**

**VZOR SMĚRNICE**

**Politika BEZPEČNOSTI INFORMACÍ**

**pro statutární město**

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

|  |
| --- |
| **VNITŘNÍ ORGANIZAČNÍ PŘEDPIS****Magistrátu města MMM** |
|  |
| **směrnice č. X/XXXX****Politika BEZPEČNOSTI INFORMACÍ****Magistrát města MMM** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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: | Primátor Magistrátu města MMM |
| Počet stran: | 8 |
| Počet příloh: | 0 |
| Vydání: | první – verze 1.0 |
| Dokument: | **INTERNÍ** |

Obsah

[Úvodní ustanovení 5](#_Toc136339536)

[Předmět úpravy 5](#_Toc136339537)

[Vymezení pojmů 5](#_Toc136339538)

[Organizace bezpečnosti informací 6](#_Toc136339539)

[Klasifikace informací 7](#_Toc136339540)

[Oblasti bezpečnosti informací 7](#_Toc136339541)

[Zásady a principy politiky 7](#_Toc136339542)

[Závaznost politiky 8](#_Toc136339543)

[Závěrečná ustanovení 9](#_Toc136339544)

**Úvodní ustanovení**

Informace jsou základní a nedílnou součástí aktiv Magistrátu města MMM. Musí být vždy chráněny, ať už je jejich podoba jakákoliv a ať už jsou sdíleny, sdělovány nebo uloženy jakýmkoliv způsobem.

Touto bezpečnostní politikou MMM 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.

Čl. 1

**Předmět úpravy**

Politika bezpečnosti informací je souhrnem základních bezpečnostních předpisů a zásad definujících způsob nakládání a zabezpečení informací v souladu s požadavky MMM a zákona a vyhlášky o kybernetické bezpečnosti. 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.

Čl. 2

**Vymezení pojmů**

Pro účely této Směrnice se rozumí:

1. primárním aktivem služby a informace
2. podpůrným aktivem data, hardware (HW), systémový SW, aplikační SW (aplikace), technická infrastruktura, komunikační systémy, , znalosti obslužného personálu, dokumentace apod.
3. zpracovatelskou smlouvou smluvní vztah, jehož předmětem je zpracování osobních údajů zpracovatelem, které správce získal v souvislosti se svou činností
4. SŘBI (Systém řízení bezpečnosti informací) komplexní dokumentované řešení pro práci s informacemi, ve kterém jsou chráněna definovaná informační aktiva, jsou řízena rizika [bezpečnosti informací](https://cs.wikipedia.org/w/index.php?title=Bezpe%C4%8Dnost_informac%C3%AD&action=edit&redlink=1) a zavedena opatření jsou kontrolována.
5. důvěrností informací zabezpečení přístupu k informačním aktivům pouze pro oprávněné osoby na základě zásady need to know
6. Integritou stav, kdy se lze spolehnout na chování systémů, aplikací, obsah informací a že nedošlo k jejich neočekávaným a nechtěným změnám
7. dostupností informací, že data jsou dostupná v okamžiku jejich potřeby
8. Výborem pro řízení kybernetické bezpečnosti orgán ve smyslu Organizačního řádu MMM, tvořený zaměstnanci, kteří jsou tajemníkem MMM pověřeni řízením a rozvojem systému řízení bezpečnosti informací (dále jen „SŘBI“).
9. Manažerem kybernetické bezpečnosti - osoba odpovědná za řízení SŘBI. Architektem kybernetické bezpečnosti osoba odpovědná za návrh implementace bezpečnostních opatření tak, aby byla zajištěna bezpečná architektura v souladu s enterprise architekturou MMM. Auditorem kybernetické bezpečnosti
10. Garantem aktiva (primárního i podpůrného) osoba odpovědná za zajištění rozvoje, použití a bezpečnosti informačních aktiv.

Čl. 3

**Organizace bezpečnosti informací**

Na organizaci a řízení bezpečnosti informací se podílejí vedoucí zaměstnanci a zaměstnanci zastávající bezpečnostní role. Mezi základní bezpečnostní role patří:

