Zajištění servisu a podpory systému dispečerských terminálů a telefonie

- část A

Příloha č. 9

Bezpečnostní požadavky

Bezpečnostní požadavky

1. Účel přílohy

Tato příloha Smlouvy stanoví způsoby a úrovně realizace bezpečnostních opatření pro Dodavatele a určuje vzájemný vztah odpovědnosti za zavedení a kontrolu bezpečnostních opatření mezi Objednatelem a Dodavatelem. Požadavky na Dodavatele jsou definovány dle platné právní úpravy, především pak dle ustanovení § 5 odst. 2 písm. e) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „**ZKB**"), § 8 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 jen „**Vyhláška o KB**").
Další požadavky na Objednatele a Dodavatele související s ochranou osobních údajů vyplývají z 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 (obecné nařízení o ochraně osobních údajů) (dále jen „**GDPR**").

2. Obecné bezpečnostně provozní požadavky

Dodavatel se při poskytování plnění pro Objednatele zavazuje plnit následující povinnosti:

a) postupovat v souladu s právními předpisy, zejména ZKB a Vyhláškou o KB.

b) jmenovat nejpozději do 30 dnů od uzavření Smlouvy zodpovědnou kontaktní osobu pro potřeby zajištění plnění bezpečnostních požadavků vyplývajících ze Smlouvy a této přílohy a související komunikaci mezi smluvními stranami (dále také jen „**Kontaktní osoba pro bezpečnost na straně Dodavatele**[1]"). Kontaktní osobu pro bezpečnost na straně Dodavatele sdělí písemně Objednateli v téže lhůtě;

c) zajistit, aby Kontaktní osoba pro bezpečnost na straně Dodavatele bezodkladně po svém jmenování určila rozsah a popsala dotčená aktiva na straně Dodavatele potřebná pro plnění této smlouvy (aktivy se rozumí např. data a informace k předmětu plnění dle této smlouvy, systémy ICT, moduly, HW prvky - infrastruktura hlasové a datové komunikace, aplikace, databáze, servery, úložiště, koncová zařízení – pracovní stanice typu osobní počítač nebo notebook, mobilní koncová zařízení – přenosná zařízení typu telefon, tablet, notebook, netbook, PDA, apod., tato aktiva **nejsou** součástí prvků kritické informační infrastruktury), a tyto skutečnosti sdělila do **30 dnů** od uzavření Smlouvy Objednateli. Pokud při plnění předmětu Smlouvy dochází ke zpracování osobních údajů, Kontaktní osoba pro bezpečnost na straně Dodavatele se zavazuje zajistit uzavření smluv (tj. smluv se svými poddodavateli, zaměstnanci a případnými dalšími osobami podílejícími se na poskytování

[1] Pro změnu Kontaktní osoby pro bezpečnost na straně Dodavatele se užije ustanovení týkající se změny kontaktních osob Smluvních stran uvedené ve Smlouvě obdobně. Změnu Kontaktní osoby pro bezpečnost na straně Dodavatele je Dodavatel povinen Objednateli nahlásit do 5 dnů od provedení změny.

plnění smlouvy) ve smyslu příslušných ustanovení GDPR, zejména pak jeho ustanovení čl. 28 odst. 3, a souvisejících ustanovení dalších právních předpisů;

d) zajistit, aby Kontaktní osoba pro bezpečnost na straně Dodavatele nejpozději do 30 dnů od uzavření Smlouvy potvrdila písemně Objednateli, že všechny osoby podílející se na poskytování plnění této Smlouvy za stranu Dodavatele a/nebo že jeho poddodavatelé byli prokazatelně seznámeni s těmito Bezpečnostními požadavky;

e) dodržovat příslušná ustanovení bezpečnostních politik, metodik a postupů Objednatele, resp. platné řídící dokumentace Objednatele či její části, pokud byl s takovými dokumenty nebo jejich částmi seznámen, a to bez ohledu na způsob, jakým byl s takovou dokumentací Objednatele seznámen (např. školením, je-li takové školení realizováno ze strany Objednatele v této věci, protokolárním předáním příslušné dokumentace Dodavateli, elektronickým předáním prostřednictvím e-mailu, zřízením přístupu Dodavateli na sdílené úložiště, apod.);

