Příloha č. 6 Smlouvy – Požadavky na zajištění kybernetické bezpečnosti

Požadavky na zajištění kybernetické bezpečnosti (Kybernetické požadavky)

Poskytovatel je povinen ve smyslu plnění stanovených Smlouvou plnit níže uvedené povinnosti zejména součinnostního a bezpečnostního charakteru dle těchto Kybernetických požadavků.

Čl. 1 Systém řízení bezpečnosti informací

Minimálně se Poskytovatel zavazuje v rozsahu poskytování Služeb na své straně:

a) Prosadit bezpečnostní zásady a procesy, které budou pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně poskytovatele při poskytování služeb

b) Na základě bezpečnostních potřeb a výsledků hodnocení rizik zavést příslušná bezpečnostní opatření v rozsahu poskytovaných Služeb, monitorovat je, vyhodnocovat jejich účinnost.

c) Vést záznamy o vytváření a zpracování dat a informací v rozsahu poskytovaných Služeb, zaznamenávat veškeré podstatné okolnosti související se zajištěním bezpečnosti těchto dat a informací a na vyžádání tyto záznamy Objednateli zpřístupnit.

d) Stanovit a udržovat aktuální opatření bezpečnosti ve formě procesů a technologií, které zajišťují na plnění bezpečnostní politiky

Čl. 2 Řízení rizik

Minimálně se Poskytovatel zavazuje v rozsahu poskytování Služeb na své straně:

a) řídit vlastní rizika, která mohou ovlivnit poskytování služeb.

Čl. 3 Organizační bezpečnost

Minimálně se poskytovatel zavazuje v rozsahu poskytování služeb na své straně:

a) Jmenovat nejpozději do 5 dnů po uzavření smlouvy odpovědnou kontaktní osobu pro potřeby zajištění plnění těchto Kybernetických požadavků a související komunikaci mezi smluvními stranami (dále také jen „Kontaktní osoba"). Kontaktní osobu sdělí poskytovatel písemně objednateli v téže lhůtě. Objednatel stanovuje, že určení Kontaktní osoby pro bezpečnost na straně poskytovatele nemá dopad na ustanovení smlouvy týkající se pověřených osob.

b) Využívat pro poskytování služeb pouze oprávněných osob, které byly řádně seznámeny příslušnými ustanoveními interních řídících aktů objednatele a mají ověřenou kvalifikaci, znalosti a zkušenosti k řádnému poskytování Služeb.

EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Čl. 4 Řízení dodavatelů

Minimálně se poskytovatel zavazuje v rozsahu poskytování služeb na své straně:

a) Využívá-li při poskytování služeb poddodavatele, zajistit adekvátní dodržování Kybernetických požadavků rovněž ve smluvních vztazích se svými poddodavateli, přičemž tuto skutečnost se poskytovatel zavazuje doložit objednateli do 10 dnů od účinnosti smlouvy, na jejímž plnění se budou poddodavatelé podílet na poskytování služeb, písemným prohlášením o dodržování Kybernetických požadavků u svých poddodavatelů.

b) Pokud při poskytování předmětu plnění dochází ke zpracování osobních údajů, zajistit nad rámec přílohy č. 5 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 GDPR Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

Čl. 5 Bezpečnost lidských zdrojů

1. Minimálně se Poskytovatel zavazuje v rozsahu poskytování Služeb na své straně:
   a) Na vyžádání doložit objednateli, že všechny osoby podílející se na poskytování Služeb 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 Poskytovatele 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 poskytovaných služeb služba dohledu, definovat a naplnit role a odpovědnosti pro monitoring sítě a zařízení v rozsahu poskytovaných služeb.
   d) Zajistit, 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);
      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 autorským zákonem;
      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.

EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

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. 6 Řízení provozu a komunikací

Minimálně se poskytovatel zavazuje v rozsahu poskytování služeb na své straně:

a) Zajistit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování služeb.

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

c) Zajistit, že pro poskytování Služeb budou využívány pouze aplikace a technologie, které jsou v souladu s platnou českou a evropskou legislativou, především s ohledem na licenční podmínky a autorský zákon.

