ŘEDITELSTVÍ SILNIC A DÁLNIC

PŘÍLOHA Č. 6

PRAVIDLA KYBERNETICKÉ BEZPEČNOSTI

I. OBECNÁ USTANOVENÍ

1.1 Tato příloha (dále jen „**Příloha**“) tvoří nedílnou součást Smlouvy (dále jen „**Smlouva**“).

1.2 Není-li dále stanoveno jinak nebo nevyplývá-li jinak z kontextu, mají pojmy počínající velkým písmenem v této Příloze shodný význam, jaký mají ve Smlouvě. Výjimkou je označení Prodávajícího, který má význam dle čl. 1.3.2 Přílohy.

1.3 Smluvní strany nad rámec Smlouvy vymezují následující pojmy:

1.3.1 **Data** znamenají data, záznamy, soubory, obsah, osobní údaje a další informace Objednatele, (a) shromážděné, přijaté nebo uchovávané Dodavatelem v souvislosti s plněním Smlouvy; (b) poskytnuté Objednatelem; nebo (c) odvozené z (a) a (b). Data podle této smlouvy jsou klasifikována jako důvěrné informace, nebo se z jiných důvodů jedná o údaje vyžadující ochranu před neoprávněným přístupem, únikem, porušením nebo jiným odhalením.

1.3.2 **Dodavatel** znamená Prodávající dle Smlouvy;

1.3.3 **ZOK** znamená zákon č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů;

1.3.4 **Kybernetické požadavky** znamenají interní dokument Objednatele Všeobecná bezpečnostní pravidla pro dodavatele z pohledu kybernetické bezpečnosti.

1.4 Rozsah zapojení Dodavatele na rozvoji a provozu primárních a podpůrných aktiv Objednatele je určen předmětem Smlouvy a jejími přílohami včetně této Přílohy. Rozsah zapojení Dodavatele na zajištění bezpečnosti těchto aktiv je určen zejména touto Přílohou a Kybernetickými požadavky.

II. BEZPEČNOST INFORMACÍ

2.1 Dodavatel se zavazuje při nakládání s Daty chránit jejich důvěrnost, dostupnost a integritu s ohledem na jejich povahu a klasifikaci v souladu se standardním bezpečnostním rámcem jako je např. ISO 27001, NIST Cyber Security Framework nebo SSAE 18 SOC 2.

2.2 Dodavatel je povinen zavést vhodná opatření pro ochranu Dat alespoň v rozsahu této přílohy.

2.3 Dodavatel jmenuje odpovědnou kontaktní osobu pro potřeby zajištění plnění požadavků podle této Přílohy a Smlouvy v oblasti kybernetické bezpečnosti a související komunikace s Objednatelem. Dodavatel je povinen oznámit kontaktní údaje této osoby Objednateli do 10 dnů od účinnosti Smlouvy.

III. UŽITÍ DAT

3.1 Dodavatel je oprávněn používat nebo sdílet Data Objednatele pouze pro účely a způsobem, který stanoví Smlouva a její přílohy, a v souladu s příslušnými právními předpisy, tj. zejména ZKB a VKB, po dobu trvání Smlouvy a po jejím ukončení, dokud má Dodavatel ve své dispozici Data Objednatele.

3.2 Dodavatel bere na vědomí, že veškerá Data zůstávají předmětem výhradních práv Objednatele, který je jediným vlastníkem Dat a pořizovatelem databází, ve kterých jsou Data uložena.

3.3 Dodavatel se zavazuje zachovávat mlčenlivost o Datech a jejich obsahu.

3.4 Dodavatel je povinen omezit přístup k Datům Objednatele pouze na ty zaměstnance a třetí strany, u kterých přístup vyžaduje plnění Smlouvy nebo plnění zákonných povinností. Dodavatel nesmí umožnit přístup k Datům Objednatele jiným třetím stranám bez předcházejícího písemného souhlasu Objednatele. Vysloví-li Objednatel ve Smlouvě nebo jinak písemně souhlas se zapojením konkrétního poddodavatele do plnění Smlouvy, uděluje tím souhlas se zpřístupněním Dat Objednatele poddodavateli v rozsahu nezbytném pro plnění Smlouvy.

