MĚSTO ČERNOŠICE

BEZPEČNOSTNÍ POLITIKA ISVS

ATESTAČNÍ MINIMUM

Verze 1.0
Listopad 2016

Zpracovatel: *COMPACT OFFICE, s.r.o.*
Se sídlem: *Hradecká 167, 378 62 Kunžak*
IČ: *281 17 166*

OBSAH:

1. Úvod

Bezpečnostní politika specifikuje obecně celkové cíle a strategii Městského úřadu Černošice (dále jen „úřad“) při koordinaci, budování a provozu informačního systému v oblasti bezpečnosti, zejména pak **bezpečnostní opatření**, která úřad uplatňuje při zajišťování bezpečnosti svých ISVS, a která odpovídají bezpečnostním cílům stanovených v dokumentu Informační koncepce tohoto orgánu veřejné správy, a vytváří tak odpovídající platformu pro naplnění povinnosti OVS na zajištění informační bezpečnosti svých ISVS podle zákona č. 365/2000 Sb. o ISVS, ve znění pozdějších předpisů.

Bezpečnostní politika je klíčovou interní směrnicí Městského úřadu Černošice, která definuje požadavky úřadu na informační bezpečnost. Jejím cílem je zajištění informační bezpečnosti, definice postupů, rolí a pravomocí v procesu řízení bezpečnosti. Bezpečnostní politika je schvalována tajemnicí úřadu.

Aby bezpečnostní politika mohla být uplatňována, je zapotřebí, aby se s ní zaměstnanci úřadu a další osoby přicházející do styku s informačními systémy (pracovníci organizací zřizovaných městem, zástupci dodavatelů, ...) seznámili a příslušnými ustanoveními se řídili. Proto musí být bezpečnostní politika vhodnými způsoby propagována a publikována.

Dodržování bezpečnostní politiky je kontrolováno.

Bezpečnostní politika je v souladu s ISO 27001 – ISMS.

1.1. Základní údaje o Bezpečnostní politice ISVS

Název dokumentu:	Bezpečnostní politika ISVS Města Černošice
Datum dokončení:	11.11.2016
Datum schválení:	30. 11. 2016
Způsob schválení:	Schváleno 30. 11. 2016 tajemnicí MěÚ Černošice
Doba platnosti:	5 let
Platnost od kdy:	1. 12. 2016
Aktuální verze:	1.0

1.2. Definice informační bezpečnosti

Pojem informační bezpečnost podle § 5b zákona o ISVS znamená pro OVS povinnost uplatnit opatření odpovídající bezpečnostním požadavkům na zajištění důvěrnosti, integrity a dostupnosti informací zpracovávaných v informačních systémech veřejné správy.

Důvěrnost znamená zajištění přístupu k informacím pouze autorizovanými uživateli s potřebným oprávněním.

Integrita obnáší zajištění správnosti a úplnosti informací a procesů.

Dostupnost zajišťuje, že oprávnění uživatelé mají přístup k informacím a souvisejícím aktivům tehdy, kdy je potřebují nebo jsou jimi požadovány.

1.3. Cíle bezpečnostní politiky

Bezpečnostní politika stanoví pravidla pro zajištění bezpečného užívání IS úřadu. Dodržování těchto bezpečnostních pravidel je jednou ze základních podmínek pro zajištění bezpečného provozu ISVS a jeho ICT infrastruktury. Cílem je zejména zajištění trvalé a kvalitní informatické podpory činnosti úřadu, zajištění bezpečného přístupu k informacím a vymezení povinností a odpovědností ve vztahu k informační bezpečnosti. BP slouží také jako podklad pro školení uživatelů v oblasti informační bezpečnosti úřadu. Každý uživatel s oprávněním přístupu k informačnímu systému úřadu musí být s ustanoveními Bezpečnostní politiky seznámen a má za povinnost je dodržovat.

1.4. Odpovědnost

Každý zaměstnanec používající prostředky informačního systému úřadu je v rámci své činnosti zodpovědný za dodržování této bezpečnostní politiky a všech stanovených souvisejících předpisů tohoto OVS.

