Mesto Malacky, Radlinského 2751/1, 901 01 Malacky

Bezpečnostná politika informačných systémov mesta Malacky

Verzia:	0.1
Počet strán / príloh:	30/1
Dátum účinnosti:	01.08.2011
Vypracoval:	ATEMSEC, a.s.

Článok 1

Úvodné ustanovenia

1) Mesto Malacky a jeho orgány (ďalej „mesto“) si uvedomuje dôležitosť informačných systémov (IS), ktoré prevádzkuje, význam údajov, ktoré sú v nich spracúvané, hodnotu majetku a technológií, ktoré používa pre svoju činnosť a povinnosť chrániť oprávnené záujmy štátu, zamestnancov a všetkých osôb, s ktorými prichádza do kontaktu. Z tohto dôvodu sa mesto rozhodlo zaviesť systém manažérstva informačnej bezpečnosti (SMIB) v súlade s požiadavkami Výnosu MF SR o bezpečnostných štandardoch pre informačné systémy verejnej správy č. 312/2010 Z.z., štandardov STN ISO/IEC 27001:2006, STN ISO/IEC27002:2006.

2) Účelom tohto dokumentu je definovanie politiky informačnej bezpečnosti, ako rámca pre riešenie informačnej bezpečnosti mesta. Politika informačnej bezpečnosti je predpokladom pre dosiahnutie informačnej bezpečnosti ako primeranej úrovne dostupnosti IS a jeho služieb, ako aj dôvernosti, dostupnosti, autenticity a integrity využívaných informácií.

3) Dokument je vytvorený hlavne na základe medzinárodných štandardov informačnej bezpečnosti ISO/IEC 27001:2005 Information security management. Specification with guidance for use, ISO/IEC 27002:2005 Information technology. Security techniques. Code of practice for information cecurity management, ISO/IEC TR 13335 – 3:1998 Information technology - Guidelines for the management of IT Security - Part 3: Techniques for the management of IT Security, štandardov štandardov Výnosu MF SR č. 312/2010 Z.z. a odporúčaní odvetvovej praxe. Dokument vychádza aj zo Zákona č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov.

Článok 2

Ciele informačnej bezpečnosti

1) Medzi strategické ciele mesta v oblasti informačnej bezpečnosti patrí:
   a) Dosahovať a udržiavať vysokú úroveň bezpečnosti v súlade s bezpečnostnými štandardami SR, normami EÚ, slovenskou legislatívou a inými relevantnými predpismi.
   b) Vytvoriť podmienky pre zaistenie informačnej bezpečnosti mesta.

c) Chrániť práva a záujmy občanov, zamestnancov a obchodných partnerov mesta (vrátane dodávateľov) ako aj právnických a fyzických osôb implementovaním efektívnych a účinných bezpečnostných mechanizmov a opatrení.

d) Vytvoriť podmienky pre ochranu informácií uložených vo svojich informačných systémoch verejnej správy (ISVS) citlivých z hľadiska dôvernosti, integrity a dostupnosti.

e) Zabezpečiť dôvernosť, dostupnosť a integritu osobných údajov, obchodného tajomstva a iných dôležitých informačných aktív mesta, obchodných partnerov, fyzických a právnických osôb pri ich spracúvaní.

f) Riadiť informačnú bezpečnosť v súlade s požiadavkami štandardov Výnosu MF SR č. 312/2010 Z.z., medzinárodnými štandardami, platnými všeobecne záväznými právnymi predpismi SR a odporúčaniami odvetvovej praxe.

g) Zaistiť bezpečnosť, spoľahlivosť a kvalitu prevádzkovaných IS využívaním moderných informačných technológií a ich postupným zlepšovaním a zefektívňovaním.

h) Vytvoriť podmienky pre zabezpečenie dostupnosti informácií podľa všeobecne záväzných právnych predpisov SR (napr.: podľa zákona o slobodnom prístupe k informáciám) a podľa požiadaviek definovaných vedením mesta.

i) Vytvoriť podmienky pre bezpečné umiestnenie najdôležitejších komponentov systému mesta a zabezpečiť ich fyzickú ochranu a ochranu pred vplyvmi okolitého prostredia.

j) Pomocou vzdelávacieho programu vytvoriť predpoklady pre zaistenie bezpečnosti informačných systémov mesta všetkými zamestnancami.

k) Zvyšovať bezpečnostné povedomie zamestnancov a prostredníctvom vzdelávacieho programu ich systematicky viesť a motivovať k zlepšovaniu a dodržiavaniu bezpečnostných zásad.

l) Zdokonaľovať systém manažérstva informačnej bezpečnosti, trvalo zlepšovať jeho efektívnosť a integritu v súlade s novými požiadavkami na poskytovanie služieb a vytvoriť podmienky pre zaistenie bezpečnosti ISVS.

