HLAVNÉ MESTO SLOVENSKEJ REPUBLIKY BRATISLAVA

Primaciálne nám. 1, P. O. Box 192, 814 99 Bratislava 1

Bratislava 7. júla 2020

R O Z H O D N U T I E č. 26/2020
primátora hlavného mesta Slovenskej republiky Bratislavy,
ktorým sa vydáva dokument Politika informačnej bezpečnosti hlavného mesta Slovenskej republiky Bratislavy

Čl. 1

Týmto rozhodnutím vydávam Politiku informačnej bezpečnosti hlavného mesta Slovenskej republiky Bratislavy, ktorá je platná 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.

Čl. 2

Toto rozhodnutie nadobúda účinnosť 15. júla 2020

Ing. arch. Matúš Vallo, v.r.
primátor

Politika informačnej bezpečnosti

hlavného mesta Slovenskej republiky Bratislavy

30. júna 2020

Tento dokument obsahuje 29 strán

Bezp_politika_final_200630.docx

Schválil:

Ing. arch. Matúš Vallo

_____

primátor

Revízia dokumentu

História verzií

Verzia	Autor	Dátum vytvorenia
1.0	Mgr. Matej Evin	30. 6. 2020

História revízií

Revízia	Revízor	Dátum revízie
1.		
2.		
3.		
4.		
5.		

Schválenie dokumentu

Meno	Podpis	Dátum schválenia

Obsah

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.

Pôsobnosť tejto politiky sa vzťahuje na všetky informačné systémy a prostriedky, prevádzkové zariadenia, programy a aplikácie, siete a komunikačné systémy mesta.

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

Pre zabezpečenie dodržiavania zásad informačnej bezpečnosti budú s touto politikou v primeranom rozsahu oboznámení všetci zamestnanci mesta. Táto politika bude dostupná v plnom rozsahu všetkým zamestnancom prostredníctvom intranetu. Skrátená verzia tohto dokumentu bude tiež zverejnená a voľne dostupná prostredníctvom webového portálu mesta.

1.3 Zoznam pojmov a skratiek

Administrátor aplikácie/IS	Osoba, ktorá vykonáva v súvislosti s konkrétnou aplikáciou alebo informačným systémom špecifické správcovské činnosti, napr. parametrizáciu, riadenie prístupových práv a pod.
Aktívum	Všetko, čo má pre mesto hodnotu a je potrebné chrániť. Pozri tiež „informačné aktívum“.
Analýza rizík	Stanovenie a vyhodnotenie rizík vyplývajúcich z hrozieb relevantných pre aktíva mesta Bratislava.
Aplikácie a služby	Skrátene „aplikácie“ sú IT prostriedky evidované mestom, ktoré sú bezprostredne využívané aktérmi procesov pri výkone ich úloh za stanoveným účelom.
Autentifikácia	Proces overenia identity. Uistenie sa, že konkrétny používateľ (proces, komponent, systém) je skutočne ten, za koho sa prehlasuje.
Bezpečnostný incident	Každá udalosť, ktorá mala alebo môže mať za následok narušenie atribútov bezpečnosti informačného aktíva (dostupnosť, dôvernosť a integrita).
Bezpečnostný manažér, BM	Osoba zodpovedná za informačnú a kybernetickú bezpečnosť mesta, písomne poverená riaditeľom sekcie informatiky a dátovej politiky.
Bezpečnostné opatrenie	Bezpečnostný mechanizmus, postup alebo riešenie, ktoré je použité na zabezpečenie bezpečnostných atribútov informačných aktív a znižuje riziko. Môže byť v podobe technického, organizačného, personálneho, právneho alebo iného opatrenia alebo ich kombinácii.

Bezpečnosť IS	Je zabezpečenie nastavenia, dosiahnutia a udržiavania dôvernosti, integrity a dostupnosti informačných systémov mesta. Informačná bezpečnosť sa dosahuje implementáciou vhodnej sady bezpečnostných opatrení.
Bezpečnostné požiadavky	Určujú typ a stupeň bezpečnosti aktív podľa potrieb mesta a platnej legislatívy.
Dátovo-procesné aktíva	Logicky súvisiaca skupina údajov, ktoré buď vznikajú ako výstup, sú modifikované alebo zaznamenávané počas výkonu jedného alebo viacerých súvisiacich procesov patriacich mestu.
Dopad incidentu	Následky bezpečnostného incidentu, najmä narušenie dôvernosti, dostupnosti alebo integrity informačných aktív, poškodenie, nefunkčnosť, finančná strata a pod.
Dostupnosť	Vlastnosť (atribút bezpečnosti), ktorá umožňuje, aby aktíva boli autorizovaným subjektom dostupné nanajvýš s dopredu definovaným oneskorením. Záruka, že daná udalosť sa stane do určenej doby.
Dôvernosť	Vlastnosť (atribút bezpečnosti), ktorá charakterizuje neprístupnosť aktíva neautorizovaným subjektom.
Gestor aktíva	Osoba majúca detailné znalosti o aktíve z procesnej a vecnej stránky. Je stanovený vlastníkom aktíva podľa týchto odborných znalostí a sú na neho delegované čiastkové zodpovednosti.
Hrozba	Hrozba je každá úmyselná alebo neúmyselná udalosť, ktorá môže ohroziť informačné aktívum.
Informačná bezpečnosť	Ochrana informácií pred rizikom. Zachovanie dostupnosti, dôvernosti a integrity informácií.
Informačné aktívum	Aktívum súvisiace so spracúvaním údajov. Ide najmä o samotné údaje (dáta) ako aj o aplikácie a informačné systémy a iné IKT zariadenia a siete, ale tiež zahŕňa budovy a priestory mesta a ľudské zdroje.

