Bezpečnostní politika IS

Městská část Praha – Kunratice

2015 - 2020

Zpracováno podle požadavků zákona č.365/2000 Sb.,
o informačních systémech veřejné správy (ISVS)

Obsah

Seznam zkratek a pojmů

AIS – Agendový informační systém

DNS – Doménový server

HMP – Hlavní město Praha

ICT – Informační a komunikační technika

IK – Informační koncepce ISVS

IS – Informační systémy

ISMS – Systém řízení bezpečnost informací (Information Security Management System)

ISVS – Informační systémy veřejné správy

ISZR – Informační systém základních registrů (správce MV, provozovatel Správa ZR)

MČ – Městská část

MHMP – Magistrát hlavního města Prahy

NDA – Smlouva o mlčenlivosti

OVM – Orgán veřejné moci

OVS – Orgán veřejné správy

SLA – Smlouva o technické podpoře

SZR – Správa základních registrů

Důvěrnost – zajištění přístupu k informacím pouze autorizovaným uživatelům s potřebným oprávněním.

Integrita – zajištění správnosti a úplnosti informací a procesů.

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

1 Identifikační údaje

Organizace		
Název organizace:	Městská část Praha – Kunratice	
Typ organizace:	Orgán veřejné správy - Obec s výkonem přenesené působnosti v základním rozsahu	
Bezpečnostní politika IS		
Aktuální verze:	1.0	
Počátek platnosti:	12.března 2015	
Konec platnosti	Do odvolání	
Schvalovatel:	Zastupitelstvo MČ Praha-Kunratice	
Datum schválení	11.března 2015	
Platná verze Informační koncepce	1.0	

1.1 Předchozí verze Bezpečnostní politiky IS

V této kapitole jsou uvedeny všechny změny provedené v dokumentu, tak jak byly po jeho schválení postupem času prováděny. Změny dokumentu jsou prováděny především po zásadních změnách v oblasti bezpečnosti IS, případně na základě odborných auditů a studií.

Změny ve verzi BP IS			
Verze	**Popis**	**Důvod**	**Lokalizace změny**

Tabulka 1-1 Změny ve verzi BP IS

2 Zdroje a východiska

2.1 Právní podklad tohoto dokumentu

Bezpečnostní politika IS MČ byla zpracována na základě požadavku zákona č. 365/2000 Sb., o ISVS a jeho prováděcí vyhlášky č. 529/2006 Sb.

Související legislativa:

- zákon č. 101/2000 Sb., o ochraně osobních údajů;
- zákon. č. 111/2009 Sb., o základních registrech

Při zpracování bezpečnostní politiky IS byla využita řada norem ČSN ISO/IEC 27000

Související dokumenty

Bezpečnostní opatření uvedená v této bezpečnostní politice IS vychází z cílů stanovených v dokumentu:

- **Informační koncepce ISVS**

3 ÚVOD

Bezpečnostní politika IS představuje dokument vycházející z požadavků zákona č. 365/2000 Sb., o ISVS a jeho prováděcí vyhlášky č. 529/2006 Sb., o dlouhodobém řízení ISVS. Bezpečnostním politika IS je součástí provozní dokumentace ISVS a jako dokument je společně s Informační koncepcí ISVS předkládán k atestaci dlouhodobého řízení ISVS.

Bezpečnostní politika IS obsahuje popis bezpečnostních opatření, která orgán veřejné správy uplatňuje při zajišťování bezpečnosti ISVS. Součástí Bezpečnostní politiky IS jsou i opatření definovaná Správou základních registrů pro případ napojení agendového IS na ISZR (viz příloha č.1).

Bezpečnostní politika IS se vztahuje na všechny IS provozované na MČ Praha-Kunratice.

Předmětem této bezpečnostní politiky není ochrana utajovaných informací podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti.

3.1 Cíle a rozsah

Cílem tohoto dokumentu je stanovení základních bezpečnostních pravidel pro provoz, používání a údržbu informačních technologií Úřadu MČ Praha-Kunratice v souladu s aktuální verzí Informační koncepce ISVS, jež mají zajistit požadovanou úroveň informační bezpečnosti v rámci IS MČ.

3.2 Závaznost

Bezpečnostní politika IS je závazným interním předpisem a je součástí celkového bezpečnostního systému úřadu.

Dodržování Bezpečnostní politiky IS je vyžadováno u všech (interních i externích) uživatelů IS bez rozdílu funkce či zařazení, tj. včetně pracovníků externích organizací zajišťujících servis ICT.

