Smlouva č. CTU/2025_0029
o dodání SW nástroje a provedení analýzy rizik informačních systémů ČTÚ

uzavřená podle § 1746 odst. 2, § 2079 a násl. a s využitím § 2358 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „smlouva"), mezi těmito smluvními stranami:

1. Česká republika – Český telekomunikační úřad

Se sídlem:	Sokolovská 58/219, Praha 9 - Vysočany
Adresa pro doručování:	poštovní přihrádka 02, 225 02 Praha 025
Bankovní spojení:	ČNB – pobočka Praha
Číslo účtu:	725001/0710
IČO:	701 06 975
DIČ:	CZ70106975 (osoba identifikovaná k dani)
Jejímž jménem jedná:	Ing. Marek Ebert, předseda Rady ČTÚ

(dále jen „objednatel") na straně jedné

a

2. DATASYS s.r.o.

Se sídlem:	Jeseniova 2829/20, 130 00 Praha 3
Zastoupená:	JUDr. Filip Efraim Plášil, prokurista
IČO:	612 49 157
DIČ:	CZ61249157
Bankovní spojení:	Komerční banka, a.s., Praha
Číslo účtu:	27-9647490267/0100

Zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze, sp. zn. C 28862

(dále jen „poskytovatel") na straně druhé.

1.
Účel a předmět smlouvy

1. Účelem této smlouvy je stanovení obsahových požadavků, postupů, obchodních podmínek a dalších smluvních ujednání, na jejichž základě dojde k realizaci předmětu plnění na základě výsledků výběrového řízení v rámci veřejné zakázky malého rozsahu na dodávky a služby s názvem „Provedení analýzy rizik vybraných informačních systémů ČTÚ včetně dodání SW nástroje pro provádění analýzy rizik" v rozsahu uvedeném v odstavci 2 tohoto článku a příloze č. 1 této smlouvy (Specifikace předmětu plnění).
2. Předmětem této smlouvy je na straně jedné závazek poskytovatele dodat objednateli softwarový (SW) nástroj pro hodnocení a analýzu rizik v oblasti kybernetické bezpečnosti (dále jen „SW nástroj"), s customizací v prostředí objednatele, a dále provést pro objednatele analýzu rizik v oblasti kybernetické bezpečnosti u vybraných informačních systémů a další navazující požadované činnosti v rozsahu a za podmínek stanovených touto smlouvou včetně její přílohy č. 1 (Specifikace předmětu plnění). Dodávka SW nástroje a provedení analýz musí být v souladu s platnou legislativou, především zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, a 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), a v souladu s metodickým materiálem Národního

úřadu pro kybernetickou a informační bezpečnost (NUKIB) – „Průvodce řízením aktiv a rizik podle vyhlášky o kybernetické bezpečnosti“, to vše v rozsahu a za podmínek podle této smlouvy včetně její přílohy č. 1 (Specifikace předmětu plnění).

3. Na straně druhé je předmětem této smlouvy závazek objednatele za řádně a včas poskytnuté plnění zaplatit poskytovateli sjednanou cenu podle čl. 7 této smlouvy.

2.
Místo plnění

Místem plnění je sídlo objednatele, nedohodnou-li se smluvní strany jinak.

3.
Termín plnění

Poskytovatel se zavazuje poskytnout řádné plnění objednateli takto:

a) dodávka SW nástroje nejpozději do 1 měsíce ode dne účinnosti smlouvy;

b) provedení analýz rizik vybraných informačních systémů nejpozději do 4 měsíců ode dne účinnosti smlouvy a dále podle bodu II odst. 8 přílohy č. 1 této smlouvy (Specifikace předmětu plnění);

c) činnosti podle bodu II odst. 7 přílohy č. 1 této smlouvy (Specifikace předmětu plnění) nejpozději do 4 měsíců ode dne účinnosti nové právní úpravy.

4.
Předání a převzetí

1. Plnění se považuje za řádně poskytnuté po předání SW nástroje (tj. včetně naplnění požadavků podle přílohy č. 1 této smlouvy) a dále veškeré dokumentace o provedení analýz rizik vybraných informačních systémů objednatele, kdy akceptace řádného plnění bude potvrzena podepsáním akceptačního protokolu.

2. Poskytovatel doručí (předá) řádně zpracované písemné výstupy v elektronické podobě ve formátu DOCX a PDF na adresu objednatele pro doručování, případně osobně (kurýrem) do podatelny v sídle objednatele, nebo elektronicky cestou Informačního systému datových schránek, případně budou součástí dodaného nástroje pro analýzu rizik.

3. O řádném předání plnění bude pořízen písemný předávací protokol, ve kterém pověřený zástupce poskytovatele (viz čl. 14 odst. 5 této smlouvy) výslovně prohlásí, že plnění je předáváno bez vad, a pověřený zástupce objednatele (viz čl. 14 odst. 5 této smlouvy) prohlásí, že plnění přebírají ke kontrole kvality (protokol o shodě) a akceptačnímu řízení (akceptační protokol). Předání a převzetí se uskuteční na písemnou výzvu poskytovatele doručenou pověřenému zástupci objednatele min. 2 pracovní dny před plánovaným předáním. Výsledkem kontroly kvality může být „Schváleno bez výhrad“ (tj. shoda se specifikací provedení - při kontrole kvality nebyly shledány nedostatky bránící akceptaci výstupu), a „Neschváleno - vráceno k přepracování“ (tj. neshoda se specifikací provedení - při kontrole kvality byly shledány vady a nedodělky bránící akceptaci výstupu; poskytovatel odstraní všechny nalezené vady a nedodělky v termínu stanoveném objednatelem; odstranění zjištěných vad a nedodělků bude ověřeno opětovnou kontrolou kvality a výsledek bude zaznamenán formou dodatku k protokolu o shodě). Akceptační řízení následuje po schválení bez výhrad v protokolu o shodě ve vztahu ke všem částem plnění a je ukončeno podepsáním akceptačního protokolu.

5.
Záruka za jakost

1. Prodávající poskytuje na plnění záruku za jakost v délce 24 měsíců. Záruční doba počíná běžet dnem podpisu akceptačního protokolu podle čl. 4 odst. 3 této smlouvy.
2. Smluvní strany sjednávají, že v případě zjištění vady se kupující zavazuje vadu oznámit prodávajícímu prokazatelným způsobem.
3. Prodávající se zavazuje vadu odstranit nejpozději do 5 dnů ode dne jejího oznámení.