Informačný systém, IS	Je funkčný celok, zabezpečujúci cieľavedomé a systematické zhromažďovanie, spracovávanie, uchovávanie a sprístupňovanie informácií.
Integrita	Vlastnosť (atribút bezpečnosti), ktorá charakterizuje, že aktívum nebolo zmenené alebo bolo zmenené len autorizovaným spôsobom.
Klasifikácia aktív	Zaradenie aktív do jednotlivých kategórii podľa požiadaviek na ich dôvernosť, integritu a dostupnosť.
Lokality	Jednotlivé pracoviská mesta, budovy, miestnosti a priestory.
Mesto	Mesto Bratislava, vrátane všetkých aktív, ktoré sú v pôsobnosti a správe mesta Bratislava.
Mimoriadna udalosť	Bezpečnostný incident s vážnym dopadom na informačné aktíva mesta.
Oddelenie PCOaI	Oddelenie Pultu centralizovanej ochrany a informatiky Mestskej polície.
Ohodnotenie aktíva	Priradenie stupňa negatívneho dopadu, ktorý by vznikol ako možný následok narušenia dostupnosti, dôvernosti alebo integrity realizáciou hrozby.
Osobný údaj	Akýkoľvek údaj týkajúci sa identifikovateľnej fyzickej osoby, pričom ju možno určiť priamo alebo nepriamo najmä na základe všeobecne použiteľného identifikátora (rodné číslo, číslo OP) alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu.
Používateľ	Osoba spracúvajúca informácie (tvorba, používanie, zmena, rušenie) počas vopred stanoveného postupu v priebehu plnenia svojej pridelenej úlohy.
Princíp najnižších privilégií	Priradenie najnižších potrebných oprávnení používateľom, procesom a aplikáciám tak, aby boli stále schopní vykonávať všetky pridelené úlohy.

Princíp úmernej klasifikácie	Použitie najnižšieho potrebného stupňa klasifikácie aktíva pri zachovaní adekvátnej úrovne bezpečnosti.
Princíp zodpovednosti	Povinnosť pracovníkov mesta označovať dokumenty v ich vlastníctve (resp. gescii) podľa definovaných postupov správnym klasifikačným stupňom na základe údajov, ktoré dané dokumenty obsahujú.
Riziko	Potenciálna možnosť, že určitá hrozba využije zraniteľnosť aktíva a spôsobí narušenie jeho bezpečnostných atribútov. Pravdepodobnosť naplnenia hrozby.
Sekcia IaDP/SIaDP	Sekcia informatiky a dátovej politiky
Systém manažérstva informačnej bezpečnosti	Časť celkového systému manažérstva, založená na prístupe k riziku podnikania, vytvorením, implementovaním, prevádzkovaním, monitorovaním, preskúmavaním, udržiavaním a zlepšovaním informačnej bezpečnosti. Systém manažérstva zahŕňa organizačnú štruktúru, politiky, plánovanie, zodpovednosti, praktiky, predpisy, procesy a zdroje.
Urgencia	Požiadavka ohlasovateľa incidentu, ako rýchlo sa má incident vyriešiť.
Útočník	Nositeľ hrozby, realizátor útoku
Útok	Naplnenie, realizácia hrozby s cieľom
Vlastník aktíva	Spravidla vedúci organizačnej jednotky, zodpovedný z celkového pohľadu za aktívum v rámci príslušnej procesnej oblasti, ktorá je v jeho pôsobnosti.
Závažný bezpečnostný incident	Bezpečnostný incident, ktorý spĺňa aspoň jedno identifikačné kritérium pre kybernetický bezpečnostný incident kategórie I., II. alebo III., podľa definície vyhlášky č. 165/2018.
Zraniteľnosť	Slabina informačného aktíva, ktorá môže byť zneužitá.

Zákon o ITVS	Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.
Zákon o KyB	Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

2 Pokyny pre používanie politiky 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 interných predpisov. Za detailné rozpracovanie politiky informačnej bezpečnosti zodpovedajú v rámci svojej zodpovednosti vedúci organizačných útvarov mesta spolu s Bezpečnostným manažérom.

Politika informačnej bezpečnosti je klasifikovaná ako interný dokument, a preto je sprístupnená všetkým zamestnancom mesta. Vybrané časti tohto dokumentu sú sprístupnené aj externým subjektom a tretím stranám, pokiaľ to bude pre výkon ich činnosti potrebné.

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 primátor mesta.

2.1 Riadia?e 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.

3 Základné bezpečnostné zásady a princípy

V tejto kapitole sú popísané zásady a princípy, ktoré je potrebné dodržiavať za účelom dosiahnutia základnej úrovne informačnej bezpečnosti v pôsobnosti mesta. Jednotlivé zásady sú rozdelené do tematických celkov podľa štruktúry štandardu ISO/IEC 27002:2013.

3.1 Bezpečnosť ľudských zdrojov

Cieľom bezpečnosti ľudských zdrojov je redukovať riziká súvisiace s ľudskými chybami, zlyhaniami, zneužitím práv, vedomými alebo nevedomými porušovaniami bezpečnostných zásad.

Pozície a zodpovednosti zamestnancov a tretích strán v oblasti bezpečnosti informačných systémov sa určujú a zadokumentujú. Táto požiadavka sa považuje za splnenú vydaním interných predpisov, ktoré vznikajú v procese implementácie bezpečnostnej politiky.

Procesu prijatia do zamestnania predchádza aj previerka bezúhonnosti žiadateľa o zamestnanie, primárne preverením výpisu z registra trestov.

Súčasťou pracovnej zmluvy je okrem všeobecného záväzku dodržiavania platných právnych predpisov a interných predpisov aj určenie zodpovednosti za dodržiavanie pravidiel a zásad v oblasti bezpečnosti informačných systémov.

Každý novoprijatý zamestnanec s prístupom do informačného systému sa zaškoľuje. Súčasťou vstupného školenia je aj poučenie o právach a povinnostiach ustanovených osobitnou legislatívou, o bezpečnostnej politike a o ďalších interných predpisoch vzťahujúcich sa na funkčné miesto novoprijatého zamestnanca. Novému zamestnancovi sa môže prideliť prístup na činnosti v informačnom systéme až po absolvovaní vstupného školenia. Písomné poučenie je súčasťou jeho osobného spisu.

Pri vzniku pracovnoprávneho vzťahu, v dôsledku ktorého vzniká oprávnenie využívať informačný systém, sa zamestnanec zaväzuje k zachovaniu mlčanlivosti o dôverných informáciách, s ktorými sa oboznámi pri plnení svojich pracovných povinností. Povinnosť zachovania mlčanlivosti o dôverných informáciách pretrváva aj po skončení pracovnoprávneho vzťahu.

Zvyšovanie bezpečnostného povedomia zamestnancov (formou školení, inštruktáží a podobne) sa vykonáva priebežne a kontinuálne. Súčasťou školenia je okrem iného aj vysvetlenie zodpovednosti používateľov informačného systému, upozornenie na bezpečnostné riziká a nahlasovanie bezpečnostných incidentov.

Pri ukončení používania informačného systému (napríklad z dôvodu skončenia pracovnoprávneho vzťahu alebo zmeny pracovnej pozície) používateľ informačného systému odovzdá nadriadenému všetky aktíva, ktoré sú v jeho správe.

