Příloha č. 6 SoD - BEZPEČNOSTNÍ POŽADAVKY VE SMLUVNÍCH VZTAZÍCH

1. ÚVOD

Účelem této přílohy je definovat závazné bezpečnostní požadavky pro Dodavatele, jejichž předmětem plnění pro Objednatele je (výhradně či jako součást předmětu plnění jiné služby) vývoj, implementace a/nebo servis software či hardware (dále také jen „SW" či „HW"), nebo kteří v souvislosti s plněním pro Objednatele přistupují do informačního systému Objednatele (dále také „IS LP"), a/nebo kteří v rámci poskytovaného plnění pro Objednatele zpracovávají, a/nebo přenášejí a/nebo ukládají a/nebo archivují jakákoli data a informace Objednatele a/nebo jeho zákazníků (dále také jen „Bezpečnostní požadavky").

2. OBECNÉ POŽADAVKY

Dodavatel se při poskytování plnění pro Objednatele zavazuje plnit následující povinnosti:

a) pokud Dodavatel využívá při poskytování plnění poddodavatele, Dodavatel se zavazuje zajistit dodržování Bezpečnostních požadavků rovněž ve smluvních vztazích se svými poddodavateli; přičemž tuto skutečnost se Dodavatel zavazuje doložit Objednateli na vyžádání předložením příslušného smluvního vztahu uzavřeného s tímto poddodavatelem Dodavatele, případně předložením čestného prohlášení o řádném naplňování této povinnosti;
b) nestanoví-li dohoda stran jinak, Dodavatel jmenuje nejpozději do 3 dnů po uzavření Smlouvy zodpovědnou kontaktní osobu pro potřeby zajištění plnění Bezpečnostních požadavků a související komunikace mezi smluvními stranami (dále také jen „**Kontaktní osoba**").
c) pokud při plnění předmětu Smlouvy dochází ke zpracování osobních údajů, Dodavatel se zavazuje zajistit uzavření samostatných smluv ve smyslu příslušných ustanovení nařízení GDPR;
d) dodržovat příslušná ustanovení bezpečnostních politik, metodik a postupů společnosti Objednatele resp. platné řídící dokumentace Objednatele či její části, pokud byl s takovými dokumenty nebo jejich částmi seznámen.

3. BEZPEČNOSTNÍ POŽADAVKY NA VÝVOJ SW

V případě, že součástí plnění je vývoj SW Dodavatel se při poskytování plnění pro Objednatele zavazuje:

a) poskytovat Objednateli v termínech stanovených Objednatelem, resp. bez zbytečného odkladu požadovanou součinnost na provedení bezpečnostního testování v průběhu vývoje SW či po jeho předání;
b) k dodání systémové a provozní bezpečnostní dokumentace nejpozději do doby předání a převzetí SW způsobem uvedeným ve Smlouvě,
c) že plnění bude obsahovat jen ty součásti, které jsou objektivně potřebné pro řádné provozování SW a/nebo které jsou specifikovány výslovně ve Smlouvě (zejména, že SW nebude obsahovat žádné nepotřebné komponenty, žádné programové vzorky apod.);
d) že pokud součástí plnění je i instalace operačního systému případně SW třetích stran, v průběhu jeho instalace budou použity nejnovější aktualizované verze těchto produktů;
e) že veškeré důvěrné informace[1] poskytnuté Objednateli při realizaci plnění nebudou uchovávány v nešifrovaném tvaru a budou chráněna vůči neautorizovanému přístupu, pokud nebude mezi smluvními stranami v konkrétním případě dohodnuto jinak;

[1] Za důvěrné informace se ve smyslu této přílohy považují zejména identifikační údaje certifikátu, hesla, konfigurační soubory, systémové programy, kritické knihovny, obnovovací procedury apod.

f) že v rámci poskytovaného plnění bude instalovat SW nebo jejich upgrade podle hardeningových bezpečnostních politik a v souladu s bezpečnostními standardy Objednatele (platí pro Dodavatele, pokud byl s takovými bezpečnostními standardy seznámen);
g) že v produkčním prostředí systému ICT bude obsažen jen kompilovaný, respektive spustitelný kód a další nezbytná data pro provozování systému ICT;
h) že pokud součástí plnění je implementace SW v produkčním prostředí IS LP provede, před jeho spuštěním kontrolu souladu daného SW s bezpečnostními požadavky hardeningových bezpečnostních politik a v případě zjištění nesouladu zajistí bez zbytečného odkladu soulad dodávaného SW s bezpečnostními požadavky hardeningových politik (platí pro Dodavatele, pokud byl s takovými bezpečnostními standardy seznámen).
i) že pokud součástí plnění je implementace SW v produkčním prostředí IS LP bude instalovat nový SW nebo nové verze SW pouze na základě Objednatelem předem schválených migračních postupů[2];

4. FYZICKÁ OCHRANA A BEZPEČNOST PROSTŘEDÍ

a) Dodavatel se zavazuje dodržovat provozní řády budov (režimová opatření) a využívaných prostor, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěny komponenty systémů ICT anebo datové nosiče (dále také jen „**Pracoviště**“).
b) Dodavatel se zavazuje, že na Pracovišti neponechá volně dostupná instalační, záložní nebo archivní média ani dokumentaci k systému ICT, který je předmětem plnění dle této Smlouvy.

