Politika bezpečnosti informací Městského úřadu Moravská Třebová

1. ÚVOD

Městský úřad Moravská Třebová (dále jen *městský úřad*) zajišťuje úkoly a činnosti v oblasti samostatné a přenesené působnosti veřejné správy.

V rámci této činnosti zpracovává značné množství informací v elektronické i listinné formě. Kromě informací přístupných veřejnosti jsou shromažďovány, zpracovávány a uchovávány také informace podléhající zákonu o krizovém řízení, zákonu o ochraně osobních údajů a informace, které jsou určeny pouze pro interní potřebu organizace.

Politika bezpečnosti informací (dále jen *politika*) definuje základní strategii a zásady týkající se bezpečnosti městského úřadu, určuje základní bezpečnostní pravidla pro provoz, používání a údržbu informací a informačních prostředků s cílem zajistit požadovanou úroveň ochrany informací v souladu s jejich významem.

2. ODPOVĚDNOST

2.1. Vymezení rozsahu působnosti politiky

Politika se vztahuje na Městský úřad Moravská Třebová.

Politika bezpečnosti informací je závazným dokumentem, se kterým musí být seznámeni všichni zaměstnanci města zařazení do městského úřadu, a který je veřejně přístupný na internetových stránkách města.

Politika je dále upřesněna ve vnitřních předpisech a ostatních dokumentech městského úřadu.

2.2. Závazek vedení

Vedení městského úřadu přijímá závazek podporovat a prosazovat tuto politiku, zejména:

- provádí pravidelné monitorování a vyhodnocování bezpečnostních rizik a přijímá odpovídající opatření vedoucí k omezení jejich vlivu
- v rámci celého úřadu a v souladu s obecně závaznými právními předpisy a smluvními požadavky provádí opatření vedoucí k neustálému zlepšování bezpečnosti informací, tj. zabezpečení včasné dostupnosti, zamezení nežádoucí modifikace, zneužití nebo ztráty informací
- způsob zpracování informací definuje souborem vnitřních předpisů a dokumentovaných postupů, které prosazuje a sděluje všem zaměstnancům
- dbá na to, aby náklady na bezpečnostní opatření byly vynakládány efektivně, tj. odpovídaly významu a ceně informací.

2.3. Odpovědnost zaměstnanců

Každý zaměstnanec, kterému byl umožněn přístup k informačním prostředkům pro potřeby výkonu pracovní činnosti, přebírá odpovědnost za bezpečné nakládání s těmito prostředky a za ochranu informací ve své působnosti. Stanovená, přijatá a schválená politika a související bezpečnostní dokumentace je závazná pro všechny uživatele s přístupem k informacím, a to bez ohledu na zastávanou funkci, pozici či roli v úřadu. Všichni uživatelé nesou v souladu s platnou legislativou a předpisy svůj díl zodpovědnosti za dodržení, resp. porušení pravidel, s nimiž byli seznámeni.

Všichni zaměstnanci jsou povinni předepsaným způsobem reagovat na závady, poruchy a bezpečnostní incidenty, které se vyskytnou a upozornit na ně v souladu s příslušnými vnitřními předpisy.

3. HLAVNÍ ZÁSADY PRÁCE S INFORMACEMI A ZPŮSOB JEJICH ZABEZPEČENÍ

- zajistit odpovídající ochranu osobních údajů v souladu s platnou legislativou
- vytvářet a prosazovat systém řízeného přístupu k informacím
- začleňovat zabezpečení informací do odpovědnosti za práci
- zajišťovat systematické vzdělávání a zvyšování kvalifikace zaměstnanců v oblasti bezpečnosti informací
- provádět stálou identifikaci bezpečnostních incidentů a přijímat účinná opatření pro zlepšování bezpečnosti informací
- zpracovávat soubory opatření pro zachování kontinuity pro případy závažného výpadku v oblasti informací; tato opatření pravidelně přezkušovat a ověřovat
- zabezpečovat informační systémy, Internet, elektronickou poštu a další způsoby výměny informací přístupných veřejnosti
- zabezpečovat systém fyzického přístupu do prostor pro snížení ohrožení informačního majetku
- nepřetržitě zajišťovat dostupnost, spolehlivost a integritu dat
- nepřetržitě monitorovat a kontrolovat stav síťových prvků a účinnost bezpečnostních prvků
- prosazovat politiku bezpečného pracoviště - čistý stůl, prázdné obrazovky a odpadkové koše
- prosazovat bezpečnostní pravidla pro přenosná počítačová zařízení a jiné nosiče informací
- zajišťovat spolehlivou kontrolu celé interní sítě proti působení zlomyslného softwaru
- udržovat, chránit a rozvíjet informační majetky, spolehlivě zálohovat informační systémy
- zajistit kvalitu poskytování informací, služeb, technických a programových prostředků v souladu s platnou legislativou a interními požadavky organizace.

4. NÁSLEDKY PORUŠENÍ INFORMAČNÍ POLITIKY

- porušování zásad této politiky bezpečnosti informací ze strany zaměstnanců i externích pracovníků je chápáno jako bezpečnostní incident, který má vliv na bezpečnost informací a v těchto intencích musí být řešen
- příčiny porušení informační politiky se musí analyzovat a přijímat účinná opatření s cílem učení se z těchto událostí.

Tento dokument byl:

1. Projednán a schválen Radou města Moravská Třebová dne 16.03.2009, číslo usnesení 2030/R/16032009.
2. Projednán a schválen v aktualizované podobě Radou města Moravská Třebová dne 17.01.2011, číslo usnesení: 139/R/170111.

JUDr. Miloš Izák
starosta města