Zároveň je zabezpečený proces odobratia alebo zmeny prístupových práv k informáciám a prostriedkom na ich spracúvanie podľa aktuálneho stavu a potrieb.

Porušenie právnych alebo interných predpisov mesta v oblasti informačnej bezpečnosti sa považuje za porušenie pracovnej disciplíny a so zamestnancom je začatý disciplinárny proces.

Z úrovne nadriadených je od zamestnancov a zmluvných partnerov vyžadované uplatňovanie bezpečnosti v súlade so zavedenými politikami a postupmi, čím sú naplnené požiadavky tzv. „manažérskej zodpovednosti“.

3.2 Riadenie a klasifikácia aktív

Cieľom tejto oblasti bezpečnosti je udržiavať adekvátnu ochranu aktív podľa ich hodnoty pre mesto. Za týmto účelom je potrebné viesť úplný a aktuálny prehľad o stave všetkých aktív mesta, s primárnym zameraním na informačné aktíva.

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

Informačné aktíva majú explicitne určený svoj životný cyklus.

Vedenie evidencie informačných aktív zabezpečuje vlastník aktív v spolupráci s gestorom príslušného informačného systému.

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

Za klasifikáciu informačných aktív podľa tejto schémy a definovanie požiadaviek na ochranu zodpovedá vlastník aktíva.

Detailná metodika klasifikácie aktív je uvedená v osobitnom internom predpise.

Za účelom ochrany informácií uchovávaných na prenosných médiách sú definované postupy na ochranu pred neoprávneným oboznámením sa, prezradením, zmenou, odstránením alebo zničením týchto informácií.

Uvedené postupy zahŕňajú aj spôsob likvidácie týchto médií, resp. ich vyradenie z prevádzky v prípade ich poškodenia alebo ukončenia životnosti.

Ochrana informácií na prenosných médiách sa zabezpečuje aj v kombinácii s kryptografickými prostriedkami v súlade s kapitolou 3.4 tejto politiky.

3.3 Riadenie prístupov do informačného systému

Cieľom tejto oblasti je predchádzať neoprávnenému prístupu do informačného systému a neoprávnenému použitiu informačného systému a zariadení v počítačových sieťach mesta.

Prístup používateľa do informačného systému sa prideľuje iba v rozsahu nevyhnutnom na plnenie jeho pracovných povinností.

Prístupy do informačného systému, ktoré sú nad rámec rozsahu nevyhnutnom na plnenie pracovných povinností používateľa informačného systému, sú zakázané (tzv. princíp Least privilege). Rovnako je používateľom udeľovaný prístup do siete a len k tým sieťovým službám, na ktorých použitie boli špecificky autorizovaní.

Systémy na riadenie hesiel sú interaktívne, poskytujú kvalitné heslá a presadzujú používanie individuálnych ID používateľov a hesiel, aby sa udržala sledovateľnosť zodpovednosti.

O pridelenom prístupe sa vytvárajú záznamy, ktoré sú archivované.

Používanie privilegovaných a špeciálnych oprávnení ako aj kritických kombinácií prístupových práv, ktoré vytvárajú zvýšené riziko zneužitia informačného systému, je potrebné čo najviac obmedziť. O pridelení takýchto prístupových práv konkrétnemu zamestnancovi rozhoduje vždy jeho nadriadený v spolupráci s BM.

Spôsoby a technickú realizáciu autentifikácie schvaľuje BM, rovnako ako aj politiku kvality hesiel, prípadne iných autentifikačných metód.

O prístupových právach je potrebné viesť osobitnú evidenciu na príslušnom útvare, zaviesť postupy na pravidelné preverovanie ich opodstatnenosti a po uplynutí potreby takéto prístupové práva neodkladne zrušiť. Pridelené prístupové práva sa v pravidelných intervaloch kontrolujú a prehodnocujú.

Za nedovolenú kombináciu prístupových práv je považovaná kombinácia vytvárajúca zvýšené riziko zneužitia informačného systému a umožňujúca u jedného používateľa informačného systému zlúčenie činností:

- zaznamenania transakcií ako vytvárania, zadávania a spracovania údajov, autorizácie transakcie (schválenia a potvrdenia údajov) a kontroly transakcie (previerky a odsúhlasenia údajov) vrátane akejkoľvek kombinácie,
- vývoja, testovania, správy, údržby aplikácie a činností podľa predchádzajúceho bodu vrátane akejkoľvek kombinácie.

Odobratie prístupových práv je možné v odôvodnených mimoriadnych prípadoch na základe rozhodnutia BM, pričom o tejto skutočnosti je neodkladne informovaný nadriadený používateľa, ktorému boli prístupové práva odobraté.

Používatelia sa zaväzujú mlčanlivosťou o spracúvaných údajoch; to neplatí, ak právny predpis ustanovuje inak a sú zodpovední za ochranu prístupových údajov a prostriedkov, ktoré sú im zverené. O tejto skutočnosti sú používatelia informovaní pri získaní prístupu k daným údajom a porozumenie tejto skutočnosti vyjadrujú písomne svojím podpisom.

Do každého informačného systému alebo aj subsystému sa zabudovávajú mechanizmy na zaznamenávanie aktivít jeho používateľov pri činnosti s údajmi

stanovených kategórií. Všetky činnosti používateľov informačného systému vykonávané pri činnosti s aplikáciami daného informačného systému sa môžu monitorovať.

Pre každú aplikáciu alebo systémový prvok informačného systému sa definujú udalosti a dôvody oprávneného prístupu do informačného systému, ktoré sa monitorujú trvalo (každá udalosť daného typu je zaznamenaná v žurnálových súboroch). Zabezpečuje sa tiež aj priebežné vyhodnocovanie údajov z monitorovania.

Za zabezpečenie systému monitorovania informačného systému a za stanovenie aktívnych a pasívnych transakcií používateľov informačného systému, ktoré majú byť monitorované, zodpovedá útvar, ktorý požaduje informačný systém alebo vývoj informačného systému v spolupráci s budúcim gestorom informačného systému.

Aktivity používateľov informačného systému s privilegovanými a špeciálnymi oprávneniami a dotazy používateľov informačného systému z dôvodu prevencie ich zneužitia a možnosti vyhodnotenia udalostí sa zaznamenávajú tak, aby bolo možné jednoznačne identifikovať kto, kedy, kde a s akou aplikáciou alebo dátami pracoval.

