Politika informačnej bezpečnosti

hlavného mesta Slovenskej republiky Bratislavy

(skrátená verejná verzia)

7. júla 2020

Tento dokument obsahuje 7 strán

Schválil:

Ing. arch. Matúš Vallo

_____v.r._____

primátor

1 Účel a oblasť platnosti

1.1 Účel dokumentu

Hlavné mesto Slovenskej republiky Bratislava (ďalej len „mesto“) si uvedomuje dôležitosť informačných systémov (ďalej len „IS“), ktoré prevádzkuje, význam údajov, ktoré sú v nich spracúvané, hodnotu majetku a technológií, ktoré používa pre svoju činnosť a povinnosť chrániť oprávnené záujmy samosprávy, štátu, zamestnancov a všetkých osôb, s ktorými prichádza do kontaktu. Z tohto dôvodu sa mesto rozhodlo zaviesť systém manažérstva informačnej bezpečnosti v súlade s požiadavkami štandardov ISO/IEC 27001:2014 a ISO/IEC 27002:2014.

Účelom tohto dokumentu je definovanie politiky informačnej bezpečnosti ako všeobecného rámca pre riešenie informačnej bezpečnosti mesta. Politika informačnej bezpečnosti (ďalej tiež ako „Bezpečnostná politika“) je predpokladom pre dosiahnutie informačnej bezpečnosti ako primeranej úrovne dôvernosti, integrity a dostupnosti informácií, informačných systémov a ich služieb, ktoré sú v správe mesta.

1.1.1 Východiská

Dokument vychádza z platnej slovenskej legislatívy, najmä zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti (ďalej len „Zákon o KyB“), zo zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe (ďalej len „Zákon o ITVS“), vyhlášky Národného bezpečnostného úradu 362/2018 (ďalej len „Vyhláška“) a je v súlade s § 29 Výnosu č. 55/2014 MF SR z 3. marca 2014 o štandardoch pre informačné systémy verejnej správy v znení neskorších predpisov.

Dokument je vytvorený na základe štandardov STN ISO/IEC 27001:2014 – „Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Požiadavky.“ a STN ISO/IEC 27002:2014 – „Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti.", ktoré vychádzajú z medzinárodných štandardov informačnej bezpečnosti ISO/IEC 27001:2013 – „Information security management. Specification with guidance for use“ a ISO/IEC 27002:2013 – „Information technology. Security techniques. Code of practice for information security management“ a odporúčaní odvetvovej praxe.

1.2 Oblasť platnosti dokumentu

Tento predpis platí pre všetky organizačné útvary Magistrátu hlavného mesta Slovenskej republiky Bratislavy, Mestskú políciu, lokality, dodávateľov IS a aplikácií a iné tretie strany, ktoré môžu mať vplyv na celkovú informačnú a kybernetickú bezpečnosť mesta.

Tento dokument nepokrýva zodpovednosti podriadených mestských podnikov ani rozpočtových a príspevkových organizácií.

2 Politika informačnej bezpečnosti

Politika informačnej bezpečnosti je platná v rámci celého mesta. Je vydaná za účelom vytvorenia podmienok pre zabezpečenie primeranej úrovne ochrany všetkých hmotných a nehmotných aktív mesta proti hrozbám, ktoré na tieto aktíva môžu pôsobiť.

Politika informačnej bezpečnosti poskytuje rámec pre všetky bezpečnostné procesy a mechanizmy. Požiadavky politiky informačnej bezpečnosti musia byť v primeranom rozsahu rozpracované vo forme predpisov, smerníc, inštrukcií alebo návodov. Za detailné rozpracovanie politiky informačnej bezpečnosti zodpovedajú v rámci svojej zodpovednosti vedúci organizačných jednotiek mesta spolu s Bezpečnostným manažérom.

Všetky princípy uvedené v politike sú platné nielen pre informácie spracovávané v elektronickej forme automatizovanými prostriedkami, ale aj pre informácie spracúvané manuálne v papierovej forme.

Zodpovednosť za presadenie tejto politiky nesie vedenie mesta.

2.1 Riadiace dokumenty informačnej bezpečnosti

V nadväznosti na Bezpečnostnú politiku mesta sú pre riadenie informačnej a kybernetickej bezpečnosti relevantné aj ďalšie bezpečnostné dokumenty mesta, smernice, nariadenia, vyhlásenia, predpisy, pokyny, metodiky a návody. Zoznam týchto dokumentov vedie oddelenie organizačné. Bezpečnostný manažér je s týmito dokumentami oboznámený a má v nich prehľad.

Obsahom týchto ďalších materiálov sú detailnejšie špecifikácie bezpečnostných opatrení stanovených v Bezpečnostnej politike, nastavení informačných systémov, bezpečnostných mechanizmov nutných pre zabezpečenie informačných systémov a nastavenie procesov či bezpečnostných procedúr nevyhnutných na operačnú činnosť informačných systémov.