Pro ISVS úřadu jsou v oblasti jeho správy stanoveny, v souladu s ustanovením § 12 vyhl. č. 529/2006 Sb. o DŘ ISVS, vždy následující dvě role:

- **správce systému** – zaměstnanec nebo jiná fyzická osoba, která zajišťuje řízení provozu ISVS (nebo jeho stanovené části) – v případě MěÚ Černošice je to externí dodavatel ICT služeb,
- **bezpečnostní správce systému** – zaměstnanec nebo jiná fyzická osoba, která zajišťuje kontrolu bezpečnosti informačního systému veřejné správy. Činnost bezpečnostního správce ISVS je stručně popsán v tomto dokumentu a dále upravena interními bezpečnostními směrnicemi úřadu

Pro uživatele ISVS je v rámci úřadu standardně stanovena role „Uživatel“ jejímž nositelem je každý příslušně autorizovaný pracovník úřadu, využívající prostředky IS úřadu a podle rozhodnutí úřadu i případné další subjekty.

1.4.1 Činnost a odpovědnost bezpečnostního správce ISVS

Bezpečnostní správce ISVS úřadu (nebo jeho stanovené části) v oblasti zajištění odpovídající informační bezpečnosti odpovídá za provedení především ale nejenom následujících činností:

- Obecně: implementace stanovené bezpečnostní politiky ISVS úřadu
- Návrh, implementace, údržba, monitoring a vyhodnocování vhodných bezpečnostních opatření,
- Identifikace možných bezpečnostních hrozeb potenciálně ohrožující ISVS a návrhy opatření na snížení nebo eliminaci rizika jejich dopadu na informační aktiva,

- Spolupracovat se správcem systému v oblasti správy softwarové infrastruktury (aplikační programové vybavení, systémový sw, speciální sw, komunikační sw, networking, atd.) a **zajišťovat její provoz a užívání v souladu s bezpečnostními pravidly úřadu a další (pokud existuje) bezpečnostní dokumentací** (např. ustanovení o bezpečnosti: v provozní dokumentaci IS, k aplikacím, poskytovaným sw službám, systémovému software apod. od jejich dodavatelů, dále bezpečnostní ustanovení v SLA pro outsourcované služby, apod.)
- V rámci své stanovené kompetence udržuje / zajišťuje údržbu dostupné provozní dokumentace týkající se informační bezpečnosti ISVS úřadu v aktuálním stavu,
- upozorňuje vedení úřadu na nedostatky v oblasti bezpečnosti spravovaných ISVS,
- průběžně kontroluje stav zálohovacích systémů a ochranných sw systémů a aplikací (antiviry, anti spamy, firewally, DLP, IPS apod.), vyhodnocuje identifikované bezpečnostní útoky a učiněná zjištění eskaluje na stanovené funkční místo nebo odpovědný subjekt,
- řeší bezpečnostní incidenty ve spolupráci se stanoveným odpovědným (nadřízeným) pracovníkem,
- chrání data, technické a programové prostředky a služby poskytované informačními systémy úřadu všemi dostupnými prostředky před neautorizovaným přístupem.

1.4.2 Odpovědnost uživatele IS

Všichni uživatelé informačního systému úřadu jsou odpovídajícím způsobem poučeni o správném používání konkrétních aktiv informačního systému a seznámeni o postupech v nestandardních situacích.

Správné používání aktiv informačního systému úřadu je průběžně kontrolováno.

Úřad definuje sankce, které hrozí za porušení bezpečnostní politiky, provozního řádu počítačové sítě a dalších bezpečnostních postupů.

Odpovědnost každého uživatele IS úřadu jej zavazuje především, ale nejenom k následujícímu chování a činnostem:

- Řídit se ustanoveními provozního řádu počítačové sítě a ostatními interními směrnicemi úřadu.
- Chránit data a prostředky IS.
- Zabezpečit svěřené prostředky (počítač, aplikace, přidělené prostory na datových úložištích, svěřené datové nosiče, ...) proti přístupu neoprávněných osob.
- Hlásit stanoveným způsobem Odboru informatiky jakoukoliv závadu na prostředcích IS.
- Hlásit informatikům jakýkoliv incident v oblasti bezpečnosti IS.
- Nakládat s osobními údaji v souladu s platnou legislativou, dodržovat ustanovení zákona č.101/200 Sb., o ochraně osobních údajů, v platném znění.
- Nesdělovat nikomu své heslo pro přístup k IS a nesnažit se o získání cizí identity.