3.5 V případě, že Objednatel při hodnocení rizik spojených s touto Smlouvou identifikuje skutečnosti, jejichž existence tvoří podstatnou kybernetickou hrozbu a riziko pro předmět této Smlouvy a tyto dosahují kritické úrovně dle VKB, může Objednatel Dodavateli uložit přijetí dalších bezpečnostních opatření ve smyslu ZKB bez nutnosti přijetí dodatku Smlouvy ve smyslu § 100 odst. 1 ZZVZ. Objednatel při naplnění podmínek výše předá Dodavateli popis vybraných bezpečnostních opatření, která navrhuje ke snížení identifikovaného rizika zavést. Dodavatel je povinen bezodkladně zavést požadovaná bezpečnostní opatření a jejich zavedení oznámit Objednateli. Dodavatel je oprávněn do 3 pracovních dní podat připomínky k formě zvolených bezpečnostních opatření a navrhnout jinou formu zvolených bezpečnostních opatření, kterou je povinen zavést bezodkladně, po jejich schválení Objednatelem, a jejich zavedení Objednateli oznámit.

3.6 V případě, že cizozemský orgán požádá o zpřístupnění nebo předání Dat zpracovávaných na území cizího státu, Objednatel takové žádosti vyhoví

a) až po provedení přezkoumání zákonnosti žádosti,

b) až po vynaložení úsilí o zabránění zpřístupnění nebo předání dat v rámci možností daných právním řádem, v jehož působnosti dochází ke zpracování dat nebo podle kterého byla žádost podána,

c) pouze v nezbytném rozsahu.

IV. BEZPEČNOSTNÍ DOKUMENTACE

4.1 Dodavatel se v souvislosti s řízením kybernetické bezpečnosti zavazuje vypracovat a udržovat příslušnou bezpečnostní dokumentaci.

4.2 Dodavatel je povinen bezpečnostní dokumentaci podle této Přílohy pravidelně revidovat a případně aktualizovat, nejméně 1x ročně, a kdykoli při významné změně a materiální změně skutečností zachycených v bezpečnostní dokumentaci.

V. ŘÍZENÍ AKTIV

5.1 Dodavatel se zavazuje minimálně:

5.1.1 identifikovat primární a podpůrná aktiva využívaná pro plnění Smlouvy;

5.1.2 určit vazby mezi primárními a podpůrnými aktivy a případně určit vazby na současná aktiva Objednatele;

5.1.3 tento seznam aktiv a jejich vazby udržovat aktuální.

VI. ŘÍZENÍ RIZIK

6.1 Dodavatel se zavazuje minimálně:

6.1.1 řídit bezpečnostní rizika, která mohou ovlivnit poskytování předmětu plnění Smlouvy, v souladu s minimálními požadavky na řízení rizik upravenými v ZKB a VKB;

6.1.2 informovat Objednatele o způsobu řízení rizik a předložit Objednateli zprávu o hodnocení aktiv a rizik, která jsou využívána pro plnění Smlouvy a o zbytkových rizicích souvisejících s aktivy využívanými pro plnění Smlouvy do 30 dnů od data účinnosti Smlouvy a následně v intervalu jednou za dva roky nebo v případě významné změny ovlivňující bezpečnost těchto aktiv;

6.1.3 provést přepočet dopadu aktuálních kybernetických rizik v souvislosti s novými hrozbami spojenými s předmětem plnění dle Smlouvy;

6.1.4 provést hodnocení rizik, které bude zohledňovat přepočet dle čl. 6.1.3 této Přílohy, toto hodnocení strukturovaně popsat a Objednateli předložit do třiceti (30) dnů od provedení;

6.1.5 reagovat na změny na a upravit na své straně bezpečnostní opatření tak, aby odpovídala novému stavu po provedení změny.

VII. BEZPEČNOST LIDSKÝCH ZDROJŮ

7.1 Dodavatel se zavazuje minimálně:

7.1.1 prověřit každého pracovníka před umožněním přístupu k aktivům Objednatele nebo před jeho zapojením do činností, které by mohly ovlivnit předmět plnění Smlouvy, a to alespoň z hlediska:

a) kontroly dosaženého vzdělání a odborné kvalifikace;

b) ověření bezpečnostní způsobilosti dle výpisu z rejstříku trestů;

c) profesních zkušeností, jde-li o pracovníky, kteří mají zastávat bezpečnostní nebo administrátorské role.