Čl. 7 Řízení změn

Minimálně se poskytovatel zavazuje v rozsahu poskytování služeb na své straně:

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. 8 Řízení přístupu

1. Minimálně se poskytovatel zavazuje v rozsahu poskytování služeb na své straně:

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

   b) Zajistit, aby udělený přístup nebyl sdílen více osobami za stranu poskytovatele, 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 účinnosti této smlouvy.

   c) Zajistit, aby osoby podílející se na poskytování služeb a mající přístup k informačním aktivům objednatele chránily autentizační prostředky a údaje a nikdy neposkytovaly neautorizovaný přístup dalším osobám.

   d) 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 zaměstnanci poskytovatele 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. 9 Akvizice, vývoj a údržba

1. Minimálně se poskytovatel zavazuje v rozsahu poskytování služeb na své straně:
   a) Zajistit bezpečnou implementaci, inovaci, aktualizaci a testování technologií, které jsou předmětem plnění
   b) Předat objednateli dokumentaci předmětu plnění 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.

V případě, že předmět plnění zahrnuje 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 kód SW a výstupy z provedeného code review (automatizovaně prostřednictvím bezpečnostního nástroje i manuálně), po jeho dokončení, pokud není ve 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 na vyžádání přiměřenou součinnost na provedení bezpečnostního testování v průběhu vývoje softwaru či kdykoliv po jeho předání.

d) Zajistit, že plnění bude obsahovat jen ty součásti, které jsou objektivně potřebné pro řádné provozování softwaru a/nebo které jsou specifikovány výslovně ve smlouvě (zejména, že software nebude obsahovat žádné nepotřebné komponenty, žádné programové vzorky apod.).

e) Pokud je součástí plnění 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) Zajistit bezpečnost testovacího prostředí u poskytovatele a ochranu poskytnutých testovacích dat objednatelem.

g) Zajistit, že do produkčního prostředí objednatele bude dodán jen předmětem smlouvy specifikovaný kompilovaný, respektive spustitelný kód a další nezbytná data pro provozování předmětu plnění.

h) Zajistit, že v rámci poskytovaného plnění bude dodávaný software:
   i. v souladu s bezpečnostními politikami a standardy objednatele, s kterými byl poskytovatel prokazatelně seznámen

EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

ii. otestován na soulad s bezpečnostními politikami objednatele (platí pro poskytovatele, pokud byl s takovými bezpečnostními politikami seznámen) a rozsahu této smlouvy

i) instalovat software pouze na základě objednatelem předem schválených migračních postupů

j) Nevyvíjet, nekompilovat a nešířit v prostředí objednatele programový kód, který má za cíl nelegální ovládnutí, narušení dostupnosti, důvěrnosti nebo integrity nebo neautorizované či nelegální získání dat a informací

Čl. 10 Zvládání kybernetických bezpečnostních událostí a incidentů

1. Minimálně se poskytovatel zavazuje v rozsahu poskytování služeb na své straně:

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 všechny bezpečnostní události a incidenty s potenciálním negativním dopadem na objednatele, a to stanoveným komunikačním kanálem nebo prostřednictvím Kontaktní osoby.

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

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

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

f) 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 odpovědnost Poskytovatele za prodlení s řádným a včasným plněním předmětu Smlouvy a nebude důvodem k jakékoli náhradě případné újmy Poskytovateli či jiné osobě ze strany Objednatele. Ostatní ustanovení ohledně odpovědnosti Poskytovatele za prodlení obsažená ve Smlouvě nejsou tímto ustanovením dotčena.

Čl. 11 Řízení kontinuity činností

Minimálně se poskytovatel zavazuje v rozsahu poskytování služeb na své straně:

a) Zajistit adekvátní kontinuitu svých aktiv, které jsou potřebné k poskytování služeb.

b) Pravidelně kontrolovat a testovat, že je schopen kontinuitu aktiv zajistit dle sjednané úrovně služeb.

EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

Čl. 12 Kontrola a audit

Minimálně se poskytovatel zavazuje v rozsahu poskytování služeb poskytnout adekvátní součinnost při výkonu kontroly Objednatele neb příslušných úřadů:

Čl. 13 Fyzická bezpečnost

Minimálně se poskytovatel zavazuje v rozsahu poskytování služeb na své straně:

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 služeb 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. 14 Bezpečnostní nástroje

1. Minimálně se poskytovatel zavazuje v rozsahu poskytování služeb na své straně:

   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 objednatelem.

   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 poskytovaných služeb:

      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 české a evropské legislativy.

h) Na vyžádání poskytnout objednateli report obsahující výsledky monitorování veškerých uživatelských a administrátorských aktivit a jiných událostí v rozsahu předmětu plnění, a to po celou dobu trvání smlouvy.

i) Zajistit sběr informací o provozních a bezpečnostních činnostech v rozsahu předmětu plnění a 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 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 předměty plnění a v souladu s interními dokumenty objednatele, se kterými byl poskytovatel seznámen.