Monitorovanie a archivácia záznamov z aktivít používateľov informačného systému sú v informačnom systéme povinné a sú nevyhnutnou súčasťou inštalácie, resp. konfigurácie IS alebo aplikácie. Doba archivácie je definovaná v registratúrnom poriadku.

Monitorovanie, vyhodnocovanie a archivácia záznamov s aktivitami používateľov informačného systému pri činnosti s údajmi sú vykonávané gestorom informačného systému na základe spresnenia technického prevádzkovateľa informačného systému.

Vykonávanie neštandardných alebo neodôvodnených aktivít používateľmi informačného systému sa považuje za porušenie pracovnej disciplíny, za ktoré príslušný nadriadený vyvodí disciplinárne opatrenia a v prípade, že to považuje za potrebné, navrhne Bezpečnostnému manažérovi odobratie prístupových práv pre daného používateľa.

Rovnako, ako je vedená evidencia prístupových práv používateľov, je vedená aj evidencia prístupov a oprávnení na úrovni jednotlivých systémov, prípadne aplikačných účtov. Táto evidencia, resp. potreba týchto prístupov je taktiež kontrolovaná a prehodnocovaná v pravidelných intervaloch Bezpečnostným manažérom.

Systémové prístupy sú rovnako predmetom auditných záznamov a logovania.

Používanie systémových programov a aplikácií, ktoré môžu spôsobiť prevzatie kontroly nad systémom alebo jeho časťou, prípadne ho poškodiť alebo inak znefunkčniť je prísne zakázané, resp. ich použitie na legitímne účely je prísne kontrolované a riadené.

Prístup k zdrojovému kódu programov je riadený a obmedzovaný len na nevyhnutné prípady.

3.4 Použitie kryptografi?ký?h opatrení

Cieľom tejto oblasti je uistenie sa, že za účelom zabezpečenia dôvernosti a integrity údajov pri zachovaní požadovanej dostupnosti sú nasadzované len schválené a bezpečné kryptografické opatrenia a algoritmy riadeným, efektívnym a najmä bezpečným spôsobom.

Bezpečnostný manažér spravuje zoznam schválených kryptografických algoritmov a ich parametrov.

Implementácia kryptografických algoritmov je realizovaná spôsobom, ktorý zamedzuje vzniku rôznych postranných kanálov alebo nesprávnej implementácie vedúcej k možnosti prelomenia týchto kryptografických algoritmov.

Nasadenie konkrétnych kryptografických algoritmov v rámci informačných aktív vyplýva z analýzy rizík, klasifikácie aktív a rozhodnutí o spôsobe riadenia rizík.

Správa kryptografických kľúčov je zabezpečovaná centralizovaným spôsobom prostredníctvom povereného zamestnanca oddelenia mestského informačného systému, resp. Bezpečnostného manažéra. Správa kryptografických kľúčov v rámci Mestskej polície je zabezpečovaná vedúcim oddelenia PCOaI.

Používanie kryptografických prostriedkov je efektívne riadené, monitorované a kontrolované.

Na používanie, ochranu a riadenie celého životného cyklu kryptografických kľúčov sa vytvorí a zavedie interná smernica.

3.5 Fyzi?ká bezpečnosť informačného systému

Cieľom tejto oblasti bezpečnosti je minimalizovať riziká neoprávneného fyzického prístupu k aktívam, ich krádeže, zneužitia, zničenia alebo ohrozenia vyššou mocou (napr. prírodné živly).

Technické prostriedky informačného systému je možné inštalovať, uchovávať a prevádzkovať len v priestoroch, ktoré sú zabezpečené jednotným systémom zabezpečenia podľa osobitného predpisu, s výnimkou technických prostriedkov určených na špeciálne terénne (externé) použitie (napr. rozbočovače).

Technické prostriedky IS je možné používať, len ak sú dodržané požadované prevádzkové podmienky v rozsahu bezpečnostných dokumentácií.

Údržba technických prostriedkov informačného systému sa vykonáva definovanými zamestnancami alebo zamestnancami zmluvných dodávateľov v súlade so stanovenými postupmi.

Kľúčové zariadenia informačného systému (servery, centrálne sieťové prvky a pod.) sa umiestňujú v priestoroch, ktoré spĺňajú špeciálne požiadavky na zabezpečenie fyzickej a objektovej bezpečnosti.

Priestory sa chránia pred nadmernou teplotou, prašnosťou, vlhkosťou, vibráciami, chemickým znečistením a podobne. Nesmú sa súčasne využívať ako kancelárske priestory alebo priestory iného pracovného charakteru. V týchto priestoroch sa upratuje alebo vykonávajú servisné služby len pod dohľadom oprávneného pracovníka.

Elektrická alebo telekomunikačná kabeláž prenášajúca dáta alebo podporujúce informačné služby je primerane chránená pred odpočúvaním, postrannými kanálmi, manipuláciou alebo poškodením.

Útvary mesta majú vytvorenú chránenú zónu s kontrolovaným a monitorovaným pohybom neoprávnených osôb (prostredníctvom vrátnice). Vstup cudzej osoby do tejto zóny sa môže umožniť až po jej identifikácii zamestnancom strážnej služby alebo informátorom a overení cieľa návštevy. Cudzia osoba sa v bezpečnostnej zóne môže pohybovať len v sprievode povereného zamestnanca mesta.

Prístupové body, akými sú priestory na nakladanie a vykladanie, ako aj iné body, kde môže neautorizovaná osoba získať prístup do priestorov organizácie, sú kontrolované a štandardne sa umiestňujú tak, aby boli izolované od prostriedkov na spracúvanie informácií.

Uvedené pracoviská sa umiestňujú v budovách primerane zabezpečenými opatreniami fyzickej a objektovej bezpečnosti. Táto požiadavka sa vzťahuje aj na prenajaté priestory a priestory dodávateľov.

V prípade používania zdieľaných prenajatých priestorov s cudzími inštitúciami sa priestor patriaci mestu vymedzuje a chráni tak, aby nedochádzalo k vstupu neoprávnených osôb.

Na pracoviskách mesta sa uplatňuje a vynucuje politika čistého stola (pokiaľ ide o dokumenty a prenosné médiá) a politika čistej obrazovky (pokiaľ ide o prostriedky spracúvania informácií). Uvedené politiky majú na zreteli najmä existujúcu klasifikáciu informácií, požiadavky vyplývajúce z uzatvorených zmlúv a legislatívne požiadavky.

