v případech stanovených občanským zákoníkem či touto smlouvou.

9.3. Kterákoliv ze smluvních stran může odstoupit od smlouvy v případě, že druhá smluvní strana poruší podstatným způsobem své povinnosti vyplývající z této smlouvy.

9.4. Za podstatné porušení smluvních povinností objednatelem se podle této smlouvy považuje prodlení objednatele s uhrazením ceny plnění o více než 30 dnů.

9.5. Za podstatné porušení smlouvy poskytovatelem se podle této smlouvy považuje zejména:

9.6. prodlení dodavatele s řádným plněním této smlouvy delší než 30 dní,

9.7. porušení povinnosti mlčenlivosti či zachování důvěrných informací.

9.8. Odstoupení od smlouvy musí být provedeno písemně a doručeno druhé smluvní straně. Právní účinky nastávají dnem doručení odstoupení od smlouvy druhé smluvní straně.

9.9. V případě ukončení této smlouvy se smluvní strany zavazují vypořádat veškeré své vzájemné závazky do 60 dnů ode dne ukončení smlouvy.

10.
Ostatní ujednání

10.1. Objednatel a poskytovatel se zavazují, že bez písemného souhlasu druhé smluvní strany neučiní informace získané při plnění této smlouvy v žádné podobě dostupné třetí straně, ani že je nepoužijí k jiným účelům než k účelům plnění této smlouvy. Toto ustanovení platí i po dobu 5 let od ukončení účinnosti této smlouvy, nemá však vliv na případné povinnosti objednatele vyplývající ze zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

10.2. Kontaktními osobami pro potřeby této smlouvy jsou:

za objednatele: [redacted]

za poskytovatele:

10.3. Tato smlouva se uzavírá na dobu 24 měsíců.

10.4. Tato smlouva vzniká dnem podpisu oprávněnými zástupci obou smluvních stran a nabývá účinnosti uveřejněním této smlouvy podle 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. Smluvní strany bezvýhradně souhlasí se zveřejněním této smlouvy, případných dodatků uzavřených k této smlouvě, jakož i se zveřejněním dalších aspektů tohoto smluvního vztahu. Uveřejnění zajistí objednatel.

10.5. Smluvní strany se zavazují, že o každé organizační změně (např. změna telefonních čísel, změna adresy atd.) se budou navzájem neprodleně písemně informovat.

10.6. Právní vztahy touto smlouvou výslovně neupravené nebo z ní vyplývající se řídí občanským zákoníkem.

10.7. Veškeré změny či doplňky této smlouvy mohou být provedeny pouze písemně, a to formou písemných, vzestupně číslovaných dodatků k této smlouvě potvrzenými oprávněnými zástupci obou smluvních stran.

10.8. Tato smlouva je vyhotovena v elektronické podobě, kdy příslušný dokument bude opatřen elektronickými podpisy zástupců obou smluvních stran.

10.9. Obě smluvní strany prohlašují, že se s textem této smlouvy seznámily, obsahu porozuměly, souhlasí s ním a na důkaz toho připojují své podpisy.

10.10. Nedílnou součástí této smlouvy jsou přílohy:

Příloha č. 1 – Specifikace poskytovaných služeb

Příloha č. 2 – Seznam lokalit objednatele

Příloha č. 3 – Specifikace plnění požadavků v oblasti kybernetické bezpečnosti.

Poskytovatel:	Objednatel:
[redacted] Digitálně podepsal Martin Milý Datum: 2025.06.19 14:35:18 +02'00'	[redacted] Elektronicky podepsal Mgr. David Krupa 25.06.2025 07:40:47
……	……
datum a podpis	datum a podpis
Martin Milý	Mgr. David Krupa
jednatel společnosti	ředitel sekce správy vnitřních věcí

Specifikace poskytovaných služeb

1) Spravované systémy

IVANTI Endpoint Manager poslední dostupná verze.

2) Hot-line – dostupnost a parametry

a) Služba technické podpory formou hot-line dostupná v pracovních dnech v době od 7:00 do 19:00 hodin.

b) Komunikace v českém jazyce.

c) Možnosti zadávání přes webové rozhraní, mail, případně přes telefon.

