BEZPEČNOSTNÍ PRAVIDLA PRO BĚŽNÉ DODAVATELE

1 ŘÍZENÍ INFORMAČNÍ BEZPEČNOSTI

1.1 Dodavatel se zavazuje

1.1.1 řídit vlastní rizika, která mohou ovlivnit poskytování předmětu plnění;

1.1.2 na základě bezpečnostních potřeb a výsledků hodnocení rizik zavést příslušná bezpečnostní opatření v rozsahu poskytovaného předmětu plnění, monitorovat je, vyhodnocovat jejich účinnost;

1.1.3 vést záznamy o vytváření a zpracování dat a informací v rozsahu poskytovaného předmětu plnění, zaznamenávat veškeré podstatné okolnosti související se zajištěním bezpečnosti těchto dat a informací a na vyžádání tyto záznamy ŘLP ČR, s. p. zpřístupnit;

1.1.4 využívá-li při poskytování předmětu plnění subdodavatele, zajistit adekvátní dodržování těchto bezpečnostních pravidel rovněž ve smluvních vztazích se svými subdodavateli.

2 PERSONÁLNÍ BEZPEČNOST

2.1 Dodavatel zajistí seznámení všech osob, účastnících se plnění dle uzavřené smlouvy s ŘLP ČR, s. p., s těmito bezpečnostními pravidly a dalšími upřesňujícími bezpečnostními informacemi prokazatelně předanými ze strany ŘLP ČR, s. p. Tyto osoby stvrdí seznámení písemně.

2.2 Osoby, účastnící se plnění dle uzavřené smlouvy s ŘLP ČR, s. p., musí mít prokazatelné kvalifikační předpoklady, zkušenosti a znalosti.

2.3 Dodavatel musí zajistit, aby osoby, účastnící se plnění dle uzavřené smlouvy s ŘLP ČR, s. p., prošly procesem prověřování a byly jim stanoveny pro jejich činnosti podmínky a odpovědnosti.

2.4 Dodavatel musí prokazatelnou formou zajistit odpovídající povědomí o bezpečnosti informací osob, účastnících se plnění dle uzavřené smlouvy s ŘLP ČR, s. p.

2.5 Dodavatel musí mít zaveden proces pro ukončení či změnu pracovního poměru zaměstnance, účastnícího se plnění dle uzavřené smlouvy s ŘLP ČR, s. p.

3 FYZICKÁ BEZPEČNOST, POŽÁRNÍ OCHRANA A BOZP

Podmínky a pravidla fyzické bezpečnosti, požární ochrany a bezpečnosti a ochrany zdraví při práci jsou popsány ve smlouvě.

4 ŘÍZENÍ PROVOZU

Dodavatel se zavazuje zajistit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování předmětu plnění v souladu s doporučeními technických norem řady ISO/IEC 27000.

5 ŘÍZENÍ PŘÍSTUPU

5.1 Identifikace

5.1.1 Každý zaměstnanec dodavatele podílející se na plnění smlouvy výpočetními prostředky dodavatele, musí mít v rámci své IT infrastruktury evidován a veden svůj vlastní jedinečný uživatelský účet, kterému jsou v jednotlivých určených systémech, modulech nebo aplikacích přiřazeny specifické role. Každý zaměstnanec dodavatele musí být veden s platnými identifikačními a aktuálními kontaktními údaji.

5.1.2 Každý zaměstnanec dodavatele, pokud přistupuje k interním systémům ŘLP ČR, s. p., má u ŘLP ČR, s. p. veden a evidován jedinečný uživatelský účet, kterému jsou v jednotlivých systémech, modulech nebo aplikacích přiřazeny specifické role související výhradně s plněním předmětu smlouvy.

5.2 Autentizace

5.2.1 Podmínky pro autentizaci při využití ICT infrastruktury ŘLP ČR, s. p.:

a) k jednoznačné identifikaci uživatelů určených systémů se využívá více faktorová autentizace;
b) ověření heslem - pokud není možné použít jednoznačnou identifikaci uživatelů více faktory, je použita autentizace pomocí kryptografických klíčů se zaručením obdobné úrovně bezpečnosti nebo použití hesla s vyžadovanými pravidly.

