PŘÍLOHA Č. 6 – POŽADAVKY NA ZAJIŠTĚNÍ KYBERNETICKÉ BEZPEČNOSTI (KYBERNETICKÉ POŽADAVKY)

Za účelem plnění povinností stanovených v Smlouvě, případně Objednateli, jakožto povinné osobě v oblasti kybernetické bezpečnosti, je Poskytovatel povinen, nad rámec povinností stanovených v těle Smlouvy, plnit níže uvedené povinnosti zejm. součinnostního a bezpečnostního charakteru dle této Přílohy.

Poskytovatel je povinen plnit relevantní povinnosti v rozsahu a způsobem tak, aby byl naplněn účel relevantní 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 vždy 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, avšak vždy pouze za účelem zajištění plnění povinnosti Poskytovatele z oblasti kybernetické bezpečnosti ve smyslu shora uvedeného.

Čl. 1 Systém řízení bezpečnosti informací

1. Poskytovatel se bude v rozsahu předmětu plnění této Smlouvy aktivně podílet na splnění zákonných povinností, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:
    a. Prosadit bezpečnostní zásady a procesy, které budou pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně Poskytovatele při poskytování Plnění dle Smlouvy a Dílčích smluv.
    b. Na základě bezpečnostních potřeb a výsledků hodnocení rizik zavést příslušná bezpečnostní opatření v rozsahu poskytovaného Plnění dle Smlouvy a Dílčích smluv, monitorovat je, vyhodnocovat jejich účinnost.
    c. Vést záznamy o vytváření a zpracování dat a informací v rozsahu poskytovaní Plnění dle Smlouvy a Dílčích smluv, 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 Plnění dle Smlouvy a Dílčích smluv. Bezpečnostní politika musí obsahovat hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací.
    e. Stanovit a udržovat aktuální opatření bezpečnosti ve formě procesů a technologií, které zajišťují naplnění bezpečnostní politiky.
    f. Poskytovatel je dále povinen dodržovat bezpečnostní politiku Objednatele, byl-li s ní seznámen.

Čl. 2 Řízení aktiv

1. Poskytovatel se bude v rozsahu předmětu plnění této Smlouvy aktivně podílet na splnění zákonných povinností, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:
    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 – přenosná zařízení typu telefon, tablet, notebook, netbook, PDA, apod.), a tato aktiva strukturovaně popsat a Objednateli předložit do třicet (30) dnů od nabytí účinnosti této Smlouvy a následně na vyžádání, a to po celou dobu trvání Smlouvy a po dobou dvou (2) let po jejím ukončení.

Čl. 3 Řízení rizik

1. Poskytovatel se bude v rozsahu předmětu plnění této Smlouvy aktivně podílet na splnění zákonných povinností, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:
    a. Řídit vlastní rizika, která mohou ovlivnit poskytování Plnění dle Smlouvy a Dílčích smluv.
    b. V minimálním intervalu 1x ročně vytvořit a předložit Objednateli zprávu o řízení kybernetických 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 těmito Kybernetickými požadavky

Čl. 4 Organizační bezpečnost

1. Poskytovatel se bude v rozsahu předmětu plnění této Smlouvy aktivně podílet na splnění zákonných povinností, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:
    a. Jmenovat nejpozději do pěti (5) dnů po uzavření této Smlouvy odpovědnou kontaktní osobu pro potřeby zajištění plnění těchto Kybernetických požadavků a související komunikaci mezi Stranami (dále také jen „**Kontaktní osoba KB**“). Kontaktní osobu KB sdělí Poskytovatel písemně Objednateli v téže lhůtě. Objednatel stanovuje, že určení Kontaktní osoby KB pro bezpečnost na straně Poskytovatele nemá dopad na ustanovení Smlouvy týkající se odpovědných osob ve věcech smluvních a technických.

b. Využívat pro poskytování předmětu plnění pouze oprávněných osob, které byly řádně seznámeny s příslušnými ustanoveními interních řídících aktů Objednatele a mají ověřenou kvalifikaci, znalosti a zkušenosti k řádnému poskytování předmětu plnění.