7.1.2 zavést pravidelné školení svých pracovníků v oblasti kybernetické bezpečnosti a základní kybernetické hygieny a vést o tomto školení spolehlivou evidenci;

7.1.3 poučit své pracovníky o požadavcích dle této přílohy před umožněním jejich přístupu k Datům nebo před jejich zapojením do činností, které by mohly ovlivnit bezpečnost v souvislosti s předmětem plnění Smlouvy;

7.1.4 realizovat alespoň 1x ročně další doplňující aktivity rozvoje povědomí v oblasti kybernetické bezpečnosti, a vést o realizovaných aktivitách evidenci;

7.1.5 zajistit, aby pracovníci před umožněním jejich přístupu k Datům nebo před zapojením do činností, které by mohly ovlivnit bezpečnost předmětu plnění Smlouvy, měli uzavřenou dohodu o zachování mlčenlivosti (důvěrnosti) Dat s adekvátní dobou trvání povinnosti mlčenlivosti;

7.1.6 zajistit procesy a pravidla vedení disciplinárního řízení (zejména odstupňované reakce) a v případě potřeby provádět disciplinární řízení k přijetí opatření vůči pracovníkům, kteří porušili povinnosti v oblasti kybernetické bezpečnosti;

7.1.7 zajistit dostatečnou míru zastupitelnosti pro technické bezpečnostní aspekty plnění smlouvy.

VIII. ŘÍZENÍ PROVOZU

8.1 Dodavatel se zavazuje minimálně:

8.1.1 stanovit práva a povinnosti administrátorů, uživatelů a osob zastávajících bezpečnostní role;

8.1.2 stanovit pravidla a postupy pro ochranu před škodlivým kódem;

8.1.3 stanovit pravidla a postupy pro řízení technických zranitelností;

8.1.4 stanovit pravidla a postupy k provádění pravidelného zálohování a kontroly použitelnosti prováděných záloh;

8.1.5 stanovit pravidla pro zajištění oddělení vývojového, testovacího a provozního prostředí.

IX. ŘÍZENÍ ZMĚN

9.1 Dodavatel se zavazuje minimálně:

9.1.1 sledovat a identifikovat změny, které mají nebo mohou mít vliv na zajištění kybernetické bezpečnosti Dat Objednatele a informovat Objednatele o této skutečnosti;

9.1.2 poskytnout Objednateli veškeré potřebné informace a součinnost v procesu řízení a evidence změn. Informace musí být poskytnuty v rozsahu, který Objednateli umožní:

a) posoudit, zda změna ve vztahu k plnění dle Smlouvy je významnou změnou;

b) posoudit rizika související s významnou změnou ve vztahu k plnění dle Smlouvy, testovat změnu před nasazením do provozu a posoudit možnost případného navrácení do původního stavu;

c) přijmout přiměřená opatření ke zvládání rizik souvisejících s touto změnou, nebo změnu vůbec neprovést, pokud nelze přijmout opatření snižující tato rizika na akceptovatelnou úroveň;

d) dokumentovat posouzení rizik souvisejících s významnou změnou ve vztahu k plnění dle Smlouvy a přijatá opatření; a

e) provést další činnosti u významných změn dle VKB.

9.1.3 reagovat na změny, zejména aktualizovat hodnocení rizik, bezpečnostní a provozní dokumentaci a upravit na své straně bezpečnostní opatření tak, aby odpovídala novému stavu po provedení změny.

X. ŘÍZENÍ KONTINUITY ČINNOSTÍ

10.1 Dodavatel se v rozsahu předmětu plnění dle Smlouvy zavazuje zavést a udržovat vhodná opatření pro zajištění kontinuity činností vč. opatření blíže stanovených v Kybernetických požadavcích. Zejména se Dodavatel zavazuje:

10.1.1 ve spolupráci s Objednatelem určit aktiva potřebná k poskytování plnění dle Smlouvy, zpracovat a poskytnout Objednateli plány kontinuity a havarijní plány v souvislosti s těmito aktivy, a případně tyto plány upravit dle požadavků Objednatele;

10.1.2 zajistit adekvátní kontinuitu aktiv, která jsou potřebná k poskytování plnění dle Smlouvy; a

10.1.3 pravidelně kontrolovat a testovat, že je schopen zajistit kontinuitu aktiv při dodržení sjednané úrovně plnění dle Smlouvy.