6.
Práva a povinnosti smluvních stran, součinnost

1. Poskytovatel se zavazuje:
   a) poskytnout plnění podle této smlouvy v souladu se všemi podmínkami a požadavky uvedenými v této smlouvě, se specifikací předmětu plnění uvedenou v Příloze č. 1 této smlouvy, a to včas, řádně, poctivě, pečlivě, podle svých schopností a s náležitou odbornou úrovní, a přitom použít každého prostředku, kterého vyžaduje povaha obstarávané záležitosti, jakož i takového, který se shoduje s vůlí objednatele,
   b) aktivně projednávat s objednatelem postup plnění, informovat o průběžných výsledcích a průběžně konzultovat své návrhy a doporučení,
   c) dodržovat pokyny objednatele při plnění předmětu této smlouvy,
   d) postupovat tak, aby nezasáhl při své činnosti do informačních systémů objednatele, a nést plnou odpovědnost za případné porušení této povinnosti,
   e) nahradit objednavateli případnou škodu, která mu vznikne v důsledku porušení povinností poskytovatele i škodu, která vznikne v důsledku činnosti poskytovatele na majetku či zdraví osob, a to bez omezení výše náhrady této škody. Poskytovatel současně odpovídá za škody, které způsobili objednateli či třetím osobám v souvislosti s poskytováním plnění zaměstnanci poskytovatele, jeho poddodavatelé či osoby v obdobném postavení porušením svých povinností při plnění této smlouvy,
   f) nejméně dva pracovní dny předem uvědomit kontaktní osobu objednatele uvedenou v čl. 14 odst. 5 této smlouvy o termínu požadovaného fyzického přístupu k některému z významných informačních systémů, které souvisí s předmětem plnění podle této smlouvy, bude-li jej poskytovatel požadovat,
   g) v rámci plnění v podobě aktualizace zpracovaných analýz rizik v oblasti kybernetické bezpečnosti u vybraných informačních systémů podle bodu II odst. 8 přílohy č. 1 této smlouvy (Specifikace předmětu plnění) poskytnout pověřenému zástupci objednatele (viz čl. 14 odst. 5 této smlouvy) k odsouhlasení nejpozději do 15 dnů od vyžádání předběžný odhad maximální pracnosti (v ČLH) ve vztahu k jednotlivým informačním systémům,
   h) bez zbytečného odkladu oznámit objednateli všechny okolnosti, které zjistil nebo měl zjistit při poskytování plnění, a které mohou mít vliv na poskytované plnění či změnu pokynů nebo zájmů objednatele,
   i) po celou dobu trvání této smlouvy zajistit:
      - plnění veškerých povinností vyplývajících z právních předpisů České republiky, zejména pak předpisů pracovněprávních, předpisů v oblasti zaměstnanosti, a dále oblasti bezpečnosti a ochrany zdraví při práci, a to vůči všem osobám, které se budou podílet na plnění této smlouvy;

- dodržování zákona č. 198/2009 Sb., o rovném zacházení a o právních prostředcích ochrany před diskriminací a o změně některých zákonů (antidiskriminační zákon), ve znění pozdějších předpisů;
- řádné a včasné plnění finančních závazků vůči svým případným poddodavatelům.

Plnění uvedených povinností zajistí poskytovatel i u svých případných poddodavatelů.

2. Objednatel se zavazuje:
   a) předat včas poskytovateli úplné, pravdivé a přehledné informace a podklady, jež jsou nezbytně nutné k plnění předmětu této smlouvy, pokud z jejich povahy nevyplývá, že je má zajistit poskytovatel v rámci své činnosti,
   b) poskytovat poskytovateli během plnění předmětu této smlouvy v případě potřeby součinnost v přiměřeném rozsahu,
   c) umožnit poskytovateli nezbytný přístup k některému z významných informačních systémů, které souvisí s předmětem plnění podle této smlouvy.
3. Nastanou-li u některé ze smluvních stran skutečnosti bránící řádnému plnění této smlouvy, je tato smluvní strana povinna ihned bez zbytečného odkladu tuto skutečnost oznámit druhé smluvní straně a vyvolat jednání vedoucí k odstranění daných překážek.
4. Poskytovatel se zavazuje poskytnout objednateli nevýhradní časově a prostorově neomezenou licenci k užívání výstupů a postoupit výkon majetkových autorských práv těmto výstupům, případně k jejich úpravám s tím, že licenční oprávnění poskytnou objednateli neomezené oprávnění ke všem činnostem, které jsou potřebné k efektivnímu využití výstupů, přičemž toto je již zahrnuto v ceně podle čl. 7 této smlouvy.
5. Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých závazků. Smluvní strany jsou povinny informovat druhou smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění smlouvy.
6. Poskytovatel je povinen poskytovat služby podle smlouvy prostřednictvím realizačního týmu, jehož složení uvedl ve své nabídce v rámci výběrového řízení, přičemž osoby, které jsou členem realizačního týmu, musí splňovat kvalifikační předpoklady uvedené ve výzvě k podání nabídky. Případná změna složení realizačního týmu musí být předem písemně odsouhlasena objednatelem, přičemž složení realizačního týmu musí splňovat požadavky na technickou kvalifikaci uvedené ve výzvě k podání nabídky.

7.
Cena a platební podmínky

1. Cena za plnění podle této smlouvy činí 1.695.000 Kč bez DPH, z toho DPH ve výši 21 % činí 355.950 Kč, tj. celková cena za plnění podle této smlouvy činí 2.050.950 Kč včetně DPH. Z toho cena za:
   a) dodání SW nástroje včetně požadovaného rozsahu podpory podle přílohy č. 1 této smlouvy (Specifikace předmětu plnění) činí 510.000 Kč bez DPH,
   b) provedení analýzy rizik v oblasti kybernetické bezpečnosti u vybraných informačních systémů a dalších navazujících požadovaných činností činí 1.145.000 Kč bez DPH,
   c) činnosti podle bodu II odst. 7 přílohy č. 1 této smlouvy (Specifikace předmětu plnění) činí 40.000 Kč bez DPH.
2. Celková cena je stanovena jako konečná, pevná a nepřekročitelná, přičemž není-li stanoveno jinak, zahrnuje veškeré náklady související s plněním předmětu smlouvy, a to včetně odměny za poskytnutí licence k užití SW nástroje v rozsahu uvedeném v této smlouvě. Cena může být změněna pouze v případě změny sazby daně z přidané hodnoty.