3) Řešení havárie a řešení problému

Servisní zásah přímo v sídle objednatele případně oblastních odborech nebo prostřednictvím vzdáleného dohledu do 4 hodin od okamžiku nahlášení.

4) Dodávka opravných a bezpečnostních záplat

Objednatel požaduje, aby poskytovatel doporučoval a na základě dohody s objednatelem bezúplatně dodával a instaloval opravné a bezpečnostní záplaty systémových modulů tak, jak budou uvolňovány příslušným výrobcem software (pozn.: nejedná se o upgrade na novou verzi produktu, ale o implementaci bezpečnostních záplat a případně záplat opravujících funkčnost stávající verze uvedených produktů).

5) Systémová a odborná podpora

Objednatel požaduje, aby poskytovatel zajistil odbornou systémovou a technickou pomoc při rozvoji, úpravách, změnách a při řešení problémů souvisejících s podporovanými systémy tím, že:

a) při jednání se subjekty třetích stran bude provádět konzultační činnost pro objednatele;

b) bude se zúčastňovat důležitých jednání a porad a zajišťovat případnou další náležitou součinnost subjektům třetích stran při implementaci jejich služeb a řešení.

6) Zajištění profylaxe

Objednatel požaduje zajištění profylaxe systému v rozsahu 1x za 3 měsíce.

7) Služba vzdáleného dohledu a technické podpory:

Objednatel požaduje, aby dálkovým dohledem byly zajišťovány zejména tyto služby:

a) kontrola správné konfigurace a otestování funkčnosti jednotlivých komponent,

b) kontrola správné aktualizace a konfigurace vzhledem k existující i budoucím bezpečnostním hrozbám,

c) instalace hotfixů a service packů pro jednotlivé produkty,

d) protokolární zaevidování provedených kontrol,

e) vyvolání incidentu technické podpory v případě potřeby (např. změna konfigurace produktu či řešení apod.),

f) vytvoření výsledného reportu pro IT management,

g) koordinace případné technické podpory s příslušnými správci systémů a technologických celků.

Lokality objednatele

Sídlo objednatele

Český telekomunikační úřad
Sokolovská 58/219
Praha 9 – Vysočany

Odbory pro oblasti

ČTÚ – odbor pro jihočeskou oblast
L.B. Schneidera 2306/34
370 01 České Budějovice 6

ČTÚ – odbor pro západočeskou oblast
Husova 2727/10
301 00 Plzeň – Jižní Předměstí

Závodu Míru 725/16
360 10 Karlovy Vary

ČTÚ – odbor pro severočeskou oblast
Mírové náměstí 3097/37
400 01 Ústí nad Labem

Kašparova 592
463 12 Liberec

ČTÚ – odbor pro východočeskou oblast
Velké náměstí 1
500 03 Hradec Králové

ČTÚ – odbor pro jihomoravskou oblast
Šumavská 525/33
602 00 Brno – Veveří

ČTÚ – odbor pro severomoravskou oblast
Havlíčkovo nábřeží 2728/38
702 00 Ostrava

ČTÚ – oddělení monitorování rádiového spektra Tehov
K Radiostanici 104
251 01 Říčany u Prahy

ČTÚ – oddělení monitorování rádiového spektra Karlovice
Karlovice 404
768 43 Kostelec u Holešova

ČTÚ – oddělení technické podpory Brno
Jurkovičova 1
638 00 Brno – Lesná

Specifikace plnění požadavků v oblasti kybernetické bezpečnosti

Vymezení pojmů

Pro potřeby této přílohy smlouvy jsou použity následující zkratky a pojmy:

ZoKB – zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů,

VoKB – vyhláška 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) v platném znění,

Kybernetické požadavky – kybernetickými požadavky se rozumí všechny bezpečnostní požadavky ve smyslu ZoKB a VoKB,

Produkční prostředí – produkčním prostředím se rozumí prostředí běžně přístupné uživatelům IS ČTÚ v ostrém provozu,

Testovací prostředí – prostředí určené k provádění testů, vzdělávání uživatelů apod, a to v podobě, nastavení a rozsahu umožňujícím účinně zkoumat funkcionality testovacích verzí IS ČTÚ,

Prostředí objednatele – fyzický perimetr určený ohraničením fyzického prostoru v nájmu nebo majetku objednatele anebo logický perimetr definovaný hraničními síťovými prvky ve správě nebo majetku objednatele,