Čl. 5 Řízení dodavatelů

1. Poskytovatel se bude v rozsahu předmětu plnění této Smlouvy aktivně podílet na splnění zákonných povinností, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:
   a. Využívá-li při poskytování Plnění poddodavatele, zabezpečit adekvátní dodržování Kybernetických požadavků rovněž ve smluvních vztazích se svými poddodavateli, přičemž tuto skutečnost se Poskytovatel zavazuje doložit Objednateli do deseti (10) dnů od uzavření Dílčí smlouvy, na jejímž plnění se budou poddodavatelé podílet v případě Služeb na objednávku nebo do deseti (10) dnů od počátku poskytování jiného Plnění, písemným prohlášením o dodržování Kybernetických požadavků u svých poddodavatelů.
   b. Pokud při poskytování předmětu plnění dochází ke zpracování Osobních údajů, zabezpečit nad rámec Smlouvy uzavření samostatných smluv (tj. smluv se svými poddodavateli, zaměstnanci a případnými dalšími osobami podílejícími se na poskytování plnění z této Smlouvy) ve smyslu příslušných ustanovení Nařízení.

Čl. 6 Bezpečnost lidských zdrojů

1. Poskytovatel se bude v rozsahu předmětu plnění této Smlouvy aktivně podílet na splnění zákonných povinností, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:
   a. zabezpečit, aby Kontaktní osoba KB nejpozději do třiceti (30) dnů od uzavření Smlouvy potvrdila písemně Objednateli, že všechny osoby podílející se na poskytování Plnění za stranu Poskytovatele byly prokazatelně seznámeny s těmito Kybernetickými požadavky a příslušnými ustanoveními interních řídících aktů Objednatele.
   b. Dodržovat příslušná ustanovení interních řídících aktů Objednatele v rozsahu, v jakém byl s těmito akty seznámen. Za prokazatelné seznámení se považuje školení pracovníků Poskytovatel zajištěné Objednatelem, protokolární či elektronické předání příslušné dokumentace nebo Objednatelem zajištěný přístup na sdílené úložiště obsahující příslušné interní akty řízení.
   c. V případě, že je součástí předmětu plnění služba dohledu nad předmětem plnění, definovat a naplnit role a odpovědnosti pro monitoring sítě a zařízení v rozsahu předmětu plnění.
   d. Zabezpečit, aby osoby podílející se na poskytování Plnění Objednateli v prostředí nebo s prostředky Objednatele, a to i tehdy, pokud jsou prostředky Objednatele používány mimo jeho prostředí:

i. Pro uložení a sdíleni dat a informací Objednatele využívaly pouze k tomu schválené prostředky (aktiva) a schválené způsoby komunikace;

ii. Neukládaly ani nesdílely data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující 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;

viii. Dodržovaly obecně závazné právní předpisy.

2. Poskytovatel si je vědom, že součástí podmínek pro získání přístupu ke zdrojům a aktivům Objednatele je na straně Objednatele zpracování Osobních údajů pracovníků Poskytovatele, kteří se podílejí na zajištění předmětu plnění. Pokud nebude Objednateli umožněno Osobní údaje dotčených pracovníků Poskytovatele v rámci plnění Smlouvy zpracovat, nebude těmto pracovníkům umožněn žádný přístup ke zdrojům Objednatele.

Čl. 7 Řízení provozu a komunikací

1. Poskytovatel se bude v rozsahu předmětu plnění této Smlouvy aktivně podílet na splnění zákonných povinností, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:

   a. Zabezpečit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování Plnění.

   b. Na vyžádání poskytnout Objednateli přehled, report, či jinou adekvátní informaci o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře.

   c. Zabezpečit, že pro poskytování Plnění 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.

Čl. 8 Řízení změn

1. Poskytovatel se bude v rozsahu předmětu plnění této Smlouvy aktivně podílet na splnění zákonných povinností, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:

a. Přiměřeně reagovat na změny 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.

Čl. 9 Řízení přístupu

1. Poskytovatel se bude v rozsahu předmětu plnění této Smlouvy aktivně podílet na splnění zákonných povinností, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:
   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, pokud sdílený přístup nevyžaduje využívaná technologie. V takovém případě musí Poskytovatel vést evidenci využívání sdílených přístupů a tuto na vyžádání předložit Objednateli kdykoli v průběhu trvání této Smlouvy a dva (2) roky po jejím ukončení.
   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 / 1 den).
   d. Zabezpečit, aby osoby podílející se na poskytování Plnění 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.
2. Poskytovatel bere na vědomí, že přístup k systému ICT je možné povolit pouze fyzické identitě zaměstnance Poskytovatele / poddodavatele Poskytovatele, a to na základě požadavku Poskytovatele na přístup.
3. Poskytovatel bere na vědomí, že přidělení oprávnění přístupu musí být řízeno principem nezbytného minima a není nárokové.
4. Poskytovatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele (osoby za stranu Poskytovatele) 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).