f) realizovat plán rozvoje bezpečnostního povědomí svých zaměstnanců, kteří se podílejí na plnění realizovaném pro Dodavatele a to **nejméně jednou za tři roky** nebo **vždy v souvislosti s prováděnými nebo plánovanými změnami**. Zaměstnanci Dodavatele musí být prokazatelně seznámeni s platnými předpisy a bezpečnostními požadavky Objednatele;

g) vést **provozní deník**, do kterého zaznamenává veškeré podstatné okolnosti související s poskytovaným předmětem plnění dle Smlouvy ve smyslu bezpečnostních požadavků uvedených v tomto dokumentu (technické záznamy, organizační záznamy o školení obsluh, pověření apod.). Provozní deník Dodavatel vede v elektronické podobě a sdílí jej s Objednatelem např. prostřednictvím zabezpečené web aplikace nebo zabezpečeného datového úložiště na straně Dodavatele, do níž Dodavatel Objednateli zprostředkuje přístup, případně je sdílení zajištěno použitím Service Desku Dodavatele[2];

h) přidělovat oprávnění svým jednotlivým pracovníkům oprávnění k výkonu činností tak, aby byla minimalizována rizika nežádoucího přístupu k aktivům Objednatele;

i) garantovat dostupnost[3], důvěrnost plnění[4], integritu[5], a nepopíratelnost původu předávaných zpráv s tím, že dodávané služby musí být v souladu s uzavřeným smluvním vztahem provozně monitorovány a **1x za měsíc**, vždy **k 10 dni** následujícího měsíce vyhodnocovány. Hodnocena bude vždy **dostupnost, důvěrnost plnění a integrita**. Hodnocení bude Dodavatel předkládat Objednateli **do 20. dne** následujícího měsíce. Hodnocení předložit jako jasně označený záznam v provozním deníku;

j) průběžně **dokumentovat** (např. záznamem v provozním deníku), **kontrolovat** a **vyhodnocovat oprávněnost přístupu**, jak fyzického, tak i logického, u všech osob na straně Dodavatele, které přistupují k předmětu plnění dle této Smlouvy;

---

[2] Po dokončení Technologického SD na straně Objednatele, budou data předávána s jeho využitím.

[3] Dostupností se rozumí skutečnost, že předmět plnění je k dispozici v okamžiku jeho potřeby na straně Objednatele.

[4] Důvěrností plnění se rozumí skutečnost, že přístup k předmětu plnění mají pouze oprávněné osoby na straně Dodavatele.

[5] Integritou se rozumí skutečnost, že předmět plnění je nastaven tak, aby byla zajištěna **správnost a úplnost všech informací bezprostředně souvisejících s předmětem plnění.**

k) dodat Objednateli postup pro zálohování dat a programového vybavení (SW). Všechny zálohy prováděné Dodavatelem a zálohovací média musí být chráněny a funkčnost záloh musí být pravidelně testována odpovědnou osobou na straně Dodavatele. Postup pro zálohování dat a programového vybavení se týká prostředků a dat vztahujících se k plnění Smlouvy;

l) v případě potřeby Objednatele musí Dodavatel garantovat schopnost zrekonstruovat funkcionalitu aktiva do stavu požadovaného dle Smlouvy;

m) průběžně **detekovat** technické zranitelnosti a konfigurační nesoulady předmětu plnění Smlouvy. Detekované technické zranitelnosti musí být vyhodnoceny s ohledem na související riziko a musí podle povahy předmětu plnění dojít k nápravným opatřením ze strany Dodavatele (přijetí rizika, aplikace bezpečnostní aktualizace, implementace jiného bezpečnostního opatření – vypnutí zranitelné služby, přidání bariérové ochrany např. firewall, IPS, zvýšení úrovně monitoringu). Nápravná opatření musí být schválena Objednatelem;

n) využívat pouze oprávněných osob na straně Dodavatele, které budou provádět analýzy topologie sítě nebo skenování aktivních částí předmětu plnění;

o) **realizovat bezpečnostní opatření** pro odstranění nebo blokování síťového spojení/síťových spojení, které/která neodpovídají požadavkům na ochranu integrity komunikační sítě;

p) uchovávat data o provozu (provozní a lokalizační údaje) v souladu s požadavky platné a účinné legislativy ČR.

