POŽADAVKY OBJEDNATELE V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

1 ÚVODNÍ USTANOVENÍ

1.1 Z důvodu nutnosti plnění povinností stanovených Objednateli jakožto povinné osobě ve smyslu Vyhlášky o kybernetické bezpečnosti je Dodavatel povinen nad rámec povinností stanovených Smlouvou plnit níže uvedené povinnosti zejm. součinnostního a bezpečnostního charakteru dle této Přílohy Smlouvy. Účelem této Přílohy Smlouvy tak je dodržet povinnost Objednatele dle § 4 odst. 4 ZKB zahrnout požadavky vyplývající z bezpečnostních opatření do smluvního ujednání s Dodavatelem.

1.2 Dodavatel 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 dle předpisů z oblasti kybernetické bezpečnosti, a to i v případě změny příslušné právní úpravy. V takovém případě je Objednatel oprávněn požadovat od Dodavatele přiměřenou součinnost i nad rámec povinností stanovených v této Příloze Smlouvy, avšak vždy pouze za účelem zajištění plnění povinnosti Dodavatele z oblasti kybernetické bezpečnosti ve smyslu shora uvedeného.

2 SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

2.1 Dodavatel je povinen se v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 3 Vyhlášky o kybernetické bezpečnosti, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění dle Smlouvy na své straně:

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

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

2.1.3 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.

2.2 Dodavatel je dále povinen dodržovat Politiku bezpečnosti informací Objednatele (byl-li s ní prokazatelně seznámen) nebo ustanovení o odsouhlasených bezpečnostních politik dodavatele nebo jejich relevantních částí.

2.3 Dodavatel je povinen v rámci plnění smluvního vztahu zajistit ochranu dat z pohledu důvěrnosti, dostupnosti a integrity, která zahrnuje zejména zabezpečení ochrany před neoprávněným manipulováním s technologickým celkem informačního systému, ochranu před neoprávněnou manipulací s daty, ochranu informací před krádeží (nelegální tvorba kopií dat) nebo poškozením, bezpečnou komunikaci a přenos dat (kryptografie), bezpečné uložení dat, dostupnost, celistvost a nepodvrhnutelnost dat.

3 ŘÍZENÍ AKTIV

3.1 Dodavatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 4 Vyhlášky o kybernetické bezpečnosti, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění dle Smlouvy na své straně:

3.1.1 Stanovit a udržovat rozsah a seznam aktiv využívaných ve smyslu předmětu a důvěrnosti, dostupnosti a integrity 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 – přenosná zařízení typu telefon, tablet, notebook, netbook, PDA, apod.), a tato aktiva strukturovaně popsat a na základě požadavku Objednateli předložit ke kontrole.

4 ŘÍZENÍ RIZIK

4.1 Dodavatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 5 Vyhlášky o kybernetické bezpečnosti, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění dle Smlouvy na své straně:

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

4.1.2 Formální evidenci rizik v rámci tohoto smluvního vztahu bude zajišťovat vždy zástupce Objednatele tak, aby bylo možné identifikovaná rizika řídit v souladu s interními principy řízení rizik a rizika následně evidovat v nástroji pro řízení rizik dle metodických postupů Objednatele.

5 ORGANIZAČNÍ BEZPEČNOST

5.1 Dodavatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 6 Vyhlášky o kybernetické bezpečnosti, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění dle Smlouvy na své straně:

5.1.1 Jmenovat nejpozději do třiceti (30) Dnů po uzavření Smlouvy odpovědnou kontaktní osobu pro potřeby zajištění plnění požadavků kybernetické bezpečnosti. Kontaktní osobu pro kybernetickou bezpečnost sdělí Dodavatel písemně Objednateli v téže lhůtě.

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

6 ŘÍZENÍ DODAVATELŮ

6.1 Dodavatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 8 Vyhlášky o kybernetické bezpečnosti, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění dle Smlouvy na své straně:

6.1.1 Využívá-li při poskytování předmětu plnění dle Smlouvy Poddodavatele, zajistit v obdobném rozsahu dodržování Kybernetických požadavků rovněž ve smluvních vztazích se svými Poddodavateli.