Čl. 10 Akvizice, vývoj a údržba

1. Poskytovatel se bude v rozsahu předmětu plnění této Smlouvy aktivně podílet na splnění zákonných povinností, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:

a. Zabezpečit bezpečnou implementaci, inovaci, aktualizaci a testování technologií, které jsou předmětem plnění Smlouvy, ledaže tyto činnosti provádí Objednatel.

b. Předat Objednateli dokumentaci 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.

2. V případě, že poskytované Plnění dle Smlouvy a Dílčích smluv zahrnují vývoj softwaru, zavazuje se Poskytovatel:

   a. Dodržovat a implementovat nejlepší praktiky pro bezpečný vývoj softwaru definované na základě smluvního vztahu.

   b. Na vyžádání umožnit Objednateli provedení auditu prováděného nebo provedeného plnění, předložit Objednateli vyvíjený zdrojový kód software a výstupy z provedeného codereview (automatizovaně prostřednictvím bezpečnostního nástroje i manuálně), po jeho dokončení, pokud není v této Smlouvě stanoveno jinak, a to zejména za účelem ověření skutečnosti, zda Poskytovatel postupuje či postupoval při poskytování plnění v souladu se Smlouvou a těmito Kybernetickými požadavky.

   c. Poskytovat Objednateli v termínech stanovených Objednatelem, resp. bez zbytečného odkladu požadovanou součinnost na provedení bezpečnostního testování v průběhu vývoje softwaru či kdykoli po jeho předání.

   d. Zabezpečit, že plnění této Smlouvy bude obsahovat jen ty součásti, které jsou objektivně potřebné pro řádné provozování softwaru anebo které jsou specifikovány výslovně ve Smlouvě (zejména, že software nebude obsahovat žádné nepotřebné komponenty, žádné programové vzorky apod.).

   e. Pokud je součástí plnění této 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 prostředí Objednatele.

   f. Zabezpečit bezpečnost testovacího prostředí u Poskytovatele a ochranu poskytnutých testovacích dat Objednatelem.

   g. Zabezpečit, že do produkčního prostředí Objednatele bude dodán jen předmětem Smlouvy specifikovaný kompilovaný, respektive spustitelný zdrojový kód a další nezbytná data pro provozování předmětu plnění této Smlouvy.

   h. Zabezpečit, 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 (platí pro Poskytovatele, pokud byl s takovými bezpečnostními politikami seznámen)

   i. Instalovat software pouze na základě Objednatelem předem schválených migračních postupů.

j. Předat zdrojový kód Objednateli bezpečnou formou zajišťující jeho integritu.

k. Zabezpečit řízení verzí zdrojového kódu.

l. Zabezpečit zálohování zdrojového kódu a jeho uložení mimo produkční prostředí.

m. Zabezpečit, aby distribuce zdrojových kódů obsahovala soubor z vývojového prostředí na řízenou kompilaci těchto zdrojových kódů.

n. Nevyvíjet, nekompilovat a nešířit v prostředí Objednatele zdrojový kód, který má za cíl nelegální ovládnutí, narušení dostupnosti, důvěrnosti nebo integrity nebo neautorizované či nelegální získání dat a informací.

