

BEZPEČNOSTNÍ PRAVIDLA PRO KLÍČOVÉ DODAVATELE

1 ŘÍZENÍ INFORMAČNÍ BEZPEČNOSTI

1.1 Dodavatel se zavazuje:

- 1.1.1 vytvořit a schválit bezpečnostní politiku, která bude pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně dodavatele při poskytování předmětu plnění. Bezpečnostní politika musí obsahovat hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací, dle technických norem řady ISO/IEC 27000;
- 1.1.2 řídit vlastní rizika, která mohou ovlivnit poskytování předmětu plnění;
- 1.1.3 na základě bezpečnostních potřeb a výsledků hodnocení rizik zavést příslušná bezpečnostní opatření v rozsahu poskytovaného předmětu plnění, monitorovat je, vyhodnocovat jejich účinnost;
- 1.1.4 stanovit a udržovat aktuální opatření bezpečnosti ve formě procesů a technologií, které zajišťují naplnění bezpečnostní politiky;
- 1.1.5 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;
- 1.1.6 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

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

4 ŘÍZENÍ PROVOZU

4.1 Dodavatel se zavazuje:

- 4.1.1 zajistit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování předmětu plnění v souladu s doporučeními technických norem řady ISO/IEC 27000;
- 4.1.2 na vyžádání poskytnout ŘLP ČR, s. p. přehled o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře, kterými plní předmět smlouvy.

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 privilegovaných uživatelů určených systémů se využívá více faktorová autentizace;
 - b) ověření heslem - pokud není možné použít jednoznačnou identifikaci privilegovaných 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 privilegovaná oprávnění jen v přiměřené míře a jen po dobu nezbytně nutnou pro vykonání činností v souladu s plněním předmětu smlouvy. Uživatelé nesmějí používat účty s privilegovanými oprávněními pro běžnou práci nesouvisející se správou určeného systému.
- 5.3.2 Zaměstnanci dodavatele jsou informováni ŘLP ČR, s. p., které informace ŘLP ČR, s. p. považuje za chráněné, 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
- 5.5 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 pečeti 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 Podmínky:
- 6.1.1 změny na straně dodavatele musí být řízeny s ohledem na kritičnost informací, systémů, procesů a opětovným posuzováním rizik.
- 6.2 Dodavatel se zavazuje
- 6.2.1 řídit a evidovat smluvní změny;
- 6.2.2 řídit a evidovat změny v poskytovaných službách v souladu s doporučeními technických norem řady ISO/IEC 27000.

7 AKVIZICE, VÝVOJ A ÚDRŽBA

7.1 Dodavatel se zavazuje:

7.1.1 zajistit bezpečnou implementaci, inovaci, aktualizaci, testování technologií, které jsou předmětem plnění.

7.1.2 předat ŘLP ČR, s. p. dokumentaci předmětu plnění minimálně v následujícím rozsahu:

- a) dokumentaci skutečného provedení;
- b) dokumentaci všech bezpečnostních nastavení, funkcí a mechanismů;
- c) dokumentaci obsahující popis autorizačního konceptu a oprávnění;
- d) dokumentaci obsahující zálohovací a archivační postupy;
- e) dokumentaci obsahující instalační a konfigurační postupy;
- f) dokumentaci zahrnující testy zranitelnosti a soulad s bezpečnostními požadavky ŘLP ČR, s. p.;
- g) dokumentaci pro zajištění kontinuity provozu a obnovy po havárii.

7.2 V případě vývoje řešení se dodavatel zavazuje:

7.2.1 dodržovat a implementovat nejlepší praktiky pro bezpečný vývoj softwaru dle doporučení technických norem řady ISO/IEC 27000;

7.2.2 pokud jsou softwarové auditní činnosti a předání zdrojového kódu k řešení součástí plnění dle smlouvy, bude umožněn audit prováděného nebo provedeného plnění a na písemnou žádost bude předložen vyvíjený zdrojový kód k řešení na provedení code review (automatizovaně prostřednictvím bezpečnostního nástroje i manuálně), a to zejména za účelem ověření skutečnosti, zda bylo postupováno dle plnění v souladu se smlouvou;

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

7.2.4 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 ŘLP ČR, s. p.;

7.2.5 zajistit bezpečnost testovacího prostředí u dodavatele a ochranu poskytnutých testovacích dat ŘLP ČR, s. p.;

7.2.6 zajistit, že v produkčním prostředí ŘLP ČR, s. p. bude dodán jen předmětem smlouvy specifikovaný kompilovaný, respektive spustitelný kód a další nezbytná data pro provozování předmětu plnění;

7.2.7 zajistit, že v rámci poskytovaného plnění bude dodávané řešení v souladu s doporučeními technických norem řady ISO/IEC 27000;

7.2.8 poskytnout ŘLP ČR, s. p. potřebnou součinnost v případě, že ŘLP ČR, s. p. vyžaduje / realizuje provedení bezpečnostních testů souvisejících s předmětem plnění;

7.2.9 předat zdrojový kód ŘLP ČR, s. p., je-li tak stanoveno ve smlouvě, bezpečnou formou zajišťující jeho integritu, a v takovém případě:

- a) zajistit řízení verzí zdrojového kódu;
- b) zajistit zálohování zdrojového kódu a jeho uložení mimo produkční prostředí;
- c) zajistit, aby distribuce zdrojových kódů obsahovala soubor z vývojového prostředí na řízenou kompilaci těchto zdrojových kódů;

7.2.10 nevyvíjet, nekompileovat a nešířit v prostředí ŘLP ČR, s. p. programový kód, který má za cíl nelegální ovládnutí, narušení dostupnosti, důvěrnosti nebo integrity nebo neautorizované či nelegální získání dat a informací.