3. Oprávnění užívat data

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

Dodavatel se při poskytování plnění pro Objednatele zavazuje nakládat s daty (včetně osobních údajů) pouze v souladu se Smlouvou a příslušnými právními předpisy, zejména GDPR, ZKB, Vyhláškou o KB a dalšími souvisejícími právními předpisy.

4. Autorství

Dodavatel se při poskytování plnění pro Objednatele zavazuje zajistit, aby instalace aktualizací SW probíhala pouze z důvěryhodných zdrojů a v souladu s platnými smluvními podmínkami výrobce daného SW (především s ohledem na licenční podmínky a zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů);

5. Kontrola souladu s požadavky bezpečnosti

Dodavatel je srozuměn s pravidelným prováděním hodnocení rizik a kontrolou zavedených bezpečnostních opatření ze strany Objednatele v souvislosti s poskytovanou službou Dodavatelem. Hodnocení a kontrola probíhají jednou ročně nebo v případě vzniku kybernetického bezpečnostního incidentu v rámci poskytované služby nebo v případě, že se vznik bezpečnostního incidentu jeví jako pravděpodobný.

6. Řetězení dodavatelů

Dodavatel se při poskytování plnění pro Objednatele zavazuje plnit následující povinnosti:

a) pokud Dodavatel využívá při poskytování plnění poddodavatele, zavazuje se, že budou dodržovat bezpečnostní požadavky vyplývající ze Smlouvy a této přílohy. Dodavatel se zavazuje bezodkladně doložit Objednateli na základě jeho výzvy smluvní dokumenty se svými poddodavateli, ze kterých bude vyplývat závazek poddodavatelů poskytovat plnění v souladu s bezpečnostními požadavky vyplývajícími ze Smlouvy a této přílohy;
b) Dodavatel odpovídá za to, že jeho poddodavatelé nebudou jednat v rozporu s bezpečnostními požadavky vyplývajícími ze Smlouvy a této přílohy; v případě, že dojde k nedodržení těchto požadavků ze strany poddodavatele Dodavatele, považuje se každé takové nedodržení požadavků za porušení povinnosti Dodavatele dle této Smlouvy.

7. Řízení změn

Má-li v průběhu plnění Smlouvy dojít ke změně plnění nebo práv a povinností Objednatele či Dodavatele založených Smlouvou, zavazuje se Dodavatel poskytnout Objednateli veškerou nezbytnou součinnost ke splnění povinností Objednatele vyplývajících z ustanovení § 11 Vyhlášky o KB, tedy zejména při analýze souvisejících rizik, přijímání opatření za účelem snížení všech nepříznivých dopadů spojených se změnami, aktualizaci bezpečnostní dokumentace, souvisejícím testováním a zajištění možnosti navrácení do původního stavu.

8. Zvládání bezpečnostních incidentů[6]

Dodavatel se při poskytování plnění pro Objednatele zavazuje, že:

a) stanoví a popíše činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání bezpečnostních událostí a incidentů, podle takto stanovených a popsaných pravidel bude postupovat, a bude **hlásit** všechny bezpečnostní události a incidenty včetně případů porušení zabezpečení osobních údajů[7] **neprodleně kontaktní osobě Objednatele uvedené v příloze č. 6 Smlouvy**. Dále se zavazuje vyhodnotit informace o bezpečnostních událostech a incidentech včetně případů porušení zabezpečení osobních údajů a tyto informace zaznamenat a uchovat pro jejich budoucí použití s ohledem na požadavky legislativy ČR;
b) v případě vzniku bezpečnostní události a následného zvládání a vyhodnocování bezpečnostního incidentu a/nebo v případě podezření na bezpečnostní incident včetně případů porušení zabezpečení osobních údajů poskytne nezbytnou součinnost Objednateli,

