



**MĚSTSKÁ ČÁST PRAHA 5
ÚŘAD MĚSTSKÉ ČÁSTI PRAHA 5**

Uživatelská příručka ISMS

ŘÍJEN 2016

IČ 063631	Název souboru v elektronické podobě:	Tel: +420 800 800 005
DIČ CZ 00063631	Uzivatel'ska_prirucka_ISMSUzivatel'ska_prirucka_ISMS_revize_I3 C_kontrola_PH5	Fax: +420 257 325 132

Obsah

1.	ÚVOD.....	4
2.	ZÁKLADNÍ BEZPEČNOSTNÍ PRAVIDLA	5
2.1	UŽIVATELÉ JSOU POVINNI.....	5
2.2	UŽIVATELŮM JE ZAKÁZÁNO	9
3.	OBLAST PLATNOSTI	10

IČ 063631

Název souboru v elektronické podobě:

Tel: +420 800 800 005

DIČ CZ 00063631

Uživatelska_prirucka_ISMSUživatelska_prirucka_ISMS_revize_I3

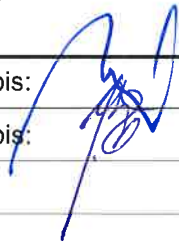
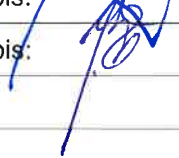
Fax: +420 257 325 132

C_kontrola_PH5

Revize dokumentu

Poř. číslo:	Datum	Výsledek revize:	Revizi provedl	Výsledek revize schválil/dne
02	18.10.2016	Úprava termínů realizace opatření	Ing. Vladimír BRENKUŠ	19.10.2016, Pavoł ŠIMKO

Platnost dokumentu

Ověřil:	Mgr. Viglaský	Dne	19.10.2016	Podpis:	
Schválil:	Bc. Žebera	Dne	19-10-2016	Podpis:	
Účinnost od:					
Vydal:					
Počet stran:					
Počet příloh:					
Vydání:	první – verze 1.1				
Dokument	INTERNÍ				

IČ 063631	Název souboru v elektronické podobě:	Tel: +420 800 800 005
DIČ CZ 00063631	Uzivatel'ska_prirucka_ISMSUzivatel'ska_prirucka_ISMS_revize_I3 C_kontrola_PH5	Fax: +420 257 325 132

1. Úvod

Tento dokument shrnuje základní pravidla nutná k zajištění bezpečnosti informací.

Detailní popis povinností uživatelů je uveden v ISMS dokumentaci Úřadu umístěné na intranetu Úřadu:

- Příručka integrovaného systému řízení kvality a bezpečnosti informací
- Směrnice č. 3/2010 Pro vystavování smluv a uzavírání objednávek
- Směrnice č. 2/2011 Standardy ICT systému úřadu
- Spisový a skartační řád Úřadu městské části Praha 5
- Pracovní řád 2012
- Směrnice č. 1/2011 O provozu budov Úřadu
- Směrnice č. 5/2012 Tvorba a evidence VOP ÚMČ P-5

Cílem dodržování bezpečnostních pravidel je zajistit bezpečnost informací z 3 základních hledisek:

- Dostupnost - aby informace byly dostupné v případě potřeby
- Důvěrnost - aby informace byly přístupné pouze oprávněným osobám
- Integrita - aby informace nebyly změněny nebo zničeny neautorizovaným způsobem

1.1. Podoby informací

- Papírová podoba
- Elektronická podoba
- Audio / video nahrávka
- Mluvené slovo při běžné komunikaci

1.2. Klasifikace informací

Dle stupně důvěrnosti jsou informace klasifikovány následujícím způsobem:

- **Veřejné** - všechny informace, které jsou určeny pro pracovníky Úřadu a širokou veřejnost
- **Interní** – informace, které jsou určeny všem zaměstnancům a spolupracujícím firmám ve smluvním vztahu, jejichž smlouva obsahuje doložku o mlčenlivosti
- **Diskrétní** - informace, které jsou z hlediska důvěrnosti určeny pouze pověřeným pracovníkům Úřadu. Tyto informace jsou viditelně označeny slovem „DISKRÉTNÍ“

Klasifikaci informací provádí vlastník informace (informace = informační aktivum), kterým je vedoucí daného odboru, do jehož působnosti informace spadá.