2. Bezpečnostní opatření

Zabezpečení jednotlivých aktiv informačního systému úřadu je dáno jejich hodnotou a charakterem zpracovávaných dat.

V dalších částech textu této BP jsou uvedena základní bezpečnostní opatření implementovaná pro ochranu dlouhodobých cílů stanovených v pro oblast bezpečnosti ISVS (vyhl. č. 529/2006 Sb., o DŘ ISVS, § 4, odst. 1), kterým jsou vždy:

- Bezpečnost dat, která jsou v těchto systémech zpracovávána,
- Bezpečnost technických a programových prostředků,
- Bezpečnost služeb, které jsou prostřednictvím těchto systémů poskytovány

2.1. Fyzická bezpečnost

2.1.1 Kontrola fyzického přístupu

Cílem fyzické bezpečnosti je zamezení neoprávněného přístupu do prostor úřadu a k prostředkům informačního systému úřadu.

V rámci těchto opatření je v budovách úřadu instalováno elektronické zabezpečovací zařízení (EZS). Bezpečnostní čidla jsou umístěna na chodbách a ve vytipovaných kritických prostorách. EZS je napojeno na pult centrální ochrany, ze kterého jsou v případě narušení objektů kontaktovány určené osoby.

Běžné kanceláře jsou v době nepřítomnosti zaměstnanců uzamčeny, a to i v případě jejich krátkodobého opuštění. Cizí osoby mohou do kanceláří vstupovat a pobývat tam pouze za přítomnosti zaměstnanců úřadu.

Každý uživatel je povinen po ukončení práce (nebo při přerušení práce na dobu delší než 30 minut) povinen ukončit všechny programy a provést odhlášení od systému, popřípadě uzamknout pracovní stanici heslem. Rovněž zabezpečí, aby na pracovišti nebyly volně přístupné dokumenty, datové nosiče a další informace.

Kritické prostředky informačního systému, jako jsou servery a centrální síťové prvky jsou umístěny ve zvláštních prostorách (serverovnách), do kterých mají přístup pouze zaměstnanci odboru informatiky, zaměstnanci servisní společnosti a tajemnice úřadu. Ostatní osoby (např. servisní technici nebo zástupci dodavatelů) tam mohou vstupovat pouze v jejich doprovodu. Pokud je nutné umístit centrální prvky sítě v běžných kancelářích nebo ve volně přístupných prostorách, jsou tyto prvky umisťovány do uzamykatelných rozvodných skříní (racků).

Síťové servery jsou vybaveny systémem nepřetržitého napájení elektrickým proudem (UPS) poskytujícím dostatečný časový prostor pro zastavení provozovaných aplikací a operačních systémů v případě výpadku dodávky elektrické energie. Serverovny jsou klimatizovány.

Do infrastruktury sítě jsou zabudovány takové síťové prvky, které dokáží zamezit neoprávněnému proniknutí do vnitřní sítě. Míra účinnosti závisí i na jejich umístění a vzájemném zapojení.

Všechna zařízení jsou provozována v souladu s doporučením výrobce.

2.1.2 Servery

Za server je považován takový hardware, který má nainstalovaný síťový operační systém nebo desktopový operační systém, který je využíván pro služby síťového provozu. Každý server musí splňovat požadavky na minimální bezpečnostní nastavení. Tyto požadavky jsou sestaveny v závislosti na použitém operačním systému a jsou průběžně aktualizovány.

Práce na konzolách serverů je povolena pouze administrátorům.

2.1.3 Přístup třetích stran

Třetí stranou se v rámci tohoto dokumentu rozumí pracovník dodavatele informačního systému (nebo jeho části) nebo jiného aktiva IS úřadu. Může se též jednat o technika specialistu, pracujícího na objednávku úřadu nebo o servisního pracovníka řešícího závadu na místě.