Sú prijaté opatrenia, aby sa zariadenia, informácie alebo softvér bez autorizácie neodnášal mimo určených pracovísk mesta; rovnako aj opatrenia na zabezpečenie vhodnej ochrany neobsluhovaných zariadení.

Likvidácia všetkých technických prostriedkov, najmä tých, ktoré obsahujú nosiče dát, je riadená formálnym a protokolárnym spôsobom v súlade s klasifikačnou schémou a o každej likvidácii je vyhotovený záznam.

3.6 Bezpečnosť prevádzky informačného systému

Cieľom tejto oblasti je zabezpečiť správnu a bezpečnú prevádzku informačného systému, predchádzať narušeniu bezpečnosti pri činnosti s pamäťovými médiami, predchádzať strate, modifikácii alebo zneužitiu informácií pri ich výmene s okolím mesta (napríklad informačný systém ďalších orgánov štátnej správy).

Pri zmenách v prevádzkovom prostredí (napríklad hardvér, aplikačné programové vybavenie, operačné systémy) nesmie byť podstatným spôsobom narušená prevádzka ani znížená bezpečnosť informačného systému.

Používanie prenosných médií (napríklad USB kľúče) sa formálne upravuje a povoľuje iba pre určené spôsoby použitia.

Pri zasielaní údajov mimo prostredia mesta sa vždy zohľadňujú požiadavky interných predpisov, hlavne klasifikačnej smernice.

Na zaistenie správneho využívania bezpečnostných mechanizmov sa spôsob ich použitia zadokumentuje. Pre každú významnú aplikáciu informačného systému sa požaduje

- používateľská dokumentácia,
- administrátorská dokumentácia,
- prevádzková dokumentácia.

Dokumentácia uvedená v predchádzajúcom odseku je udržiavaná, posudzovaná, v prípade potreby aktualizovaná a dostupná stanoveným spôsobom pre všetkých relevantných používateľov.

Zmeny v prevádzkovom prostredí informačného systému sa vykonávajú riadeným spôsobom pokrývajúc zmeny:

- aplikácií a databáz,
- v operačných systémoch, ich konfigurácii a technologickej infraštruktúre informačného systému,
- prevádzkových postupov.

Zmeny aplikácií a databáz sa vykonávajú iba v odôvodnených prípadoch po schválení schvaľovateľom zmeny.

Všetky zmeny musia byť schválené schvaľovateľom zmeny a v prípade zmeny majúcej vplyv na bezpečnosť IS alebo aktíva aj Bezpečnostným manažérom. Plánovaná zmena sa vopred schvaľuje vedúcim oddelenia mestského informačného systému. V rámci IS Mestskej polície sú zmeny schvaľované vedúcim Oddelenia PCOaI v súčinnosti s vedúcim oddelenia mestského informačného systému.

Zmeny musia byť otestované mimo produkčného prostredia. Všetky zmeny sa zadokumentujú.

Všetky zmeny v rámci informačného systému je možné vykonávať len s využitím štandardizovaných postupov schválených mestom.

Na ochranu pred stratou alebo poškodením sa všetky dôležité databázy chránia zálohovaním. Zálohovanie sa vykonáva pravidelne a takým spôsobom, aby nenarúšalo bežnú prevádzku informačného systému. Pre médiá obsahujúce záložné kópie sa zaisťuje rovnaký stupeň bezpečnosti, ako je požadovaný pre údaje, ktoré sú na nich uložené. Tieto médiá sa zároveň uchovávajú mimo lokalít s centrálnymi komponentmi informačného systému tak, aby sa minimalizovalo riziko súčasného poškodenia originálnych aj záložných údajov.

Ako prevencia zlyhaní informačného systému sa využíva pravidelné monitorovanie podľa osobitného predpisu v týchto oblastiach:

- záťaž kľúčových komponentov informačného systému a komunikačnej infraštruktúry,
- kapacitné rezervy kľúčových komponentov informačného systému (napríklad voľné miesto na systémovom disku),
- výskyt chýb v informačnom systéme (z hľadiska technického aj aplikačného).

Prevádzkové prostredie je logicky aj galvanicky oddelené od testovacieho alebo vývojového prostredia.

Prevádzkové záznamy sú pravidelne kontrolované a vyhodnocované nielen z pohľadu funkčnosti a dostatočnej kapacity ale aj z pohľadu bezpečnosti, najmä z pohľadu výskytu možných bezpečnostných incidentov.

Auditné záznamy a logy sú chránené voči neoprávnenej zmene alebo zničeniu aj voči privilegovaným používateľom.

Softvér nasadzovaný do produkčného prostredia musí byť náležite otestovaný. V prípade mimoriadne citlivých systémov by malo byť zabezpečené prezretie zdrojových kódov a následne zabezpečená formálna, protokolárna kompilácia aplikácie v prostredí pod kontrolou mesta. Proces nasadenia alebo inštalácie softvéru je rovnako zabezpečený formálnym spôsobom eliminujúcim prípadné bezpečnostné riziká.

Jednotlivé systémy sú pravidelne podrobované testovaniu zraniteľností. Za dodržiavanie harmonogramu a dostatočnej úrovne testovania zodpovedá Bezpečnostný manažér.

Možnosti prieniku škodlivého kódu (napríklad počítačové vírusy) do informačného systému sa minimalizujú, rovnako ako aj následky takéhoto prieniku. S týmto cieľom sa implementujú adekvátne bezpečnostné mechanizmy a pracovné postupy,

pre všetkých používateľov informačného systému platí striktný zákaz ich obchádzania.

Synchronizácia času na všetkých relevantných systémoch mesta je zabezpečená prostredníctvom schváleného presného referenčného zdroja času.

3.7 Bezpečnosť komunikácie

Cieľom tejto oblasti je zabezpečenie údajov pri ich prenose v rámci počítačových sietí a sieťových prvkov.

Sieťová architektúra musí byť budovaná tak, aby minimalizovala riziká vyplývajúce z rôznych typov útokov.

Interné segmenty LAN sietí mesta sa chránia tak, aby mohli byť považované za dôveryhodné prostredia.

Celková sieťová architektúra by mala byť budovaná zo sieťových segmentov, ktoré spolu komunikujú a sú navzájom oddelené. Segmenty sú vytvorené za účelom prepojenia zariadení rovnakého typu, zariadení určených na konkrétny jednotný účel alebo zariadení, ktoré spracúvajú informácie klasifikované rovnakým klasifikačným stupňom.