3. Celková cena nezahrnuje náklady na aktualizaci zpracovaných analýz rizik v oblasti kybernetické bezpečnosti u vybraných informačních systémů podle bodu II odst. 8 přílohy č. 1 této smlouvy (Specifikace předmětu plnění). Cena za 1 ČLH provádění aktualizace zpracovaných analýz rizik v oblasti kybernetické bezpečnosti u vybraných informačních systémů podle bodu II odst. 8 přílohy č. 1 této smlouvy (Specifikace předmětu plnění) činí 1.190 Kč bez DPH. K dohodnuté ceně bude připočtena příslušná DPH ve výši odpovídající aktuální právní úpravě ke dni zdanitelného plnění. Cena za skutečný rozsah provádění aktualizace bude hrazena na základě písemného odsouhlasení řádného plnění včetně skutečného rozsahu pověřeným zástupcem objednatele (viz čl. 14 odst. 5 této smlouvy), a to postupem obdobným čl. 4 této smlouvy.
4. Nárok na úhradu ceny za plnění vzniká poskytovateli okamžikem podpisu akceptačního protokolu podle čl. 4 odst. 3 této smlouvy.
5. Celková cena bude uhrazena bezhotovostním převodem na účet poskytovatele, a to na základě daňového dokladu – faktury (dále jen „faktura“) vystavené poskytovatelem se splatností nejméně 30 dnů ode dne jejího doručení kupujícímu.
6. Faktura musí obsahovat náležitosti účetního dokladu předepsané příslušnými právními předpisy (podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a § 435 občanského zákoníku) a současně číslo této smlouvy. Nedílnou součást faktury bude tvořit kopie akceptačního protokolu.
7. V případě, že faktura nebude obsahovat některou z předepsaných náležitostí či bude obsahovat chyby v psaní či počtech, je objednatel oprávněn vrátit takovou fakturu poskytovateli k doplnění či opravě. Lhůta splatnosti se v takovém případě přerušuje a počíná znovu běžet od vystavení opravené či doplněné faktury.
8. Platební povinnosti objednatele plynoucí z této smlouvy jsou splněny dnem odepsání částky z účtu objednatele ve prospěch účtu poskytovatele.

8.
Povinnost mlčenlivosti
Důvěrnost informací

1. Objednatel a poskytovatel se zavazují, že obchodní, technické, jakož i netechnické informace, které mají nebo by mohly mít potenciální hodnotu, a které jim byly svěřeny smluvním partnerem, nezpřístupní třetím osobám bez předchozího písemného souhlasu druhé smluvní strany a nepoužijí tyto informace ani pro jiné účely než pro plnění svých závazků podle podmínek této smlouvy. Za důvěrnou informaci se pokládá vždy taková informace, která je takto kteroukoliv smluvní stranou kdykoliv označena. To však neplatí v případě, že by se stala tato informace, k níž se zavazují k povinnosti mlčenlivosti či k povinnosti zachovat důvěrnost informace, podle tohoto ustanovení smlouvy, obecně známou či dostupnou. To se nevztahuje na výstupy z plnění podle této smlouvy.
2. Poskytovatel se výslovně zavazuje, že předmět plnění ani jakékoliv dílčí plnění sám neužije k jinému účelu než výlučně k plnění této smlouvy.
3. Poskytovatel a objednatel se zavazuje, že informace, týkající se této smlouvy či jinak získané v souvislosti s plněním této smlouvy, nezneužije ve svůj prospěch ani ve prospěch jiné osoby, ani je nezveřejní v jakékoliv formě a dále se zavazuje, že veškeré výstupy provedené podle této smlouvy budou poskytovatelem užity pouze a výlučně v souladu s touto smlouvou.
4. Poskytovatel se zavazuje po ukončení své činnosti pro objednatele k vymazání veškerých informací a dat, které mu byly v souvislosti s plněním této smlouvy zpřístupněny, ať už se jedná o informace a data předané objednatelem, nebo které mohl zjistit poskytovatel sám v rámci plnění této smlouvy.

5. Osoby (zástupci poskytovatele), kterým byl sjednán přístup k některému z informačních systémů, které souvisí s předmětem plnění podle této smlouvy, se zavazují jej nepředávat dalším osobám (včetně ostatních zaměstnanců poskytovatele) bez jednoznačného souhlasu objednatele k případnému předání přístupu těmto dalším osobám. Tyto osoby jsou povinny neprodleně informovat objednatele, pokud vznikne podezření na odcizení či jiné zneužití těchto přístupových oprávnění.
6. Poskytovatel je povinen informovat objednatele o případném bezpečnostním incidentu (odcizení přístupových oprávnění, únik důvěrných informací apod.) souvisejícím s plněním této smlouvy. V případě závažného bezpečnostního incidentu, jehož povaha může mít další vliv na bezpečnost systému či jeho samotné provozní fungování, je poskytovatel povinen informovat neprodleně telefonicky kontaktní osobu objednatele. O každém bezpečnostním incidentu souvisejícím s plněním této smlouvy je poskytovatel také povinen neprodleně informovat kontaktní osobu objednatele elektronicky e-mailem, nejpozději však do 24 hodin. Kontaktní osoby objednatele jsou uvedeny v čl. 14 odst. 5 této smlouvy.
7. Poskytovatel je povinen důkladně informovat veškeré další osoby, které se budou na straně poskytovatele podílet na plnění této smlouvy, o povinnostech vyplývajících z tohoto článku.

9.
Vyšší moc

1. Smluvní strany nebudou odpovědné za částečné nebo úplné neplnění smluvních závazků následkem okolností vylučujících odpovědnost v případech tzv. vyšší moci.
2. Výraz vyšší moc znamená a zahrnuje zejména: přírodní katastrofu, požár, záplavy, zemětřesení a dále povstání, stávky, pracovní boje jakéhokoliv druhu nebo terorismus, které mají přímou souvislost a brání plnění povinností ze smlouvy a plnění povinností nelze zajistit jinak nebo je nahradit, nehody, pád letadla včetně nehod, kterým se nedalo vyhnout v souvislosti s plněním této smlouvy včetně přijetí zákona nebo mimořádného rozhodnutí příslušného úřadu v souvislosti se zásahem vyšší moci, pokud příčiny a události mají vliv na plnění povinností stran ze smlouvy a plnění povinností vyplývajících ze smlouvy nelze zajistit jinak.
3. Vyskytne-li se působení překážky v důsledku vyšší moci, s níž jsou spojeny účinky vylučující odpovědnost, lhůty ke splnění smluvních závazků se prodlouží o dobu trvání takové překážky. Smluvní strana, která je postižena takovou překážkou, je však povinna okamžitě, písemně, uvědomit druhou smluvní stranu o této skutečnosti, o začátku trvání této překážky a předpokládané době jejího trvání.