[6] Pojem bezpečnostní incident a bezpečnostní událost je ekvivalentní pojmům Kybernetická bezpečnostní událost / Kybernetický bezpečnostní incident definovaných ZKB. Pro potřeby tohoto dokumentu jsou pojmy definovány takto:
Bezpečnostní událost: událost, která může způsobit narušení bezpečnosti informací, porušení bezpečnostní politiky nebo selhání bezpečnostních opatření. Může se také jednat o jinou situaci, která dříve nenastala a může být z pohledu bezpečnosti informací důležitá. Může být příčinou nebo mít vliv na vznik bezpečnostního incidentu.
Bezpečnostní incident: narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku bezpečnostní události. Za bezpečnostní incident jsou považovány také případy porušení zabezpečení osobních údajů.
[7] Pojem porušení zabezpečení osobních údajů je ekvivalentní témuž pojmu ve smyslu čl. 33 a čl. 34 GDPR.

např.: poskytne logy a identifikační údaje (např. IP adresa, MAC adresa, HW typ, sériové číslo případně IMEI) dotyčného koncového zařízení nebo mobilního koncového zařízení zaměstnance Dodavatele nebo zaměstnance poddodavatele podílející se na realizaci plnění, k analýze obsahu, případně bez zbytečného odkladu zrealizuje opatření požadovaná Objednatelem;

c) provede analýzu příčin bezpečnostního incidentu včetně případů porušení zabezpečení osobních údajů a navrhne opatření s cílem zamezit jeho opakování v případě, že Dodavatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

9. Informační povinnost Dodavatele a povinnosti Smluvních stran při výměně informací

Dodavatel se během poskytování plnění pro Objednatele zavazuje informovat kontaktní osobu Objednatele uvedenou v příloze č. 5 Smlouvy o**:**

a) způsobu řízení rizik, zbytkových rizicích souvisejících s plněním Smlouvy a bez zbytečného odkladu také o změnách ve způsobu řízení rizik;
b) významné změny ovládání Dodavatele podle zákona č. 90 /2012 Sb., o obchodních korporacích;
c) změny vlastnictví zásadních aktiv, využívaných Dodavatelem k plnění Smlouvy, a změny oprávnění nakládat s těmito aktivy.

Dodavatel se během poskytování plnění pro Objednatele zavazuje:

a) dostatečně zabezpečit veškerý přenos dat a informací z pohledu bezpečnostních požadavků na jejich důvěrnost, integritu a dostupnost;
b) případné on-line transakce realizované prostřednictvím webových technologií chránit SSL certifikáty.

10. Povinnosti při ukončení Smlouvy

Nebude-li Dodavatel s Objednatelem nadále spolupracovat v rámci sjednané služby, zavazuje se předat Objednateli, nejpozději k poslednímu dni platnosti Smlouvy, ve formátu předem odsouhlaseném Objednatelem data, provozní údaje a informace, které má k dispozici v souvislosti s plněním Smlouvy, a po předání bez zbytečného odkladu prokazatelně a bezpečně zničit ve svém digitálním prostředí jejich kopie a umožnit Objednateli dohled nad průběhem zničení kopií dat, provozních údajů a informací.

11. Specifikace podmínek pro řízení kontinuity činností

Podmínky pro řízení kontinuity činností jsou specifikovány zejména v příloze č. 1 Smlouvy.

12. Povinnost poskytnout informace na vyžádání

Dodavatel je povinen na vyžádání Objednatele bez zbytečného odkladu předat data, provozní údaje a informace ve formátu předem odsouhlaseném Objednatelem, které má k dispozici v souvislosti s plněním předmětu Smlouvy.