Dokumentom pridruženým k Bezpečnostnej politike je aj Stratégia kybernetickej bezpečnosti. Stratégia určuje hlavne bezpečnostné ciele, ktoré je treba pre zachovanie informačnej a kybernetickej bezpečnosti v rámci mesta dosiahnuť a tiež roly, právomoci a zodpovednosti zamestnancov v oblasti kybernetickej bezpečnosti.

V tejto skrátenej verzii Bezpečnostnej politiky je zahrnutá aj relevantná časť Stratégie kybernetickej bezpečnosti mesta, hlavne ciele informačnej bezpečnosti a vyjadrenie podpory zo strany vedenia mesta.

2.2 Ciele informačnej bezpečnosti

2.2.1 Strategické (globálne) ciele

- Zabezpečiť trvalú integritu, dôvernosť a dostupnosť spracúvaných informácií a vytvárať tak predpoklady pre napĺňanie záujmov a poslania mesta Bratislava.
- Zabezpečiť súlad spracovávania informácií a osobných údajov s platnou legislatívou.

2.2.2 Hlavné ciele

- Zabezpečiť primeranú úroveň ochrany informačných systémov a údajov.
- Navrhovať bezpečnostné riešenia na základe rizík, ktoré ohrozujú informačné aktíva (softvér, hardvér, dáta).
- Zabezpečiť správnu a bezpečnú prevádzku systémov, ktoré slúžia na spracúvanie informácií a údajov.
- Zabezpečiť fyzické aj logické riadenie prístupu zamestnancov a poverených osôb k spracúvaným informáciám tak, aby nemali prístup k informáciám a systémom, ktoré k výkonu svojich pracovných úloh a funkcie nepotrebujú.
- Zabrániť fyzickému neautorizovanému prístupu osôb do lokalít mesta, ktoré nie sú prístupné verejnosti.
- Zabrániť elektronickému prístupu neoprávnených osôb k informačným systémom a údajom.
- Predchádzať prerušeniam a výpadkom, ktoré môžu pri prevádzke informačných systémov nastať a definovať postupy na obnovu dostupnosti v prípade ich výpadku.
- Monitorovať fyzické prostredie aj prostredie informačných systémov, analyzovať podozrivé udalosti a riešiť bezpečnostné incidenty, aby sa predišlo ich opakovaniu v budúcnosti.
- Zabezpečovať informovanie a školenia zamestnancov, externých pracovníkov a zamestnancov zmluvných strán, aby sa systematicky zvyšovalo ich bezpečnostné povedomie, aby svoje úlohy a činnosti vykonávali v súlade s Bezpečnostnou politikou.
- Zabezpečiť dodržiavanie zákonných a zmluvných požiadaviek v oblasti informačnej a kybernetickej bezpečnosti a zabezpečiť dodržiavanie zákonných požiadaviek na ochranu osobných údajov.

2.2.3 Operatívne ciele

Operatívne ciele sú obsiahnuté v jednotlivých interných smerniciach a politikách, ktoré obsahujú konkrétne opatrenia pre identifikáciu a elimináciu rizík a súvisia s realizáciou jednotlivých krokov pre zabezpečenie a zlepšovanie informačnej a kybernetickej bezpečnosti mesta.

2.3 Podpora a zodpovednosť zo strany vedenia mesta

Vedúci predstavitelia hlavného mesta Slovenskej republiky Bratislavy podporujú informačnú a kybernetickú bezpečnosť deklarovaním jej dôležitosti pred zamestnancami, preukazovaním angažovanosti a delegovaním zodpovedností. Základné zodpovednosti v rámci informačnej a kybernetickej bezpečnosti sú nasledovné:

- Riaditeľ magistrátu zodpovedá za zavedenie a priebežné zlepšovanie informačnej bezpečnosti a za zabezpečenie k tomu potrebných zdrojov.
- Bezpečnostný manažér spolu s vedúcim sekcie informatiky a dátovej politiky zodpovedajú za koordináciu, metodické riadenie a kontrolu dodržiavania informačnej a kybernetickej bezpečnosti.
- Vedúci oddelenia ľudských zdrojov zodpovedá za výber kvalifikovaných zamestnancov a za zabezpečenie ich vzdelávania v oblasti informačnej bezpečnosti.
- Osoby uvádzané v zmluvách so zmluvnými partnermi zodpovedajú za oboznámenie relevantných zmluvných partnerov s Bezpečnostnou politikou a relevantnými časťami bezpečnostnej dokumentácie.
- Zamestnanci v rámci svojich pracovných povinností v primeranej miere zodpovedajú za ochranu im zverených aktív (informácií, osobných údajov, aplikácií, dát, IT zariadení a pod.).

