ORGANIZAČNÍ SMĚRNICE

Název:

Politika bezpečnosti informací

Číslo dokumentu:	OS4402	**Vydání č.:**	06	**Výtisk č.:**	01
Platnost od:	15.04.2016	**Účinnost od:**	29.04.2016	**Platnost do:**	

Zpracoval:	Ing. Vladimír Fikejs	**Dne**:	23.03.2016	**Podpis**:	
Přezkoumal:		**Dne**:		**Podpis**:	
Schválil:	Ing. Ivan Prchal	**Dne**:	04.04.2016	**Podpis**:	

Obsah:

1 Úvod

Městský úřad Žamberk (dále „úřad") zajišťuje úkoly a činnosti veřejné správy v oblasti samostatné a přenesené působnosti. Tato činnost je významnou měrou závislá na zpracování informací, včetně osobních údajů a utajovaných informací. Pro potřeby zpracování informací jsou použity moderní výpočetní a telekomunikační technologie umístěné v prostorách úřadu a je prováděna řízená personální politika.

Pojmy:
Bezpečnostní politika úřadu je základním vyjádřením činností a postupů v oblasti bezpečnosti informací.
Bezpečnost informací je zajištěna opatřeními k ochraně informací, které jsou pro úřad cenné a je nutné je chránit.
Vedení úřadu – tvoří v souladu se zákonem č. 128/2000 Sb. (o obcích) v posledním platném znění starosta a tajemník. V rámci systému ISMS tvoří vedení i vedoucí odborů MěÚ a informační fórum.

Zkratky:
ISMS – Information security management systém
ICT – Informační a komunikační technologie
IT – Informační technologie
IS – Informační systém
ISVS – Informační systém veřejné správy

2 Cíl politiky

Cílem politiky bezpečnosti informací je vytyčení hlavních zásad pro bezpečnost informací, pro činnost úřadu a zodpovědných osob, k podpoře a zabezpečení realizace bezpečnosti a stanovení základních postupů a opatření kladených na zaměstnance úřadu, včetně opatření při jejich porušení.
Dlouhodobým cílem ISVS v oblasti bezpečnosti je

- bezpečnost dat v systémech – řeší Kodex ICT
- bezpečnost technických a programových prostředků – řeší Kodex ICT a pracovní postupy IT
- bezpečnost poskytovaných služeb – řeší pracovní postupy IT.

3 Rozsah politiky

Politika bezpečnosti informací je závazná pro zaměstnance Městského úřadu Žamberk, smluvní strany a třetí osoby (vázané dohodou) přicházející do styku s informacemi úřadu, které je nutné chránit. Politika se vztahuje na veškerá aktiva v oblasti bezpečnosti informací. Bezpečnost informací musí být zajišťována bezpečnými technickými prostředky, relevantními opatřeními a vlastní činností vedení a zaměstnanců úřadu. Do oblasti bezpečnosti informací je zahrnuta i oblast ISVS, jejíž současný stav je uveden v Plánu rozvoje IS.

4 Prohlášení vedení úřadu k dosažení bezpečnosti informací

Tajemník Městského úřadu Žamberk, úřadu obce s rozšířenou působností, je hlavním koordinátorem činností a plně podporuje prováděná opatření v rámci bezpečnosti informací, zkvalitňování všech druhů souvisejících aktiv a vytváří podmínky pro ochranu informací v souladu s ostatními řídícími procesy úřadu. Politika bezpečnosti informací úřadu je plně podporována vedením úřadu i města Žamberka.
Vedení úřadu svou činností vytváří podmínky pro vytvoření bezpečnostního prostředí v souladu s normou ČSN ISO / IEC 27001.

5 Hlavní opatření v rámci úřadu a základní bezpečnostní zásady

Zajištění kvality poskytovaných informací a služeb:

- cílem je zajistit kvalitu dat technických a programových prostředků a kvalitu služeb v souladu s platnou legislativou a interními požadavky úřadu včetně jejich financování.