10.
Nebezpečí škody a nabytí vlastnického práva

Nebezpečí škody na plnění a vlastnické právo k němu přechází z prodávajícího na kupujícího okamžikem, kdy kupující potvrdí převzetí plnění způsobem uvedeným v čl. 4 odst. 3 této smlouvy.

11.
Salvátorské ustanovení

Obě smluvní strany prohlašují, že pokud se kterékoliv ustanovení této smlouvy nebo s ní související ujednání ukáže být neplatným nebo se neplatným stane, že tato skutečnost neovlivní platnost smlouvy jako celku. V takovém případě se obě smluvní strany zavazují nahradit neprodleně neplatné ustanovení ustanovením platným; obdobně se zavazují postupovat v případě ostatních nedostatků smlouvy či souvisejících ujednání.

12.
Ukončení smlouvy

1. Tato smlouva může být ukončena splněním, písemnou dohodou obou smluvních stran nebo odstoupením od smlouvy.
2. Smluvní strany jsou oprávněny od této smlouvy odstoupit v případech stanovených občanským zákoníkem či touto smlouvou.
3. Kterákoliv ze smluvních stran může odstoupit od smlouvy v případě, že druhá smluvní strana poruší podstatným nebo neodstranitelným způsobem své povinnosti vyplývající z této smlouvy.
4. Za podstatné porušení smluvních povinností poskytovatelem se považuje:
   a) nedodržení stanoveného termínu poskytnutí plnění,
   b) neodstranění vady či nedodělku ve sjednané lhůtě,
   c) existence vady bránící naplnění účelu smlouvy,
   d) neposkytnutí součinnosti,
   e) uvedení nepravdivých údajů v nabídce ze strany poskytovatele,
   f) porušení mlčenlivosti a bezpečnostních pravidel objednatele podle čl. 8, resp. přílohy č. 2 této smlouvy,
5. Stanoví-li oprávněná smluvní strana druhé smluvní straně pro splnění jejího závazku náhradní (dodatečnou) lhůtu, vzniká jí právo odstoupit od smlouvy až po marném uplynutí této lhůty, to neplatí, jestliže druhá smluvní strana v průběhu této lhůty prohlásí, že svůj závazek nesplní.
6. Odstoupení od smlouvy musí být provedeno písemně a doručeno druhé smluvní straně. Právní účinky nastávají dnem doručení písemného oznámení o odstoupení od smlouvy druhé smluvní straně.
7. V případě, že tato smlouva zanikne odstoupením z viny poskytovatele podle odstavce 3 tohoto článku smlouvy, nemá poskytovatel nárok na náhradu vynaložených nákladů.

13.
Smluvní pokuty, odpovědnost za škody

1. V případě prodlení objednatele s uhrazením faktury má poskytovatel právo na úrok z prodlení v zákonné výši z dlužné částky za každý i započatý den prodlení.
2. V případě prodlení poskytovatele s termínem plnění podle čl. 3 této smlouvy je poskytovatel povinen zaplatit objednateli smluvní pokutu ve výši 1.000 Kč za každý i započatý den prodlení.
3. V případě prodlení poskytovatele s odstraněním ohlášené vady plnění podle čl. 5 odst. 3 této smlouvy je poskytovatel povinen zaplatit objednateli smluvní pokutu ve výši 1.000 Kč za každý i započatý den prodlení.
4. V případě porušení povinnosti poskytovatele stanovené v čl. 6 odst. 6 této smlouvy je poskytovatel povinen zaplatit objednateli smluvní pokutu ve výši 20.000 Kč za každý jednotlivý případ porušení takové povinnosti.
5. V případě porušení jiné povinnosti poskytovatele stanovené touto smlouvou je poskytovatel povinen zaplatit objednateli smluvní pokutu ve výši 5.000 Kč za každý jednotlivý případ porušení takové povinnosti.
6. Smluvní pokuty a úrok z prodlení jsou splatné ve lhůtě 10 dnů ode dne doručení písemné výzvy k jejich úhradě.

7. Dnem úhrady smluvní pokuty se rozumí den, kdy je částka odpovídající její výši připsána ve prospěch účtu objednatele.
8. Zaplacením smluvní pokuty podle této smlouvy není dotčena povinnost poskytovatele nahradit škodu vzniklou objednateli porušením smluvní povinnosti, které se smluvní pokuta týká, a to v celém rozsahu způsobené škody.
9. Uplatněním nároku na smluvní pokutu ani jejím skutečným uhrazením nezaniká povinnost poskytovatele splnit povinnost, jejíž plnění bylo zajištěno smluvní pokutou.
10. Žádná ze smluvních stran neodpovídá za škodu vzniklou jako následek vyšší moci.

14.
Závěrečná ustanovení

1. Poskytovatel se zavazuje, že při práci s daty objednatele bude plně respektovat nařízení zákona č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů, a Nařízení 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.
2. Poskytovatel se zavazuje, že bude respektovat požadavky vyplývající ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, 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) a v souladu s přílohou č. 2 této smlouvy (Kybernetická bezpečnost).
3. Jestliže bude mít objednatel jakékoli výhrady, ať již ve vztahu k poskytovanému plnění předmětu této smlouvy nebo k osobám podílejících se na straně poskytovatele na plnění předmětu této smlouvy, sdělí je důvěrným způsobem kontaktní osobě poskytovatele uvedené v odstavci 5 tohoto článku. Jestliže se bude domnívat, že tyto výhrady nejsou adekvátně řešeny nebo že jejich charakter či vážnost to vyžadují, bude výslovně kontaktovat odpovědnou osobu uvedenou v záhlaví této smlouvy.
4. Jestliže výhrada podle odstavce 3 tohoto článku nebude vyřešena způsobem uspokojivým pro obě smluvní strany, jmenují obě smluvní strany po jednom vedoucím zaměstnanci, který bude oprávněn vyvolat jednání a s vynaložením veškeré dobré vůle vyřešit spornou záležitost. Schůzka se musí uskutečnit v přiměřeně krátké době po písemném vyzvání jedné ze smluvních stran. Pokud nedojde k dohodě, je objednatel oprávněn odstoupit od smlouvy v souladu s čl. 12 odst. 2 této smlouvy.
5. Pověřenými zástupci pro potřeby této smlouvy jsou:

- za objednatele: (*pozn.: bude doplněno před podpisem smlouvy*)

  ve věcech obchodních: [redacted]

  ve věcech technických:

- za poskytovatele:

  ve věcech obchodních:

  ve věcech technických:

6. Pověření zástupci ve věcech obchodních jsou osoby, které mohou vést jednání a připravovat dokumenty vedoucí ke změně smlouvy, vést s druhou smluvní stranou jednání obchodního charakteru a za objednatele udělovat souhlas se změnou poddodavatelů a členů v realizačním týmu poskytovatele.
7. Pověření zástupci ve věcech technických jsou osoby, které mohou jednat v záležitostech věcného plnění smlouvy, vést jednání technického charakteru, poskytovat stanoviska v technických otázkách a podepisovat předávací/akceptační protokoly.
8. Tato smlouva je vyhotovena v elektronické podobě, kdy bude příslušný dokument opatřen elektronickými podpisy zástupců obou smluvních stran.
9. Nedílnou součástí této smlouvy je: příloha č. 1 - Specifikace předmětu plnění
   příloha č. 2 – Kybernetická bezpečnost.
10. Tato smlouva a práva a povinnosti z ní vyplývající se řídí českým právem. Práva a povinnosti smluvních stran, pokud nejsou upraveny touto smlouvou, se řídí občanským zákoníkem a předpisy souvisejícími.
11. Veškeré změny či doplňky této smlouvy mohou být provedeny pouze písemně, a to formou písemných, vzestupně číslovaných dodatků k této smlouvě potvrzenými oběma smluvními stranami, a to osobami oprávněnými jednat za smluvní strany ve věcech smluvních.
12. 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.
13. Jakékoli oznámení ve smyslu této smlouvy od druhé smluvní strany musí být písemné.
14. Případnou změnu pověřených zástupců jsou poskytovatel i objednatel povinni neprodleně prokazatelně písemně oznámit druhé smluvní straně.
15. Tato smlouva se vztahuje i na právní nástupce smluvních stran.
16. Jednacím jazykem je čeština, všechny písemné výstupy budou předávány v češtině.
17. Smluvní strany prohlašují, že smlouvu před jejím podepsáním přečetly, jejímu obsahu rozumí a s jejím obsahem souhlasí. Na důkaz svého souhlasu připojují obě smluvní strany své podpisy.

V Praze dne dle elektronického podpisu

Za poskytovatele:

[redacted]
JUDr. Filip Efraim Plášil
Digitální podpis: 20.06.2025 10:19:05

JUDr. Filip Efraim Plášil
prokurista
DATASYS s.r.o.

V Praze dne dle elektronického podpisu

Za objednatele:

[redacted]
Digitálně podepsal Ing. Marek Ebert
Datum: 2025.06.24 14:52:05 +02'00'

.....

Ing. Marek Ebert
předseda Rady
Českého telekomunikačního úřadu

Specifikace předmětu plnění

I. Popis současného stavu

Objednatel (ČTÚ) má vytvořené níže uvedené dokumenty:

1. Politiku systému řízení bezpečnosti (ZP č. 63)
2. Metodiku řízení a hodnocení rizik.
3. Analýzu rizik pro Centrální IS VSS (vrstva společných služeb) a IS elektronické pošty v rámci, které je zpracováno:
   a) Seznam primárních aktiv
   b) Seznam podpůrných aktiv
   c) Mapování závislostí
   d) Hodnocení aktiv
   e) Mapování hrozeb a zranitelností na aktiva
   f) Hodnocení hrozeb
   g) Hodnocení aktuálního stavu implementovaných opatření
   h) Vyhodnocení aktuálních rizik
   i) Návrh opatření
   j) Určení zbytkových rizik
   k) Zpráva o hodnocení rizik
4. Bezpečnostní politiku ve struktuře požadované vyhláškou 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).

II. Požadavek na provedení analýz a zpracování souvisejících dokumentů

1. Provedení analýz rizik pro následující IS:
   a) Automatizovaný systém monitorování kmitočtového spektra (ASMKS)
   b) Spisová služba GINIS (GINIS SSL)
   c) Modulární správní systém (MOSS)
   d) Společný katalog subjektů SKS)
   e) Spectra plus
   f) Měřicí systém elektronických komunikací (MSEK)
   g) Ekonomický systém (EKIS)
   h) Webové stránky ČTÚ (web ČTÚ).
2. Aktualizace analýzy rizik pro následující IS:
   a) Informační systém elektronické pošty (IS EP)
   b) Informační systém Vrstva společných služeb (IS VSS)
3. Následná revize existující Bezpečnostní politiky tak, aby byla zohledněna všechna opatření, která vyplynula z analýz rizik.

4. Dokončení kompletního rozpadu aktiv (do úrovně podrobnosti, která bude pro následné řízení pro ČTÚ potřebná, např. tvorba a implementace pravidel pro SIEM).
5. Vytvoření dalších dokumentů, resp. jejich šablon, pro následné dokončení ČTÚ (resp. dodavatelů), navazujících na Bezpečnostní politiku (typicky DRP, incident management, směrnice pro administrátory). Předpokladem je vytvořit společný dokument pro IS, které využívají jen společné služby, pro ostatní IS dokumenty samostatné.
6. Vytvoření vzorové dokumentace interních auditů (vytvoření checklistů, vytvoření šablon zprávy a auditu a plánu auditu).
7. Po nabytí účinnosti nové právní úpravy podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů
   a) Zařazení ČTÚ jakožto povinné (regulované) osoby a jeho IS vzhledem k požadavkům nového zákona o kybernetické bezpečnosti.
   b) Vytvoření přehledu plnění požadavků nové právní úpravy v kontextu zařazení ČTÚ jakožto regulovaného subjektu.
   c) Návrh opatření k realizaci (jejich doplnění do Plánu zvládání rizik)

      Poznámka:

      Předpokládáno je minimálně doplnění Bezpečnostní politiky a související úprava mapování opatření. Provedení souvisejících úprav do SW nástroje (aplikace pro hodnocení a analýzu rizik).
8. Aktualizace všech zpracovaných analýz rizik 1x ročně a při významných změnách po dobu poskytování technické a uživatelské podpory nástroje pro hodnocení a analýzu rizik.