Osoba na straně poskytovatele – fyzická osoba podílející se na poskytování předmětu plnění a mající pracovněprávní či obdobný smluvní vztah s poskytovatelem nebo jeho poddodavateli,

Osobní údaje – každá informace o identifikované nebo identifikovatelné fyzické osobě (subjektu údajů), jestliže lze subjekt údajů přímo či nepřímo pomocí tohoto údaje identifikovat,

Zpracování osobních údajů – jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

1 ÚVODNÍ USTANOVENÍ

1.1 Z důvodu nutnosti plnění povinností stanovených objednateli jakožto povinné osobě ve smyslu VoKB je poskytovatel povinen nad rámec povinností stanovených smlouvou plnit níže uvedené povinnosti zejména součinnostního a bezpečnostního charakteru dle této přílohy č. 3 smlouvy. Účelem této přílohy č. 3 smlouvy tak je dodržet povinnost objednatele dle § 4 odst. 4 ZoKB zahrnout požadavky vyplývající z bezpečnostních opatření do smluvního ujednání s poskytovatelem.

2 SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

2.1 Poskytovatel je povinen se v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 3 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

a) Prosadit bezpečnostní zásady a procesy, které budou pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně poskytovatele při poskytování předmětu plnění dle smlouvy.

b) Na základě bezpečnostních potřeb a výsledků hodnocení rizik zavést příslušná bezpečnostní opatření v rozsahu poskytovaného předmětu plnění, monitorovat je, vyhodnocovat jejich účinnost.

c) Vést záznamy o vytváření a zpracování dat a informací v rozsahu poskytovaného předmětu plnění, zaznamenávat veškeré podstatné okolnosti související se zajištěním bezpečnosti těchto dat a informací a na vyžádání tyto záznamy objednateli zpřístupnit.

d) Stanovit a udržovat aktuální bezpečnostní politiku, která bude pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně poskytovatele při poskytování předmětu plnění. Bezpečnostní politika musí obsahovat hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací.

2.2 Poskytovatel je dále povinen dodržovat bezpečnostní politiku objednatele, byl-li s ní prokazatelně seznámen.

3 ŘÍZENÍ AKTIV

3.1 Poskytovatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 4 VoKB, které musí splnit objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění dle Smlouvy na své straně:

3.1.1 Stanovit a udržovat rozsah a seznam aktiv využívaných pro plnění této smlouvy (aktivy se rozumí např. data a informace k předmětu plnění dle této smlouvy, systémy ICT, moduly, hardware prvky – infrastruktura hlasové a datové komunikace, aplikace, databáze, servery, úložiště, koncová zařízení – pracovní stanice typu osobní počítač nebo notebook, mobilní koncová zařízení apod.), a tato aktiva strukturovaně popsat a objednateli předložit následně na vyžádání, a to po celou dobu trvání smlouvy.

4 ŘÍZENÍ RIZIK

4.1 Poskytovatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 5 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

4.1.1 Řídit vlastní rizika, která mohou ovlivnit poskytování předmětu plnění dle smlouvy.

4.1.2 V minimálním intervalu jednou ročně (nebo i v případě významných změn činností prováděných pro objednatele nebo změn spravovaných aktiv) vytvořit a bude-li to objednatel požadovat, předložit mu zprávu o hodnocení rizik, která bude minimálně pokrývat:

a) Vyhodnocení stavu kybernetické bezpečnosti za hodnocený rok;

b) Identifikaci a hodnocení rizik s vazbou na předmět plnění;

c) Realizovaná bezpečnostní opatření;

d) Nepokrytá bezpečnostní rizika a návrh opatření;

e) Vyhodnocení bezpečnostních událostí a incidentů;

f) Aktuální stav souladu poskytovatele s kybernetickými požadavky včetně přehledu kybernetických požadavků, které:

- nebyly aplikovány, včetně odůvodnění, a
- byly aplikovány, včetně způsobu plnění.

5 ORGANIZAČNÍ BEZPEČNOST

5.1 Poskytovatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 6 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

5.1.1 Jmenovat nejpozději do 30 dnů po uzavření smlouvy odpovědnou kontaktní osobu/y pro potřeby zajištění plnění kybernetických požadavků a související komunikace mezi smluvními stranami (dále jen „kontaktní osoba pro kybernetickou bezpečnost“). Kontaktní osobu/y pro kybernetickou bezpečnost sdělí poskytovatel písemně objednateli v téže lhůtě.