V rámci celého úřadu musí být zabezpečena hlavně opatření pro:

- pravidelné monitorování a vyhodnocování rizik a incidentů bezpečnosti informací
- musí být přijímána měřitelná opatření vedoucí k omezení vlivu tak, aby docházelo ke zlepšování úrovně bezpečnosti a aby náklady na realizaci opatření odpovídaly hodnotě chráněných informací,
- zabezpečení požadavků vyplývajících ze smluvních závazků, obecně závazných právních předpisů a nařízení - musí být veden přehled těchto požadavků a odpovědnost za jejich plnění,
- zabezpečení včasné dostupnosti informací - doba kritické dostupnosti informací musí být stanovena, a to v souladu s jejich významem,
- zamezení nežádoucí modifikace informací - musí být určen rozsah kontroly a opatření k zamezení modifikace,
- případné zneužití nebo ztráta informací - musí být definována odpovědnost a způsob ochrany při přístupu k informacím a do prostor kde se nachází informační aktiva,
- zabezpečení výběru zaměstnanců z hlediska ochrany informací; se zaměstnanci úřadu provádět pravidelná školení v oblasti bezpečnosti informací,
- pro zajištění použitelnosti a účinnosti politiky bezpečnosti informací je ze strany vedení úřadu a informačním fórem (interní orgán vytvořený tajemníkem úřadu v oblasti bezpečnosti informací) tato politika pravidelně přezkoumávána a monitorována.

Základní bezpečnostní zásady úřadu vycházejí z těchto požadavků:
- dodržení právních předpisů, závazných norem, vnitřních předpisů a smluvních požadavků,
- dosažení stanoveného cíle – provedenými opatřeními zabezpečit ochranu informací,
- provedená bezpečnostní opatření nesmí omezovat standardní provoz úřadu,
- požadavky na činnost a pracovní povinnosti zaměstnanců v oblasti ISMS musí být úměrné hodnotě informačních aktiv,
- náklady spojené s přijetím opatření na snížení rizik musí být v rovnováze s případnými škodami způsobenými selháním bezpečnosti.

6 Stanovení odpovědnosti v oblasti bezpečnosti informací

a) stanovení odpovědnosti

Za bezpečnost informací spojených s činností úřadu odpovídá tajemník úřadu. Za bezpečnost informací používaných a spojených s činností jednotlivých odborů úřadu odpovídají tajemníkovi vedoucí odborů (vedoucí zaměstnanci). Všichni zaměstnanci dodržují bezpečnost v souladu s touto politikou, dalšími postupy a opatřeními a požadují její dodržování od svých podřízených zaměstnanců, klientů, smluvních a třetích stran.
Za ochranu konkrétních informací, které zaměstnanec používá k plnění pracovních povinností a úkolů a s kterými přichází do styku a manipuluje s nimi, nese plnou odpovědnost tento zaměstnanec úřadu, popř. smluvní nebo třetí strana pokud je na tuto stranu zaměstnanec přenese.

b) řízení odpovědnosti

Oblast bezpečnosti informací u úřadu řídí tajemník úřadu osobně nebo prostřednictvím ustanoveného orgánu – informačního fóra složeného za zaměstnanců úřadu:

- vedoucí: vedoucí odboru obrany a krizového řízení (OBR)
- členové: vedoucí právního odboru (PRAV)
  referent pokladna (SPDO)
  vedoucí oddělení informatiky (KTAJ)

vedoucí oddělení územního plánování (REUP)
referent finančního odboru – kontrola, příspěvkové organizace (FIN)

Při řešení odborných otázek, konzultací, analýzy bezpečnosti a při kontrolní činnosti je možné využít i činností externích subjektů zabývajících se bezpečností informací.

7 Závěr

S politikou bezpečnosti informací Městského úřadu Žamberk musí být seznámeni všichni zaměstnanci, smluvní strany a třetí osoby podle potřeby a smluvního ujednání.
Bezpečnostní politika je pravidelně vedením úřadu a informačním fórem přezkoumávána v plánovaných intervalech (minimálně však 1 x ročně) a vždy když nastane významná změna.

Řízení výtisků			
Název a pořadí výtisku	**Médium** (papír, databáze, audio kazeta....)	**Za výtisk odpovídá**	**Místo uložení**
OS4402	digi	správce OŘD	předpisy města PMD
OS4402 – výtisk 01	papír	správce OŘD	registr předpisů

+ složka OŘD úklid/údržba (1x)
+ složka školení praktikantů (2x)
+ složka vstupního školení (2x)

Směrnice je určena všem zaměstnancům MěÚ Žamberk a představitelům samosprávy.