6.1.2 Dodržovat podmínky pro zapojení Dalšího zpracovatele při zpracování Osobních údajů.

7 BEZPEČNOST LIDSKÝCH ZDROJŮ

7.1 Dodavatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 9 Vyhlášky o kybernetické bezpečnosti, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění dle Smlouvy na své straně:

7.1.1 Zajistit, aby Kontaktní osoba pro kybernetickou bezpečnost nejpozději do šedesáti (60) Dnů od uzavření Smlouvy potvrdila písemně Objednateli, že všechny osoby podílející se na poskytování předmětu plnění dle Smlouvy za Dodavatele byly prokazatelně seznámeny s těmito Kybernetickými požadavky a příslušnými ustanoveními interních předpisů Objednatele, existují-li takové a byl-li s nimi Provozovatel prokazatelně seznámen.

7.1.2 Dodržovat příslušná ustanovení interních předpisů Objednatele v rozsahu, v jakém byl s těmito akty seznámen. Za prokazatelné seznámení se považuje školení pracovníků Dodavatel zajištěné Objednatelem, protokolární či elektronické předání příslušné dokumentace nebo Objednatelem zajištěný přístup na sdílené úložiště obsahující příslušné interní akty řízení.

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

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

7.3 Dodavatel je dále povinen:

7.3.1 Prohlubovat znalostí osob podílejících se na poskytování plnění Objednateli v oblasti bezpečnosti informací.

7.3.2 Stanovit práva a povinnosti osob podílejících se na poskytování plnění Objednateli v oblasti bezpečnosti informací.

8 ŘÍZENÍ PROVOZU A KOMUNIKACÍ

8.1 Dodavatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 10 Vyhlášky kybernetické bezpečnosti, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění dle Smlouvy na své straně:

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

8.1.2 Zajistit, že pro poskytování předmětu plnění dle Smlouvy budou využívány pouze aplikace a technologie, které jsou v souladu s platnou českou a evropskou legislativou, především s ohledem na licenční podmínky a předpisy upravující ochranu duševního vlastnictví.

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

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

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

8.2.3 Zavedení pravidel a postupů pro ochranu informací a dat.

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

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

9 ŘÍZENÍ ZMĚN

9.1 Dodavatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 11 Vyhlášky o kybernetické bezpečnosti, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění dle Smlouvy na své straně:

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

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

10 ŘÍZENÍ PŘÍSTUPU

10.1 Dodavatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 12 Vyhlášky kybernetické bezpečnosti, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění dle Smlouvy na své straně:

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

10.1.2 Zajistit, aby udělený přístup nebyl sdílen více osobami za stranu Dodavatele. V takovém případě musí Dodavatel 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 šest (6) Pracovních dnů, ledaže bude příslušným orgánem veřejné moci požadováno jinak.

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

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

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

10.2 Dodavatel bere na vědomí, že přístup k systému ICT Objednatele je možné povolit pouze fyzické identitě zaměstnance Dodavatele/Poddodavatele, a to na základě požadavku Dodavatele na přístup.

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

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

10.5 Dodavatel je dále povinen omezit přidělování administrátorských oprávnění.

11 AKVIZICE, VÝVOJ A ÚDRŽBA

11.1 Dodavatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 13 Vyhlášky o kybernetické bezpečnosti, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění dle Smlouvy na své straně:

11.1.1 Zajistit bezpečnou implementaci, inovaci, aktualizaci a testování technologií, které jsou předmětem plnění dle Smlouvy.

11.1.2 Předat Objednateli dokumentaci předmětu plnění dle Smlouvy nad rámec rozsahu stanoveného ve Smlouvě minimálně v následujícím rozsahu:

a) dokumentaci všech bezpečnostních nastavení, funkcí a mechanismů;
b) dokumentaci obsahující popis autorizačního konceptu a oprávnění;
c) dokumentaci obsahující instalační a konfigurační postupy.