13. Požadavky na systémovou a provozní bezpečnostní dokumentaci

a) Nedílnou součástí poskytovaného plnění je **zdokumentování** všech **bezpečnostních nastavení**, **funkcí** a **mechanismů** formou zpracování **bezpečnostní dokumentace**. Dodavatel se v rámci poskytovaného plnění pro Objednatele zavazuje předat Objednateli dokumentaci v následujícím nebo obdobném rozsahu, dle předmětu a povahy Smlouvy:

   - dokumentaci strategie obnovy,
   - dokumentaci skutečného provedení,
   - dokumentaci obsahující popis autorizačního konceptu a oprávnění,
   - dokumentaci obsahující zálohovací a archivační postupy,
   - dokumentaci obsahující instalační a konfigurační postupy,
   - dokumentaci obsahující bezpečností nastavení související s předmětem plnění smlouvy;

   dále jen souhrnně „**Systémovou a provozní a bezpečnostní dokumentaci**";

b) Systémová a provozní bezpečnostní dokumentace uvedená výše bude Objednateli Dodavatelem předána, a to **do 60 dní** od podpisu Smlouvy, nebo na základě dohody smluvních stran, nejpozději však ke konci plnění Smlouvy nebo v příslušném rozsahu při každé provedené změně technologického nebo komunikačního systému.

14. Fyzická ochrana a bezpečnost prostředí

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

b) Dodavatel se zavazuje, že na Pracovišti neponechá volně dostupná instalační, záložní nebo archivní média ani dokumentaci k předmětu plnění dle této Smlouvy.

15. Požadavky na Řízení přístupu

a) Dodavatel bere na vědomí, že **přístup** k dispečerským terminálům a datům, informacím či zařízením souvisejícím s předmětem Smlouvy je možné povolit pouze fyzické identitě zaměstnance Dodavatele / poddodavatele Dodavatele zaevidované v registru Objednatele, a to na základě požadavku Dodavatele na přístup.

b) Dodavatel se zavazuje, že v požadavku na přístup stanoví rozsah dat/informací, služby a účely, pro které je přístup k dispečerským terminálům požadován a časový údaj o délce platnosti přístupu (např.: na dobu neurčitou / 1 rok / 1 měsíc / 1 den).

c) Dodavatel bere na vědomí, že přidělení oprávnění zaměstnanci Dodavatel musí být řízeno principem nezbytného minima a není nárokové.

d) Dodavatel se zavazuje, že udělený přístup nesmí být sdílen více zaměstnanci Dodavatele nebo poddodavatele Dodavatele.

e) Dodavatel se zavazuje, že přístup prostřednictvím mobilní aplikace bude vždy uskutečněn pouze prostřednictvím zabezpečeného připojení VPN dle pokynů Objednatele.

f) Dodavatel se zavazuje, že před připojením koncového zařízení, mobilního koncového zařízení nebo aktivního síťového prvku jako síťové switche, WiFi access pointy, routery či huby do počítačové sítě zažádá o schválení připojení Objednatele.

g) Dodavatel se zavazuje, že bez zbytečného odkladu deaktivuje všechny nevyužívané zakončení sítě anebo nepoužívané porty aktivního síťového prvku.

h) Dodavatel se zavazuje, že nebude instalovat a používat tyto typy nástrojů:

- Keylogger - software nebo hardware, který neautorizovaně zaznamenává stisky kláves s cílem narušit důvěrnost zadávaných dat a informací. Softwarová verze je považována za škodlivý kód (malware), hardwarová verze se zapojuje mezi počítač a klávesnici;
- Sniffer[8] - SW nebo HW prostředek umožňující odposlouchávání síťového provozu, který je přijímán/odesílán;
- Analyzátor zranitelností – (scanner zranitelností) softwarový nebo hardwarový nástroj umožňující vyhledávání zranitelností systémů ICT, detekování dostupných síťových služeb běžících procesů, běžících aplikací a jejich verzí a Port Scanner,
- Backdoor – skrytý softwarový nebo hardwarový nástroj, který umožňuje obejití schválených autentizačních procedur. Je instalován s cílem budoucího snadnějšího a neautorizovaného přístupu do systému ICT, rootkit (tj. program umožňující maskovat přítomnost zákeřného softwaru v počítačovém systému. Dokáže tak před uživatelem skrýt vybrané běžící procesy, soubory na disku, či další systémové údaje) a trojský kůň (tj. program, který plní na první pohled užitečnou funkci, ale obsahuje zároveň skrytou škodlivou funkci (např. odesílání důvěrných dat na neautorizovaný cílový systém ICT). Trojský kůň se sám nereplikuje, šíří se díky viditelně užitné funkci, kterou poskytuje. Jedná se o program spadající do kategorie škodlivých kódů nebo jinou podobu malware (tj. program, např. počítačové viry, trojské koně, červy, špionážní software, který má za účel vykonat nějakou škodlivou činnost. Jednotlivé typy škodlivý kódů se liší svými vlastnostmi, svým cílem i metodou jakou se šíří a vykonává svou úlohu).

i) Dodavatel se zavazuje, že všechny ICT systémy Dodavatele, které se připojují do síťové infrastruktury Objednatele, jsou a budou chráněny proti malware.

j) Dodavatel se zavazuje, že nebude vyvíjet, kompilovat a šířit v jakékoliv části technologického nebo komunikačního systému programový kód, který má za cíl nelegální ovládnutí, narušení, nebo diskreditaci technologického nebo komunikačního systému nebo nelegální získání dat a informací.

k) Dodavatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednateli na zařízených určených pro poskytování plnění:

- nenavštěvovaly internetové stránky s eticky nevhodným obsahem[9];

[8] Použití snifferu je ve výjimečných, předem schválených situacích možné povolit a to pouze se souhlasem, součinností a přítomnosti Objednatele, pouze k jednorázovému časově omezenému použití a garantovaného vypnutí a likvidace získaných dat o čemž Dodavatel provede záznam v provozním deníku. Využití je možné při nasazování systému pro kontrolu provozu.

- neukládaly a/nebo nesdílely data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno Objednatele;
- nestahovaly, nesdílely, neukládaly, nearchivovaly a/nebo neinstalovaly datové a spustitelné soubory v rozporu s licenčními podmínkami nebo autorským zákonem;
- neukládaly a/nebo nesdílely data a informace Objednatele na nepovolených datových úložištích nebo médiích;
- nezasílaly řetězové emaily.

l) Dodavatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednateli, kteří přistupují do interní sítě a/nebo technologického nebo komunikačního systému, respektovaly a dodržovaly následující omezení:

- Zařízení typu notebook/počítač musí mít:
  - aplikovány bezpečnostní záplaty (operačního systému, internetového prohlížeče a Javy)
  - nainstalovanou, spuštěnou a aktualizovanou antivirovou ochranu.

m) Dodavatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednateli, kteří přistupují do interní sítě a/nebo technologického nebo komunikačního systému chránily autentizační prostředky a údaje k systémům Objednatele. Dodavatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet zablokován a řešen jako bezpečnostní incident ve smyslu příslušné řídící dokumentace a mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu (např. okamžité zrušení přístupu k informačním aktivům fyzických osob externího subjektu platí pro Dodavatele, pokud byl s takovou řídící dokumentací Objednatele seznámen).

n) Dodavatel bere na vědomí, že postup zvládání bezpečnostního incidentu či skutečnost vzniklá v důsledku porušení Bezpečnostních požadavků nebude posuzován jako okolnost vylučující odpovědnost Dodavatele za prodlení s řádným a včasným plněním předmětu Smlouvy a nebude důvodem k jakékoli náhradě případné újmy Dodavateli či jiné osobě ze strany Objednatele. Ostatní ustanovení ohledně odpovědnosti Dodavatele za prodlení obsažená v Smlouvě nejsou tímto ustanovením dotčena.