Jednotlivé segmenty by mali byť od seba oddelené na rôznych úrovniach. Nezabezpečené segmenty a segmenty DMZ musia byť oddelené fyzicky – použitím samostatných prepínačov pre každý segment. Serverové segmenty a segmenty s pracovnými stanicami môžu byť od seba oddelené na fyzickej úrovni alebo na logickej úrovni – takzvanými VLAN.

Použité komunikačné smerovače a prepínače je nutné zabezpečiť proti neautorizovanej zmene ich konfigurácie.

Jednotlivé segmenty by mali byť od seba oddelené zariadeniami s funkcionalitou firewallu, ktoré umožnia filtrovať sieťovú premávku medzi segmentmi aspoň podľa zdroja, cieľa a typu služby.

Pravidlá pre filtrovanie musia byť nastavené tak, aby boli pre jednotlivé segmenty a zariadenia v nich pripojené dostupné len nevyhnutne potrebné služby.

Pre každý typ použitého zariadenia by mal existovať konfiguračný štandard, popisujúci jeho bezpečnú konfiguráciu.

Zapájanie ľubovoľných zariadení do počítačových sietí a ostatnej komunikačnej infraštruktúry môžu vykonávať iba zamestnanci sekcie informatiky a dátovej politiky a tretia strana na základe zmluvného vzťahu. V prípade Mestskej polície sú oprávnení týmito úkonmi tiež zamestnanci oddelenia PCOaI. Zmeny v komunikačnej infraštruktúre a jej prepojenia s externými sieťami sa schvaľujú Bezpečnostným manažérom.

Požadovaná bezpečnosť prenášaných informácií prostredníctvom všetkých druhov komunikačných zariadení v rámci organizácie a s ktoroukoľvek treťou stranou je zabezpečená implementáciou interných politík, postupov a opatrení.

3.8 Nákup, vývoj a údržba informačného systému

Cieľom tejto oblasti bezpečnosti je zaistiť identifikáciu a implementáciu bezpečnostných opatrení nutných na bezpečnú prevádzku nových informačných technológií počas vývoja a nasadzovania a zaistiť, aby projekty informačných systémov prebiehali riadeným a bezpečným spôsobom.

Rozhodnutia o akvizícii alebo vývoji a realizácii nového informačného systému, aplikácie alebo subsystému v rámci informačného systému sa prijímajú v súlade s požiadavkami gestora informačného systému.

Mali by sa vytvoriť, dokumentovať, udržiavať a zaviesť princípy bezpečného vývoja systémov pre všetky činnosti spojené so zavedením informačných systémov mesta.

Je potrebné vytvoriť a primerane chrániť vývojové prostredie na vývoj systémov a ich integráciu s úsilím, ktoré pokryje celý životný cyklus vývoja.

Vývoj softvéru prostredníctvom outsourcingu (externých zdrojov) by mal byť pod dohľadom mesta a mali by sa monitorovať a vyhodnocovať jednotlivé aktivity vývoja systému, ktorý sa vykonáva takouto formou.

Súčasťou každého projektu informačného systému je analýza rizík súvisiacich s vývojom a prevádzkovým prostredím nových prvkov informačného systému.

Pre každý projekt informačného systému sa identifikujú a špecifikujú bezpečnostné požiadavky v spolupráci s Bezpečnostným manažérom a IT architektom.

Súčasťou každého projektu informačného systému je návrh bezpečnostných testov a návrh formy overenia dostatočnosti bezpečnosti nových prvkov informačného systému pred ich zavedením do bežnej prevádzky.

Súčasťou každého projektu informačného systému je vypracovanie príslušnej projektovej dokumentácie a popis bezpečnostnej architektúry a jej zavedenie do evidencie, ktorý vedie poverený zamestnanec oddelenia mestského informačného systému.

Predpokladom zavedenia informačného systému do produkčnej prevádzky je spracovanie prevádzkovej, administrátorskej a používateľskej dokumentácie k informačnému systému.

Prevádzkovú dokumentáciu tvorí najmä:

- popis prevádzkových postupov,
- popis postupov zotavenia sa z bežných chýb,

- rozdelenie a popis rolí a funkcií pri prevádzke informačného systému,
- popis konfigurácie informačného systému a umiestenia jeho jednotlivých fyzických a aplikačných komponentov,
- politika použitia kryptografických opatrení,
- podrobný popis aktivít rutinne vyžadovaných pri prevádzke informačného systému,
- šablóny operátorských denníkov a uvedenie typov udalostí, ktoré sa do nich zapisujú,
- popis spôsobov riadenia a plánovania zmien a implementácie nových verzií a rozšírení,
- popis spôsobov zálohovania údajov,
- popis spôsobov monitorovania prevádzky (z hľadiska záťaže, kapacít, konfigurácie, chýb).

Administrátorskú dokumentáciu tvorí najmä:

- popis správy bezpečnostných mechanizmov a procedúr vo vzťahu k administrátorom informačného systému,
- popis správy používateľov informačného systému,
- popis správy údajov v informačnom systéme,
- vysvetlenie spôsobu konfigurácie informačného systému,
- rozdelenie a popis funkcií pri administrácii informačného systému,
- šablóny administrátorských denníkov a uvedenie typov udalostí, ktoré sa do nich zapisujú.

Používateľskú dokumentáciu tvorí najmä:

- popis ovládania informačného systému a využívanie jeho služieb,
- pravidlá používania informačného systému,
- popis bezpečnostných procedúr a ovládanie bezpečnostných mechanizmov vo vzťahu k používateľom informačného systému,
- popis chybových hlásení.

V každom projekte informačného systému je zriadená a obsadená rola, ktorá zodpovedá za integráciu bezpečnostných opatrení do predmetu projektu informačného systému. Ďalej táto rola zabezpečuje:

- zohľadnenie právnych predpisov a technologických požiadaviek na bezpečnosť,
- vykonanie analýzy rizík,
- špecifikovanie bezpečnostných opatrení,
- zabezpečenie súladu s celkovou bezpečnostnou architektúrou mesta a strategickou architektúrou verejnej správy.

Na zaistenie primeranej úrovne bezpečnosti v každom projekte informačného systému sa vývojové a testovacie prostredie oddeľujú od produkčného prostredia tak, aby nemohlo dochádzať k ich bezpečnostne neprípustnému prelínaniu. Pri testovaní vyvíjaných komponentov sa nepoužívajú údaje z produkčných databáz, v opačnom prípade pre testovacie prostredie sa vytvárajú rovnaké bezpečnostné opatrenia ako pre produkčné prostredie.