III. Požadavky na SW nástroj pro hodnocení a analýzu rizik s customizací v prostředí objednatele

Objednatel poptává nástroj / aplikační SW pro hodnocení a analýzu rizik organizace který zajistí bezpapírovou evidenci analýz rizik, správu metodik pro hodnocení rizik organizace, správu analýz rizik, správu bezpečnostních a nápravných opatření. Nástroj musí umožňovat nastavení metodiky hodnocení rizik různých oblastí podle legislativních norem i podle specifických směrnic organizace a výstupy podle legislativních požadavků.

IV. Požadované základní vlastnosti SW nástroje

1. SW nástroj musí splňovat následující funkční požadavky:
   - Správa jednotlivých analýz rizik vč. správy aktiv prostřednictvím modelu aktiv
   - Správa životního cyklu analýzy rizik (příprava, realizace, ukončení, sledování nápravných opatření) – tzv. user friendly (aplikace je intuitivní, provede uživatele analýzou rizik krok za krokem, kontextová nápověda)
   - Modelování aktiv (definování aktiv, identifikace vazeb mezi primárními a podpůrnými aktivy, hodnocení aktiv, hodnocení sdružených aktiv)
   - Evidence dodavatelů a smluv s vazbou na hodnocená aktiva
   - Evidence interních a externích předpisů
   - Evidence auditů a neshod z auditů
   - Nastavení metodiky a parametrů na analýze rizik

- Export analýzy rizik (kompletní, vč. nápravných opatření)
- Export hrozeb a bezpečnostních opatření
- Import hrozeb a bezpečnostních opatření
- Import kompletní analýzy rizik včetně hodnotících údajů včetně/bez nápravných opatření
- Výstupy analýzy rizik podle legislativních požadavků – exportovací a tiskové sestavy pro Přehled rizik, Pokrytí rizik opatřeními, Prohlášení SOA a Plán zvládání rizik
- Správa a řízení přístupů podle týmových rolí na úrovni jednotlivých analýz rizik
- Notifikace uživatelů (možnost nastavení notifikací podle účelu a potřeb organizace – upozornění na termín, přidání člena týmu, přidělení úkolu zajištění opatření apod.)
- Auditní log aktivit, historie
- Přehled analýz rizik, modelů aktiv, bezpečnostních opatření
- On-premise nasazení v prostředí Zadavatele
- Lokalizace do českého jazyka

2. SW nástroj musí naplňovat následující funkce správy hrozeb a zranitelností:
   - Správa a hodnocení aktiv
   - Správa a hodnocení hrozeb
   - Správa a hodnocení zranitelností (katalogových)
   - Evidence zjištěných technických zranitelností a jejich vlivu na aktiva
   - Evidence bezpečnostních událostí a incidentů a jejich vlivu na aktiva
   - Podpora různých „workflow“ pro řešení zranitelností, událostí a incidentů
   - Šablony postupů pro řešení bezpečnostních incidentů s předdefinovanými úkoly
   - Automatizované generování výstupů k bezpečnostním incidentů (např. pro NÚKIB)
3. SW nástroj musí naplňovat následující funkce správy bezpečnostních opatření (BO)
   - Každé BO má jedinečný identifikační kód
   - Je možné BO přidat, rušit, změnit oblast BO, je možný export a import sady / katalogu BO.
4. SW nástroj musí naplňovat následující funkce správy nápravných opatření (NO)

   SW nástroj musí zajistit správu NO a jejich řízení k předcházení rizika. SW nástroj zajišťuje celý životní cyklus NO – přípravu NO a jeho schválení, jeho realizaci, monitorování NO a archivaci implementovaného NO. NO musí být provázána na BO.
   - Správa NO samostatně i ve vazbě na BO (příprava, schválení k realizaci, realizace, ukončení NO – splnění úkolu)
   - Každé NO má jedinečný identifikační kód
   - Je možné NO přidat, rušit, změnit
   - Je možné přidělit jedno NO k „n“ bezpečnostním opatřením
   - Je možné přidělit konkrétní přístupy k danému NO
   - Je možné odesílat notifikace podle nastavených pravidel
   - Je možné realizovat export/import NO z analýzy rizik

5. SW nástroj musí naplňovat následující požadavky na Metodiku hodnocení rizik (správa rizik)

   SW nástroj musí umožnit zadání různé metodiky hodnocení rizik ve vazbě na oblast hodnocení rizik.

   SW nástroj též musí automaticky vypočítávat inherentní, výchozí a zbytková rizika, je možné zobrazit přehled všech rizik.

   Požadovaným výstupem je Přehled rizik, Pokrytí rizik opatřeními, Prohlášení SOA a Plán zvládání rizik.

   Metodika hodnocení rizik se v aplikaci musí nastavovat minimálně těmito parametry – typy aktiv, úrovně rizik (včetně barevné škály). Toto nastavení provádí administrátor.

   SW nástroj musí umět pracovat minimálně s metodikou podle legislativních požadavků:

   - zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů
   - 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), v platném znění
   - ČSN EN ISO/IEC 27002 Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací.

   SW nástroj dále musí podporovat zadání další metodiky (podle směrnic a metodiky Objednatele).

6. Nástroj musí naplňovat následující funkce správy aktiv a evidence závislostí mezi aktivy (modelování aktiv)

   SW nástroj musí zajistit vytváření seznamů aktiv, evidenci závislostí mezi souvisejícími aktivy, hodnocení aktiv i sdružených aktiv. Dále SW nástroj musí vést uživatele procesem hodnocení a určování závislostí mezi aktivy. Evidenci těchto závislostí požaduje i vyhláška o kybernetické bezpečnosti.