1. Výbor pro řízení kybernetické bezpečnosti - Organizovaná skupina tvořená osobami, pověřenými tajemníkem úřadu k řízení a zajištění rozvoje bezpečnosti informační infrastruktury a významně se podílející na řízení a koordinaci činností spojených se zajištěním kybernetické a informační bezpečnosti v působnosti MMM. Typicky se jedná o vedoucí odborů;
2. Manažer kybernetické bezpečnosti - Osoba odpovědná za systém řízení bezpečnosti informací;
3. Architekt kybernetické bezpečnosti - Osoba odpovědná za návrh a implementaci bezpečnostních opatření;
4. Auditor kybernetické bezpečnosti - Osoba odpovědná za provádění auditu kybernetické bezpečnosti. Auditor kybernetické bezpečnosti vykonává svoji roli nestranně a výkon jeho role je oddělen od výkonu rolí manažera, architekta a výboru kybernetické bezpečnosti.
5. Garant aktiva ve spolupráci s  Manažerem kybernetické bezpečnosti zajišťuje klasifikaci aktiva z pohledu důvěrnosti, integrity a dostupnosti, stanoví pravidla přístupu k primárnímu aktivu, informuje Manažera KB o změně primárního aktiva.

Činnosti v oblasti bezpečnosti informací musí být koordinovány prostřednictvím pověřených pracovníků MMM s odpovídajícími rolemi a pracovním zařazením.

Všechny útvary MMM jsou povinny sladit své procesy a činnosti s požadavky bezpečnostních politik a pravidel a zohlednit tyto v příslušných metodikách a interních aktech řízení v jejich věcné působnosti.

Čl. 4

**Klasifikace informací**

MMM musí zabezpečit, aby informace získaly odpovídající úroveň ochrany. S informacemi musí být nakládáno s ohledem na jejich hodnotu, právní požadavky a citlivost. Pro splnění tohoto požadavku musí být informace organizace klasifikovány a označovány. V souladu klasifikačním schématem musí být vytvořena a do praxe zavedena pravidla pro označování informací a zacházení s nimi.

Čl. 5

**Oblasti bezpečnosti informací**

Politika bezpečnosti informací souvisí s:

1. ochranou informačních aktiv pomocí přiměřených a odpovídajících opatření tak, aby poskytla odpovídající míru jistoty třetím stranám;
2. organizační bezpečností, určením bezpečnostních rolí, jejich práv a povinností;
3. bezpečností lidských zdrojů, která definuje požadavky na ochranu aktiv pro snížení a eliminaci rizika lidské chyby, krádeže, podvodu nebo zneužití aktiv, a to jak ze strany zaměstnanců, tak i třetích stran;
4. fyzickou a objektovou bezpečností, definující způsob zabezpečení a přístupu do objektů a chráněných prostorů;
5. bezpečností informačních a komunikačních technologií a s požadavkem začlenění bezpečnosti informací do všech fází řízení projektů a projektových cílů.

 Čl. 6

**Zásady a principy politiky**

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

1. **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;
2. **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;
3. **Princip přiměřenosti** znamená, že bezpečnostní opatření musí být navržena tak, aby odpovídala velikosti rizika a hodnotě aktiv, která chrání;
4. **Princip koordinace bezpečnosti** znamená, že bezpečnostní působení v rámci ochrany informací musí být koordinované, aby se zabezpečil soulad a návaznost jednotlivých bezpečnostních opatření;
5. **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;
6. **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;
7. **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;
8. **Princip integrace znamená**, že prosazování bezpečnosti informací je řízeno komplexním SŘBI, který integruje a koordinuje činnosti všech dotčených útvarů i zúčastněných třetích stran;
9. **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;
10. **Princip bezpečnostního povědomí** znamená poučení o bezpečném nakládání s informacemi, jejich vytváření a zpracování;
11. **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;
12. **Princip nepřetržitosti** znamená, že přijatá bezpečnostní opatření pro zajištění bezpečnosti informací musí být vždy přiměřeně účinná a musí být uplatňována nepřetržitě na všech aktivech;
13. **Princip řízení rizik** znamená, že rizika jsou průběžně vyhodnocována a jsou zvládána zaváděním opatření k jejich snížení nebo eliminaci.

Čl. 7

**Závaznost politiky**

Politika bezpečnosti informací je závazná pro všechny fyzické osoby v pracovním poměru k MMM a fyzické osoby činné v MMM 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.

Tento dokument se nevztahuje na zabezpečení, řízení přístupu a postupy práce v prostorách, které spadají pod zvláštní režim nakládání s utajovanými informacemi.

Na tuto politiku navazují politiky, které stanoví postupy při zavedení organizačních a technických opatření ve smyslu zákona 181/2014 Sb. o kybernetické bezpečnosti a návazných předpisů. Tyto navazující politiky jsou v gesci tajemníka MMM.

Čl. 8

**Závěrečná ustanovení**

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

………………………………….

Tajemník