5.1.2 Využívat pro poskytování předmětu plnění dle smlouvy pouze oprávněných osob, které byly řádně seznámeny s příslušnými ustanoveními interních předpisů objednatele a mají ověřenou kvalifikaci, znalosti a zkušenosti k řádnému poskytování předmětu plnění dle smlouvy a stanovit bezpečnostní role těchto oprávněných osob s jasně definovanými odpovědnostmi a pravomocemi.

6 ŘÍZENÍ POSKYTOVATELŮ

6.1 Poskytovatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 8 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

6.1.1 Využívá-li při poskytování předmětu plnění dle smlouvy subdodavatele, zajistit v obdobném rozsahu dodržování kybernetických požadavků rovněž ve smluvních vztazích se svými subdodavateli.

6.1.2 Dodržovat podmínky při zpracování osobních údajů pro zapojení každého dalšího poskytovatele.

7 BEZPEČNOST LIDSKÝCH ZDROJŮ

7.1 Poskytovatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 9 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

7.1.1 Zajistit, aby kontaktní osoba pro kybernetickou bezpečnost nejpozději do 30 dnů od uzavření smlouvy potvrdila písemně objednateli, že všechny osoby podílející se na poskytování předmětu plnění dle smlouvy za poskytovatele byly prokazatelně seznámeny s těmito kybernetickými požadavky a příslušnými ustanoveními interních předpisů objednatele.

7.1.2 Dodržovat příslušná ustanovení interních předpisů objednatele v rozsahu, v jakém byl s těmito akty seznámen. Za prokazatelné seznámení se považuje:

- školení pracovníků poskytovatele zajištěné objednatelem
- protokolární či elektronické předání příslušných předpisů nebo
- objednatelem zajištěný přístup na sdílené úložiště obsahující příslušné interní předpisy, jejichž konkrétní jmenovitý seznam bude poskytovateli – současně s poskytnutím přístupu – protokolárně předán

7.1.3 Při provádění dohledu nad předmětem plnění dle smlouvy, definovat a naplnit role a odpovědnosti pro monitoring sítě a zařízení v rozsahu předmětu plnění dle smlouvy.

7.1.4 Zajistit, aby osoby podílející se na poskytování plnění objednateli v prostředí/nebo s prostředky objednatele, a to i tehdy, pokud jsou prostředky objednatele používány mimo jeho prostředí:

a) pro uložení a sdíleni dat a informací objednatele využívaly pouze k tomu schválené prostředky (aktiva);

b) neukládaly ani nesdílely data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující dobré jméno objednatele;

c) nestahovaly, nesdílely, neukládaly, nearchivovaly ani neinstalovaly datové a spustitelné soubory v rozporu s licenčními podmínkami nebo předpisy upravující ochranu duševního vlastnictví;

d) nenavštěvovaly internetové stránky s eticky nevhodným obsahem;

e) nerealizovaly pokusy o neautorizovaný přístup ke zdrojům objednatele ani ke zdrojům jiných subjektů;

f) nerealizovaly pokusy o neoprávněnou modifikaci ani jiné neoprávněné zásahy do prostředků objednatele, a to ani v případě, kdy jim byl prostředek objednatele svěřen do správy;

g) nepodílely se s prostředky objednatele na šíření spamu ani škodlivého softwaru.

7.2 Poskytovatel si je vědom, že součástí podmínek pro získání přístupu ke zdrojům a aktivům objednatele je na straně objednatele zpracování osobních údajů pověřených osob poskytovatele, které se podílejí na poskytování plnění dle smlouvy. Pokud nebude objednateli umožněno osobní údaje pověřených osob poskytovatele zpracovat, nebude těmto pracovníkům umožněn žádný přístup ke zdrojům objednatele.

8 ŘÍZENÍ PROVOZU A KOMUNIKACÍ

8.1 Poskytovatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 10 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

8.1.1 Zajistit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování předmětu plnění dle smlouvy.

8.1.2 Na vyžádání ve lhůtě, která nebude kratší než 10 pracovních dnů, poskytnout objednateli přehled, report, či jinou adekvátní informaci o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře.