2) Potrebná úroveň bezpečnosti bude dosiahnutá návrhom takých bezpečnostných opatrení, ktoré zaisťujú primeranú ochranu informačných aktív mesta počas všetkých fáz ich životného cyklu.

3) Medzi čiastkové ciele mesta v oblasti bezpečnosti informačných systémov verejnej správy patrí:

a) Pre oblasť politiky informačnej bezpečnosti mesta:

- **Základný cieľ:** Definícia presného smeru postupu v oblasti informačnej bezpečnosti.
- **Vedľajší cieľ:** Preukázanie podpory politiky informačnej bezpečnosti zo strany vedenia.
- **Požadované bezpečnostné opatrenia:** Vypracovanie, schválenie a sprístupnenie dokumentácie informačnej bezpečností všetkým zamestnancom.
- **Kvantifikácia cieľa:** 100% dokumentácie (nariadení, usmernení, metodík, a pod.) týkajúcich sa informačnej bezpečnosti je sprístupnených a dostupných určeným skupinám zamestnancov mesta. Stredná doba pre sprístupnenie aktualizovaných dokumentov je menšia ako 5 pracovných dní.

b) Pre oblasť organizačnej bezpečnosti:

- **Základný cieľ:** Riadiť bezpečnosť informácií.
- **Vedľajší cieľ:** Udržiavať bezpečnosť prostriedkov na spracovávanie informácií. Udržiavať bezpečnosť informačných aktív mesta, ktoré sú prístupné tretím stranám. Udržiavať bezpečnosť informácií v prípadoch, keď bola zodpovednosť za spracovávanie informácií prenesená na inú organizáciu.
- **Požadované bezpečnostné opatrenia:** Vytvorenie riadiaceho rámca pre riadenie implementácie systému manažérstva bezpečnosti informácií v orgánoch mesta.
- **Kvantifikácia cieľa:** Únik alebo neautorizované získanie informácie, s obsahom osobných údajov predstavuje 0 prípadov za rok.

c) Pre oblasť klasifikácie a riadenie aktív:

- **Základný cieľ:** Zaistiť primeranú ochranu informačných aktív a iných aktív mesta.
- **Požadované bezpečnostné opatrenia:** Pri všetkých dôležitých informačných aktívach bude určený ich konkrétny vlastník a jeho zodpovednosť za aktíva podľa stanovenej klasifikácie.

- **Kvantifikácia cieľa:** Pre 100% kritických informačných aktív je definovaný vlastník. Frekvencia prípadov poškodenia, zneužitia alebo znehodnotenia informačného aktíva je menšia ako 10^{-2} za rok. Stredná veľkosť vyčíslenej škody vzniknutej v dôsledku poškodenia, zneužitia alebo znehodnotenia informačného aktíva nepresahuje hodnotu 3 000 € za rok.

d) Pre oblasť personálnej bezpečnosti:

- **Základný cieľ:** Znížiť riziko ľudskej chyby, krádeže, podvodu alebo zneužitia prostriedkov mesta.
- **Vedľajší cieľ:** Zaistiť, aby si boli používatelia vedomí bezpečnostných hrozieb a aby dodržiavali politiku informačnej bezpečnosti počas svojej práce. Minimalizovať škody spôsobené incidentmi a chybami.

e) Požadované bezpečnostné opatrenia: Zohľadnenie zodpovednosti za bezpečnosť v rámci prijímacieho konania a v pracovných zmluvách, ako aj sledovanie jej dodržiavania počas trvania pracovného pomeru. Školenie zamestnancov v oblasti bezpečnostných postupov a v správnom používaní prostriedkov na spracovanie informácií, aby sa minimalizovali bezpečnostné riziká.