Informácie a dáta obsiahnuté v transakciách aplikačných služieb musia byť chránené, aby sa zabránilo nekompletným prenosom, nesprávnemu smerovaniu, neautorizovaným úpravám správ, neautorizovanému prezradeniu, neautorizovanému duplikovaniu správ alebo neautorizovaným odpovediam.

Implementácia zmien do systémov v rámci ich životného cyklu musí byť riadená prostredníctvom formálne zavedených procedúr riadenia zmien.

Pri zmene operačného systému sa vykoná revízia kritických aplikácií, ako aj testovanie s cieľom zabezpečiť, že to nebude mať za následok negatívny vplyv na prevádzku organizácie alebo na bezpečnosť.

Testovacie údaje sa musia starostlivo a vhodne vyberať, chrániť a riadiť. Používanie prevádzkových údajov, ktoré obsahujú osobné alebo iné citlivé informácie na testovacie účely nie je povolené, pokiaľ testovacie prostredie nespĺňa rovnaké bezpečnostné opatrenia ako produkčné prostredie.

Súčasťou každého projektu informačného systému je definícia bezpečnostných testov. Tieto testy sa vykonávajú pred spustením predmetu projektu informačného systému v produkčnom prostredí. Záverečná správa zahŕňajúca výsledky z týchto testov je súčasťou projektovej dokumentácie. Za definovanie, poverenie výkonom a vyhodnotenie testov je zodpovedný Bezpečnostný manažér.

V každom projekte informačného systému sa určujú roly, ktoré budú vykonávať údržbu predmetu projektu informačného systému po jeho zavedení do rutinnej prevádzky. Pri definícii týchto rolí a ich následnom personálnom obsadzovaní sa špecifikujú a zohľadňujú požiadavky na ich nezlučiteľnosť a vzájomnú zastupiteľnosť.

3.9 Riadenie vzťahov s tretími stranami

Pri uzatváraní zmlúv s treťou stranou sa zmluvne stanovia primerané opatrenia pre tretiu stranu tak, aby nedošlo k porušeniu bezpečnostnej politiky, právnych predpisov a interných predpisov.

Pred prístupom tretej strany k aktívam mesta sú vždy definované bezpečnostné požiadavky na tretie strany, ktoré musí tretia strana dodržiavať za účelom ochrany aktív mesta.

Dohodnuté zmluvné podmienky musia vyžadovať aj umožnenie výkonu auditu bezpečnosti a kontroly dodržiavania stanovených podmienok treťou stranou zo strany mesta.

Tretia strana a jej zamestnanci musia byť poučení o bezpečnostných požiadavkách, ktoré sú kladené na používateľov zo strany mesta, vrátane spôsobov identifikácie, nahlasovania a riešenia bezpečnostných incidentov.

Na komunikáciu alebo výmenu dát s tretími stranami sa na základe analýzy rizík môžu použiť kryptografické prostriedky podľa kapitoly 3.4 tejto politiky.

3.10 Riadenie bezpečnostných incidentov

Cieľom tejto oblasti je zabezpečiť identifikovanie a nahlasovanie bezpečnostných incidentov spôsobom, ktorý umožní včasnú reakciu vedúcu k náprave a k minimalizácii škôd a zaisteniu účinného prístupu k zvládaniu bezpečnostných incidentov.

Pre zvládanie bezpečnostných incidentov sa definujú a zavedú jasné postupy ako aj mechanizmy pre kvantifikáciu a monitorovanie typov a rozsahu bezpečnostných incidentov vrátane nákladov na ich zvládanie.

Zamestnanci mesta alebo tretie strany bezodkladne hlásia akékoľvek zistenia alebo podozrenia na bezpečnostné riziká v informačnom systéme mesta.

V prípade, že je bezpečnostný incident zistený na strane dodávateľa (napr. ak tretia strana zabezpečuje výkon jednotky SOC pre pôsobnosť mesta), ohlasovateľ incidentu je určený na základe zmluvnej dohody s dodávateľom.

Bezpečnostné incidenty sa nahlasujú definovaným spôsobom na stanovenom kontaktnom mieste a definovanej kontaktnej osobe okamžite a bez zbytočného zdržania.

Okamžite ako vznikne podozrenie, že došlo k bezpečnostnému incidentu, je potrebné začať zaznamenávať všetky fakty a dôkazy, ktoré s ním môžu súvisieť pre potreby možnej forenznej analýzy dôkazov.

Bezpečnostné incidenty, ktoré presahujú rámec mesta a závažné bezpečnostné incidenty sa oznamujú národnej jednotke SK-CERT NBÚ a vládnej jednotke CSIRT.SK ÚPVII v rozsahu definovanom zákonom.

Pri riešení bezpečnostných incidentov presahujúcich rámec mesta a závažných bezpečnostných incidentov, ktorých riešenie iniciovala národná jednotka SK-CERT NBÚ alebo vládna jednotka CSIRT.SK ÚPVII, je poskytovaná maximálna potrebná súčinnosť.

Poznatky získané z analýzy a riešenia incidentov informačnej bezpečnosti sú zaznamenávané a mali by sa použiť na zníženie pravdepodobnosti alebo následkov budúcich incidentov.

3.11 Riadenie kontinuity činností

Cieľom v tejto oblasti je zabezpečiť funkčnosť činností mesta závislých na informačnom systéme počas výpadkov informačného systému a včasné zotavenie sa z výpadku informačného systému alebo jeho častí.

Za týmto účelom je definovaná politika a stratégia kontinuity činností mesta a sú definované a udržiavané plány obnovy činností mesta.

Pre každý informačný systém sa na základe analýzy rizík a najmä analýzy dopadov vyžaduje:

- určenie kategórie jeho kritickosti podľa klasifikačnej smernice,
- stanovenie maximálnych tolerovateľných výpadkov informačného systému,
- definovanie priority obnovy pri globálnom výpadku informačného systému,
- spracovanie náhradných postupov činností počas výpadku informačného systému,
- spracovanie postupov obnovy funkčnosti informačného systému pri jeho výpadku.

Pre prípady poruchy informačného systému sa spracovávajú havarijné plány informačného systému.

Havarijný plán informačného systému obsahuje najmä:

- vymedzenie rozsahu, účelu a prípadov využitia,
- popis interných a externých rolí podieľajúcich sa na tvorbe a použití plánu,
- popis činností súvisiacich s inicializáciou plánu a rozhodnutí o aktivácii plánu,
- popis havarijných procedúr – činností slúžiacich na návrat z havarijného stavu do normálneho prevádzkového stavu.