4 Organizace bezpečnosti

4.1 Role a odpovědnosti

Bezpečnostní politika IS je ustanovena vedením MČ, které odpovídá za celkové zajištění bezpečnosti na MČ.

Vedení MČ Praha - pověřuje řízením bezpečnosti IS tajemníka MČ Praha-Kunratice,

Tajemník dále:

- zodpovídá za dodržování bezpečnosti IS MČ,
- spolupracuje s vedením MČ a správci IS,
- řídí zavádění bezpečnostních opatření podle definovaných bezpečnostních cílů,
- průběžně organizuje monitoring bezpečnostních incidentů a účinnost bezpečnostní politiky a ověřuje funkčnost zavedených bezpečnostních opatření,
- podílí se na zvyšování bezpečnostního uvědomění uživatelů IS,
- navrhuje hlavní kroky vedoucí ke zvýšení bezpečnosti dat a prostředků v IS,
- navrhuje specifické role a odpovědnosti v oblasti bezpečnosti IS v rámci celého úřadu,
- navrhuje metody a postupy v oblasti bezpečnosti IS,
- zajišťuje, aby dodavatelé služeb dodržovali bezpečnostní politiku úřadu a ostatní relevantní vnitřní předpisy.

je oprávněn navrhovat nezbytná opatření k zajištění bezpečnosti IS.

Správce IS

Správce IS je odpovědný za správu lokální počítačové sítě a připojení k externím subjektům včetně internetu, je výkonným článkem řízení bezpečnosti počítačových sítí.

Dále provádí vzdálenou správu a monitorování stavu sítě a klíčových prvků sítě, servis a instalaci výpočetní techniky včetně příslušného SW vybavení zapojeného v síti úřadu, poskytování odborné pomoci uživatelům.

Uživatel

Uživatelem je každá fyzická nebo právnická osoba, jíž byl přidělen přístup k IS a příslušná přístupová oprávnění do informačního systému úřadu. Jedná se o zaměstnance v zaměstnaneckém poměru k úřadu, volené zástupce městské části (RMČ a ZMČ), praktikanty, stážisty, brigádníky, ale i pracovníky třetích stran (servisní organizace apod.).

.

5 Klasifikace a řízení aktiv

Všechna aktiva na MČ musí být identifikována. Aktiva IS MČ se dělí do těchto kategorií:

- fyzická aktiva – veškeré HW vybavení, počítače, sítě, technická zařízení, budovy a ostatní vybavení, dodávky energie, vody, tepla, klimatizace, osvětlení;
- softwarová aktiva – programové vybavení, operační systémy, technologie, SW aplikace a dílčí (samostatné) informační systémy, agendy, zdrojové kódy aplikací vyvíjených externími dodavateli, speciální systémy a jejich nastavení;
- informační aktiva – veškerá data, informace a údaje zpracovávané v IS ;
- lidské zdroje ;
- služby – služby pro veřejnost, resp. pro zaměstnance MČ.

5.1 Klasifikace informačních aktiv

Informační aktiva mají z hlediska své povahy různé požadavky na zajištění informační bezpečnosti. Za účelem přijetí opatření jsou na MČ stanoveny následující kategorie klasifikace informací:

- **osobní údaje** – informace dle zákona č. 101/2000 Sb., o ochraně osobních údajů
- **interní** – neveřejné informace určené pouze pro příslušné zaměstnance MČ
- **veřejné** – informace určené veřejnosti za účelem výkonu veřejné správy

Na základě výše uvedené klasifikace přijímají vedoucí zaměstnanci přiměřená bezpečnostní opatření pro zajištění bezpečnosti dané kategorie.

- **osobní údaje** – vysoká míra zabezpečení v souladu s požadovanou legislativou
- **interní** – opatření jsou implementována z důvodu zajištění dostupnosti informací
- **veřejné** – opatření jsou přijímána s důrazem na zajištění správnosti (integrity) informací

Nakládání s danými informacemi mohou dále upravovat interní směrnice MČ.

6 Personální bezpečnost

7.1 Povinnosti zaměstnanců a uživatelů

Povinnosti zaměstnanců úřadu a všech uživatelů, jimž byl přidělen přístup k IS MČ:

- dodržovat schválená pravidla informační bezpečnosti daná bezpečnostní dokumentací a interními směrnicemi;
- chránit osobní údaje dle zákona č. 101/2000 Sb. (výslovně zakotvena v pracovní smlouvě každého zaměstnance);
- dodržovat pravidla ochrany informací v souladu se stupněm jejich klasifikace;
- zachovávat mlčenlivost o všech chráněných skutečnostech, s nimiž přijdou do styku při plnění svých pracovních povinností;
- využívat IS jen v souladu s uživatelskými postupy;
- používat pouze legálně získaný software,
- využívat ICT k pracovním účelům,
- převzít odpovědnost za bezpečné nakládání s ICT a ochranu informací ve své působnosti.