8.1.3 Zajistit, že pro poskytování předmětu plnění dle smlouvy budou využívány pouze aplikace a technologie, které jsou v souladu s platnou českou legislativou, a to především s ohledem na licenční podmínky a předpisy upravující ochranu duševního vlastnictví (zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů).

8.2 Poskytovatel je dále povinen provést a zabezpečit dodržování následujících opatření:

8.2.1 Implementaci procesů pro řízení ICT (tj. řízení incidentů, řízení změn, řízení životního cyklu systémů apod.).

8.2.2 Zavedení postupů pro ochranu proti škodlivému kódu včetně řízení technických zranitelností v informačním systému, který je využíván k poskytování předmětu plnění dle smlouvy.

8.2.3 Zavedení pravidel a postupů pro ochranu informací a dat.

8.2.4 Stanovení pracovních postupů pro instalaci, spouštění, ukončování provozu technických aktiv a pracovní postupy pro řešení mimořádných stavů.

8.2.5 Řízení přístupu k datům a systémům, které spadají do rozsahu poskytování předmětu plnění dle smlouvy.

9 ŘÍZENÍ ZMĚN

9.1 Poskytovatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 11 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

9.1.1 Přiměřeně reagovat na změny v oblasti kybernetické bezpečnosti na straně objednatele a upravit na své straně technická a organizační opatření tak, aby odpovídala novému stavu po provedení změny.

9.1.2 Aktivně spolupracovat při testování významné změny v oblasti kybernetické bezpečnosti na straně objednatele.

10 ŘÍZENÍ PŘÍSTUPU

10.1 Poskytovatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 12 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

10.1.1 Přidělovat oprávnění svým jednotlivým pracovníkům ve smyslu oprávnění k výkonu činností tak, aby byla minimalizována rizika nežádoucího přístupu k aktivům objednatele.

10.1.2 Zajistit, aby udělený přístup nebyl sdílen více osobami za stranu poskytovatele. V opačném případě musí poskytovatel vést evidenci využívání sdílených přístupů a tuto na vyžádání předložit objednateli kdykoli v průběhu trvání účinnosti této smlouvy a tři měsíce po jejím ukončení, ve lhůtě, která nebude kratší než 6 pracovních dnů.

10.1.3 Stanovit v požadavku na přístup rozsah dat/informací, služby, účelu, pro které je přístup k systému ICT objednatele požadován a časový údaj o délce platnosti přístupu (např.: na dobu neurčitou, 1 rok, 1 měsíc apod).

10.1.4 Zajistit, aby osoby podílející se na poskytování předmětu plnění dle smlouvy a mající přístup k informačním aktivům objednatele chránily autentizační prostředky a údaje a nikdy neposkytovaly neautorizovaný přístup dalším osobám.

10.1.5 Průběžně kontrolovat a vyhodnocovat oprávněnost a potřebu přístupu, jak fyzického, tak i logického, u všech osob na straně poskytovatele, které přistupují do prostředí objednatele.

10.2 Poskytovatel bere na vědomí, že oprávnění přístupu k systémům ICT objednatele je možné povolit pouze fyzické identitě zaměstnance poskytovatele/subdodavatele, a to na základě příslušného požadavku poskytovatele.

10.3 Poskytovatel bere na vědomí, že přidělení oprávnění přístupu musí být řízeno principem nezbytného minima a není nárokové.

10.4 Poskytovatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele (osoby za stranu poskytovatele) může být příslušný účet objednatelem zablokován a řešen jako bezpečnostní incident a dále mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu (např. okamžité zrušení přístupu k informačním aktivům objednatele).

11 AKVIZICE, VÝVOJ A ÚDRŽBA

11.1 Poskytovatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 13 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

11.1.1 Zajistit bezpečnou implementaci, inovaci, aktualizaci a testování technologií, pokud jsou předmětem plnění dle smlouvy či jeho součástí.