Takovéto osoby mohou přistupovat k prostředkům IS úřadu jen pod stálým dohledem pověřeného pracovníka úřadu.

Je-li přístup třetí strany realizován prostřednictvím dálkové správy, je to možné pouze za předpokladu, že se tak děje prostřednictvím zvláštního účtu s nejnutnějšími přístupovými právy.

2.1.4 Protipožární ochrana

Protipožární ochrana budov a dalšího majetku je řešena pomocí dalších vnitřních organizačních směrnic úřadu.

2.2. Bezpečnost SW infrastruktury ISVS

Pro řízení bezpečnosti má úřad implementován systém řízení bezpečnosti informací (ISMS) se zohledněním povinností vyplývajících ze zákona č. 101/2000 Sb., o ochraně osobních údajů.

Realizace **bezpečnosti** systémové infrastruktury (HW + SW), pomocí které je zajištěna požadovaná funkcionalita a služby tohoto ISVS, je řešena vlastními silami a v případě potřeby je zabezpečována dodavatelsky. V tomto ohledu se jedná zejména o outsourcing služeb pro podporu a údržbu SW, jako např. instalace nových verzí serverových operačních systémů, popř. operačních systémů klientských stanic, aplikačního SW, bezpečnostních a aplikačních service packů atd.

Pro centralizovanou správu, údržbu a aktualizaci SW a OS pracovních stanic se využívají příslušné SW nástroje a prostředky dle provozní dokumentace.

V průběhu procesu údržby a rozvoje technických a programových prostředků ISVS úřadu musí být zajištěno, že jak fyzický přístup, tak i přístup k funkcím a datům ISVS, pracovníků třetích stran, které tyto činnosti zajišťují, musí být pod odpovídající kontrolou bezpečnostního správce systému.

2.2.1 Uživatelské účty

Zřizování, aktualizace a rušení přístupů k informačnímu systému provádí určený pracovník (informatik) Odboru informatiky.

Zřízení, změna či zrušení uživatelského účtu je provedena odborem informatiky a je podmíněna doručením žádosti pomocí vyplněného formuláře – viz. příslušná příloha provozního řádu počítačové sítě.

V případě nástupu nového zaměstnance je zřízen nový přístup na základě požadavku vedoucího odboru, do kterého nový zaměstnanec nastupuje, nebo personalisty. Informatik pak zřídí uživatelský účet včetně přístupů k příslušným aplikacím a po poučení předá přístupové údaje zaměstnanci.

V případě převedení zaměstnance na jinou pracovní pozici aktualizuje informatik soubor přístupových oprávnění na základě požadavku vedoucího odboru nebo oddělení, do kterého je zaměstnanec převáděn.

V případě ukončení pracovního poměru zaměstnance informatik na žádost vedoucího odboru nebo oddělení zruší uživatelský účet a přidělená oprávnění odcházejícího zaměstnance. Zároveň provede zálohu osobních uživatelských dat a tuto zálohu uloží na určené místo.

2.2.2 Hesla

Hesla a podobné přístupové údaje jsou primární součástí bezpečnosti. Uživatelé jsou odpovědni za ochranu svých informací a proto dbají při práci s hesly zvýšené ostražitosti.

Uživatel nikdy nesděluje svá hesla další osobě a při podezření na vyzrazení příslušné heslo musí okamžitě změnit. Hesla nesmějí být nikde uložena v písemné podobě, je zakázáno je přeposílat pomocí elektronické pošty. Rovněž je zakázáno používat stejná hesla do různých systémů.

V rámci informačního systému úřadu smí být používána jen silná hesla, splňující následující požadavky:

- Minimální délka 8 znaků.
- Nesmí být založeno na jménech či osobních údajích.
- Obsahuje alespoň jednu číslici.
- Nesmí být totožné s předchozím heslem.

Uživatelská hesla jsou pravidelně (1 x ročně) obměňována, expirované heslo může být po uplynutí platnosti použito pouze 6x.