1.3. Bezpečnostní a technické incidenty

Bezpečnostní incident je událost, při které dochází nebo může dojít k porušení stanovených pravidel,

IČ 063631

Název souboru v elektronické podobě:

Tel: +420 800 800 005

DIČ CZ 00063631

Uzivatel'ska_prirucka_ISMSUzivatel'ska_prirucka_ISMS_revize_I3

Fax: +420 257 325 132

C_kontrola_PH5

případně úmyslnému či neúmyslnému ohrožení bezpečnosti informací.

Technickými incidenty jsou závady na uživatelských i ostatních technických zařízeních, zvláště pokud by mohly narušit bezpečnost informací Úřadu.

Zranitelnost je slabé místo systému, které může být využito hrozbou. Mimořádná událost je jakákoli událost, která může potenciálně ovlivnit bezpečnost informací Úřadu.

2. Základní bezpečnostní pravidla

2.1 Uživatelé jsou povinni

Pravidlo:

V případě odchodu z kanceláře, kde se již nenachází žádný další zaměstnanec Úřadu, zavřít okna a tuto místnost zamknout.

Možné dopady nedodržení pravidla:

- odcizení movitého majetku Úřadu
- odcizení majetku zaměstnanců
- odcizení a následné zneužití informací

Pravidlo:

Dodržovat pravidlo zavřených dveří mezi schodištěm a chodbami v jednotlivých patrech (při každém průchodu skleněnými dveřmi ze/na schodiště do/z chodby tyto dveře zavírat):

Výjimku tvoří úřední hodiny na těchto odborech:

- Odbor občanskoprávní a živnostenský
- Odbor sociální problematiky a prevence kriminality
- Odbor stavební
- Zvláštní organizační jednotka Infrastruktura
- Hlavní pokladna (Odbor vnitřní správy)

Možné dopady nedodržení pravidla:

- odcizení movitého majetku Úřadu
- odcizení majetku zaměstnanců
- odcizení a následné zneužití informací

IČ 063631

Název souboru v elektronické podobě:

Tel: +420 800 800 005

DIČ CZ 00063631

Uzivatel'ska_prirucka_ISMSUzivatel'ska_prirucka_ISMS_revize_I3

Fax: +420 257 325 132

C_kontrola_PH5

Pravidlo:

Udržovat vstupní kódy dveří mezi schodištěm a chodbami v jednotlivých patrech v tajnosti.

Možné dopady nedodržení pravidla:

- odcizení movitého majetku Úřadu
- odcizení majetku zaměstnanců
- odcizení a následné zneužití informací

Pravidlo:

V případě přítomnosti cizí osoby v kanceláři a nutnosti odchodu zaměstnance z kanceláře, kde se již nenachází žádný další zaměstnanec Úřadu, vyprovodit cizí osobu na chodbu, kancelář zamknout a opětovný vstup cizí osoby do kanceláře umožnit až při vlastním návratu zaměstnance do kanceláře (neponechávat cizí osoby bez dozoru v kanceláři).

Možné dopady nedodržení pravidla:

- odcizení movitého majetku Úřadu
- odcizení majetku zaměstnanců
- odcizení a následné zneužití informací

Pravidlo:

Dodržovat pravidlo čistého stolu (neponechávat volně položené dokumenty klasifikované jako důvěrné nebo interní bez dozoru na svém pracovním stole).

Možné dopady nedodržení pravidla:

- postihy za nedodržení legislativních požadavků
- odcizení a následné zneužití informací

Pravidlo:

Aktivovat spořič obrazovky chráněný heslem kdykoli se vzdálí od pracovní stanice.