10.2 Dodavatel se zavazuje poskytnout nezbytnou součinnost při zpracování a testování plánů kontinuity a havarijních plánů a plnění dalších povinností Objednatele.

XI. AKVIZICE, VÝVOJ A ÚDRŽBA

11.1 Dodavatel se zavazuje minimálně:

11.1.1 zajistit, aby bezpečnost informací byla zahrnuta do všech vývojových, implementačních či akvizičních projektů, kde je reálné narušení informační bezpečnosti Dat a ochrany soukromí, a vyčlenit pro tento účel potřebné zdroje;

11.1.2 zajistit oddělení vývojového, testovacího a provozního prostředí.

XII. ŘÍZENÍ PŘÍSTUPU

12.1 Dodavatel se zavazuje minimálně:

12.1.1 provozovat ke zpracování Dat pouze taková aktiva, která umožňují správu rolí a uživatelů a která neumožní činnost uživatelů bez autentizace a zároveň umožňují ochranu autentizačního mechanismu před neoprávněným přístupem a prolomením autentizačních parametrů;

12.1.2 zajistit, aby uživatelské účty byly adekvátně chráněny prostřednictvím autentizačních mechanismů;

12.1.3 zajistit, aby uživatelé chránili své uživatelské účty, zejména své autentizační údaje a nástroje a aby neposkytli tyto údaje třetí straně;

12.1.4 udělovat přístup pracovníkům podle zásady need-to-know a průběžně kontrolovat a vyhodnocovat oprávněnost a potřebu přístupu,

12.1.5 v případě potřeby bezodkladně odebrat přístupová oprávnění, zejména pokud

a) zaměstnanec již nepotřebuje přístup k plnění svých pracovních povinností (např. pokud došlo ke změně pozice zaměstnance),

b) zaměstnanec se dopustil závažného porušení povinností v oblasti kybernetické bezpečnosti nebo existují důvodné obavy, že se takového porušení dopustí,

c) zaměstnanec nesplňuje požadavky na přístup k Datům nebo požadavky na zapojení do činností, které by mohly ovlivnit bezpečnost předmětu plnění Smlouvy,

d) se ukáže potřeba přijmout mimořádné bezpečností opatření spočívající v odebrání přístupu (zejména pokud Dodavatel dal zaměstnanci výpověď z výpovědního důvodu podle § 52 písm. f), g) a h) zákoníku práce),

e) byl ukončen pracovní poměr (nebyl-li přístup odebrán dříve),

f) došlo k úniku autentizačních údajů (hesla).

12.1.6 vést evidenci o udělených a odebraných přístupových oprávněních.

XIII. ZVLÁDÁNÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ A INCIDENTŮ

13.1 Dodavatel se zavazuje minimálně:

13.1.1 zajistit, aby jeho pracovníci a dodavatelé oznamovali neobvyklé chování technických aktiv a podezření na jakékoliv zranitelnosti a hrozby;

13.1.2 vést a uchovávat záznamy o kybernetických bezpečnostních incidentech a o jejich zvládání;

13.1.3 prošetřit a určit příčiny kybernetického bezpečnostního incidentu;

13.1.4 poskytnout Objednateli aktivní součinnost a relevantní informace o příčinách, podezřelém zařízení či osobě na straně Dodavatele v případě kybernetického bezpečnostního incidentu souvisejícího s Daty;

13.1.5 navrhnout a realizovat bezpečnostní opatření dle požadavků Objednatele v dohodnutých termínech pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu nebo hrozby.

XIV. FYZICKÁ BEZPEČNOST

14.1 Dodavatel se zavazuje minimálně:

14.1.1 zajistit dodržování politiky čistého stolu;

14.1.2 zajistit kanceláře, pracovní místnosti a prostory v případě jejich opuštění tak, aby nemohlo dojít k nedovolenému vstupu neoprávněných osob;

14.1.3 zajistit uzamykání pracovních stolů, skříní, kontrolovat uzavření oken;

14.1.4 zajistit dodržování režimových opatřeních v případě režimových pracovišť (perimetr s řízeným vstupem).

14.2 Dodavatel bere na vědomí, že Objednatel vede evidenci osob, které vstupují do neveřejných částí objektů Objednatele, a evidenci vozidel, která vjíždějí do objektů Objednatele.