- **Kvantifikácia cieľa:** 100% používateľov informačných systémov je oboznámených so svojimi zodpovednosťami a povinnosťami vo vzťahu k informačnej bezpečnosti. Maximálna doba na oboznámenie nového používateľa so svojimi zodpovednosťami je 20 pracovných dní. Maximálna doba na oboznámenie existujúceho používateľa s aktualizovanými postupmi a pravidlami a s nich vyplývajúcimi zodpovednosťami je 20 pracovných dní. Početnosť incidentov spojených s personálnou bezpečnosťou nepresahuje 5.10^{-3} na osobu za rok.

f) Pre oblasť fyzickej bezpečnosti a bezpečnosti prostredia:

- **Základný cieľ:** Predchádzať neautorizovanému prístupu, poškodeniu a zásahom do priestorov a informácií mesta.
- **Vedľajší cieľ:** Predchádzať strate, poškodeniu alebo prezradeniu aktív a prerušeniu činnosti orgánov mesta. Predchádzať prezradeniu alebo odcudzeniu informácií a prostriedkov na spracovávanie informácií.
- **Požadované bezpečnostné opatrenia:** Prostriedky, ktoré spracúvajú kritické alebo citlivé informácie mesta, sú umiestnené v zabezpečených zónach a chránené

definovaným bezpečnostným perimetrom s odpovedajúcimi bezpečnostnými bariérami a vstupnými kontrolami. Tieto prostriedky sú fyzicky chránené pred neautorizovaným prístupom, poškodením a narušením. Zavedenie zásady prázdneho stola a prázdnej obrazovky monitora.

- **Kvantifikácia cieľa:** Technický prostriedok informačných systémov, ktorého hodnota je väčšia ako horný kvantil súboru všetkých technických prostriedkov informačných systémov mesta, je zabezpečený prvkami fyzickej ochrany. Frekvencia incidentov neautorizovaného prístupu do zabezpečených priestorov je maximálne 5.10^{-1} na priestor za rok. Škody v dôsledku nezabezpečenia priestorov a zariadení informačných systémov prvkami fyzickej ochrany nepresahujú 2 000 € za rok.

g) Pre oblasť riadenia komunikácie a prevádzky:

- **Základný cieľ:** Zaistiť správnu a bezpečnú prevádzku prostriedkov na spracovávanie informácií.
- **Vedľajší cieľ:** Minimalizovať riziko poruchy systému. Chrániť integritu programov a dát. Udržiavať integritu a dostupnosť informačných a komunikačných služieb. Zabezpečiť ochranu informácií v počítačových sieťach a ochranu ich infraštruktúry. Predchádzať poškodeniu aktív a prerušeniu činnosti orgánov mesta. Predchádzať strate, modifikácii alebo zneužitiu informácií vymieňanými medzi organizáciami.
- **Požadované bezpečnostné opatrenia:** Stanovenie postupov a zodpovednosti pre riadenie a správu prostriedkov, ktoré spracúvajú informácie. Oddelenie funkcií, aby sa znížilo riziko úmyselného zneužitia systému alebo zneužitia z nedbalosti. Vykonanie prípravy a plánovania na zaistenie odpovedajúcej kapacity a zdrojov systému, ako aj odhadovanie budúcich kapacitných požiadaviek. Zdokumentovanie a otestovanie prevádzkových požiadaviek ešte pre uvedením nových systémov do prevádzky. Zavedenie primeraných opatrení na prevenciu a zistenie škodlivých programov. Vytvorenie postupov realizujúcich schválenú zálohovaciu stratégiu. Kontrola médií a ich fyzické zabezpečenie (pásky, diskety, kazety, vstupné a výstupné dáta, systémová dokumentácia). Výmena informácií a programov medzi mestom a jej partnermi bude kontrolovaná, bude v zhode s platnou legislatívou a bude sa vykonávať na základe zmlúv.

- **Kvantifikácia cieľa:** 90% informačných systém v rámci mesta má definované najmenej 2 používateľské kategórie, ktoré zabezpečujú rozličné úrovne prístupu k informáciám. 60% informačných systém v rámci mesta má definované najmenej 3 používateľské kategórie, ktoré zabezpečujú rozličné úrovne prístupu k informáciám. 100% prevádzkových požiadaviek na nové systémy je definovaných vo forme testovacích prípadov. Pred zavedením nového systému do praxe skončí pri testovaní 95% testovacích prípadov úspešne. Početnosť incidentov napadnutí alebo infikovaní škodlivým programom je najviac 5.10^{-1} prípadov na informačný systém za rok. 1 krát za 12 mesiacov je vykonaná kontrola zálohovacích médií.

h) Pre oblasť riadenia prístupu:

- **Základný cieľ:** Riadiť prístup k informáciám.
- **Vedľajší cieľ:** Predchádzať neoprávnenému prístupu k informačným systémom. Predchádzať neoprávnenému používateľskému prístupu. Ochraňovať sieťové služby a prístup k nim. Predchádzať neautorizovanému prístupu k počítačom. Predchádzať neoprávnenému prístupu k informáciám uloženým v počítačových systémoch. Detegovať neautorizované aktivity. Zaistiť bezpečnosť informácií pri používaní mobilnej výpočtovej techniky a pri využití prostriedkov práce na diaľku.
- **Požadované bezpečnostné opatrenia:** Prístup k informáciám a procesom mesta riadiť na základe prevádzkových a bezpečnostných požiadaviek. Vypracovanie formálnych postupov pre prideľovanie používateľských práv k informačnému systému a službám. Kontrola prístupových práv používateľov. Používanie vhodnej heslovej politiky. Riadenie prístupu k interným a externým sieťovým službám. Na obmedzenie prístupu k prostriedkom počítačov budú použité bezpečnostné prostriedky na úrovni operačného systému, ktoré sú schopné identifikovať a overiť totožnosť, zaznamenať úspešné a neúspešné pokusy o prístup, poskytnúť primerané autentizačné prostriedky a v prípade potreby obmedziť dobu pripojenia používateľa. Logický prístup k programom a informáciám bude obmedzený iba pre oprávnených používateľov. Systémy budú monitorované z dôvodu možného odhalenia nedodržiavania politiky riadenia prístupu a z dôvodu zaznamenania udalosti využiteľnej ako dôkazový materiál v prípade bezpečnostných incidentov. V

prípade práce na diaľku bude zavedená ochrana na mieste výkonu práce a budú zaistené vhodné podmienky pre tento spôsob práce.

- **Kvantifikácia cieľa:** 100% informačných systémov má riadený prístup prostredníctvom autentifikácie používateľov. 70% informačných systémov má riadený prístup prostredníctvom autorizácie používateľov. Používateľské heslá ku kritickým informačným systémom sú menené 1 krát za 6 mesiacov. Početnosť incidentov neautentifikovaného prístupu do informačného systému mesta predstavuje 1.10^{-2}.

i) Pre oblasť vývoja a údržby systémov:

- **Základný cieľ:** Zaistiť implementáciu bezpečnosti do informačných systémov.
- **Vedľajší cieľ:** Predchádzať strate, modifikácii alebo zneužitiu používateľských dát v aplikačných systémoch. Ochrániť dôvernosť, autenticitu alebo integritu informácií. Zaistiť, aby boli projekty IT a podporné činnosti vykonávané bežným spôsobom. Udržovať bezpečnosť programov a informácií aplikačných systémov.
- **Požadované bezpečnostné opatrenia:** Stanoviť všetky bezpečnostné požiadavky, vrátane požiadaviek na náhradnú prevádzku už vo fáze definície požiadaviek a tieto zdôvodniť, odsúhlasiť a zdokumentovať ako súčasť vývoja informačného systému. Do aplikačných systémov zahrnúť vhodné kontroly, auditné záznamy alebo záznamy aktivít. Vstupné a výstupné dáta validovať z hľadiska správnosti a adekvátnosti. Pre potreby ochrany informácií, ktoré sú považované za rizikové alebo pre ktoré ostatné opatrenia neposkytujú dostatočnú ochranu, použiť kryptografické systémy a techniky. Delegovať zodpovednosť za udržanie integrity aplikačného systému na používateľov alebo skupiny vývojárov, ktorým aplikačný systém patrí. Projektové a podporné prostredie bude pod prísnou kontrolou.
- **Kvantifikácia cieľa:** Najmenej 75% používateľských aktivít je v informačných systémoch zaznamenávaných. Najmenej 60% komunikačných rozhraní využíva kryptografické systémy a techniky. V rámci testovania funkčných požiadaviek na implementované systémy je najmenej 10% testov zameraných na bezpečnosť a integritu informácii.

j) Pre oblasť riadenia kontinuity činností mesta:

- **Základný cieľ:** Zabrániť prerušeniu prevádzkových činností a chrániť kritické procesy mesta pred následkami závažných chýb a katastrof.
- **Požadované bezpečnostné opatrenia:** Pre potrebu minimalizácie výpadkov, nehôd, chýb a úmyselného konania zaviesť proces riadenia kontinuity činností mesta. Riadenie kontinuity činnosti mesta bude zahŕňať opatrenie identifikácie a minimalizácie rizík, obmedzovať dôsledky škodlivých incidentov a zaisťovať včasné obnovenie nevyhnutných činností.
- **Kvantifikácia cieľa:** Dostupnosť informačného systému mesta je 99% času. 75% technických prostriedkov zabezpečujúcich chod informačných systémov je zabezpečených náhradných zdrojom napájania. Početnosť škodlivých incidentov s dôsledkami na prerušenie činnosti časti IS mesta na dobu do 1 hodiny je menšia ako 5.10^{-2} na IS za rok. Početnosť škodlivých incidentov s dôsledkami na prerušenie činnosti časti IS mesta na dobu nad 1 hodinu je menšia ako 3.10^{-2} na IS za rok.