5. ŘÍZENÍ PŘÍSTUPU

V případě, že součástí plnění je přístup zaměstnanců LP k externím webovým službám, musí být dodrženy následující požadavky:

a) Přihlašovací údaje nesmí být uloženy v čitelné podobě, ale musí být chráněny dostatečně silnými kryptografickými prostředky.
b) Systém, ke kterému zaměstnanci LP přistupují, musí být pravidelně testován, aktualizován a být dostatečně odolný tak, aby byla zajištěna bezpečnost informací a dat.
c) V případě, že výsledkem penetračního testování jsou kritická zjištění je Dodavatel povinen neprodleně informovat LP o těchto skutečnostech a přijmout dostatečná nápravná opatření.
d) LP si vyhrazuje možnost provedení pravidelného penetračního testování v průběhu trvání smlouvy.
e) Přístupová hesla musí být dostatečně silná, tzn. minimálně 12 znaků, komplexnost hesla (heslo musí obsahovat znaky z minimálně 3 typů), maximální a minimální doba používání hesla a možnost opakování hesel musí být nastavitelná.

V případě, že součástí plnění je přístup k produkčnímu prostředí IS LP musí být dodrženy následující požadavky:

a) Dodavatel bere na vědomí, že přístup k systémům IS LP je možné povolit pouze fyzické identitě zaměstnance Dodavatele nebo poddodavatele Dodavatele zaevidované v registru identit Objednatele, a to na základě požadavku Dodavatele na přístup.
b) Přístupová hesla musí být dostatečně silná, tzn. minimálně 12 znaků, komplexnost hesla (heslo musí obsahovat znaky z minimálně 3 typů), maximální a minimální doba používání hesla a možnost opakování hesel musí být nastavitelná.
c) Dodavatel bere na vědomí, že zaměstnanec Dodavatele musí prokazatelně souhlasit se zpracováním osobních údajů potřebných pro zřízení přístupu, v opačném případě Objednatel není povinen přístup k systému ICT zaměstnanci Dodavatele povolit. Zaměstnanec Dodavatele s přiděleným přístupem (fyzickým, logickým) k systému ICT musí prokazatelně souhlasit se zpracováním osobních údajů

[2] Migrační postup – soubor kroků definující převod dat mezi dvěma nebo více systémy ICT.

zpracovávaných během vyhodnocování údajů o pohybu a prováděných aktivitách v prostorách Objednatele (např.: monitoring pomocí řešení Security Incident and Event Monitoring), přičemž takový souhlas musí být proveden souhlasem písemným nebo digitálním formou emailu, není-li smluvními stranami dohodnuto jinak.

d) Dodavatel bere na vědomí, že přidělení oprávnění zaměstnanci Dodavatele musí být řízeno principem nezbytného minima a není nárokové.

e) Dodavatel se zavazuje, že udělený přístup nesmí být sdílen více zaměstnanci Dodavatele nebo poddodavatele Dodavatele.

f) Dodavatel se zavazuje, že přístup do systému ICT prostřednictvím mobilní aplikace bude vždy uskutečněn pouze prostřednictvím zabezpečeného připojení VPN.

g) Dodavatel se zavazuje, že před připojením koncového zařízení, mobilní koncového zařízení nebo aktivního síťového prvku jako síťové switche, WiFi access pointy, routery či huby do počítačové sítě zažádá o schválení připojení Kontaktní osobu na straně Objednatele

h) Dodavatel se zavazuje, že bez zbytečného odkladu deaktivuje všechny nevyužívané zakončení sítě anebo nepoužívané porty aktivního síťového prvku.

i) Dodavatel se zavazuje, že nebude instalovat a používat tyto typy nástrojů:
   - Keylogger,
   - Sniffer,
   - Analyzátor zranitelností a Port Scanner,
   - Backdoor, rootkit a trojský kůň nebo jinou podobu malware.

j) Dodavatel se zavazuje, že všechny ICT systémy Dodavatele, které se připojují do síťové infrastruktury Objednatele, jsou a budou chráněny proti malware.

k) Dodavatel se zavazuje, že nebude vyvíjet, kompilovat a šířit v jakékoliv části systému ICT programový kód, který má za cíl nelegální ovládnutí, narušení, nebo diskreditaci systému ICT nebo nelegální získání dat a informací.

l) Dodavatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednateli:
   - nenavštěvovali internetové stránky s eticky nevhodným obsahem[3];
   - neukládali a/nebo nesdíleli data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno Objednatele;
   - nestahovali, nesdíleli, neukládali, nearchivovali a/nebo neinstalovali datové a spustitelné soubory v rozporu s licenčními podmínkami nebo autorským zákonem;
   - neukládat a/nebo nesdíleli data a informace společnosti na nepovolených datových úložištích nebo médiích; nezasílali řetězové emaily.

m) Dodavatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednateli, kteří přistupují do interní sítě a/nebo systému ICT Objednatele, respektovali a dodržovali následující omezení. Zařízení typu notebook/počítač musí mít aplikovány bezpečnostní záplaty (operačního systému, internetového prohlížeče a Javy) a nainstalovanou, spuštěnou a aktualizovanou antivirovou ochranu;

n) Dodavatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednateli, kteří přistupují do interní sítě a/nebo systému ICT Objednatele chránili autentizační prostředky a údaje k systémům ICT Objednatele. Dodavatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet zablokován a řešen jako bezpečnostní incident ve smyslu příslušné řídící dokumentace a mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu (např. okamžité zrušení přístupu k informačním aktivům fyzických osob externího subjektu). Dodavatel bere na vědomí, že postup zvládání bezpečnostního incidentu či jiný důsledek porušení Bezpečnostních požadavků nebude posuzován jako okolnost vylučující odpovědnost Dodavatele za prodlení s řádným a včasným plněním

[3] Data a informace obsahující prvky extrémismu, terorismu, pornografie anebo podněcování k nesnášenlivosti a společenským předsudkům vztahujícím se ke společenské skupině identifikované na základě rasy, náboženství nebo víry, pohlaví, sexuální orientace, národnostní a etnické příslušnosti či jiné odlišnosti.

předmětu Smlouvy a nebude důvodem k jakékoli náhradě případné újmy Dodavateli či jiné osobě ze strany Objednatele.

6. MONITOROVÁNÍ

a) Dodavatel bere na vědomí, že veškerá aktivita Dodavatele a jeho plnění realizované v systémovém prostředí Objednatele budou Objednatelem průběžně a pravidelně monitorovány a vyhodnocovány s ohledem na obsah Smlouvy a interních dokumentů Objednatele, se kterými byl Dodavatel seznámen.
b) Dodavatel se zavazuje, že auditní záznamy obsahující výsledky monitorování, úspěšná a neúspěšná přihlášení do ICT systému a záznamy o správě uživatelů je povinen na vyžádání a bez zbytečného odkladu předložit Objednateli, a to po celou dobu trvání Smlouvy i o jejím ukončení.

7. PŘEDÁNÍ A PŘEVZETÍ PLNĚNÍ

a) Dodavatel bere na vědomí, že nedodržení Bezpečnostních požadavků včetně požadavku na předání kompletní systémové a provozní dokumentace je vadou bránící převzetí předmětu Smlouvy (je vadou kategorie A), přičemž Objednatel není do doby odstranění příslušné vady plnění povinen plnění převzít.
b) Dodavatel odpovídá za to, že systémy ICT budou obsahovat nejnovější bezpečnostní aktualizace (patche)[4].

8. OPRÁVNĚNÍ UŽÍVAT DATA

10.1 Dodavatel je při poskytování plnění pro Objednatele oprávněn užívat data předaná Dodavateli Objednatelem za účelem plnění předmětu Smlouvy, avšak vždy pouze v rozsahu nezbytném ke splnění předmětu Smlouvy.

10.2 Dodavatel se při poskytování plnění pro Objednatele zavazuje nakládat s daty pouze v souladu se Smlouvou a příslušnými právními předpisy, zejména ZoKB a Vyhláškou a dalšími souvisejícími právními předpisy.

9. VÝMĚNA INFORMACÍ

a) Pokud je předmětem Smlouvy výměna informací mezi smluvními stranami, musí být mezi smluvními stranami uzavřena dohoda o ochraně předmětných informací, zejména při jejich výměně, uložení, archivaci a ukončení Smlouvy.
b) Dodavatel se zavazuje, že veškerý přenos dat a informací musí být dostatečně zabezpečen z pohledu bezpečnostní klasifikace a tedy požadavků na důvěrnost, integritu a dostupnost dat a informací.
c) Dodavatel se zavazuje, že on-line transakce realizované prostřednictvím webových technologií budou chráněny SSL certifikáty.

10. ZVLÁDÁNÍ BEZPEČNOSTNÍCH INCIDENTŮ

Dodavatel se při poskytování plnění pro Objednatele zavazuje, že v případě kdy dojde k narušení bezpečnosti informací:

a) neprodleně nahlásí tuto skutečnost Kontaktní osobě Objednatele uvedenou ve Smlouvě;
b) v případě vzniku bezpečnostní události a následného zvládání a vyhodnocování bezpečnostního incidentu a/nebo v případě podezření na bezpečnostní incident, poskytne Objednateli požadovanou

[4] Aktualizace software na vyšší vývojovou verzi.

součinnost (např.: poskytne logy a identifikační údaje (např. IP adresa, MAC adresa, HW typ, sériové číslo případně IMEI) dotyčného koncového zařízení nebo mobilního koncového zařízení zaměstnance Dodavatele nebo zaměstnance poddodavatele podílející se na realizaci plnění, k analýze obsahu, případně bez zbytečného odkladu zrealizuje opatření požadovaná Objednatelem). provede analýzu příčin bezpečnostního incidentu a navrhne opatření s cílem zamezit jeho opakování v případě, že Dodavatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.