7. SW nástroj musí naplňovat následující požadavky na funkčnosti a procesy, které nástroj musí podporovat:

   - identifikací aktiv vč. klasifikace aktiv na primární a sekundární (podpůrná) aktiva
   - identifikaci závislostí mezi aktivy
   - hodnocení primárních aktiv – hodnocení aspektů aktiv
   - hodnocení sekundárních (podpůrných) aktiv s ohledem na závislosti mezi aktivy – pokud sekundární (podpůrné) aktivum závisí na primárním aktivu, sekundární aktivum musí přebrat hodnotu primárního aktiva v jednom nebo ve více aspektech:
     - na jednom primárním aktivu může záviset více sekundárních (podpůrných) aktiv – aktivum vystupující jako „potomek“ v každém aspektu samostatně přebírá maximální hodnotu od aktiv v roli „rodiče“.
   - Závislosti aktiv – nástroj musí identifikovat:
     - které aktivum vystupuje v roli „potomka“, resp. „rodiče“,
     - zda je typ závislosti pevná, či volná,
     - jaké aspekty daná závislost ovlivní.
   - Seznam / přehled modelů aktiv (nové, aktivní, zrušené, uzavřené, všechny)

8. SW nástroj musí naplňovat následující požadavky na administraci a konfiguraci:

   Nástroj musí umožnit konfiguračně upravovat (číselníky):

   - Oblasti analýzy rizik
   - Aspekty
   - Typy aktiv
   - Typy metodik
   - Výpočetní metody
   - Úrovně rizik, vč. barevné škály
   - Role a oprávnění přístupů

9. SW nástroj musí naplňovat následující požadavky na správu přístupů:

   Zadavatel požaduje, aby systém umožňoval správu přístupů na základě rolí. Řízení oprávnění k jednotlivým analýzám, opatřením apod. bude založeno na globálním řízení pomocí aplikačních rolí, super aplikačních rolí a týmových rolí v určených úrovních oprávnění.

   Úrovně oprávnění jsou nastavitelná pro týmové role pro analýzu rizik, pro metodiku, pro nápravná opatření, modely aktiv.

   Přístupy do aplikace musí být integrovatelné s Active Directory.

10. Technické podmínky

    - Instalace do prostředí Objednatele
    - Školení klíčových uživatelů

V. Další požadavky na plnění

- Instalace on-premise do prostředí a na výpočetní prostředky objednatele
- Příprava a import stávajících dat objednatele v rozsahu:
  - Kontrola a úprava stávající metodiky objednatele pro řízení rizik tak, aby byla v souladu s možnostmi nástroje
  - Import stávající analýzy rizik objednatele pro Vrstvu společných služeb a IS elektronické pošty
  - Import stávajícího seznamu aktiv pro Vrstvu společných služeb a IS elektronické pošty
- Poskytování technické a uživatelské podpory SW nástroje na dobu 5 let:
  - Aktualizace nástroje při vydání nové verze
  - Řešení chybových stavů SW nástroje (čas odezvy: do 3 pracovních dnů, čas vyřešení: do 5 pracovních dnů)
  - Úprava nástroje pro shodu s relevantními právními předpisy (nový chystaný zákon a vyhlášky o kybernetické bezpečnosti na základě směrnice NIS2)
- Součástí plnění je požadavek na předání formou provedení otestování celého SW nástroje před jeho předáním objednateli.
- Naplnění databází existujícími vstupními daty do softwaru SW nástroje a paralelně s tím bude objednateli poskytnuta podpora při naplnění dalších dat.

- Zaškolení uživatelů objednatele k obsluze SW nástroje.
- Prodávající poskytuje okamžikem předání plnění objednateli nevýhradní, územně a časově neomezené právo produkt užít, a to v počtu min. 3 licencí s plným přístupem na úrovni administrátora a 47 licencí pro běžného uživatele s možností čtení a zápisu a provádění změn.
- K produktu musí být poskytnuta technická a zákaznická podpora v režimu 8/5

  Pravidla a postupy pro hlášení požadavků servisní podpory:

  Požadavky na poskytování servisní podpory dle této smlouvy hlásí objednatel výhradně prostřednictvím webové aplikace Helpdesk na adrese [redacted]

  Zadání požadavku do aplikace Helpdesk bude považováno za požadavek na Služby.

  Poskytovatel potvrdí příjem hlášení prostřednictvím webové aplikace. Dříve než dojde k vyřešení požadavku, může být objednatel požádán, aby provedl systémový diagnostický test, který mu pro tento účel poskytne poskytovatel.

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

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 podle této přílohy č. 2 smlouvy. Účelem této přílohy č. 2 smlouvy tak je dodržet povinnost objednatele podle § 4 odst. 4 ZoKB zahrnout požadavky vyplývající z bezpečnostních opatření do smluvního ujednání s poskytovatelem.

1.2 Poskytovatel je povinen plnit relevantní povinnosti v rozsahu a způsobem, aby byl naplněn účel právní úpravy v oblasti bezpečnostních opatření, kybernetických bezpečnostních incidentů, reaktivních opatření, náležitostí podání v oblasti kybernetické bezpečnosti a likvidaci dat ve vztahu k povinnostem, které tato právní úprava stanovuje objednateli jakožto povinné osobě podle předpisů z oblasti kybernetické bezpečnosti, a to i v případě změny příslušné právní úpravy. V takovém případě je objednatel oprávněn požadovat od poskytovatele přiměřenou součinnost i nad rámec povinností stanovených v této příloze smlouvy, avšak vždy pouze za účelem zajištění plnění povinnosti poskytovatele z oblasti kybernetické bezpečnosti ve smyslu shora uvedeného.

2. SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

2.1 Poskytovatel je povinen se v rozsahu předmětu plnění podle smlouvy aktivně podílet na splnění povinností uvedených v § 3 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění podle 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 podle 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 podle smlouvy aktivně podílet na splnění povinností uvedených v § 4 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění podle smlouvy na své straně:

a) 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 podle smlouvy aktivně podílet na splnění povinností uvedených v § 5 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění podle smlouvy na své straně:

a) Řídit vlastní rizika, která mohou ovlivnit poskytování předmětu plnění podle smlouvy.

b) 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:

i) Vyhodnocení stavu kybernetické bezpečnosti za hodnocený rok;

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

iii) Realizovaná bezpečnostní opatření;

iv) Nepokrytá bezpečnostní rizika a návrh opatření;

v) Vyhodnocení bezpečnostních událostí a incidentů;

vi) 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 podle smlouvy aktivně podílet na splnění povinností uvedených v § 6 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění podle smlouvy na své straně:

a) 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.

b) 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 DODAVATELŮ

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

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

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

7. BEZPEČNOST LIDSKÝCH ZDROJŮ

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

a) Zajistit, aby kontaktní osoba pro kybernetickou bezpečnost nejpozději do 60 dnů od uzavření smlouvy potvrdila písemně objednateli, že všechny osoby podílející se na poskytování předmětu plnění podle smlouvy za poskytovatele byly prokazatelně seznámeny s těmito kybernetickými požadavky a příslušnými ustanoveními interních předpisů objednatele.