8 UŽÍVÁNÍ KRYPTOGRAFICKÝCH PROSTŘEDKŮ

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

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

- 8.1.2 šifrování pomocí digitálních certifikátů vydaných obecně uznávanou CA nebo CA, které explicitně důvěřují obě strany;
- 8.1.3 pokud nelze ověřit platnost certifikátu vůči CRL, je certifikát považován za neplatný a nelze jej použít k šifrování nebo podpisu;
- 8.1.4 šifrování pomocí PGP klíčů odsouhlasených oběma stranami nebo ověřené nezávislou důvěryhodnou třetí stranou;
- 8.1.5 pro VPN přístup k určeným systémům se používá ze strany ŘLP ČR, s. p. standardizovaná definovaná šifra;
- 8.1.6 pro webové servery prezentující data pocházející z určených informačních systémů mimo samotný systém používají HTTPS protokol v ŘLP ČR, s. p. standardizovanou šifrou;
- 8.1.7 pro webové servery prezentující data pocházející z určených systémů pro uživatele mimo ŘLP ČR, s. p. se používá EV certifikát obecně uznávané certifikační autority.

9 MONITORING

- 9.1 Přístup zaměstnanců dodavatele k vybraným chráněným interním informacím 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:
 - 9.1.1 úspěšné a neúspěšné přihlášení a odhlášení uživatelů;
 - 9.1.2 činnosti provedené administrátory;
 - 9.1.3 úspěšné a neúspěšné manipulace s účty, oprávněními a právy;
 - 9.1.4 neprovedení činností v důsledku nedostatku přístupových oprávnění;
 - 9.1.5 činnosti uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému;
 - 9.1.6 zahájení a ukončení činností technických aktiv;
 - 9.1.7 automatická varovná nebo chybová hlášení technických aktiv;
 - 9.1.8 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.
- 9.2 Ke každému záznamu v logu přiřazuje ŘLP ČR, s. p.:
 - 9.2.1 datum a čas;
 - 9.2.2 typ činnosti;
 - 9.2.3 název relevantního technického aktiva;
 - 9.2.4 identifikaci uživatele;
 - 9.2.5 identifikaci síťového zařízení původce;
 - 9.2.6 úspěšnost nebo neúspěšnost provedení činnosti;
 - 9.2.7 úroveň závažnosti.
- 9.3 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.

10 OCHRANA DATOVÝCH ÚLOŽIŠŤ A PŘENOSNÝCH MÉDIÍ

- 10.1 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.
- 10.2 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.

- 10.3 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.

11 KYBERNETICKÉ BEZPEČNOSTNÍ UDÁLOSTI / INCIDENTY

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

11.1.1 odpovědné osobě ŘLP ČR, s. p.;

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

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

11.1.4 s popisem:

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

12 AUDIT DODAVATELE (ZÁKAZNICKÝ AUDIT)

12.1 Oprávnění k provedení auditu

12.1.1 ŘLP ČR, s. p. si vyhrazuje právo provádět audity dodavatele.

12.1.2 ŘLP ČR, s. p. s dostatečným předstihem alespoň 5 pracovních dnů oznámí dodavateli záměr na provedení auditu. Obě strany si dohodnou obsah, potřebnou součinnost a časový plán auditu s tím, že ŘLP ČR, s. p. se zavazuje postupovat tak, aby nenarušil provozní potřeby dodavatele.

12.1.3 ŘLP ČR, s. p. si vyhrazuje právo v případě závažných důvodů (např. podezření na rizikové chování dodavatele) v souvislosti s plněním smlouvy provést neohlášený audit u dodavatele s přihlédnutím k provozní situaci dodavatele.

12.1.4 Auditor / inspektor ustanovuje při zjištění neshod nápravná opatření ke zjištění a datum jejich zavedení. Dodavatel je povinen nápravná opatření realizovat v rozsahu stanoveného opatření a v požadovaném termínu.

12.1.5 Dokumentace auditů prováděných ŘLP ČR, s. p. je vedena v útvaru odpovědném za provádění auditů. Záznamy týkající se určitého auditu jsou vždy označovány stejným identifikátorem. Jednotlivé záznamy auditů tvoří:

- a) plán auditu;
- b) oznámení o auditu;
- c) dotazník k auditu (seznam otázek auditora, pokud auditor uzná za vhodné);
- d) zpráva z auditu;
- e) písemné, fotografické nebo jiné záznamy provozu, postupů nebo zařízení, které souvisí s auditem (pokud je nezbytné pro dokumentování nálezů);
- f) záznam o zjištění (nápravných opatřeních a následné kontrole).

12.1.6 Auditovaná strana (dodavatel) obdrží k vyjádření závěrečnou zprávu auditu obsahující případná zjištění, na jejichž základě

- a) dodavatel navrhne opatření a termíny řešení a předá jejich seznam ŘLP ČR, s. p. k odsouhlasení;
- b) ŘLP ČR, s. p. následně potvrdí souhlas s navrženými opatřeními nebo je vrátí s připomínkami dodavateli k přepracování.

12.2 Nápravná opatření

12.2.1 Auditovaná strana (dodavatel) má za povinnost v určeném čase zajistit realizaci dohodnutých nápravných opatření.

12.2.2 Zprávu o realizovaných opatřeních dodavatel oznamuje a předává ŘLP ČR, s. p.

13 OCHRANA AKTIV PROTI NEAUTORIZOVANÝM ČINNOSTEM

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

14 PODMÍNKY PŘI UKONČENÍ SMLOUVY

- 14.1 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.
- 14.2 Pokud byla zaměstnancům dodavatele poskytnuta aktiva ŘLP ČR, s. p., musí být tato aktiva vrácena nejpozději k termínu ukončení smluvního vztahu.
- 14.3 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.