Každý uživatel je dále povinen se seznamovat s bezpečnostními směrnicemi, navazující dokumentací o používání IS a pravidly pro práci v něm.

7.2 Dohoda o mlčenlivosti

Všichni zaměstnanci pracující na pozicích zajišťujících provoz, správu, údržbu a rozvoj technologických úloh musí být zavázáni mlčenlivostí. Ujednání o mlčenlivosti a dodržování důvěrnosti klasifikovaných informací úřadu je uvedeno v pracovní smlouvě nebo v dodatku ke smlouvě (případně popisu pracovního místa).

Povinnost mlčenlivosti je uplatňována také prostřednictvím smluv s externími pracovníky a institucemi (NDA), jež při plnění pracovních povinností, poskytování služeb či prací mohou přijít do styku s těmito informacemi.

Zahrnutí bezpečnosti do pracovních povinností / odpovědností

Každý zaměstnanec nese svůj díl zodpovědnosti za bezpečnost a ochranu informací, se kterými přichází při plnění svých pracovních povinností do styku. Tato odpovědnost je zakotvena jednak v pracovní smlouvě, jednak v popisu práce zaměstnance pro danou funkci.

7.5 Během pracovního poměru

Vstupní školení

Všichni uživatelé IS MČ musí být při nástupu nebo nejpozději před zahájením používání IS (převzetí uživatelského přístupu) prokazatelně seznámeni s Bezpečnostní politikou IS a navazující dokumentací - proškoleni v bezpečnostních pravidlech, zásadách a platných směrnicích pro uživatele IS. To se týká jak stálých zaměstnanců, tak i zaměstnanců na časově omezenou dobu práce s IS, stážistů, servisních pracovníků a pracovníků outsourcingu.

Evidenci záznamů o školení, požadavků na vzdělávání v oblasti bezpečnosti IS vede pověřený zaměstnanec/odbor/oddělení, které je odpovědné za vzdělávání zaměstnanců.

7.6 Ukončení nebo změna pracovního poměru

Zaměstnanec musí při ukončení pracovního poměru uspořádat a předat všechny písemnosti včetně dat a informací uložených na používaných prostředcích výpočetní techniky přímému nadřízenému. O předání musí být vedoucím příslušného oddělení/odboru vytvořen záznam ve výstupním listu.

Zaměstnanec je povinen nejpozději v den ukončení pracovního/služebního poměru předat výstupní list se všemi příslušnými záznamy pověřenému zaměstnanci/odboru/oddělení, které je založí do příslušného personálního spisu.

7 Fyzická bezpečnost a bezpečnost prostředí

Fyzické zabezpečení IS v objektech úřadu je realizováno několika prvky ochrany použitými v závislosti na hodnotě aktiv ICT a finančních možnostech MČ. V rámci ochrany IS MČ využívá minimálně některý z následujících prvků ochrany:

- ostraha (bezpečnostní služba),
- zámky dveří,
- mříže v oknech,
- kamerový systém se záznamem (CCTV),
- autentizační zařízení pro řízení vstupu osob budovy na základě čipových karet,
- EZS (elektronický zabezpečovací systém),
- EPS (elektronický protipožární systém).

7.1 Bezpečnostní perimetr

V rámci MČ jsou dané prostory klasifikovány jako:

- veřejné – přístup do veřejných prostor je určen veřejnosti,
- neveřejné prostory – přístup do neveřejných prostor je umožněn pouze oprávněným zaměstnancům MČ, případně třetím stranám s doprovodem či na základě platné smlouvy.

Konkrétní klasifikaci daných prostor provádí zaměstnanec pověření vedení MČ realizací bezpečnostní politiky IS.

7.1.1 Fyzický přístup

Fyzický přístup k prostředkům IS je vyhrazen pouze povolaným osobám – uživatelům IS, a to pouze na základě pracovní smlouvy (zaměstnanci), případně na základě jiného smluvního vztahu (servisní a dodavatelské organizace, dohody o provedení práce apod.) nebo se souhlasem určené odpovědné osoby, kterou může být např. Starosta, Tajemník, vedoucí odboru.