2.2.3 Rozsah oprávnění

Každý uživatel má takový rozsah přístupu k informačnímu systému, jaký odpovídá jeho pracovnímu zařazení. Přístup k informačnímu systému je uživateli přidělen až po náležitém poučení o jeho odpovědnostech a povinnostech. Přidělený přístup uživatele trvá jen po dobu jeho zaměstnaneckého (nebo obdobného) poměru.

Platí zásada, že privilegovaný přístup (nejvyšší úroveň oprávnění - např. systémoví administrátoři apod.) ke zdrojům ISVS se uděluje pouze výjimečně, a pokud je to možné, tak jen na určitou dobu.

Konkrétní oprávnění uživatelů přiděluje informatik, který odpovídá za vedení a aktualizaci evidence o uživatelích a jejich autorizaci ke zdrojům ISVS.

2.2.4 Antivirová a antispamová ochrana

Na každé uživatelské stanici s přístupem k informačnímu systému úřadu musí být nainstalován antivirový software, který je pravidelně, nejméně jedenkrát denně aktualizován. Stanice jsou rovněž v pravidelných intervalech kontrolovány na přítomnost virů. Antivirová ochrana stanic je centrálně spravována a monitorována.

Prostředky antivirové ochrany je rovněž kontrolována všechna příchozí a odchozí elektronická pošta.

Uživatelům je zakázáno:

- Vypínat prostředky antivirové ochrany na stanici během pracovní činnosti.
- Manipulovat s nastavením antivirového software.
- Přerušovat probíhající testy na přítomnost virů.

2.3. Bezpečnost dat

Pro dodržení vysoké míry datové bezpečnosti jsou na serverech použita disková pole RAID. Tak i v případě poruchy na jednom či dvou discích současně je možno dodržet nepřerušený provoz IS bez ztráty dat s minimálními náklady na jeho obnovu.

Zachování důvěrnosti dat platí pro celý IS úřadu, zvýšený důraz na bezpečnost je kladen na specializovaných pracovištích (úsek krizového řízení a kontroly, personální a mzdový útvar apod.).

2.3.1 Ochrana osobních údajů

Osobní údaje a citlivá data odpovídající definici zákona o ochraně osobních údajů (zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů) musí být zabezpečeny odpovídajícím způsobem proti zneužití a neoprávněnému přístupu.

Povinnosti vyplývající ze zákona č. 101/200 Sb., o ochraně osobních údajů jsou zohledněny v implementovaném systému řízení bezpečnosti informací (ISMS).

2.3.2 Zálohování dat

Pro případy nenadálé havárie a z ní vyplývající možné ztráty dat a dostupnosti poskytovaných služeb ISVS je nutné zabezpečit jejich co nejrychlejší obnovu.

Zálohování je prováděno pravidelně v potřebných intervalech a kopiích. Centrálně zálohována jsou pouze data (daty zde rozumíme kompletní provozní „datovou“ část produktivního systému ISVS - databáze, parametry pro nastavení, programy, a případné další komponenty provozní sw infrastruktury) umístěné na sdílených serverech. Data jsou zálohována na dvou oddělených lokalitách (Praha, Černošice).

Za proces realizace zálohování serverové části sw infrastruktury ISVS je odpovědný Odbor informatiky.

Za zálohování dat umístěných na lokálních stanicích jsou odpovědni konkrétní uživatelé, kterým je přidělen harmonogram provádění záloh a potřebná datová média.

Plán záloh je souhrn závazných pravidel pro centrální zálohování uživatelských dat v domovských a skupinových adresářích, centrálních databází a pošty. Na lokálně uložená data se plán záloh nevztahuje, pokud není uvedeno jinak. Uživatel má právo požadovat obnovení dat ze zálohy. Termín nejbližší použitelné zálohy určí odbor informatiky na základě plánu záloh. Obnovení dat v termínu kratším než 24 hodin není možné.

Plán obnovy po havárii je souhrn závazných pravidel pro obnovu činnosti částí počítačové sítě (serverů a úložišť dat) po jejich havárii. Obsahuje základní priority a termíny, v závislosti na potřebách subjektů a organizačních složek města Černošice, s přihlédnutím ke škodám, způsobeným nedostupností dat a služeb počítačové sítě.