Čl. 11 Zvládání kybernetických bezpečnostních událostí a incidentů

1. Poskytovatel se bude v rozsahu předmětu plnění této Smlouvy aktivně podílet na splnění zákonných povinností, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:

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

   b. Bez zbytečného odkladu hlásit Objednateli (nejpozději do 12 hodin od zjištění) všechny bezpečnostní události a incidenty s potenciálním negativním dopadem na Objednatele, neobvyklé chování technických aktiv a podezření na zranitelnosti, a to stanoveným komunikačním kanálem nebo prostřednictvím Kontaktní osoby.

   c. Bez zbytečného odkladu (nejpozději do 12 hodin po zjištění) hlásit Objednateli všechny kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty dle ZKB na straně Poskytovatele souvisejících s plněním dle Smlouvy, které by mohly mít dopad na kybernetickou bezpečnost u Objednatele nebo potenciální negativní dopad na Objednatele, a to stanoveným komunikačním kanálem nebo prostřednictvím kontaktní osoby pro kybernetickou bezpečnost.

   d. Poskytnout Objednateli veškerou součinnost v rámci hlášení kybernetických bezpečnostních incidentů, včetně součinnosti při vypracování dokumentů a zpráv dle § 16 ZKB.

   e. Vyhodnocovat informace o bezpečnostních incidentech a uchovávat je pro budoucí použití s ohledem na požadavky platné české a evropské legislativy.

   f. V případě vzniku bezpečnostní události a následného zvládání a vyhodnocování bezpečnostního incidentu anebo v případě podezření na bezpečnostní incident poskytnout Objednateli aktivní součinnost a relevantní informace o podezřelém zařízení či osobě na straně Poskytovatele.

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

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

2. Poskytovatel bere na vědomí, že postup zvládání bezpečnostního incidentu či jiný důsledek porušení Kybernetických požadavků, jehož příčina je na straně Poskytovatele, nebude posuzován jako okolnost vylučující povinnost k náhradě újmy 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.

Čl. 12 Řízení kontinuity činností

1. Poskytovatel se bude v rozsahu předmětu plnění této Smlouvy aktivně podílet na splnění zákonných povinností, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:
    a. Dodržovat požadavky Objednatele na řízení kontinuity činností (zejména plány kontinuity činností a plány obnovy).
    b. Zajistit adekvátní kontinuitu svých aktiv, které jsou potřebné k poskytování Plnění.
    c. Pravidelně kontrolovat a testovat, že je schopen kontinuitu aktiv zajistit dle sjednané úrovně služeb.

Čl. 13 Kontrola a audit

1. Poskytovatel se bude v rozsahu předmětu plnění Smlouvy aktivně podílet na splnění zákonných povinností, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění poskytnout adekvátní součinnost při výkonu kontroly Objednatele ze strany Národního úřadu pro kybernetickou a informační bezpečnost dle příslušných právních předpisů.

Čl. 14 Fyzická bezpečnost

1. Poskytovatel se bude v rozsahu předmětu plnění této Smlouvy aktivně podílet na splnění zákonných povinností, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:
    a. Dodržovat provozní řády budov (režimová opatření) a využívaných prostor, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěny aktiva systémů ICT, anebo datové nosiče.
    b. V rozsahu poskytování Plnění 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.

Čl. 15 Bezpečnostní nástroje

1. Poskytovatel se bude v rozsahu předmětu plnění této Smlouvy aktivně podílet na splnění zákonných povinností, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:
    a. Realizovat bezpečnostní opatření pro odstranění nebo blokování síťového spojení/síťových spojení, které/která neodpovídají požadavkům na ochranu integrity komunikační sítě.
    b. Realizovat přístup z mobilního zařízení do prostředí Objednatele pouze prostřednictvím zabezpečeného připojení virtuální privátní sítě (VPN) nebo zvolit adekvátní technické opatření.
    c. 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 osobu ve věcech technických na straně Objednatele určenou v této Smlouvě.
    d. Bez zbytečného odkladu deaktivovat všechna nevyužívaná zakončení sítě anebo nepoužívané porty aktivního síťového prvku, který je v rozsahu předmětu plnění a je ve správě Poskytovatele.
    e. Na aktiva Objednatele neinstalovat a nepoužívat v prostředí Objednatele tyto typy nástrojů, pokud nejsou součástí předmětu plnění 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 systému ICT.
        v. Malware a jiný škodlivý software, který narušuje, obchází či jinak omezuje bezpečnostní opatření v prostředí Objednatele.
    f. Připojovat do prostředí Objednatele pouze zařízení ICT, která jsou chráněna proti malware a jinému škodlivému softwaru, pokud to jejich technologie umožňuje.
    g. Průběžně zaznamenávat a uchovávat data o provozu zařízení ICT (provozní a lokalizační údaje) v rozsahu předmětu plnění a v souladu s požadavky platné a účinné české a evropské legislativy.
    h. Na vyžádání poskytnout Objednateli report obsahující výsledky monitorování veškerých uživatelských a administrátorských aktivit a jiných událostí

v rozsahu poskytování Plnění dle Smlouvy a Dílčí smlouvy, a to po celou dobu trvání Smlouvy a po dobu (2) let po jejím ukončení.

