**BEZPEČNOSTNÍ POLITIKA**

**Magistrátu hlavního města Prahy**

**POLITIKA SYSTÉMU ŘÍZENÍ BEZPEČNOSTI INFORMACÍ**

1. Zkratky a pojmy
* **Aktivum –** vše, co je v rámci Magistrátu hlavního města Prahy (dále jen „MHMP“) ohraničitelné a má pro něj nějakou hodnotu;

jako aktivum jsou chápány veškeré procesy realizované v rámci činnosti MHMP a veškeré informace zpracovávané v prostředí či na pracovních prostředcích MHMP (na prostředcích výpočetní techniky, v informačních systémech, v listinné podobě i informace v nehmotné podobě); aktivum lze rozlišovat na:

* **Primární aktivum** – informace nebo služba, která je zpracovávána nebo poskytována na prostředcích výpočetní techniky, v informačních systémech, v listinné podobě a informace v nehmotné podobě;
* **Podpůrné aktivum** – technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji a správě informačního systému, komunikačního systému; přičemž technické aktivum je technické vybavení, komunikační prostředky a programové vybavení informačního systému nebo komunikačního systému a objekty, ve kterých jsou tyto systémy umístěny;
* **Analýza rizik –** procespochopení povahy rizika a určení úrovně rizika;
* **Bezpečnostní událost (BU) –** identifikovatelnýstav (systému, služby, sítě apod.) ukazující na možné porušení bezpečnostní politiky MHMP, nebo selhání bezpečnostních opatření; může se také jednat o jinou předtím nenastalou situaci, která může být důležitá z pohledu bezpečnosti;
* **Bezpečnostní incident (BI) –** jedna nebo více nechtěných nebo neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost narušení bezpečnosti osob, majetku, informací nebo kompromitace činností MHMP;
* **Bezpečnost informací –** zachování dostupnosti, důvěrnosti a integrity informací, přičemž:
* **Dostupnost** – zajištění stavu, aby informace byla dostupná oprávněným subjektům v čase, kdy k ní potřebují přistupovat;
* **Důvěrnost** – zajištění stavu, aby informace byla dostupná pouze oprávněným subjektům;
* **Integrita** – zajištění stavu, aby informace byla dostupná oprávněným subjektům v neporušené, nezměněné a úplné podobě;
* **Garant aktiva –** zaměstnanec podle organizačního řádu MHMP zajišťující rozvoj, použití a bezpečnost aktiva; garant aktiva rozhoduje o všech změnách, které mají dopad na rozvoj primárních aktiv a jejich použití: řízení přístupových práv ke službám a datům informačního systému, nastavení parametrů provozu a bezpečnosti informací; v případě významných informačních systémů jmenuje garanty primárních aktiv ředitel MHMP na návrh ředitele věcně příslušného odboru MHMP;
* **Bezpečnostní cíl –** stavbezpečnosti, kterého má daný systém nebo produkt dosáhnout;
* **Systém řízení bezpečnosti informací (ISMS)** – systém založený na přístupu k rizikům, který stanovuje způsob ustavení, implementování, provozování, monitorování, přezkoumávání, spravování a zlepšování bezpečnosti informací;
* **Kontinuita bezpečnosti informací** – procesy a postupy k zajištění nepřetržitých operací bezpečnosti informací v informačních technologiích;
* **Opatření** – prostředky modifikující riziko, včetně politik, strategií, postupů, směrnic, obvyklých postupů nebo organizačních struktur, které mohou být administrativní, technické, řídící nebo právní povahy;
* **Riziko –** možnost,že určitá hrozba využije zranitelnosti aktiva nebo skupiny aktiv a způsobí organizaci škodu;
* **Hrozba** – potenciální příčina incidentu, jejímž výsledkem může být poškození aktiva;
* **Zranitelnost –** slabé místoaktiva nebo opatření, které může být využito jednou nebo více hrozbami;
* **Externí pracovník** – fyzická osoba vykonávající činnosti pro MHMP na základě dohody o pracích konaných mimo pracovní poměr nebo na základě smlouvy s právnickou či fyzickou osobou, jež má uzavřený smluvní vztah s hlavním městem Prahou;
* **Výbor pro řízení kybernetické bezpečnosti** – definovaná skupina osob s příslušnými pravomocemi a odbornou způsobilostí v souladu se zákonem o kybernetické bezpečnosti, která je pověřena celkovým řízením a rozvojem informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému, anebo se významně podílí na řízení a koordinaci činností spojených s bezpečností těchto systémů;
* **GDPR** – nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES;
* **ZoKB –** zákonč. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů.

1. **Magistrát hlavního města Prahy**

ISMS vychází z cílů bezpečnosti informací a dále z určených a ohodnocených rizik. ISMS dále zahrnuje určení povinností a odpovědností spolu s vytvořením a dodržováním zdokumentovaných bezpečnostních zásad a postupů. ISMS současně stanovuje kritéria hodnocení rizik a zahrnuje kontroly dodržování stanovených pravidel, definici zákonných, regulatorních a smluvních požadavků, vzdělávání pracovníků a postupy pro reakci na bezpečnostní incidenty a události.