2.3.3 Předávání dat

Veškeré evidence o předávání dat a informací mimo úřad musí být vedeny podle příslušných předpisů tak, aby bylo kdykoliv zjistitelné, jak bylo s daty manipulováno. Přitom se daty a informacemi ve smyslu tohoto ustanovení rozumí jak elektronické údaje v počítačích a na technických nosičích dat, tak i údaje na papírových mediích.

Data a informace mohou být oprávněné osobě předány jen v rozsahu daném prokazatelně jejím oprávněním nebo zmocněním.

Osobní data chráněná dle zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, v platném znění, může předat v souladu s platnými předpisy vždy jen pracovník k tomu oprávněný. Oprávněnost vyplývá z organizačního zařazení pracovníka a popisu jeho pracovní činnosti.

Jakékoliv identifikované pokusy o získání dat neoprávněnými osobami je třeba okamžitě oznámit přímo nadřízenému vedoucímu pracovníkovi.

2.4. Bezpečnost vazeb ISVS

Aktuálně platná zákonná ustanovení pro oblast ISVS a jejich vazeb rozlišuje dva přístupy k zajištění jejich bezpečnosti, které souvisejí s rolí ISVS. Bezpečnostní požadavky jsou odvozeny od toho, zda je ISVS v roli poskytovatele služby nebo v roli příjemce služby.

ISVS v roli poskytovatele služby

V případě, že se na konkrétní ISVS úřadu a jím poskytované služby vztahuje povinnost atestace referenčního rozhraní podle prováděcí vyhlášky (zákona o ISVS) č. 53/2007 Sb. o referenčním rozhraní, pak je bezpečnost této vazby a v rámci ní poskytovaných služeb zajištěna povinným atestem RR.

ISVS v roli příjemce služby

V případě, že je konkrétní ISVS v roli příjemce služby poskytované informačním systémem veřejné správy jiného správce – typický příklad je automatizovaná datová výměna mezi ISVS orgánu veřejné správy (např. územní samosprávní celek) a ISVS SZR (správa základních registrů), který poskytuje k ověření referenční data ze Základních

registrů (více viz dokumentace eGovernmentu, např. na portálu MVČR), pak musí ISVS v roli příjemce splňovat následující bezpečnostní požadavky:

- akceptovat technickou specifikaci rozhraní a bezpečnostní politiky poskytované služby publikované pro tento účel v dokumentaci k poskytované službě správcem ISVS poskytujícího služby,

- zabezpečit vhodným autentizačním procesem, že jeho ISVS v rámci vydání žádosti o vytvoření vazby s ISVS poskytujícím službu, komunikuje s autentickým ISVS (zabránit podvržení identity),

- zajistit přístup k požadované službě prostřednictvím funkcionality svého ISVS pouze příslušně autentizovaným a autorizovaným uživatelům,

- v případě potřeby realizovat v rámci této datové komunikace další bezpečnostní opatření vydaná bezpečnostním správcem informačního systému úřadu.

2.5. Bezpečnost provozu ISVS v režimu outsourcingu

Podle vyhl. č. 529/2006 Sb. o DŘ ISVS, má povinnost vypracovat bezpečnostní politiku ISVS také ten správce ISVS, který není jejich provozovatelem. V praxi se typicky jedná o ISVS jejichž provoz je zajišťován dodavatelsky, např. v hostingovém centru specializovaného dodavatele apod. V takovém případě je bezpečnost konkrétního ISVS dána zpravidla ustanoveními o zabezpečení jeho dat, dostupnosti jím poskytovaných služeb a zabezpečení jeho technických a programových prostředků ve smlouvě o úrovni poskytovaných služeb (SLA), uzavřené mezi správcem ISVS a jeho provozovatelem.

MěÚ Černošice provozuje své ISVS v režimu outsourcingu následující informační systémy:

- webové stránky města a aplikaci registru oznámení veřejných funkcionářů podle zákona 159/2006 Sb., o střetu zájmů, - obě aplikace jsou umístěny na prostředcích poskytovatele – Galileo Corporation, s.r.o. se kterým má město smluvně zajištěny podmínky provozu, zajištění bezpečnosti dat a úroveň poskytovaných služeb.