5.3 Autorizace

5.3.1 Zaměstnanci dodavatele jsou povinni v ICT infrastruktuře ŘLP ČR, s. p. využívat uživatelská oprávnění jen v přiměřené míře a jen po dobu nezbytně nutnou pro vykonání činností v souladu s plněním předmětu smlouvy.

5.3.2 Zaměstnanci dodavatele jsou informováni ŘLP ČR, s. p., které informace ŘLP ČR., s. p. považuje za chráněně, ke kterým chráněným informacím ŘLP ČR, s. p. mají přístup a jak s nimi mohou nakládat. Jakékoliv manipulace a další operace s chráněnými informacemi ŘLP ČR, s. p., které nebyly výslovně v instrukcích uvedeny, nemá dodavatel povoleny.

5.4 Vzdálený přístup

5.4.1 Pracovní stanice dodavatele přistupující k infrastruktuře ŘLP ČR, s. p. prostřednictvím VPN (Virtual Private Network) musí mít:

a) pokročilou funkční antivirovou ochranu (s real time protection mod), s pečetí AV-TEST APPROVED (av-test.org) nebo s certifikátem VB100 (virusbulletin.com) – platí pro prostředí MS Windows a Android;
b) funkční personal firewall;
c) funkční nastavené automatické aktualizace systému;
d) operační systém, který není mimo servisní podporu výrobce (pokud není smluvním ujednáním výslovně stanoveno jinak);
e) aktualizované aplikace třetích stran za dodržení autorských práv třetích stran;
f) zajištěno šifrování všech paměťových médií, na kterých jsou uložena chráněná data a informace ŘLP ČR, s. p. Přístup k paměťovým médiím a k dešifrování chráněných dat a informací ŘLP ČR, s. p. musí být umožněno jen oprávněným osobám dodavatele;
g) nainstalovaného VPN klienta, instalovaného výlučně v odpovědnosti dodavatele;
h) druhý autentizační faktor (HW nebo SMS token) pro přístup k VPN, který bude poskytnut určeným zaměstnancem ŘLP ČR, s. p. proti podpisu předávacího protokolu.

6 ŘÍZENÍ ZMĚN

6.1 Dodavatel se zavazuje:

6.1.1 řídit a evidovat smluvní změny;

6.1.2 řídit a evidovat změny v poskytovaných službách.

7 UŽÍVÁNÍ KRYPTOGRAFICKÝCH PROSTŘEDKŮ

7.1 Je-li v rámci předmětu plnění vyžadováno použití kryptografických prostředků, technické podmínky jsou následující:

7.1.1 šifrování standardizovaným symetrickým heslem, jehož metodu definuje ŘLP ČR, s. p. Heslo musí být předáno jiným komunikačním kanálem;

7.1.2 šifrování pomocí digitálních certifikátů vydaných obecně uznávanou CA nebo CA, které explicitně důvěřují obě strany;

7.1.3 pokud nelze ověřit platnost certifikátu vůči CRL, je certifikát považován za neplatný a nelze jej použít k šifrování nebo podpisu;

7.1.4 šifrování pomocí PGP klíčů odsouhlasených oběma stranami nebo ověřené nezávislou důvěryhodnou třetí stranou;

7.1.5 pro VPN přístup k určeným systémům se používá ze strany ŘLP ČR, s. p. standardizovaná definovaná šifra;

7.1.6 pro webové servery prezentující data pocházející z určených informačních systémů mimo samotný systém se používá HTTPS protokol v ŘLP ČR, s. p. standardizovanou šifrou;

7.1.7 pro webové servery prezentující data pocházející z určených systémů pro uživatele mimo ŘLP ČR, s. p. se používá EV certifikát obecně uznávané certifikační autority.