7.1.1.1 Serverovna

Přístup do serverovny je povolen pouze **oprávněným** zaměstnancům MČ.

Pohyb cizích osob v prostorách serverovny (úklid, servisní zásah dodavatelů třetích stran, revize zařízení apod.) je možný pouze v doprovodu odpovědných pracovníků MČ.

7.1.1 Správa klíčů

Klíče od jednotlivých místností mají k dispozici pouze oprávnění zaměstnanci MČ , kteří jsou povinni předcházet jejich ztrátě, krádeži či poškození.

Klíče ke společným místnostem, které jsou k dispozici většímu množství zaměstnanců MČ, musí být uloženy v neveřejných prostorech v uzamykatelném boxu.

8 Bezpečnost vybavení a zařízení

Uživatelé IS jsou povinni chránit zařízení před krádeží a poškozením:

- Přenosná zařízení notebooky nenechávat mimo budovu bez dozoru (např. v autě);
- Zabránit styku zařízení s kapalinou;
- Vystavovat zařízení vysokým teplotám;
- Vystavovat zařízení mechanickým nárazům;
- Rozebírat, opravovat, měnit komponenty zařízení pokud tato činnost není součástí jejich pracovní náplně;
- Využívat zařízení v souladu s příslušným manuálem.

Ochrana napájení – zdroje energie

Hlavní centrální zařízení počítačové sítě, tj. zejména servery, jsou zabezpečeny před poklesem, kolísáním či výpadkem elektrické energie samostatným náhradním zdrojem – aktivním UPS. Tento zdroj energie musí umožnit uživatelům dostatečný čas pro bezpečné uložení dat a korektní ukončení činnosti serverů a dalších zařízení komunikační infrastruktury při dlouhodobější poruše.

9 Řízení komunikací a provozu

9.1 Bezpečnost při zacházení s médii

V rámci IS MČ mohou uživatelé používat média (např. USB flash disky, zapisovatelná média CD a DVD). Před prací s přenosným médiem musí uživatel provést antivirovou kontrolu přenosného média.

Uživatel, který uložení informací provedl, je dále zodpovědný za ochranu informací, které na přenosné medium uložil. Na přenosná média nesmí být ukládány osobní nebo důvěrné informace, v případě nutnosti uložení takových informací, musí být před uložením zašifrovány.

Při ztrátě, odcizení nebo poškození média je uživatel informačního systému povinen informovat bez zbytečného odkladu správce IS.

Bezpečnou likvidaci dat nebo médií zajistí, na vyžádání uživatele informačního systému, správce IS.

9.2 Ochrana před škodlivým malwarem

Všechny koncové stanice uživatelů IS a servery provozované v prostředí MČ musí být chráněny před škodlivým malwarem odpovídající ochranou (např. antivirová ochrana, IPS). Tato ochrana musí plnit jak detekční funkce, tak preventivní opatření k zabránění průniku nebo rozšíření škodlivého malwarem do IS MČ.

Všechny stanice jsou pravidelně kontrolovány antivirovým programem na přítomnost malwaru a musí mít povinně zapnutou rezidentní antivirovou ochranu.

Za aktualizaci antivirové ochrany odpovídá správce IS.Uživatelé IS MČ nesmí bez souhlasu správce IS vypínat antivirovou ochranu.

9.3 Zálohování

V rámci IS MČ Praha - je prováděno pravidelné zálohování dat takovým způsobem, aby v případě incidentu bylo možné tato data zpětně k danému datu obnovit.

K záložním souborům IS mají přístup pouze oprávnění zaměstnanci MČ.

Za proces zálohování a obnovy odpovídá správce IS.

10 Řízení přístupu

10.1 Řízení přístupu uživatelů

Uživatelé IS MČ mají vždy zřízen přístup pouze do těch částí IS MČ, které potřebují pro výkon svých činností.

Přístup pro konkrétní uživatele definuje tajemník MČ Praha-Kunratice. V případě ukončení potřeby daného zaměstnance MČ je přístup k IS odebrán.

Nastavení přístupů zaměstnanců MČ provádí správce IS a tajemník.

10.2 Zabezpečeni přístupu

Zaměstnanci jsou povinni dle pokynů správce IS zabezpečit přístup k IS a informacím (v elektronické i tištěné podobě) před zneužitím, poškozením či krádeží jak v mimopracovní době, tak i v případě krátkodobého opuštění pracoviště.

V případě krátkodobého opuštění pracoviště musí uživatel minimálně uzamknout pracovní plochu (klávesová zkratka tlačítko Windows + L).