Možné dopady nedodržení pravidla:

- neoprávněná úprava dat v informačním systému Úřadu
- odcizení a následné zneužití informací klasifikovaných jako neveřejné
- postihy za nedodržení legislativních požadavků
- poškození zaměstnance aktuálně přihlášeného k neuzamčenému pracovní stanici úpravou příp. vymazáním dat z informačního systému Úřadu

IČ 063631

Název souboru v elektronické podobě:

Tel: +420 800 800 005

DIČ CZ 00063631

Uzivatel'ska_prirucka_ISMSUzivatel'ska_prirucka_ISMS_revize_I3

Fax: +420 257 325 132

C_kontrola_PH5

Pravidlo:

Veškerá data musí být (vždy v nejbližším možném termínu) ukládána na sdílené disky serverů, které jsou pravidelně zálohovány.

Možné dopady nedodržení pravidla:

- *ztráta dat uložených na lokálním disku počítače v případě jeho poruchy*

Pravidlo:

Při práci s elektronickou poštou věnovat zvýšenou pozornost doručené poště s přílohou.

Možné dopady nedodržení pravidla:

- *zavedení škodlivého programu do ICT systému Úřadu, možnost následného odcizení a zneužití informací*
- *postihy za nedodržení legislativních požadavků*

Pravidlo:

Udržovat své heslo v tajnosti:

- nezapisovat si hesla (na papír, do souboru, apod.)
- neprozrazovat hesla žádné další osobě
- nezasílat hesla v přítomnosti další osoby

Možné dopady nedodržení pravidla:

- *umožnění přístupu neoprávněným osobám do ICT systému Úřadu*
- *odcizení a následné zneužití informací klasifikovaných jako neveřejné*
- *postihy za nedodržení legislativních požadavků*
- *poškození zaměstnance, jehož heslo bylo použito k přístupu do ICT systému Úřadu*

Pravidlo:

Pokud je to technicky, možné, používat komplexní heslo:

- délka hesla nejméně 8 znaků
- požadavek na komplexitu hesla, tzn. splňovat alespoň 3 z následujících podmínek:
 - velká písmena (A až Z)
 - malá písmena (a až z)
 - čísla (0 až 9)
 - ne-alfanumerické znaky (např. !, \$, #, %)

Možné dopady nedodržení pravidla:

- *snadné zjištění použitého hesla a následný neoprávněný přístup do ICT systému Úřadu*

IČ 063631

Název souboru v elektronické podobě:

Tel: +420 800 800 005

DIČ CZ 00063631

Uzivatel'ska_prirucka_ISMSUzivatel'ska_prirucka_ISMS_revize_I3

Fax: +420 257 325 132

C_kontrola_PH5

- *odcizení a následné zneužití informací*
- *postihy za nedodržení legislativních požadavků*
- *poškození zaměstnance, jehož heslo bylo použito k přístupu do ICT systému Úřadu*

Pravidlo:

V případě prozrazení nebo podezření na prozrazení hesla musí uživatel heslo okamžitě změnit.

Možné dopady nedodržení pravidla:

- *umožnění přístupu neoprávněným osobám do ICT systému Úřadu*
- *odcizení a následné zneužití informací*
- *postihy za nedodržení legislativních požadavků*
- *poškození zaměstnance, jehož heslo bylo použito k přístupu do ICT systému Úřadu*

Pravidlo:

Neprodleně hlásit jakékoli incidenty (poruchy, problémy, nesrozumitelné jevy) prostřednictvím hot-line.

Možné dopady nedodržení pravidla:

- *pozdní řešení vzniklého problému a možné poškození ICT systému Úřadu*
- *zavedení škodlivého programu do ICT systému Úřadu, možnost následného odcizení a zneužití informací*
- *postihy za nedodržení legislativních požadavků*

Pravidlo:

Před vypnutím pracovní stanice provést řádné ukončení všech spuštěných aplikací a odhlásit se ze sítě.