2.4 Zodpovednosť a povinnosti zamestnancov

Zamestnanci a pracovníci mesta dodržiavajú pri každodennej práci zásady informačnej bezpečnosti, opatrenia pre elimináciu rizík, pokyny pre prácu s informáciami a osobnými údajmi, a to predovšetkým:

- Chránia spracúvané informácie a osobné údaje dostupnými a vhodnými prostriedkami, aby neprišlo k ich poškodeniu, prezradeniu alebo zneužitiu.
- Zachovávajú mlčanlivosť, nezverejňujú, neposkytujú alebo nesprístupňujú údaje iným osobám, ak to priamo nevyplýva z ich pracovných pokynov alebo úloh.
- Pravidelne sa vzdelávajú v oblasti informačnej a kybernetickej bezpečnosti.
- Počas svojej práce sú obozretní a pozorní, pri pochybnostiach alebo neznalosti, či postupujú správne a v súlade s Bezpečnostnou politikou sa obrátia so žiadosťou o vysvetlenie a pokyny na nadriadených pracovníkov alebo na Bezpečnostného manažéra.

2.5 Klasifikácia informácií a aktív

Všetky informačné aktíva majú priradeného vlastníka a vedie sa ich evidencia. Vlastníkom aktíva je rola, predovšetkým riaditeľ sekcie.

S cieľom diferencovať požiadavky na ochranu informačných aktív (napríklad osobné údaje, utajované skutočnosti, citlivé informácie, atď.) je zavedená ich klasifikačná schéma.

Klasifikačná schéma rozlišuje podľa citlivosti aktíva 4 stupne:

- Verejné (dostupné verejnosti)
- Interné (dostupné všetkým zamestnancom mesta)
- Chránené (dostupné iba určitej skupine zamestnancov)
- Prísne chránené (dostupné iba vybraným jednotlivcom)

2.6 Riadenie súladu a audit

Cieľom tejto oblasti bezpečnosti je pravidelne, efektívne a objektívne kontrolovať dodržiavanie bezpečnostnej politiky a predchádzať porušeniam zákonných a zmluvných povinností a bezpečnostných požiadaviek.

Všetky právne a zmluvné požiadavky s dopadmi na informačný systém sa priebežne identifikujú a dokumentujú.

Kontrolné činnosti sa zameriavajú najmä na kontrolu dôvodu prístupu do informačného systému, dodržiavanie ustanovení bezpečnostnej politiky, právnych predpisov, interných predpisov a smerníc, nákup licencií a softvéru a dodržiavanie predpísaných pracovných postupov pri spracúvaní osobných údajov a pri používaní informačného systému.

Kontrola bezpečnosti informačného systému sa realizuje priebežne v rámci plnenia pracovných povinností zamestnancov v rozsahu stanovenom platnou legislatívou o vnútornom kontrolnom systéme mesta.

S cieľom priebežného a nezávislého vyhodnocovania stavu informačnej bezpečnosti a napĺňania cieľov bezpečnostnej politiky sekcia zabezpečí vykonanie pravidelného interného a/alebo externého auditu bezpečnosti jednotlivých informačných systémov mesta.

Audit bezpečnosti informačného systému sa realizuje nezávislým audítorom (nezávislá odborne kvalifikovaná tretia strana, ktorá sa priamo nepodieľala na vývoji, implementácii, údržbe alebo prevádzke informačného systému, ktorý je predmetom auditu).

2.7 Správa, revízia a kontrola dodržiavania

Politika informačnej bezpečnosti je revidovaná Bezpečnostným manažérom v ročnej periodicite v spolupráci s gestormi informačných systémov, resp. pri významných zmenách v architektúre IS, po závažných incidentoch alebo pri zmenách v legislatíve.

Zmeny zásad a cieľov stanovených bezpečnostnou politikou sú v odôvodnených prípadoch navrhované a spracovávané kompetentnými odbornými pracovníkmi zabezpečujúcimi metodické riadenie a výkon činností bezpečnosti a ochrany informačných systémov.

Kontrola dodržiavania politiky informačnej bezpečnosti a jej obsahovej náplne prebieha aj formou interných auditov informačnej bezpečnosti so zameraním na jednotlivé oblasti informačnej bezpečnosti.

2.8 Distribúcia dokumentu

Bezpečnostná politika mesta v jej plnom znení je interným dokumentom, ktorý obsahuje citlivé údaje a preto nie je voľne prístupná pre verejnosť. Skrátená verzia bezpečnostnej politiky (tento dokument) je prístupná verejnosti prostredníctvom webového portálu mesta.

2.9 Záver

Bezpečnostná politika nadobúda účinnosť po podpise primátorom dňa 15. 7. 2020.