11.1.2 Není-li Smlouvou stanoveno jinak, předat při ukončení smlouvy objednateli kompletní provozní a bezpečnostní dokumentaci předmětu plnění dle smlouvy. Ta musí být předána minimálně v následujícím rozsahu:

i) dokumentaci skutečného provedení;

ii) dokumentaci všech bezpečnostních nastavení, funkcí a mechanismů;

iii) dokumentaci obsahující popis autorizačního konceptu a oprávnění;

iv) dokumentaci obsahující instalační a konfigurační postupy;

v) dokumentaci obsahující zálohovací a archivační postupy;

vi) dokumentaci pro zajištění DR (obnovy po havárii), eventuálně pro zajištění kontinuity provozu.

Bezpečnostní dokumentaci poskytovatel předá objednateli v přiměřené lhůtě, nejpozději pak dle předchozí dohody smluvních stran.

11.2 V případě, že předmět plnění dle smlouvy zahrnuje částečně i vývoj softwaru, je poskytovatel povinen:

11.2.1 Dodržovat a implementovat obecně uznávané „nejlepší praktiky“ pro bezpečný vývoj softwaru (např. u webových aplikací OWASP). Základním pravidlem zde je myslet na bezpečnost softwaru ve všech jeho vývojových fázích.

11.2.2 Pokud jsou softwarové auditní činnosti a předání zdrojového kódu k softwaru součástí plnění dle smlouvy, umožní poskytovatel objednateli audit prováděného nebo provedeného plnění a na písemnou žádost objednatele předloží poskytovatel ve stanovené lhůtě - nejdříve však 5 pracovních dnů od podání žádosti - vyvíjený zdrojový kód na provedení tzv. codereview, a to především za účelem ověření skutečnosti, zda poskytovatel postupuje či postupoval při poskytování plnění v souladu se smlouvou a těmito bezpečnostními požadavky.

11.2.3 Poskytovat objednateli v termínech stanovených objednatelem, resp. bez zbytečného odkladu požadovanou součinnost na provedení bezpečnostního testování v průběhu vývoje softwaru (nejdříve však od zahájení testovacího provozu) či kdykoli po jeho předání.

11.2.4 Pokud je součástí plnění dle smlouvy i instalace operačního systému, případně softwaru třetích stran, zajistit v průběhu jeho instalace, že budou použity předepsané verze těchto produktů kompatibilní a funkční v testovacím prostředí či produkčním prostředí objednatele.

11.2.5 Zajistit bezpečnost testovacího prostředí u poskytovatele a ochranu poskytnutých testovacích dat objednatelem.

11.2.6 Zajistit, že v rámci poskytovaného plnění bude dodávaný software

i) v souladu s bezpečnostními politikami a standardy objednatele;

ii) otestován na soulad s bezpečnostními politikami objednatele, pokud byl s takovými bezpečnostními politikami prokazatelně seznámen.

11.2.7 Instalovat software pouze na základě předem schválených migračních postupů objednatelem.

11.2.8 Předat zdrojový kód objednateli bezpečnou formou zajišťující jeho integritu.

11.2.9 Zajistit řízení verzí zdrojového kódu, jeho zálohování a jeho uložení mimo produkční prostředí.

12 ZVLÁDÁNÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ A INCIDENTŮ

12.1. Poskytovatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 14 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění dle smlouvy:

12.1.1 Stanovit a popsat na své straně činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání bezpečnostních událostí a incidentů.

12.1.2 Bez zbytečného odkladu hlásit objednateli všechny bezpečnostní události a incidenty s potenciálním negativním dopadem na objednatele, a to stanoveným komunikačním kanálem nebo prostřednictvím kontaktní osoby pro kybernetickou bezpečnost.

12.1.3 Vyhodnocovat informace o bezpečnostních incidentech a uchovávat je pro budoucí použití, a to s ohledem na požadavky použitelné platné a účinné legislativy.

12.1.4 V případě vzniku bezpečnostní události a následného vyhodnocování možného bezpečnostního incidentu a/nebo v případě podezření na možný bezpečnostní incident, poskytnout objednateli aktivní součinnost a relevantní informace o podezřelém zařízení či podezřelém jednání osob na straně poskytovatele.

12.1.5 Spolupracovat při analýze příčin bezpečnostního incidentu a v případě, že bude prokazatelně zjištěno, že poskytovatel bezpečnostní incident zapříčinil nebo se na jeho vzniku částečně spolupodílel, navrhnout seznam všech možných opatření s cílem zamezit možnému budoucímu opakování.