Výše uvedenou dokumentaci, není-li již zahrnuta v Dokumentaci, Dodavatel předá Objednateli na vyžádání v přiměřené lhůtě dle dohody Smluvních stran.

12 ZVLÁDÁNÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ A INCIDENTŮ

12.1 Dodavatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 14 Vyhlášky o kybernetické bezpečnosti, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění dle Smlouvy na své straně:

12.1.1 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.

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

12.1.3 V případě vzniku kybernetické bezpečnostní události a následného zvládání a vyhodnocování kybernetického bezpečnostního incidentu a/nebo v případě podezření na kybernetický bezpečnostní incident poskytnout Objednateli aktivní součinnost a relevantní informace o podezřelém zařízení či osobě na straně Dodavatele.

12.1.4 Bez zbytečného odkladu a po dohodě s Objednatelem realizovat opatření požadovaná Objednatelem v dohodnutých termínech ke snížení dopadu kybernetického bezpečnostního incidentu nebo zamezení pokračování kybernetického bezpečnostního incidentu.

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

12.2 Dodavatel bere na vědomí, že postup zvládání kybernetického bezpečnostního incidentu či jiný důsledek porušení Kybernetických požadavků, jehož příčina je na straně Dodavatele, 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 ve Smlouvě nejsou tímto ustanovením dotčena.

13 ŘÍZENÍ KONTINUITY ČINNOSTÍ

13.1 Dodavatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 15 Vyhlášky o kybernetické bezpečnosti, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění dle Smlouvy na své straně:

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

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

13.1.3 Dodavatel na základě požadavku Objednatele doloží výsledky testování havarijních plánů kontinuity činností.

14 KONTROLA A AUDIT

14.1 Dodavatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 8 a § 16 Vyhlášky o kybernetické bezpečnosti, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění dle Smlouvy poskytnout adekvátní součinnost při výkonu kontroly Objednatele ze strany Národního úřadu pro kybernetickou a informační bezpečnost dle § 23 ZKB.

14.2 Dodavatel umožní Objednateli alespoň jednou ročně po dobu účinnosti Smlouvy a pak jeden (1) rok po ukončení Smlouvy provedení auditu kybernetické bezpečnosti u Dodavatele a jeho Poddodavatelů:

14.2.1 jehož rozsah bude ohraničen využíváním ICT prostředků Dodavatele pro potřeby plnění Smlouvy a uloženými či zpracovávanými daty a informacemi Objednatele v ICT prostředí Dodavatele a

14.2.2 jehož předmětem bude naplnění Kybernetických požadavků a vyhodnocení rizik dle bodu 4 této Přílohy Smlouvy.

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

14.4 Dodavatel umožní Objednateli audit kybernetické bezpečnosti provedený prostředky Objednatele nebo třetí strany, a to v lokalitě Dodavatele i vzdáleně, pokud to technické prostředky Dodavatele umožňují.

14.5 Dodavatel je povinen odstranit nedostatky zjištěné:

14.5.1 na základě provedení hodnocení rizik dle bodu 4 v této Příloze Smlouvy; nebo

14.5.2 v rámci auditu kybernetické bezpečnosti dle bodu 14.2 této Přílohy Smlouvy;

14.5.3 odstranit ve lhůtě určené v písemném oznámení Objednatele, která nebude kratší než dvacet (20) Pracovních dnů. Nestanoví-li Objednatel lhůtu v písemném oznámení, zavazují se Smluvní strany dohodnout na lhůtě pro odstranění nedostatku, která nepřevýší devadesát (90) Dnů.

14.6 Dodavatel je dále povinen:

14.6.1 Poskytnout na vyžádání Objednateli dokumenty a obdobné vstupy, které budou prokazovat naplnění Kybernetických požadavků.

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

14.6.3 Neprodleně informovat Objednatele o všech významných změnách v naplnění Kybernetických požadavků, které nastanou kdykoli v průběhu trvání této Smlouvy.

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

14.6.5 Při výkonu své činnosti včas a prokazatelně upozornit Objednatele na zřejmou nevhodnost jeho příkazů či doporučení vztahující se ke Kybernetickým požadavkům, jejichž následkem může vzniknout újma nebo nesoulad se zákony nebo jinými obecně závaznými právními předpisy.