XV. BEZPEČNOST KOMUNIKAČNÍCH SÍTÍ

15.1 Dodavatel se zavazuje minimálně:

15.1.1 zajistit vhodnou segmentaci komunikační sítě,

15.1.2 zajistit, aby komunikační síť byla chráněna bezpečným rozhraním, přičemž bude povolena pouze nutná komunikace;

15.1.3 zajistit, aby na síťových zařízeních byly spuštěny pouze nutné služby;

15.1.4 zajistit, aby byly sledovány zranitelnosti nasazených síťových zařízení a aby byly odstraňovány zjištěné zranitelnosti v dostatečných intervalech;

15.1.5 zajistit, aby přenos informací a dat v rámci komunikační sítě byl šifrován.

XVI. SPRÁVA A OVĚŘOVÁNÍ IDENTIT

16.1 Dodavatel se zavazuje minimálně:

16.1.1 používat nástroj pro správu a ověření identity (autentizační mechanismus), který přenáší a ukládá autentizační parametry v šifrované podobě;

16.1.2 používat autentizační mechanismus, který je založený na více faktorové autentizaci s nejméně dvěma různými typy faktorů, pokud je to možné;

16.1.3 v případě ztráty, vyzrazení nebo podezření na kompromitaci autentizačních nástrojů nebo parametrů je třeba okamžitě změnit parametry autentizace;

16.1.4 aktiva, která nepodporují více faktorovou autentizaci, mohou dočasně zajistit autentizaci pomocí podobně silných kryptografických klíčů nebo hesel.

16.1.5 pokud je autentizace založena na heslech a nevyužívá se více faktorové autentizace, musí systém vynucovat hesla s vlastnostmi podle aktuální nejlepší praxe.

XVII. OCHRANA PŘED ŠKODLIVÝM KÓDEM

17.1 Dodavatel se zavazuje minimálně:

17.1.1 zajistit použití nástroje pro nepřetržitou automatickou ochranu koncových zařízení;

17.1.2 monitorovat a řídit používání výměnných zařízení a datových nosičů a řídit jejich automatické spouštění;

17.1.3 provádět pravidelnou a účinnou aktualizaci nástroje pro ochranu před škodlivým kódem.

XVIII. DETEKCE, ZAZNAMENÁVÁNÍ A VYHODNOCOVÁNÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ

18.1 Dodavatel se zavazuje minimálně:

18.1.1 zajistit, aby všechny klíčové prvky propojující významné uzly interních komunikačních sítí, bezpečnostní síťové prvky a všechny prvky na vnějším perimetru měly aktivní monitorování kybernetických bezpečnostních událostí;

18.1.2 zajistit, aby monitorování sítě zajišťovalo ověření a kontrolu přenášených dat v rámci komunikační sítě a mezi komunikačními sítěmi, ověření a kontrolu přenášených dat na perimetru komunikační sítě;

18.1.3 zajistit, aby v interních sítích byl provozován IDS/IPS.

18.1.4 zajistit, aby detekovaná nežádoucí komunikace byla automaticky blokována;

18.1.5 zajistit, aby byly zaznamenávány kybernetické bezpečnostní události narušující integritu síťových prvků nebo síťové komunikace, aby tyto záznamy byly uchovány a poskytnuty Objednateli na vyžádání;

18.1.6 nasadit nástroje typu SIEM pro počáteční posouzení, zda zachycené události představují bezpečnostní událost nebo incident, přičemž tyto nástroje budou schopné rozdělit a zpracovat událost nebo řetězec událostí alespoň do 3 kategorií:

a) pozitivní – událost nebo sled událostí jednoznačně představuje bezpečnostní událost nebo bezpečnostní incident;

b) negativní – událost nebo sled událostí jednoznačně nepředstavuje bezpečnostní událost;

c) nejasný (falešně pozitivní / falešně negativní) – událost nebo sled událostí může v určitém kontextu představovat bezpečnostní událost nebo incident, ale v době hodnocení není možné událost jednoznačně klasifikovat, přičemž tyto události jsou dále hlášeny a hodnoceny pomocí jiných technik a nástrojů, případně ručně.

18.1.7 zajistit, aby primární reakcí byla eskalace bezpečnostní události nebo incidentu do příslušných hlášení, případně přímá eskalace na příslušné odpovědné pracovníky.