12.1.6 Po dohodě s objednatelem realizovat bez zbytečného odkladu opatření požadovaná objednatelem ke snížení dopadu bezpečnostního incidentu nebo zamezení pokračování bezpečnostního incidentu, nejpozději pak v termínech prokazatelně stanovených objednatelem.

12.2 Poskytovatel bere na vědomí, že postup zvládání bezpečnostního incidentu či jiný důsledek porušení bezpečnostních požadavků, jehož příčina je na straně poskytovatele, 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. Ostatní ustanovení ohledně odpovědnosti poskytovatele za prodlení obsažená ve smlouvě nejsou tímto ustanovením dotčena.

13 ŘÍZENÍ KONTINUITY ČINNOSTÍ

13.1. Poskytovatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 15 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

13.1.1 Zajistit adekvátní kontinuitu svých aktiv, které jsou potřebné k poskytování předmětu plnění dle smlouvy.

13.1.2 Pravidelně kontrolovat a testovat, že je schopen kontinuitu těchto aktiv zajistit dle sjednané SLA.

14 KONTROLA A AUDIT

14.1 Poskytovatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 8 a § 16 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění dle smlouvy poskytnout adekvátní součinnost při výkonu kontroly objednatele ze strany Národního úřadu pro kybernetickou a informační bezpečnost dle § 23 ZoKB.

14.2 Poskytovatel umožní objednateli alespoň jednou ročně po dobu účinnosti smlouvy provedení auditu kybernetické bezpečnosti (dále jen audit) u poskytovatele a jeho případných subdodavatelů:

14.2.1 jehož rozsah bude ohraničen v rámci ICT prostředků poskytovatele používaných pro potřeby plnění smlouvy a uloženými či zpracovávanými daty a informacemi objednatele v ICT prostředí poskytovatele a

14.2.2 jehož předmětem bude naplnění kybernetických požadavků a vyhodnocení rizik dle bodu 4 této přílohy č. 3 smlouvy.

14.3 Objednatel je oprávněn při provedení auditu využít třetí stranu. V případě využití třetí strany bude objednatel odpovídat za třetí stranu, jako by audit kybernetické bezpečnosti prováděl sám, včetně odpovědnosti za případnou způsobenou újmu.

14.4 Poskytovatel umožní objednateli audit provedený prostředky objednatele nebo třetí strany, a to v lokalitě poskytovatele i vzdáleně, pokud to technické prostředky poskytovatele umožňují.

14.5 Poskytovatel je povinen nedostatky zjištěné:

14.5.1 na základě provedení hodnocení rizik dle bodu 4 této přílohy č. 3 smlouvy; nebo

14.5.2 v rámci auditu kybernetické bezpečnosti dle bodu 14 této přílohy č. 3 smlouvy;

odstranit ve lhůtě určené v písemném oznámení objednatele, která nebude kratší než 20 pracovních dnů. Nestanoví-li objednatel lhůtu v písemném oznámení, zavazují se smluvní strany dohodnout na lhůtě pro odstranění nedostatku, která nepřevýší 60 dnů.

14.6 Poskytovatel je dále povinen:

14.6.1 Poskytnout na vyžádání objednateli dokumenty a obdobné vstupy, které budou prokazovat naplnění kybernetických požadavků.

14.6.2 Na požádání s objednatelem konzultovat kdykoli v průběhu realizace plnění dle smlouvy detailní nastavení bezpečnostních opatření k naplnění kybernetických požadavků a pro takovéto konzultace zajistit účast kvalifikovaných pracovníků.

14.6.3 Neprodleně informovat objednatele o všech významných změnách v naplnění kybernetických požadavků, které nastanou kdykoli v průběhu trvání smlouvy.

14.6.4 Bezodkladně a s vyvinutím maximálního úsilí zajistit náhradní způsob naplnění kybernetických požadavků, pokud stávající řešení přestalo být funkční a efektivní.

14.6.5 Při výkonu své činnosti včas a prokazatelně upozornit objednatele na případnou zřejmou nevhodnost jeho příkazů či doporučení, vztahujících se ke kybernetickým požadavkům, jejichž následkem může vzniknout případná újma anebo nesoulad s příslušnými zákony nebo jinými obecně závaznými právními předpisy.

