Bezpečnostní požadavky pro poskytovatele konzultační a poradenské činnosti

1 Účel

a) Definovat bezpečnostní požadavky pro Poskytovatele konzultační a poradenské činnosti, kdy v této souvislosti Poskytovatel přistupuje k informacím Objednatele. Využívá-li Poskytovatel při poskytování předmětu plnění poddodavatele, je povinen zajistit adekvátní dodržování těchto Bezpečnostních požadavků rovněž ve smluvních vztazích se svými poddodavateli.

b) Zajistit ochranu informací Objednatele, se kterými se Poskytoval seznámí v rámci jednání a následném plnění smlouvy.

2 Bezpečnostní požadavky

Poskytovatel bere na vědomí, že Objednatel má zaveden systém řízení bezpečnosti informací dle ISO/IEC 27001 a zároveň je osobou dle § 3 odst. c) a d), příp. f) a g) zákona č. 181/2018, Sb., o kybernetické bezpečnosti a je povinen naplnit požadavky související legislativy.

2.1 Systém řízení bezpečnosti informací

Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na dodržování, provozu a rozvoji bezpečnostních opatření Objednatele a zároveň se 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 předmětu plnění.

b) Řídit vlastní rizika, která mohou ovlivnit poskytování předmětu plnění.

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

d) Vytvořit a schválit bezpečnostní politiku, která bude pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně Poskytovatele při poskytování předmětu plnění.

e) Stanovit a udržovat aktuální opatření bezpečnosti ve formě procesů a technologií, které zajišťují naplnění bezpečnostní politiky.

f) Zajistit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování předmětu plnění.

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

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

2.2 Přístup k informacím Objednatele

Veškeré zpřístupněné informace zůstávají výhradním vlastnictvím Objednatele a Poskytovatel je oprávněn tyto informace užít jen pro účely plnění smlouvy Objednavatele.

Poskytovatel se zavazuje:

a) sdělit informace Objednatele pouze těm svým zaměstnancům nebo spolupracujícím osobám, které nezbytně informace potřebují znát pro účely plnění této smlouvy, jsou současně zavázáni k mlčenlivosti

a byli seznámeni s těmito Bezpečnostními požadavky;

b) nezneužít informace Objednatele k jinému účelu, než je plnění předmětu smlouvy, zejména nenakládat s informacemi v rozporu s oprávněnými zájmy Objednatele;

c) zabezpečit informace Objednatele před jejím zpřístupněním nepovoleným třetím osobám, a to přijetím potřebných technickoorganizační opatření, která zamezí neoprávněnému nebo nahodilému přístupu k informacím Objednatele, k jejich zničení či ztrátě, nebo neoprávněnému užití ze strany nepovolené osoby;

d) pořizovat kopie informací Objednatele pouze v nezbytných případech;

e) veškeré informace poskytnuté Objednatelem chránit vhodným šifrováním a proti neautorizovanému přístup, a to zejména na mobilních zařízeních.

f) po skončení plnění smlouvy bez zbytečného odkladu skartovat veškeré informace a data Objednatele, které mu byly v souvislosti s plněním smlouvy předány.

V případě, že Poskytovatel přistupuje do systému ICT Objednatele:

g) Poskytovatel bere na vědomí, že přístup k systému ICT společností Skupiny ÚJV je možné povolit pouze fyzické identitě zaměstnance poskytovatele / poddodavatele poskytovatele ověřené dokladem totožnosti a pro přístup do ICT systému vygenerovaným jednoznačným identifikátorem, dále pak zaevidované v registru identit, a to na základě požadavku poskytovatele na přístup. Pro zaevidování v registru identit je nezbytné sdělení těchto osobních údajů zaměstnance Poskytovatele:

- Jméno (Registr identit)
- Příjmení (Registr identit)
- Rodné příjmení (Registr identit)
- Pohlaví (pouze při ověření, bez záznamu v registru identit)
- Datum narození (Registr identit)
- Rodné číslo (pouze při ověření, bez záznamu v registru identit, RČ v systémech neukládáme, nepožadujeme jeho zasílání ani zaznamenání do formuláře, ale je vyžadováno při ověření fyzické identity, kdy toto fyzická identita sdělí v okamžiku ověření. V případě nesouhlasu fyzické osoby s použitím RČ je ověření provedeno na základě data narození a dalších osobních údajů fyzické osoby).
- Email (Registr identit)
- Mobilní telefon případně pevná linka (Registr identit)

h) Poskytovatel se zavazuje informovat své zaměstnance a poddodavatele, kterým bude přidělen přístup (fyzický, logický) k systému ICT, o způsobu zpracování jejich osobních údajů.

i) Poskytovatel bere na vědomí, že přidělení oprávnění zaměstnanci poskytovatele musí být řízeno principem nezbytného minima a není nárokové.

j) 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).

2.3 Bezpečnost přenosu dat a informací

K účelům přenosu dat a informací musí být na obou stranách určena (jmenována) Kontaktní osoba, která je autorizována přenos dat a informací provádět. Bezpečné možnosti přenosu dat a informací jsou:

a) Šifrovaná emailová komunikace (MIP, S/MIME nebo zip s heslem)

b) Datové úložiště Skupiny ÚJV s řízeným externím přístupem

c) Šifrované přenosné zařízení zabezpečené PINem (USB disk)

d) Předání tištěných informací (osobně / poštou)

e) Datová schránka

f) Zabezpečená sekce pro dodavatele na portálech společností Skupiny ÚJV

2.4 Zvládání bezpečnostních událostí a incidentů

Poskytovatel se zavazuje:

a) 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.

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

c) Bez zbytečného odkladu a po dohodě s Objednatelem realizovat opatření, požadovaná Objednatelem v dohodnutých termínech, ke snížení dopadu bezpečnostního incidentu nebo zamezení pokračování incidentu, který může mít dopad na Objednatele.

d) 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.

Poskytovatel bere na vědomí, že postup zvládání bezpečnostního incidentu či jiný důsledek porušení Bezpečnostních požadavků, jehož příčina je na straně Poskytovatele, nebude posuzován jako okolnost vylučující odpovědnost Poskytovatele za prodlení s řádným a včasným plněním předmětu této smlouvy a nebude důvodem k jakékoli náhradě případné újmy poskytovateli či jiné osobě ze strany objednatele. Ostatní ustanovení ohledně odpovědnosti Poskytovatele za prodlení obsažená v této smlouvě nejsou tímto ustanovením dotčena.