Pre potreby zabezpečenia kľúčových činností závislých na informačnom systéme počas výpadkov informačného systému sa spracovávajú postupy náhradného výkonu činností. Za udržiavanie aktuálnosti a výkon týchto postupov je zodpovedný vedúci oddelenia mestského informačného systému v spolupráci s Bezpečnostným manažérom.

Zariadenia používané pre zabezpečenie kľúčových činností mesta by mali byť zriadené s dostatočnou redundanciou, aby sa dosiahli definované požiadavky na dostupnosť.

Za spracovanie, pravidelné revidovanie a testovanie havarijných plánov informačného systému, spracovanie postupov náhradného výkonu činností počas výpadku informačného systému, stanovenie procedúr pre zálohovanie a obnovu funkčnosti rozhodujúcich prvkov informačného systému a prípadnú evakuáciu prvkov informačného systému a zabezpečenie prechodu na funkčné záložné riešenie v prípade neakceptovateľného trvania havarijného stavu je zodpovedný technický prevádzkovateľ informačného systému v spolupráci s gestorom informačného systému a Bezpečnostným manažérom.

3.12 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.

Opatrenia a zodpovednosti za naplnenie požiadaviek sa zadokumentujú a zavedú do praxe.

Pri posudzovaní právnych dosahov na informačný systém a informačné aktíva je potrebné zamerať najmä na tieto oblasti:

- používanie autorských diel v súlade s autorskými zmluvami a licenčnými ustanoveniami,
- tvorba autorských diel zamestnancami mesta,
- ochrana spracúvaných osobných údajov,
- využitie všeobecne záväzných právnych predpisov,
- právne pokračovanie riešenia bezpečnostných incidentov v rámci právnych predpisov a interných predpisov.

Kontrolné činnosti sa zameriavajú najmä na kontrolu dôvodu prístupu do informačného systému, dodržiavanie ustanovení bezpečnostnej politiky, právnych

predpisov, interných predpisov a dodržiavanie predpísaných pracovných postupov pri spracúvaní 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.

Kontrolu implementovania a dodržiavania zásad, opatrení a technológií slúžiacich na zaistenie bezpečnosti príslušného informačného systému mesta je oprávnený vykonávať:

- riaditeľ sekcie IaDP alebo ním poverená osoba,
- Bezpečnostný manažér,
- poverená zodpovedná osoba za ochranu osobných údajov.

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

Detailné postupy na dodržanie súladu sú uvedené v osobitnom predpise.

Základné ciele auditu sú najmä:

- posudzovanie adekvátnosti a efektívnosti systému riadenia informačnej bezpečnosti a jeho zložiek,
- posudzovanie dostatočnosti, účinnosti a využitia bezpečnostných opatrení,
- poskytovanie dostačujúcej istoty, že informačná bezpečnosť a jej riadenie je na primeranej úrovni,
- vyhodnocovanie súladu aktuálneho stavu informačnej bezpečnosti mesta s bezpečnostnou politikou a ďalšími internými predpismi, normami a štandardmi pre oblasť informačnej a kybernetickej bezpečnosti a iniciovanie návrhov nových bezpečnostných opatrení.

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).

Z auditu musí byť vypracovaná záverečná audítorská správa obsahujúca nedostatky zistené auditom a navrhované opatrenia na ich odstránenie. Následne Bezpečnostný manažér vypracuje tzv. akčný plán, v ktorom určí zodpovednosti a termíny realizácie odstránenia zistených nedostatkov a tento predloží na schválenie riaditeľovi sekcie IaDP.

Na základe správy audítora a schváleného akčného plánu riaditeľom sekcie IaDP všetky dotknuté organizačné útvary zabezpečia návrh a implementáciu adekvátnych opatrení na nápravu zistených nedostatkov v súlade s ustanoveniami tohto nariadenia.

4 Správa politiky informačnej bezpečnosti

4.1 Správa, revízia a kontrola dodržiavania

Dôležitou úlohou, ktorá je nevyhnutná pre dlhodobé zaistenie informačnej bezpečnosti, je udržiavanie bezpečnostnej politiky v aktuálnom stave. Z tohto dôvodu je politika informačnej bezpečnosti revidovaná Bezpečnostným manažérom:

- v prípade významných organizačných a technických zmien, ktoré môžu mať dopad na informačnú bezpečnosť alebo prevádzkované informačné systémy a komunikačnú infraštruktúru,
- pri zmene legislatívnych podmienok,
- pri zistení nových, doteraz neuvažovaných rizík,
- v prípade zvýšenia počtu bezpečnostných incidentov.

Pokiaľ nie je bezpečnostná politika aktualizovaná z vyššie uvedených dôvodov, posudzuje jej aktuálnosť a potrebu revidovania BM v ročnej periodicite v spolupráci s gestormi informačných systémov.

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.

Politiku informačnej bezpečnosti a jej zmeny schvaľuje na základe odporúčaní Bezpečnostného manažéra primátor.

Všetky zmeny politiky informačnej bezpečnosti prebiehajú riadeným spôsobom. Proces vykonaných posúdení aktuálnosti bezpečnostnej politiky a jej revízií je písomne zadokumentovaný. Táto dokumentácia je uložená u Bezpečnostného manažéra.

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

4.2 Distribú?ia dokumentu

Bezpečnostná politika mesta je interným dokumentom, ktorý obsahuje citlivé údaje a preto nie je voľne prístupná pre verejnosť.

Originál dokumentu je uložený u Bezpečnostného manažéra. Aktuálne kópie dokumentu sú prístupné všetkým interným zamestnancom mesta prostredníctvom intranetu.

Neriadené rozmnožovanie politiky je zakázané. Za riadenie a revízie politiky informačnej bezpečnosti zodpovedá Bezpečnostný manažér. Poskytovanie politiky informačnej bezpečnosti v tlačenej forme je povolené iba so súhlasom BM a len na obmedzenú dobu. Možnosť vydania politiky v tlačenej forme má iba BM.

Do bezpečnostnej politiky, resp. jej vybraných častí, môžu nahliadnuť aj tretie strany a dodávatelia, ak si to vyžaduje charakter poskytovaných služieb a ak boli splnené procedurálne požiadavky pre prístup externých subjektov ku citlivým údajom platným v rámci mesta.

4.3 Záver

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