- Informační systém městské policie MP Manager - aplikace je umístěna na prostředcích poskytovatele – FT Technologies, a.s., se kterým má město rovněž smluvně zajištěny podmínky provozu, zajištění bezpečnosti dat a úroveň poskytovaných služeb.

3. Řešení bezpečnostních incidentů

Veškeré bezpečnostní incidenty v rámci ISVS jsou neprodleně řešeny bezpečnostním správcem systému.

Řešení incidentu má zpravidla následující průběh:

- Identifikace bezpečnostního incidentu.

  Incident je ihned po jeho zjištění nahlášen telefonicky a potvrzen v písemné formě (např. e-mail) bezpečnostnímu správci systému.

- Analýza incidentu.

  Bezpečnostní správce provede zjištění přesného rozsahu, a pokud je to možné i příčiny incidentu.

- Oznámení bezpečnostního incidentu.

  Po analýze rozsahu, příčin a možných důsledků jsou na bezpečnostní událost stanoveným komunikačním kanálem (prostřednictvím elektronické pošty, intranet úřadu, popř. telefonicky) bezpečnostním správcem systému upozorněni všichni nebo dotčení uživatelé IS, a současně je jim sdělen rozsah dočasných omezení provozu informačního systému (pokud k nim v důsledku incidentu dojde).

- Nouzový režim provozu ISVS.

  Je-li to relevantní a vyžaduje-li to konkrétní situace (zejména potrvá-li odstranění následků incidentu delší dobu), stanoví bezpečnostní správce ve spolupráci se správcem systému a tajemnicí úřadu (v případě potřeby také s vedoucími dotčených útvarů) náhradní nouzový režim provozu IS. Bezpečnostní správce systému a správce systému vydají potřebné pokyny pro nouzový režim provozu ISVS platné až do jeho odvolání.

- Následky incidentu jsou odstraněny.

  Celý průběh včetně řešení je zaevidován. Pokud byl stanoven nouzový režim provozu IS, je tento po otestování správné funkčnosti IS odvolán. Záznamy o průběhu, důsledcích a řešení bezpečnostní události musí být uloženy a chráněny proti neautorizované manipulaci.

- Vyhodnocení incidentu a přijetí opatření.

  Podle charakteru incidentu jsou vyvozeny důsledky. Jedná se například o vznik nového požadavku na IS úřadu, který zabrání opakování stejné, změnu či doplnění interních směrnic úřadu, poučení uživatelů, proč k incidentu došlo, apod.

V případě ohrožení důvěrnosti dat v IS OVS je v obecném smyslu postupováno podle platné legislativy ČR, této Bezpečnostní politiky a dalších relevantních interních směrnic úřadu.

4. Vysvětlení použitých zkratek a pojmů

4.1. Zkratky

BP	dokument Bezpečnostní politika ISVS,
DLP	data loss prevention – systém zachování bezpečnosti při zachování přístupnosti
DŘ ISVS	dlouhodobí řízení informačních systémů veřejné správy (více viz zákon o ISVS a jeho prováděcí vyhlášky),
HW	hardware,
IPS	intrusion prevention system – systém pro prevenci průniku do IS
IS	informační systém,
ISVS	informační systém veřejné správy ve smyslu zákona o ISVS a jeho prováděcích předpisů,
OVS	orgán veřejné správy,
OVM	orgán veřejné moci,
RR	referenční rozhraní,
SLA	service level agreement - dohoda o úrovni poskytovaných služeb mezi dodavatelem a zákazníkem.
SW	software,

4.2. Pojmy

Outsourcing

činnosti zajišťované externími zdroji na základ smlouvy,

Referenční rozhraní ISVS

viz zákon o ISVS, §2, písm. j): způsobilost k realizaci vazeb ISVS s jinými ISVS prostřednictvím tzv. referenčního rozhraní. Toto rozhraní je v rámci metodiky MVČR definováno jako souhrn právních, technických, organizačních a jiných opatření vytvářejících jednotné integrační prostředí inf. systémů veřejné správy, které poskytuje kvalitní soustavu společných služeb, včetně služeb (viz níže) výměny oprávněně vyžadovaných informací mezi jednotlivými SVS orgánů veřejné správy,