Každý uživatel IS musí mít nastaven spořič obrazovky s heslem. Aktivace spořiče je nastavena na 30 minut při nečinnosti.

Povinnosti fyzické ochrany se vztahují i na mobilní prostředky výpočetní techniky (přenosné počítače, notebooky, média apod.).

10.3 Bezpečnost přístupu třetích stran

Provozovaný IS MČ včetně zpracovávaných informací a používaných technologií vyžadují v některých případech přístup tzv. třetích stran, jedná se např. o servisní zásahy pracovníků dodávajících SW či HW nebo poskytujících podporu IS.

Pokud provozovaný IS vyžaduje přístup tzv. třetích stran, ať se jedná o fyzický či logický přístup nebo o časově omezenou činnost externích pracovníků (pracovníci třetí strany), musí být přístup třetích stran řešen v souladu s Bezpečnostní politikou IS tak, aby byla zajištěna adekvátní úroveň bezpečnosti informací.

Jakákoliv spolupráce s externí organizací musí být ošetřena smluvně, zejména z pohledu bezpečnosti a odpovědnosti za možná rizika ve vztahu k IS MČ.

Požadavek třetích stran na zřízení přístupu k IS úřadu, musí být vždy schválen oprávněným zaměstnancem MČ.

10.4 Bezpečnostní požadavky ve smlouvách, outsourcing

Dodavatelské a smluvní vztahy (smlouvy uzavírané s dodavateli, případně odběrateli a jinými externími subjekty) a především vlastní přístup (fyzický či logický) třetích stran k IT/IS musí být dostatečně řízen.

Tam, kde vznikne potřeba přístupu třetí strany, musí být provedeno zhodnocení rizik plynoucích z tohoto přístupu tak, aby se zjistily důsledky z hlediska bezpečnosti a aby se definovaly požadavky na bezpečnostní opatření. Opatření musí být schválena a definována ve smlouvě se třetí stranou.

Vedení MČ odpovídá za to, že veškeré bezpečnostní požadavky na ochranu ICT jsou zakotveny ve smluvních vztazích se třetími stranami ještě předtím, než je povolen adekvátní přístup k IS, případně k technické dokumentaci IS, a pouze v rozsahu nezbytně nutném pro výkon smluvních závazků.

Dodavatel se musí zavázat také k tomu, že bude (a všichni jeho pracovníci) dodržovat relevantní interní předpisy MČ. Ve smlouvách s těmito subjekty musí být definována povinnost mlčenlivosti a ochrany dat včetně informací, na které se vztahuje platná legislativa (typu osobních údajů ap.), rozsah odpovědnosti za škody způsobené činností v IS a v odůvodněných případech také např. autorská práva (majetková autorská práva), případně licenční ujednání k oprávnění výkonu majetkových práv.

Ve smlouvách musí být definován rozsah odpovědnosti za škody způsobené činností v IS a povinnosti, které jsou pro tyto subjekty závazné.

11 Heslová politika

Heslo k IS MČ musí splňovat minimální parametry:

- délka hesla min. 6 znaků,
- obsahuje min. jednu číslici,
- obsahuje min. jedno velké písmeno.

Uživatelé IS udržují heslo v tajnosti a nesdělují je ostatním zaměstnanců MČ či třetím osobám. Heslo lze jiným osobám sdělit pouze v naléhavém případě, jehož dopad by mohl ovlivnit chod organizace či ohrozit bezpečnost obyvatel MČ. V takovém případě musí majitel hesla bez zbytečného odkladu heslo změnit.

Hesla nesmí být zaznamenána v blízkosti daného přístupu k IS MČ, tak aby byla snadno čitelná i neoprávněnými osobami (uvedena na monitoru, pracovní desce atd.)

V případě zapomenutí hesla kontaktují uživatele IS příslušného správce IS.

12 Hlášení bezpečnostních incidentů

Všichni uživatelé IS úřadu jsou povinni hlásit zjištěné závady v IS, bezpečnostní incidenty a slabiny telefonicky nebo emailem správci IS případně vedoucím zaměstnancům.

13 Řízení zachování kontinuity činností

Pro případ výpadku některé části IS MČ musí být uživatelé seznámeni s postupy, které zajistí obnovu dané části IS.

14 Přílohy

Příloha č. 1 - Bezpečnostní požadavky na AIS pro připojení k produkčnímu prostředí Základních registrů

Ing. Lenka **A l i n č o v á**

starostka MČ

Jitka **V o ř í š k o v á**

tajemnice ÚMČ

V Praze dne 30.4.2015