XIX. APLIKAČNÍ BEZPEČNOST

19.1 Dodavatel se zavazuje minimálně:

19.1.1 užívat technická aktiva, která jsou podporována;

19.1.2 sledovat dostupnost opravných balíčků nebo záplat a zajistit bezodkladnou bezpečnostní aktualizaci;

19.1.3 pokud není bezpečnostní aktualizace dostupná, zajistit jiné kompenzační řešení, případně zranitelnost může být akceptována.

XX. KRYPTOGRAFICKÉ ALGORITMY

20.1 Dodavatel se zavazuje minimálně:

20.1.1 používat pouze aktuálně doporučované a odolné kryptografické algoritmy a kryptografické klíče podle nejlepší praxe.

XXI. KONTROLA A AUDIT

21.1 Objednatel je oprávněn, na základě předchozí výzvy ze strany Objednatele doručené v přiměřeném časovém předstihu, provést kontrolu a audit údajů, účtů, záznamů, pracovních postupů, dokumentace, aktiv, prostor (včetně kontroly fyzického perimetru) a technických prostředků vztahujících se k plnění Smlouvy a této Přílohy, a to za účelem ověření plnění povinností vyplývajících ze Smlouvy, jejích příloh a této Přílohy (dále jen "**Audit**").

21.2 Audit bude prováděn dle potřeb Objednatele a pak mimořádně v případech bezpečnostních událostí, důvodného podezření na nedostatečnou úroveň ochrany aktiv Objednatele, důvodného podezření na nakládání s aktivy v rozporu s relevantními ustanoveními Smlouvy a důvodného podezření na nedodržení bezpečnostních opatření podle této Přílohy.

21.3 Audit bude prováděn Objednatelem nebo jím pověřenou třetí stranou smluvně zavázanou k mlčenlivosti minimálně v rozsahu odpovídajícím povinnostem mlčenlivosti Objednatele dle Smlouvy, a která není k Dodavateli v soutěžním nebo jiném konkurenčním postavení.

21.4 Dodavatel poskytne veškerou nezbytnou součinnost k řádnému provedení a dokončení Auditu, zejména umožní přístup k údajům, účtům, záznamům, pracovním postupům, dokumentaci, jiným dokladům či podkladům, k aktivům, do prostor (včetně kontroly fyzického perimetru) a k technickým prostředkům vztahujícím se k plnění Smlouvy a této Přílohy za účelem uskutečnění Auditu. Dodavatel zajistí součinnost kvalifikovaných pracovníků.

21.5 Jakákoliv data, informace nebo jiná aktiva získaná při Auditu mohou být použita výhradně pro účely Auditu, vyhodnocení jeho výsledků a přijetí navazujících opatření, a další potřeby Objednatele při řízení vztahu s Dodavatelem.

21.6 Dodavatel je povinen bez zbytečného odkladu, nejpozději však do 1 měsíce od ukončení auditu, předložit Objednateli návrhy opatření napravujících nedostatky zjištěné při Auditu. Jednotlivá opatření navržená v návaznosti na výsledky Auditu podléhají před jejich přijetím Dodavatelem předchozímu schválení ze strany Objednatele. Návrhy zřejmě nevhodných či neúčinných opatření Objednatel odmítne a Dodavatel je povinen v přiměřené lhůtě stanovené Objednatelem navrhnout jiná vhodná opatření. Dodavatel je taktéž povinen se na výzvu Objednatele podrobit dodatečné kontrole ze strany Objednatele nebo osoby, která Audit provedla, za účelem ověření nápravy nedostatků zjištěných při Auditu a kontroly přijatých opatření.

XXII. PODDODAVATELÉ A JEJICH ŘETĚZENÍ

22.1 Dodavatel se zavazuje, že pravidla dle této Přílohy budou dodržovat i poddodavatelé Dodavatele a jejich pracovníci podílející se na plnění Smlouvy. Dodavatel Objednateli doloží, že u poddodavatelů smluvně vyžaduje dodržování pravidel dle této Přílohy, a to poskytnutím příslušné smlouvy do 10 dnů od jejího uzavření.

22.2 Dodavatel se zavazuje soustavně (případně pravidelně dle povahy) dohlížet na plnění této Přílohy ze strany jeho poddodavatelů a jejich zaměstnanců.