Služba

činnost informačního systému uspokojující dané požadavky oprávněného subjektu spojená s funkcí informačního systému; podle platné metodiky pro oblast RR od MVČR: služba je reakce (a činnost) informačního systému na žádost o službu nebo informace,

Správce ISVS

viz zákon o ISVS, §2, písm. c): správcem ISVS je subjekt, určující podle tohoto zákona účel a prostředky zpracování informací a za informační systém odpovídá,

SW infrastruktura

soubor softwarového vybavení umožňující požadovanou funkčnost ISVS; zejména se jedná o

- systémový software (operační systémy a jejich součásti, komunikační software, databázové systémy, webové servery, middleware, zálohovací softwarové systémy atd.), dále o
- aplikační software, jako jsou modulární informační systémy, samostatné speciální aplikace, kancelářské programy, a
- komunikační a speciální software (sw v oblasti networking, webové služby atd.),

Vazba

viz zákon o ISVS, §2, písm. s): vazbou mezi ISVS je vzájemné nebo jednostranné poskytování služeb a informací; příslušná metodika MVČR pro ISVS upřesňuje, že jde o automatizované vzájemné nebo jednostranné poskytování služeb a informací,

Zákon o ISVS

zákon č. 365/2000 Sb., o informačních systémech veřejné správy a změně některých dalších zákonů, ve znění pozdějších předpisů.

5. Literatura, zdroje

- Zákon č. 365/2000 Sb. o ISVS a změně některých dalších zákonů, ve znění pozdějších předpisů.
- Vyhláška č. 529/2006 Sb. o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality ISVS (vyhláška o dlouhodobém řízení ISVS).
- Vyhláška č. 53/2007 Sb. o technických a funkčních náležitostech uskutečňování vazeb mezi ISVS prostřednictvím referenčního rozhraní (vyhláška o referenčním rozhraní).
- Metodika MVČR vydaná pro oblast ISVS, zveřejněno na webu MVČR http://www.mvcr.cz/metodicke-pokyny.aspx

Atestační středisko pro ISVS

RELSIE spol. s r.o., Na Valentince 644/15, PRAHA 5, IČ 62417339 DIČ CZ62417339

Atestační středisko pro ISVS, jako příslušná součást inspekčního orgánu A-TEST, akreditovaného u Českého institutu pro akreditaci o.p.s., zřízeného společností RELSIE spol. s r. o., která je atestačním střediskem pověřeným k výkonu atestací MVČR ve smyslu § 6 zákona 365/2000 Sb., ve znění pozdějších předpisů, rozhodnutím číslo MV/66271-2/EG-2016 ze dne 29. dubna 2016, vydává v souladu s metodickým pokynem IO-MP-365:

ATEST
reg. číslo: 01-20161201

ORGANIZACE: Město Černošice

REGISTROVANÉ SÍDLO: Riegrova 1209, 252 28 Černošice

ATEST VYDÁN DNE: 6. 12. 2016

PLATNOST ATESTU DO: 30. 11. 2021

PLATNOST PRODLOUŽENA DO: –

STUPEŇ HODNOCENÍ: Splňuje

ROZSAH ATESTACE

Stanovení shody dlouhodobého řízení informačních systémů veřejné správy s požadavky zákona 365/2000 Sb., ve znění pozdějších předpisů, a prováděcí vyhlášky 529/2006 Sb., ve znění pozdějších předpisů k tomuto zákonu.

Tento atest osvědčuje shodu v rozsahu atestace.

I 4042

Platnost tohoto atestu je stanovena v souladu se zákonem 365/2000 Sb., ve znění pozdějších předpisů.

Proti tomuto rozhodnutí je možné se odvolat k řediteli Inspekčního orgánu A-TEST.

V Praze dne 6. 12. 2016

Ing. Martin Dudek
ředitel atestačního střediska pro ISVS

ID projektu: A20161201