8 MONITORING

8.1 Přístup zaměstnanců dodavatele k vybraným interním informacím a datům a k informačním a komunikačním systémům ŘLP ČR, s. p. je nepřetržitě zaznamenáván, monitorován a vyhodnocován. Události v systémech jsou ŘLP ČR, s. p. zaznamenávány do logů:

8.1.1 úspěšné a neúspěšné přihlášení a odhlášení uživatelů;

8.1.2 činnosti provedené administrátory;

8.1.3 úspěšné a neúspěšné manipulace s účty, oprávněními a právy;

8.1.4 neprovedení činností v důsledku nedostatku přístupových oprávnění;

8.1.5 činnosti uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému;

8.1.6 zahájení a ukončení činností technických aktiv;

8.1.7 automatická varovná nebo chybová hlášení technických aktiv;

8.1.8 přístupy k logům, pokusy o manipulaci s logy a změny nastavení nástroje pro zaznamenávání činností a použití mechanismů autentizace včetně změny údajů, které slouží k přihlášení.

8.2 Ke každému záznamu v logu přiřazuje ŘLP ČR, s. p.:

8.2.1 datum a čas;

8.2.2 typ činnosti;

8.2.3 název relevantního technického aktiva;

8.2.4 identifikaci uživatele;

8.2.5 identifikaci síťového zařízení původce;

8.2.6 úspěšnost nebo neúspěšnost provedení činnosti;

8.2.7 úroveň závažnosti.

8.3 Dodavatel je povinen průběžně monitorovat v rámci své ICT infrastruktury zveřejněné a známé bezpečnostní chyby, které mohou ovlivnit hladký a bezpečný provoz systémů souvisejících s jím poskytovanými službami. Jedná se například o zranitelnosti v operačních systémech, software třetích stran, webové komponenty atd.

9 OCHRANA DATOVÝCH ÚLOŽIŠŤ A PŘENOSNÝCH MÉDIÍ

9.1 Uložení dat ŘLP ČR, s. p. do datových úložišť dodavatele, na přenosná média a případný transport médií mimo prostory ŘLP ČR, s. p. podléhá schválení ŘLP ČR, s. p.

9.2 V případě ukládání dat ŘLP ČR, s. p. do datových úložišť dodavatele a na přenosná média má dodavatel povinnost ukládat, případně vyžadovat uložení těchto dat v šifrované podobě a u přenosných médií vést evidenci těchto médií.

9.3 Dodavatel je povinen zajistit likvidaci operativních dat ŘLP ČR, s. p. ihned po pominutí účelu jejich zpracování nebo uložení způsobem dle standardu NIST 800-88. Po likvidaci dat na elektronickém médiu nesmí být možné informaci obnovit. O provedení likvidace dat musí dodavatel vést protokol.

10 KYBERNETICKÉ BEZPEČNOSTNÍ UDÁLOSTI / INCIDENTY

10.1 Dodavatel má za povinnost hlásit veškerá podezření na kybernetické bezpečnostní události / incidenty:

10.1.1 odpovědné osobě ŘLP ČR, s. p.;

10.1.2 v termínu bezprostředně (bez prodlení) po zjištění kybernetické bezpečnostní události / incidentu;

10.1.3 prostřednictvím emailu, telefonicky se zajištěním evidence hovoru na obou stranách, nebo osobně;

10.1.4 s popisem

a) data a času zjištění;
b) povahy události;
c) zdroje události;
d) cíle / oběti události;
e) potencionálního dopadu.

11 OCHRANA AKTIV PROTI NEAUTORIZOVANÝM ČINNOSTEM

Dodavatel na aktiva ŘLP ČR, s. p. neinstaluje a nepoužívá nástroje, které nejsou součástí předmětu plnění.

12 PODMÍNKY PŘI UKONČENÍ SMLOUVY

12.1 V případě ukončení smluvního vztahu musí být ukončeny veškeré přístupy dodavatele a jeho zaměstnanců k aktivům ŘLP ČR, s. p. nejpozději k termínu ukončení smluvního vztahu.

12.2 Pokud byla zaměstnancům dodavatele poskytnuta aktiva ŘLP ČR, s. p., musí být tato aktiva vrácena nejpozději k termínu ukončení smluvního vztahu.

12.3 Pokud byla dodavateli poskytnuta informační aktiva (data) ŘLP ČR, s. p., musí být nejpozději k termínu ukončení smluvního vztahu vrácena a beze zbytku smazána způsobem dle standardu NIST 800-88 ze všech systémů dodavatele a nosičů dodavatele taková aktiva obsahujících.