Možné dopady nedodržení pravidla:

- *ztráta dat kvůli nekorektnímu ukončení aplikace*
- *poškození aplikace a její následná nefunkčnost*

Pravidlo:

Při tisku informací klasifikovaných jako důvěrné a interní tyto nikdy neponechávat bez dozoru na tiskárně.

Možné dopady nedodržení pravidla:

- *odcizení a následné zneužití informací*
- *postihy za nedodržení legislativních požadavků*

IČ 063631

Název souboru v elektronické podobě:

Tel: +420 800 800 005

DIČ CZ 00063631

Uzivatel'ska_prirucka_ISMSUzivatel'ska_prirucka_ISMS_revize_I3

Fax: +420 257 325 132

C_kontrola_PH5

2.2 Uživatelům je zakázáno

Pravidlo:

Měnit nastavení internetového prohlížeče.

Možné dopady nedodržení pravidla:

- *umožnění zavedení škodlivého programu do ICT systému Úřadu, možnost následného odcizení a zneužití informací*
- *postihy za nedodržení legislativních požadavků*

Pravidlo:

Přeposílat informace klasifikované jako důvěrné a interní na své jiné soukromé e-mailové schránky (např. seznam.cz)

Možné dopady nedodržení pravidla:

- *možné odchyčení zasílaných informací neoprávněnými osobami a jejich následné zneužití*
- *postihy za nedodržení legislativních požadavků*

Pravidlo:

Ukládat na veřejné servery Internetu (např. uschovna.cz) jakékoli informace klasifikované jako důvěrné a interní.

Možné dopady nedodržení pravidla:

- *odcizení a následné zneužití informací*
- *postihy za nedodržení legislativních požadavků*

Pravidlo:

Provádět na svěřených prostředcích jakýkoliv hardwarové zásahy (např. měnit komponenty počítače, připojovat vlastní externí zařízení apod.) a spouštět či instalovat jakýkoliv nepovolený software.

Možné dopady nedodržení pravidla:

- *umožnění zavedení škodlivého programu do ICT systému Úřadu, možnost následného odcizení a zneužití informací*
- *poškození konfigurace pracovní stanice neodborným zásahem a způsobení její nefunkčnosti*
- *postihy za nedodržení legislativních požadavků*

IČ 063631

Název souboru v elektronické podobě:

Tel: +420 800 800 005

DIČ CZ 00063631

Uzivatel'ska_prirucka_ISMSUzivatel'ska_prirucka_ISMS_revize_I3

Fax: +420 257 325 132

C_kontrola_PH5

Pravidlo:

Jakkoliv měnit nastavení, případně vypínat ochranu proti škodlivému kódu (antivirový program, antispyware apod.)

Možné dopady nedodržení pravidla:

- *umožnění zavedení škodlivého programu do ICT systému Úřadu, možnost následného odcizení a zneužití informací*
- *postihy za nedodržení legislativních požadavků*

Pravidlo:

Ukládat na vyměnitelná média jakékoliv informace klasifikované jako neveřejné (mimo jednorázově schválených výjimek). Vyměnitelnými médii rozumíme:

- CD/DVD disky
- přepisovatelné CD/DVD
- pevné počítačové disky externí
- USB flash paměti, apod.

Možné dopady nedodržení pravidla:

- *možnost ztráty vyměnitelných médií a zneužití informací*
- *postihy za nedodržení legislativních požadavků*

Pravidlo:

Každý zaměstnanec, který přichází do styku s neveřejnými informacemi uloženými na médiích (CD, DVD, papírové dokumenty, flash paměťové moduly) je povinen zajistit jejich bezpečnou likvidaci (skartování, vymazání, fyzické zničení)

Možné dopady nedodržení pravidla:

- *možnost obnovení dat na vyměnitelných médiích a zneužití informací*
- *postihy za nedodržení legislativních požadavků*

3. OBLAST PLATNOSTI

Tento dokument je závazný pro Úřad městské části Praha 5.