16. Monitorování činností

a) Dodavatel bere na vědomí, že veškerá aktivita Dodavatele a jeho plnění realizované v rámci plnění předmětu Smlouvy nebo s ním úzce související budou Objednatelem průběžně a pravidelně monitorovány a vyhodnocovány s ohledem na obsah Smlouvy a interních dokumentů Objednatele, se kterými byl Dodavatel seznámen.

b) Dodavatel se zavazuje, že záznamy/logy obsahující výsledky monitorování, úspěšná a neúspěšná přihlášení do ICT systému a záznamy o správě uživatelů prováděná na straně

[9] Data a informace obsahující prvky extrémismu, terorismu, pornografie anebo podněcování k nesnášenlivosti a společenským předsudkům vztahujícím se ke společenské skupině identifikované na základě rasy, náboženství nebo víry, pohlaví, sexuální orientace, národnostní a etnické příslušnosti či jiné odlišnosti.

Dodavatel je povinen na vyžádání a bez zbytečného odkladu předložit Objednateli, a to po celou dobu trvání Smlouvy i o jejím ukončení.

17. Likvidace dat

Dodavatel se zavazuje plnit požadavky interní legislativy Objednatele v oblasti likvidace dat (ať už dat na papírových médiích, dat zpracovávaných elektronicky nebo prostřednictvím jakýchkoli dalších nosičů dat).

18. Technické bezpečnostní požadavky na hardwarové prvky

a) Aktivní síťové prvky musí z důvodu plnění požadavků na bezpečnost plnit minimálně tato technická kritéria (dle jejich relevantnosti) a kompatibilitu se stávajícími systémy Objednatele:
   - podpora logování a odesílání logů na log server (SIEM);
   - podpora protokolu SNMP (Simple Network Management Protocol);
   - u zařízení typu router a FW podpora protokolu pro monitorování síťového provozu na základě IP toků (např. NetFlow, sFlow);
   - podpora mechanismu AAA (autentizace, autorizace, účtování);
   - podpora autentizace a autorizace za využití RADIUS a TACACS+, LDAP, AD;
   - podpora autentizace za využití certifikátu;
   - podpora zabezpečení za využití hesla nebo jiného autentizačního mechanismu při přístupu prostřednictvím konzolové linky;
   - u zařízení typu router a FW podpora využití a konfigurace VPN;
   - podpora SSH nebo HTTPS pro realizaci zabezpečení vzdáleného přístupu;
   - podpora využití port-security;
   - podpora VLAN;
   - u zařízení typu router a FW podpora ACL;
   - podpora nastavení úrovně uživatelských práv (privilege level);
   - podpora využívání zabezpečených verzí protokolů (HTTPS, SSH, IPSec, Secure Shell Protocol apod.);
   - podpora zakázat nebo nezapínat nepoužívané služby;
   - zajištění podpory v oblasti hardeningu a upgrade ze strany výrobce minimálně po dobu životnosti zařízení.

b) Koncová pracovní stanice a severy musí z důvodu plnění požadavků na bezpečnost plnit minimálně tato technická kritéria (dle jejich relevantnosti):
   - podpora standardizovaných operačních systémů, pro které jsou pravidelně vydávány bezpečnostní patche a mají zajištěnu technickou podporou;
   - podpora víceuživatelského přístupu;
   - podpora lokální autentizace uživatelů s využitím uživatelského účtu a hesla;
   - podpora autentizace a autorizace uživatelů s využitím integrace do provozovaného systému adresářových služeb LDAP Objednatele;
   - podpora logování událostí a odesílání logů na log server (SIEM);
   - podpora skupinových bezpečnostních politik kompatibilních se systémy Objednatele;
   - podpora vzdálené správy s možností ovládání vzdáleného počítače v modelu klient-server prostřednictvím připojení k jeho desktopovému prostředí (např. RDP);

- zajištění podpory v oblasti hardeningu a upgrade ze strany výrobce minimálně po dobu životnosti zařízení.