Pro ochranu svých i svěřených informací MHMP vybudoval, udržuje a rozvíjí Systém řízení bezpečnosti informací v souladu s řadou norem ISO 27000, ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů a ve smyslu nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

MHMP, s vědomím svých povinností jako povinné osoby ve smyslu ZoKB, přikládá velký význam zabezpečení informací, které jsou mu svěřeny do péče a které zpracovává. Vnímá ochranu informací svých i informací třetích stran jako ucelenou a řízenou soustavu vyvážených opatření, jejichž cílem je přiměřeně chránit všechna důležitá aktiva. Základním úkolem je zajištění dostupnosti, důvěrnosti a integrity informačních aktiv MHMP.

MHMP se zavazuje na základě analýzy rizik plnit bezpečnostní opatření, v prioritách daných dokumentem Plán zvládání rizik, a bezpečnostní požadavky v následujících oblastech:

* **Identifikace a řízení aktiv –** určovat způsob identifikace a ohodnocení aktiv, způsob klasifikace informací a způsob zacházení s nimi. Oblast postihuje i samotnou analýzu rizik, včetně stanovení její struktury a kritérií hodnocení.
* **Organizační bezpečnost –** definovat odpovědnosti a rozsah ISMS.
* **Bezpečnost lidských zdrojů** – zajistit, aby se s důvěrnými informacemi seznamovala pouze osoba k tomu určená (ve specifikovaných rolích).
* **Řízení provozu a komunikací** – stanovovat postupy pro řádný a bezpečný provoz prostředků pro zpracování informací MHMP a služeb s tím souvisejících.
* **Řízení přístupu** – definovat ochranu a kontrolu přístupu k informacím, službám a procesům.
* **Akvizice, vývoj a údržba systémů** – definovat bezpečnostní pravidla vývoje a údržby systémů od fáze návrhu, vývoje, testování až po vlastní provoz a údržbu.
* **Fyzická bezpečnost a bezpečnost prostředí –** předcházet neautorizovanému přístupu, zcizení, poškození, zničení či jiným zásahům do informací MHMP a do prostor, ve kterých se nacházejí zařízení MHMP.
* **Zvládání bezpečnostních událostí/incidentů** – stanovovat postupy reakce na porušení pravidel, bezpečnosti a odolnosti systému ISMS.
* **Řízení kontinuity činností organizace –** stanovit rámec prevence a reakce na krizové situace formou plnění plánů kontinuity.
* **Zajištění souladu s požadavky** – zpracovat konkrétní postupy v oblasti zajištění shody přijímaných opatření s legislativou a bezpečnostními a technologickými požadavky.

**Vedení MHMP trvale zajišťuje, že politika bezpečnosti informací:**

* Odpovídá záměrům a potřebám organizace.
* Zahrnuje odpovědnost k plnění požadavků a k neustálému zlepšování efektivnosti systému.
* Poskytuje rámec pro stanovení a přezkoumání bezpečnostních cílů.
* Je sdělována a pochopena v organizaci při školeních uživatelů (zaměstnanců, externích subjektů atd.).
* Je pravidelně přezkoumávána z hlediska kontinuity činností MHMP společně s ostatními řídícími akty organizace.
1. **Rozsah Systému řízení bezpečnosti informací**

ISMS pokrývá všechna pravidla, procesy, organizační části, lidské a technické zdroje činností MHMP.

Základní rozsah systému řízení bezpečnosti informací je vymezen primárními a podpůrnými aktivy MHMP, která byla identifikována v rámci analýzy rizik.

ISMS pokrývá všechna aktiva a informační a komunikační systémy, zejména:

* Identifikované podle řady norem ISO 27000.
* Identifikované podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti ve znění pozdějších předpisů a příslušných platných prováděcích nebo určujících vyhlášek.
* Identifikované v oblasti ochrany osobních údajů ve smyslu nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

Výbor pro řízení kybernetické bezpečnosti je integračním prvkem zajišťujícím vzájemnou informovanost, výměnu zkušeností a koordinaci společného postupu při zavádění ISMS. Jedná se o vrcholový řídící orgán kybernetické bezpečnosti na MHMP.

1. **Strategické cíle a principy bezpečnosti informací**

MHMP, s vědomím svých povinností jako povinné osoby ve smyslu řady norem ISO 27000, ZoKB a GDPR přikládá velký význam zabezpečení informací, které jsou mu svěřeny do péče a které zpracovává. Vnímá ochranu informací svých i informací třetích stran jako ucelenou a řízenou soustavu vyvážených opatření, jejichž cílem je chránit všechna důležitá aktiva.

* 1. Strategické cíle

**MHMP pro ochranu svých důležitých aktiv stanovil následující cíle:**

* Zajištění jednotné ochrany informací podle požadavků legislativy a její postupné rozšiřování ve všech oblastech MHMP.
* Zajištění odpovídajících zdrojů (personálních a finančních) pro oblast bezpečnosti informací MHMP.
* Zajištění ochrany všech aktiv MHMP.
* Implementace bezpečnostních technologií a jejich průběžná aktualizace a modernizace.
* Trvalé zajištění schopnosti zvládání bezpečnostních událostí a incidentů, včetně sdílení a rozvíjení znalostí o hrozbách.
	1. Principy

**K zajištění bezpečnosti informací použije MHMP následující principy:**

* **Princip jednotného řízení bezpečnosti informací**

Je tvořen jednotnými procesy, metodikami a postupy ve všech oblastech činností MHMP.

* **Princip jednotného sdílení informačních zdrojů**

Stávající informační zdroje budou bezpečně využívány v rámci MHMP.

* **Princip sdílení znalostí a spolupráce**

MHMP deklaruje efektivní výměnu znalostí v rámci MHMP, a to včetně řešení bezpečnostních událostí a incidentů.