14.6.6 Dodavatel umožní dle § 16 VoKB Zadavateli jako Povinné osobě audit kybernetické bezpečnosti za předpokladu, že Zadavatel bude audit provádět pouze jednou za dvanáct měsíců v rozsahu max. 3 hodin, pokud ZKB nevyžaduje častější audity. Zadavatel předá Dodavateli termín auditu minimálně 2 kalendářní týdny předem.

15 TECHNICKÁ OPATŘENÍ

15.1 Dodavatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 17 až § 27 Vyhlášky o kybernetické bezpečnosti, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění dle Smlouvy na své straně:

15.1.1 Dodržovat interní předpisy Objednatele, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěny aktiva systémů ICT Objednatele, anebo datové nosiče.

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

15.1.3 Realizovat opatření pro odstranění nebo blokování síťového spojení/síťových spojení, které/která neodpovídají požadavkům na ochranu integrity a bezpečnosti komunikační sítě.

15.1.4 Realizovat přístup z mobilního zařízení do prostředí Objednatele pouze prostřednictvím zabezpečeného připojení virtuální privátní sítě (VPN).

15.1.5 Připojovat do prostředí Objednatele pouze ta síťová zařízení (switch, přístupový bod wifi, router, hub apod.), která prošla schvalovacím procesem, a jejich připojení bylo schváleno oprávněnou osobou ve věcech technických na straně Objednatele.

15.1.6 Bez zbytečného odkladu deaktivovat všechna nevyužívaná zakončení sítě anebo nepoužívané porty aktivního síťového prvku, který je v rozsahu předmětu plnění dle Smlouvy a je ve správě Dodavatele.

15.1.7 Připojovat do prostředí Objednatele pouze zařízení ICT, která jsou chráněna proti malware a jinému škodlivému softwaru a která jsou v souladu s interními předpisy Objednatele.

15.1.8 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.

15.1.9 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 jednoho (1) roku po jejím ukončení.

15.1.10 Zajistit sběr informací o provozních a bezpečnostních činnostech v rozsahu předmětu plnění dle Smlouvy a ochranu získaných informací před jejich neoprávněným čtením nebo změnou.

15.1.11 Veškeré neveřejné informace poskytnuté Objednatelem chránit vhodným šifrováním a proti neautorizovanému přístupu.

15.2 Dodavatel bere na vědomí, že veškeré aktivity Dodavatele a jeho plnění realizované v prostředí Objednatele jsou monitorovány a vyhodnocovány v rozsahu předměty plnění a v souladu s interními dokumenty Objednatele, se kterými byl Dodavatel seznámen.

16 DALŠÍ POVINNOSTI SMLUVNÍCH STRAN V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

16.1 S ohledem na to, že Dodavatel je významným dodavatelem ve smyslu § 2 písm. n) a § 8 odst. 1 písm. f) a odst. 2 Vyhlášky o kybernetické bezpečnosti, je Objednatel povinen po uzavření smluvního vztahu s Dodavatelem do 30 dnů zpřístupnit Dodavateli relevantní interní bezpečnostní předpisy Objednatele.

16.2 Písemný výstup poskytování Služeb bude vždy předán v listinné podobě a v elektronické podobě v editovatelném datovém formátu (MS Office), případně po vzájemné dohodě ve formátu PDF. Elektronická komunikace bude vedena elektronickou poštou nebo v aplikaci MS Teams, OneDrive případně cestou sdíleného úložiště Objednatele.

16.3 Dodavatel se zavazuje zejména poskytovat Služby v obvyklé kvalitě tak, aby požadavky Objednatele byly uspokojovány v souladu se Smlouvou s obecně závaznými právními předpisy uvedenými ve smlouvě nebo jasně se vztahující k předmětu smlouvy a poskytované službě.

16.4 Dodavatel je povinen být certifikován dle normy ISO/IEC 27001:2014 *Information security management systems* (v platném znění) po dobu trvání smluvního vztahu.