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

i) školení pracovníků poskytovatele zajištěné objednatelem,

ii) protokolární či elektronické předání příslušných předpisů, nebo

iii) objednatelem zajištěný přístup na sdílené úložiště obsahující příslušné interní předpisy, jejichž konkrétní jmenovitý seznam bude poskytovateli – současně s poskytnutím přístupu – protokolárně předán.

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

d) Zajistit, aby osoby podílející se na poskytování plnění objednateli v prostředí/nebo s prostředky objednatele:

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

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

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

iv) nenavštěvovaly internetové stránky s eticky nevhodným obsahem,

v) nerealizovaly pokusy o neautorizovaný přístup ke zdrojům objednatele ani ke zdrojům jiných subjektů,

vi) 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,

vii) nepodílely se s prostředky objednatele na šíření spamu ani škodlivého softwaru,

a to i tehdy, pokud jsou prostředky objednatele používány mimo jeho prostředí.

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.

7.3 Poskytovatel je dále povinen:

a) Prohlubovat znalostí osob podílejících se na poskytování plnění objednateli v oblasti bezpečnosti informací.

b) Stanovit práva a povinnosti osob podílejících se na poskytování plnění objednateli v oblasti bezpečnosti informací.

8. ŘÍZENÍ PROVOZU A KOMUNIKACÍ

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

a) Zajistit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování předmětu plnění podle smlouvy.

b) 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.

c) Zajistit, že pro poskytování předmětu plnění podle 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:

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

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

c) Zavedení pravidel a postupů pro ochranu informací a dat.

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

e) Řízení přístupu k datům a systémům, které spadají do rozsahu poskytování předmětu plnění podle smlouvy.

9. ŘÍZENÍ ZMĚN

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

a) 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.

b) 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 podle smlouvy aktivně podílet na splnění povinností uvedených v § 12 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění podle smlouvy na své straně:

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

b) 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.

c) 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).

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

e) 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 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 podle smlouvy aktivně podílet na splnění povinností uvedených v § 13 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění podle smlouvy na své straně:

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

b) Předat objednateli dokumentaci předmětu plnění podle Smlouvy nad rámec rozsahu stanoveného ve smlouvě minimálně v následujícím rozsahu:

i) dokumentaci všech bezpečnostních nastavení, funkcí a mechanismů;

ii) dokumentaci obsahující popis autorizačního konceptu a oprávnění;

iii) dokumentaci obsahující instalační a konfigurační postupy;

Výše uvedenou dokumentaci poskytovatel předá objednateli v přiměřené lhůtě, nejpozději pak podle předchozí dohody smluvních stran.

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

a) Dodržovat a implementovat obecně uznávané „nejlepší praktiky“ pro bezpečný vývoj softwaru. Základním pravidlem zde je myslet na bezpečnost softwaru ve všech jeho vývojových fázích.

b) Na vyžádání alespoň 6 pracovních dnů předem umožnit objednateli audit prováděného nebo provedeného plnění a na písemnou žádost objednatele předložit ve stanovené lhůtě 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.

c) 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.

d) 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.

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

f) 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.

g) Instalovat software pouze na základě předem schválených migračních postupů objednatelem.

h) Předat zdrojový kód objednateli bezpečnou formou zajišťující jeho integritu.

i) Zajistit řízení verzí zdrojového kódu, jeho zálohování a jeho uložení mimo produkční prostředí objednatele.

12. ZVLÁDÁNÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ A INCIDENTŮ

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

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

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

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

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

e) Spolupracovat při analýze příčin kybernetického bezpečnostního incidentu a navrhnout opatření s cílem zamezit jeho opakování v případě, že Zhotovitel kybernetický bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

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

12.2 Poskytovatel bere na vědomí, že postup zvládání kybernetického 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 podle smlouvy aktivně podílet na splnění povinností uvedených v § 15 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění podle smlouvy na své straně:

a) Zajistit adekvátní kontinuitu svých aktiv, které jsou potřebné k poskytování předmětu plnění podle smlouvy.

b) 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 podle 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:

a) 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

b) jehož předmětem bude naplnění kybernetických požadavků a vyhodnocení rizik dle bodu 4 této přílohy 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:

a) na základě provedení hodnocení rizik dle bodu 4 této přílohy smlouvy, nebo

b) v rámci auditu kybernetické bezpečnosti dle bodu 14.2 této přílohy 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:

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

b) 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.

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

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

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

a) 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.

b) V rozsahu předmětu plnění podle 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.

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

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

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

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

g) Na aktiva objednatele bez jeho písemného souhlasu neinstalovat a nepoužívat v prostředí objednatele následující typy nástrojů, pokud vysloveně nejsou součástí předmětu plnění podle 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.

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

   i) 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;

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

i) Průběžně zaznamenávat a uchovávat data o provozu zařízení ICT (provozní a lokalizační údaje) v rozsahu předmětu plnění a v souladu s požadavky platné české a evropské legislativy.

j) Na vyžádání poskytnout objednateli report obsahující výsledky monitorování veškerých uživatelských a administrátorských aktivit a jiných událostí v rozsahu předmětu plnění dle smlouvy, a to po celou dobu trvání Smlouvy a pak po dobu 2 let po jejím ukončení.

k) Zajistit sběr informací o provozních a bezpečnostních činnostech v rozsahu předmětu plnění podle smlouvy a ochranu získaných informací před jejich neoprávněným čtením nebo změnou.

l) Pro veškeré on-line transakce realizované prostřednictvím webových technologií implementovat doporučené a schválené TLS/SSL certifikáty s cílem zajistit důvěrnost a integritu komunikace protistran.

m) Veškeré neveřejné informace poskytnuté objednatelem 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 a jeho plnění realizované v prostředí objednatele mohou být monitorovány a vyhodnocovány v rozsahu předmětu plnění smlouvy a v souladu s příslušnými interními dokumenty objednatele, se kterými byl poskytovatel prokazatelně seznámen.