MĚSTO JESENÍK

BEZPEČNOSTNÍ POLITIKA ISVS

ATESTAČNÍ MINIMUM

Verze 1.0
Září 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 Jeseník (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 nedílnou součástí souboru bezpečnostních směrnic úřadu.

1.1. Základní údaje o Bezpečnostní politice ISVS

Název dokumentu:	Bezpečnostní politika ISVS Města Jeseník
Datum dokončení:	9. 9. 2016
Datum schválení:	12. 9. 2016
Způsob schválení:	Schváleno tajemníkem MěÚ Jeseník
Doba platnosti:	5 let
Platnost od kdy:	12.9.2016
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. od 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 Jeseník 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

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

- chránit prostředky informačního systému, k nimž mu byl udělen přístup
- přijmout odpovědnost za aktiva jemu svěřené,
- hlásit bezpečnostním správci systému veškeré zjištěné nedostatky v zabezpečení IS, a uživatelsky identifikované bezpečnostní incidenty nebo podezření na ně,
- dodržovat ustanovení Bezpečnostní politiky ISVS, Provozního řádu IS a dalších závazných směrnic úřadu, relevantních k oblasti bezpečného provozu ISVS.

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

Úřad využívá ke střežení svých objektů [redacted]

Běžné kanceláře - pracoviště s PC a periferiemi - jsou [redacted]

Klíčová aktiva IS úřadu – servery a centrální aktivní prvky počítačové sítě jsou umístěny ve zvláštních prostorách – serverovnách [redacted]

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 nastaven. Tyto požadavky jsou sestaveny v závislosti na použitém operačním systému a jsou průběžně aktualizovány.

[redacted]

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 vnitroorganizačních směrnic úřadu.

2.2. Bezpečnost SW infrastruktury ISVS

Realizace **bezpečnosti** softwarové infrastruktury, pomocí které (a nezbytné technické ICT infrastruktury) je zajištěna požadovaná funkcionalita a služby tohoto ISVS, je řešena ve spolupráci s dodavateli. 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

Prvotní požadavek na vytvoření přístupu uživatele k IS je zřízen na základě pokynu jeho vedoucího nebo přímého nadřízeného.

Každý uživatel IS úřadu musí mít svůj vlastní uživatelský účet. Uživatel nese plnou odpovědnost za všechny činnosti v informačním systému, které byly vykonány pod jeho uživatelským účtem.

Účet pracovníka, jehož pracovní poměr byl ukončen, je uzamčen a zablokován.

2.2.2 Hesla

Heslem se rozumí posloupnost znaků používaná pro ověření totožnosti uživatele. Zadávání hesel představuje základní ověřovací mechanismus v IS úřadu.

Každý uživatel si musí být vědom svojí osobní odpovědnosti za správnou práci s hesly. Uživatel je při zadávání hesla povinen chovat se tak, aby heslo nemohla zjistit a zneužít neoprávněná osoba. Zároveň si každý musí uvědomit, že je nutné důsledné odhlašování při skončení nebo dlouhodobějším přerušení práce.

Hesla jsou konstruována tak, aby:

- byla delší než [redacted]

- nebyla snadno odhadnutelná [redacted]

[redacted]

2.2.3 Rozsah oprávnění

Rozsah oprávnění uživatelského účtu stanoví, není-li zvláštním předpisem stanoveno jinak, přímý vedoucí uživatele (u pracovníků úřadu), popřípadě tajemník úřadu (u jiných osob).

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 externí dodavatel ICT služeb, který odpovídá za vedení a aktualizaci evidence o uživatelích a jejich autorizaci ke zdrojům ISVS.

2.2.4 Antivirová a antispamová ochrana

Na každé stanici připojené do počítačové sítě úřadu musí být nainstalován a zprovozněn antivirový, a antispamový systém, provádějící nepřetržitou antivirovou/antispamovou kontrolu a celkovou kontrolu stanice, automaticky naplánovaným spouštěním příslušné aplikace. Pro antivirovou a antispamovou ochranu stanic, serverů i pro ochranu elektronické pošty se používá odpovídající bezpečnostní aplikace, jejichž aktualizace je prováděna zpravidla automatizovaně prostředky vzdálené správy.

Nefunkčnost antivirového/antispamového systému nebo zjištění viru/spamu je nutné ihned oznámit bezpečnostnímu správci systému, který prošetří příčinu a zajistí nápravu.

2.3. Bezpečnost dat

Pro dodržení vysoké míry datové bezpečnosti je na serverech použito [redacted]

Zachování důvěrnosti dat platí pro celý IS úřadu, zvýšený důraz na bezpečnost je kladen na specializovaných pracovištích (obrana, krizové řízení, 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.

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 [redacted]

[redacted] Za proces realizace zálohování serverové části sw infrastruktury ISVS je odpovědné Oddělení informatiky.

Za zálohování dat umístěných na lokálních stanicích jsou odpovědni konkrétní uživatelé.

Kontrola technického stavu záloh

- Vytvořené zálohy musí být pravidelně kontrolovány, zda jsou v takovém technickém stavu, že z nich lze požadovanou obnovu kompletního ISVS (sw, data) provést.
- Kontrolu technického stavu vytvořených záloh provádí Oddělení informatiky.
- O provedení takové kontroly vede bezpečnostní správce průkazné záznamy, které musí být odpovídajícím způsobem chráněny před zničením nebo neoprávněným zásahem.
- Každá záloha musí být patřičně označena všemi potřebnými a požadovanými údaji (co obsahuje záložní médium, datum vytvoření, expiraci atd.).

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 Jeseník provozuje v režimu outsourcingu [redacted]

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 tajemníkem 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 syslu 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,
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