22.3 Za porušení pravidel dle této Přílohy poddodavatelem odpovídá Dodavatel Objednateli tak, jako by je porušil sám. Dodavatel odpovídá za zajištění dostatečné znalosti pravidel dle této Přílohy, ze strany svých dodavatelů a jejich zaměstnanců.

22.4 Dodavatel je oprávněn využít k plnění dle Smlouvy poddodavatele jen v případě, že to Smlouva nebo její přílohy výslovně připouští, a to za podmínek v ní uvedených. Nestanoví-li Smlouva nebo její přílohy jinak, podléhají jednotliví poddodavatelé předchozímu písemnému schválení ze strany Objednatele.

XXIII. KYBERNETICKÉ POŽADAVKY

23.1 Dodavatel se seznámil před podpisem Smlouvy s dokumentem Kybernetické požadavky.

23.2 Dodavatel se Kybernetické požadavky zavazuje dodržovat a seznámit s nimi své pracovníky podílející se na poskytování plnění dle Smlouvy.

23.3 V případě změny Kybernetických požadavků se Objednatel zavazuje aktuální znění bez zbytečného odkladu od provedení změny předat Dodavateli. Objednatel zašle Dodavateli aktuální znění způsobem pro doručování dle Smlouvy nebo do datové schránky. Dodavatel se zavazuje v přiměřené lhůtě a ne později, než 10 pracovních dnů od předání Kybernetických požadavků protokolárně Objednateli potvrdit, že se s aktuálním zněním Kybernetických požadavků seznámil, že se je zavazuje dodržovat a že s nimi seznámil své pracovníky podílející se na poskytování plnění dle smlouvy.

XXIV. INFORMAČNÍ POVINNOST DODAVATELE

24.1 Dodavatel je povinen Objednatele bez zbytečného odkladu informovat o identifikovaných kybernetických bezpečnostních incidentech a hrozbách souvisejících s plněním Smlouvy a/nebo s Daty, nejpozději však do 24 hodin od jejich výskytu.

24.2 Dodavatel je povinen poskytnout Objednateli veškerou součinnost nutnou ke splnění povinností Objednatele v oblasti řízení rizik, zejména při:

24.2.1 identifikaci aktiv v rámci předmětu plnění Smlouvy a jejich kategorizaci, hodnocení a zařazení do bezpečnostních úrovní;

24.2.2 identifikaci, analýze a hodnocení rizik pro aktiva dle odst. 24.2.1;

24.2.3 ošetření rizik včetně zpracování prohlášení o aplikovatelnosti a plánu zvládání rizik pro aktiva dle odst.24.2.1;

přičemž je Dodavatel povinen postupovat podle Kybernetických požadavků, nebo pokud Kybernetické požadavky tuto oblast neupracují, pak podle zavedených postupů v odvětví.

24.3 Dodavatel je povinen Objednatele informovat o:

24.3.1 významné změně ovládání Dodavatele, přičemž ovládáním se rozumí vliv, ovládání či řízení dle § 71 a násl. ZOK či ekvivalentní postavení, a to do 20 pracovních dnů od uskutečnění této změny; a

24.3.2 o změně vlastnictví či oprávnění nakládat se Zásadními aktivy využívanými Dodavatelem k plnění Smlouvy, a to do 20 pracovních dnů od uskutečnění této změny,

přičemž k informování využije Dodavatel nástroj Objednatele specifikovaný v Kybernetických požadavcích či jiný prostředek dle písemného pokynu Objednatele.

24.4 Dodavatel je povinen poskytnout Objednateli a příslušným dozorovým orgánům veškerou nutnou součinnost v případě dozorového auditu za účelem ověření řízení kybernetické bezpečnosti.

24.5 Učiní-li orgány činné v trestním řízení nebo jiné orgány státní správy jakoukoli právně závaznou žádost o poskytnutí Dat Objednatele směrem k Dodavateli, je Dodavatel povinen tuto skutečnost oznámit Objednateli s předstihem před poskytnutím takových informací, pokud mu to právní předpisy nezakazují.

24.6 Dodavatel je povinen Objednatele informovat o žádosti cizozemského orgánu o zpřístupnění nebo předání Dat zpracovávaných na území cizího státu, vyjma situace, kdy by takové informování bylo v rozporu s právním řádem, v jehož působnosti dochází ke zpracování dat nebo podle kterého byla žádost podána.