i. Zabezpečit sběr informací o provozních a bezpečnostních činnostech v rozsahu poskytování Plnění dle Smlouvy a Dílčí smlouvy ochranu získaných informací před jejich neoprávněným čtením nebo změnou.

j. Pro on-line transakce realizované prostřednictvím webových technologií implementovat TLS/SSL certifikáty s cílem zajistit jejich důvěrnost, integritu a identitu komunikujících protistran.

k. Veškeré neveřejné informace poskytnuté Objednatelem chránit vhodným šifrováním a proti neautorizovanému přístupu, a to zejména na mobilních zařízeních.

2. Poskytovatel bere na vědomí, že v případě, kdy technické spojení Objednatele s Poskytovatelem narušuje chod služeb Objednatele, může být toto spojení ihned ukončeno bez předchozího upozornění, pokud tato Smlouva nestanoví jinak.

3. Poskytovatel bere na vědomí, že veškeré aktivity Poskytovatele a jeho plnění realizované v prostředí Objednatele jsou monitorovány a vyhodnocovány v rozsahu poskytování Plnění a v souladu s interními dokumenty Objednatele, se kterými byl Poskytovatel seznámen.

Čl. 16 Úroveň služeb (SLA) a realizace bezpečnostních opatření

1. Pokud se Strany výslovně dohodnou, bude součástí plnění i poskytování servisních služeb, jejichž rozsah, úroveň a podmínky budou vymezeny ve smlouvě o úrovni služeb (SLA). SLA bude zejména obsahovat parametry dostupnosti, reakční doby, doby obnovy a podmínky pro eskalaci incidentů, včetně způsobu jejich měření a vyhodnocování.

2. Je-li součástí plnění rovněž zajištění bezpečnostních opatření, zavazuje se Poskytovatel realizovat taková opatření, která odpovídají aktuálním hrozbám, rizikům a povaze poskytovaného plnění, a to v souladu s požadavky stanovenými právními předpisy v oblasti kybernetické bezpečnosti, pokud se na Objednatele vztahují. Poskytovatel je dále povinen tato opatření udržovat, pravidelně vyhodnocovat a na žádost Objednatele doložit jejich implementaci a účinnost.

Čl. 17 Zpřístupnění nebo předání dat na základě žádosti cizozemského orgánu

1. Poskytovatel je povinen bezodkladně informovat Objednatele o obdržení 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. Objednatel je oprávněn poskytnout k žádosti své vyjádření, které je Poskytovatel povinen zohlednit v dalším postupu.

2. Poskytovatel se zavazuje, že v případě, kdy obdrží žádost o zpřístupnění nebo předání dat, která jsou zpracovávána na území cizího státu nebo podle právního řádu jiného než českého, ze strany cizozemského orgánu, učiní veškeré kroky k ochraně těchto dat a postupuje následovně:

    a. data budou zpřístupněna nebo předána až po přezkoumání zákonnosti takové žádosti;

    b. Poskytovatel vynaloží veškeré přiměřené úsilí v rámci možností daných příslušným právním řádem ke zmaření nebo omezení povinnosti zpřístupnit či předat data;

    případné zpřístupnění nebo předání dat bude provedeno výhradně v rozsahu nezbytném k naplnění právní povinnosti, která Poskytovateli vznikne.

Čl. 18 Plnění protiopatření

1. Poskytovatel se bude v rozsahu předmětu plnění Smlouvy aktivně podílet na splnění povinností zákonných povinností, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:

2. poskytnout Objednateli veškerou součinnost při provádění protiopatření vydaných Národním úřadem pro kybernetickou a informační bezpečnost a postupovat v souladu s danými protiopatřeními (§ 20 ZKB);

    a. poskytnout Objednateli veškerou součinnost a informace pro splnění povinnosti Objednatele oznámit Národnímu úřadu pro kybernetickou a informační bezpečnost provedení reaktivního protiopatření a jeho výsledek (§ 23 odst. 6 ZKB).