15 TECHNICKÁ OPATŘENÍ

15.1 Poskytovatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 17 až § 27 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

15.1.1 Dodržovat příslušné interní předpisy objednatele, s nimiž byl prokazatelně seznámen, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěna aktiva systémů ICT, anebo datové nosiče.

15.1.2 V rozsahu předmětu plnění dle smlouvy zajistit fyzické zabezpečení, zejména označení, uchování a likvidaci, instalačních, záložních nebo archivních médií a dokumentace v souladu s klasifikací aktiv objednatele, pokud s ní byl poskytovatel seznámen.

15.1.3 Realizovat doporučená bezpečnostní opatření pro odstranění nebo blokování komunikačních spojení, která neodpovídají požadavkům na ochranu integrity a bezpečnosti komunikační sítě.

15.1.4 Realizovat přístupy z mobilních zařízení k aktivům v produkčním i testovacím prostředí objednatele pouze prostřednictvím zabezpečeného připojení virtuální privátní sítě (VPN).

15.1.5 Připojovat do produkčního prostředí objednatele pouze ta síťová zařízení (switch, wifi router apod.), která prošla schvalovacím procesem a jejich připojení bylo schváleno oprávněnou osobou ve věcech technických na straně objednatele, určenou v této smlouvě.

15.1.6 Bez zbytečného odkladu deaktivovat všechna nevyužívaná zakončení sítě anebo nepoužívané porty aktivního síťového prvku, pakliže tento je součástí sjednaného rozsahu předmětu plnění dle smlouvy a je současně ve správě poskytovatele.

15.1.7 Na aktiva objednatele bez jeho písemného souhlasu neinstalovat a nepoužívat v prostředí objednatele následující typy nástrojů, pokud vysloveně nejsou součástí předmětu plnění dle smlouvy:

i) Keylogger – software nebo hardware, který neautorizovaně zaznamenává stisky kláves s cílem narušit důvěrnost zadávaných dat a informací.

ii) Sniffer – software nebo hardware umožňující odposlouchávání síťového provozu.

iii) Analyzátor zranitelností (scanner zranitelností) – softwarový nebo hardwarový nástroj umožňující vyhledávání zranitelností systémů ICT, detekování dostupných síťových služeb a portů, běžících procesů, běžících aplikací a jejich verzí apod.

iv) Backdoor – skrytý softwarový nebo hardwarový nástroj, který umožňuje obejití schválených autentizačních procedur, instalovaný s cílem budoucího snadnějšího a neautorizovaného přístupu do počítačového systému.

v) Malware a jiný škodlivý software, který narušuje, obchází či jinak omezuje stávající bezpečnostní opatření v prostředí Objednatele.

15.1.8 Připojovat do prostředí objednatele pouze zařízení ICT, která splňují následující požadavky:

- jsou příslušným způsobem zabezpečena a chráněna proti malware a jinému škodlivému softwaru – minimálně instalovaný a aktivní antivir

s aktuální definiční sadou, pokud možno instalované veškeré doporučené bezpečnostní záplaty pro OS a používaný SW, správně nakonfigurovaný a aktivní firewall

- způsob jejich připojení je definován v příslušné provozní nebo projektové dokumentaci nebo je v souladu s příslušnými interními předpisy objednatele.

15.1.9 Zajistit sběr informací o provozních a bezpečnostních činnostech v rozsahu předmětu plnění dle smlouvy a ochranu získaných informací před jejich neoprávněným čtením nebo změnou:

- pro veškeré on-line transakce realizované prostřednictvím webových technologií implementovat doporučené a schválené TLS/SSL certifikáty s cílem zajistit důvěrnost a integritu komunikace protistran.
- pro neveřejné informace poskytnuté objednatelem a ukládané na mobilní zařízení anebo přenosná paměťová média, která jsou ve správě poskytovatele, chránit vhodným šifrováním a proti neautorizovanému přístupu.

15.2 Poskytovatel bere na vědomí, že v případě, kdy technické spojení ze strany poskytovatele narušuje bezpečný chod ostatních služeb objednatele, může být toto spojení ze strany objednatele bez předchozího upozornění ihned ukončeno.

15.3 Poskytovatel bere na vědomí, že veškeré jeho aktivity realizované v prostředí objednatele mohou být monitorovány a vyhodnocovány v souladu s příslušnými interními dokumenty objednatele.