XXV. PŘEDÁNÍ A LIKVIDACE DAT

25.1 Dodavatel se zavazuje na základě výzvy Objednatele bez zbytečného odkladu předat Objednateli bezpečným způsobem, ve strojově čitelné podobě a ve formátu zaručujícím kompatibilitu v procesu migrace jakákoli Data v dispoziční sféře Dodavatele. Dodavatel se k výzvě Objednatele zavazuje poskytnout nezbytnou součinnost, přičemž si Smluvní strany mohou písemně dohodnout jiný způsob předání Dat. Dodavatel je povinen i bez výzvy Objednatele předat Objednateli Data do 7 dnů po skončení účinnosti Smlouvy.

25.2 Smluvní strany při ukončení Smlouvy z jakéhokoli důvodu vyvinou veškeré úsilí k tomu, aby do doby dokončení migrace Dat či převodu plnění dle Smlouvy k Objednateli nebo jinému provozovateli, nedošlo k narušení parametrů plnění ve Smlouvě do té doby definovaných, a aby případný nový provozovatel dostal veškeré informace o plnění Smlouvy potřebné pro pokračování nebo nahrazení takového plnění.

25.3 Součástí plnění dle odst. 25.2 je i povinnost Dodavatele provádět činnosti spočívajících v přípravě a předání předmětu plnění Smlouvy novému dodavateli Objednatele, poskytování součinnosti, dokumentace a informací novému dodavateli. Za účelem poskytování součinnosti při ukončení se Dodavatel zavazuje do 30 dnů od obdržení výzvy Objednatele vypracovat dle a na základě pokynů Objednatele plán vymezující veškeré podmínky pro převedení služeb či jejich příslušné části na nového dodavatele.

25.4 Dodavatel se zavazuje do 30 dnů od obdržení výzvy Objednatele předat Objednateli:

25.4.1 aktualizovanou dokumentaci, kterou vytvořil nebo spravuje;

25.4.2 úplný a aktuální zdrojový kód tam, kde je to s ohledem na plnění Smlouvy smysluplné;

25.4.3 seznam platných administrátorských účtů využívaných v prostředí Objednatele;

25.4.4 úplnou knowledge base týkající se poskytování služeb, pokud bylo předmětem poskytování průběžně poskytovaných služeb, vč. popisu a seznamu uzavřených a neuzavřených servisních požadavků;

25.4.5 aktuální seznam standardních provozních úkonů pro údržbu aktiv Objednatele.

25.5 Dodavatel se zavazuje při ukončení účinnosti Smlouvy, případně na písemnou žádost Objednatele, bez zbytečného odkladu po předání Dat, nejpozději však do 14 dnů, zlikvidovat Data v souladu s Kybernetickými požadavky za podpůrného užití VKB, to vše za možného dozoru zástupce Objednatele.

25.6 V případě, že má Dodavatel na svých nosičích Data vysoké či kritické úrovně dle VKB (úroveň Chráněné ve smyslu Kybernetických požadavků), má povinnost tato Data ve lhůtě podle odst. 25.5 zlikvidovat protokolárně.

XXVI. ZÁVĚREČNÁ UJEDNÁNÍ

26.1 Smluvní strany se zavazují postupovat v souladu s relevantními obecně závaznými právními předpisy.

26.2 Dodavatel se zavazuje přenést na jakéhokoli poddodavatele, který bude schválen Objednatelem, ujednání k zajištění kybernetické bezpečnosti uvedené ve Smlouvě a v této příloze v celém jejich rozsahu a tato ujednání nebudou v rozporu s požadavky uvedenými ve Smlouvě a v této příloze.

26.3 Dodavatel se zavazuje při výkonu své činnosti včas a prokazatelně upozornit Objednatele na zřejmou nevhodnost jeho příkazů či doporučení vztahujících se k pravidlům bezpečnosti, jejichž následkem může vzniknout újma nebo nesoulad s právními předpisy a zajistit ve spolupráci s Objednatelem náhradní způsob naplnění pravidel bezpečnosti, pokud stávající řešení přestalo být funkční nebo efektivní.

26.4 Pokud není ve Smlouvě nebo v této Příloze uvedeno jinak, odměna za provádění povinností a opatření dle této Přílohy a Kybernetických požadavků je součástí odměny dle Smlouvy.

[redacted]

[redacted]

[redacted]