**

**VZOR SMĚRNICE**

**Politika BEZPEČNOSTI INFORMACÍ**

**pro obec 2. typu**

Dokument byl zpracován v rámci realizace projektu

„Efektivní řízení rozvoje obcí jako základní předpoklad efektivnosti výkonu veřejné správy

a poskytování veřejných služeb z úrovně obcí“,

registrační číslo projektu: č.CZ.03.4.74/0.0/0.0/15\_019/0010159

|  |
| --- |
|  |
|  |
| **směrnice č. X/XXXX**  **Politika BEZPEČNOSTI INFORMACÍ** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Poř.  číslo: | Datum: | Výsledek revize: | Revizi provedl: | Výsledek revize schválil/dne: |
| 1. | XX.XX.XXXX | Schváleno |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Platnost dokumentu

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ověřil: |  | Dne: | XX.XX.XXXX | Podpis: |
| Schválil: |  | Dne: | XX.XX.XXXX | Podpis: |
| Účinnost od: | XX.XX.XXXX | | | |
| Vydal: | Tajemník městského úřadu XXX | | | |
| Počet stran: | 8 | | | |
| Počet příloh: | 0 | | | |
| Vydání: | první – verze 1.0 | | | |
| Dokument: | **INTERNÍ** | | | |

Obsah

[Úvodní ustanovení 5](#_Toc136336922)

[Předmět úpravy 5](#_Toc136336923)

[Zásady a principy 5](#_Toc136336924)

[Závaznost politiky 6](#_Toc136336925)

[Závěrečná ustanovení 6](#_Toc136336926)

**Úvodní ustanovení**

Informace jsou základní a nedílnou součástí aktiv Městského úřadu XXX (dále jen MěÚ XXX). Musí být vždy chráněny, ať už je jejich podoba jakákoliv a ať už jsou sdíleny, sdělovány nebo uloženy jakýmkoliv způsobem.

Touto bezpečnostní politikou MĚÚ XXX deklaruje svoji všestrannou podporu pro zajištění organizačních a technických podmínek pro bezpečné využívání informací cestou zavedení organizačních a technických opatření ve smyslu zákona 181/2014 Sb. o kybernetické bezpečnosti a návazných předpisů.

**Předmět úpravy**

Politika bezpečnosti informací byla vytvořena pro dosažení základních bezpečnostních cílů:

1. ochrany informací organizace, veřejnosti a dotčených třetích stran a prostředků informačních systémů;
2. trvalého zajištění důvěrnosti, integrity a dostupnosti dat a prokazatelnosti při jejich využívání;
3. zajištění bezpečné komunikace s okolím;
4. ochrany veřejných financí;
5. ochrany dobrého jména organizace.

**Zásady a principy**

Principy řízení bezpečnosti informací vycházejí z obecně platného pravidla, že jedině u řízené a koordinované činnosti lze očekávat synergický efekt bezpečnostních opatření.

**Princip need-to-know** znamená, že přístup a rozsah oprávnění zaměstnance nebo dotčené třetí strany má být odvozen od toho, co potřebuje znát pro výkon práce;

**Princip kompaktnosti a úplného pokrytí** znamená, že bezpečnost informací je tak odolná, jak odolný je její nejslabší článek. Bezpečnost informací musí být navrhována tak, aby působila vyváženě a chránila všechna aktiva. Zásady bezpečnosti informací musí být jednotně prosazovány do všech činností a procesů;

**Princip přiměřenosti** znamená, že bezpečnostní opatření musí být navržena tak, aby odpovídala velikosti rizika a hodnotě aktiv, která chrání;

**Princip koordinace bezpečnosti** znamená, že bezpečnostní působení v rámci ochrany informací musí být koordinované, aby se zabezpečil soulad a návaznost jednotlivých bezpečnostních opatření;

**Princip vedení bezpečnostní dokumentace** znamená, že postupy a procesy musí být dokumentovány, aby byla zachována jejich přesná opakovatelnost a dohledatelnost. O bezpečnostních událostech se vedou záznamy;

**Princip soustavného sledování, přezkoumání a zlepšování bezpečnosti** znamená, že se bezpečnost informací postupem času vyvíjí a tím se mění i bezpečnostní podmínky a požadavky a zachová se stálá a odpovídající ochrana aktiv;

**Princip odpovědnosti znamená**, že prosazení stanovených zásad, pravidel a postupů SŘBI je vždy na všech úrovních řízení v souladu s deklarovanými cíli a spojeno s individuální odpovědností jednotlivých osob;

**Princip integrace znamená**, že prosazování bezpečnosti informací je řízeno

**Princip souladu s právními předpisy** znamená, že všechny zásady, pravidla a postupy jsou v souladu s právními předpisy, závaznými pro organizaci a relevantními technickými normami a jsou v souladu s uzavřenými smluvními závazky;

**Princip bezpečnostního povědomí** znamená poučení o bezpečném nakládání s informacemi, jejich vytváření a zpracování;

**Princip formalizace znamená**, že prosazování a řízení bezpečnosti informací je spojeno s formalizovanými, jednoznačně definovanými a náležitě popsanými postupy, jejichž uplatňování je řádně dokumentováno. Nedílnou součástí řízení jsou nástroje kontroly a nezávislého auditu, které důsledně ověřují míru a kvalitu skutečné realizace všech přijatých opatření;

**Princip nepřetržitosti** znamená, že přijatá bezpečnostní opatření pro zajištění bezpečnosti informací musí být vždy přiměřeně účinná a musí být uplatňována nepřetržitě na všech aktivech;

**Princip řízení rizik** znamená, že rizika jsou průběžně vyhodnocována a jsou zvládána zaváděním opatření k jejich snížení nebo eliminaci.

**Závaznost politiky**

Politika bezpečnosti informací je závazná pro všechny fyzické osoby v pracovním poměru k MĚÚ XXX a fyzické osoby činné v MĚÚ XXX na základě dohod o pracích konaných mimo pracovní poměr a dotčené třetí strany, a to bez ohledu na zastávanou funkci, pozici či roli v organizaci.

**Závěrečná ustanovení**

1. Směrnice nabývá platnosti dnem jejího schválení Radou MĚÚ XXX a účinnosti dnem ...........
2. Tato Směrnice byla schválena usnesením č. MĚÚ XXX

…………………………………

Starosta

………………………………….

Tajemník