k) Pre oblasť súladu s požiadavkami:

- **Základný cieľ:** Vyvarovať sa porušeniu noriem trestného alebo občianskeho práva, zákonných alebo zmluvných povinností a bezpečnostných požiadaviek. Zabezpečiť súlad systémov s bezpečnostnou politikou mesta a normami.
- **Vedľajší cieľ:** Maximalizovať efektivitu a minimalizovať interferenciu pri vykonávaní systémového auditu.
- **Požadované bezpečnostné opatrenia:** Špecifické požiadavky vyplývajúce zo zákona budú konzultované s právnymi poradcami mesta alebo s inými kvalifikovanými právnikmi. V priebehu vlastného auditu budú definované opatrenia pre zaistenie bezpečnosti prevádzkového systému a nástrojov auditu. Bude zaistená aj ochrana nástrojov auditu, aby bola zabezpečená ich integrita a predišlo sa zneužitiu.
- **Kvantifikácia cieľa:** Interný audit bezpečnosti IS mesta, ktorý overí súlad IS s bezpečnostnou politikou a aktuálnymi legislatívnymi požiadavkami, je vykonávaný 1 krát za rok. Aktualizácia dokumentácie bezpečnosti IS je vykonávaná 1 krát za rok.

4) Politika informačnej bezpečnosti je platná v rámci všetkých orgánov mesta. Je vydaná za účelom vytvorenia podmienok pre zabezpečenie primeranej úrovne ochrany všetkých

hmotných a nehmotných aktív informačných systémov mesta proti hrozbám, ktoré na ne pôsobia.

5) Politika informačnej bezpečnosti poskytuje rámec pre všetky bezpečnostné procesy a informačné systémy verejnej správy, vo vzťahu ku ktorým vystupuje ako povinná osoba. Požiadavky politiky informačnej bezpečnosti musia byť v primeranom rozsahu rozpracované vo forme vnútorných noriem a ostatnej bezpečnostnej dokumentácie (napr. bezpečnostný projekt, plán, metodika, príručka a pod.).

6) Politika informačnej bezpečnosti je sprístupnená všetkým zamestnancom mesta. Vybrané časti tohto dokumentu sú sprístupnené aj zamestnancom tretích strán, pokiaľ to bude pre výkon ich činnosti potrebné. O sprístupnení bezpečnostnej politiky tretím stranám rozhoduje manažér informačnej bezpečnosti.

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

Článok 3

Role, zodpovednosti a právomoci

1) **Primátor mesta** - zodpovedá za celkovú informačnú bezpečnosť v rámci mesta Malacky, za jej bezpečné fungovanie a prevádzku. Rozhoduje o úlohách v oblasti informačnej bezpečnosti a schvaľuje veľké iniciatívy podporujúce riadenie informačnej bezpečnosti. Schvaľuje politiku informačnej bezpečnosti. Zodpovedá za pridelenie potrebných kompetencií a zodpovedností za riadenie informačnej bezpečnosti jednotlivým pozíciám.

2) **Manažér informačnej bezpečnosti** (MIB) – zamestnanec Mestského úradu v Malackách, ktorý zodpovedá za všetky aktivity týkajúce sa informačnej bezpečnosti a za celkový stav informačnej bezpečnosti v jednotlivých orgánoch mesta. Zodpovednosti a právomoci MIB:

   a) má právomoc požadovať podporu manažmentu, odborných a organizačných zložiek pri riešení otázok týkajúcich sa informačnej bezpečnosti,

   b) zodpovedá za metodické riadenie činnosti správcov siete a technických zamestnancov v oblasti informačnej bezpečnosti,

   c) zodpovedá za spracovanie a revíziu bezpečnostnej dokumentácie informačných systémov mesta,

d) zodpovedá za spracovanie dokumentu Analýza rizík ISVS mesta Malacky pre daný kalendárny rok, ktorú predkladá na schválenie primátorovi mesta,
e) zodpovedá za spracovanie dokumentu Správa o stave informačnej bezpečnosti mesta Malacky pre daný kalendárny rok, ktorú predkladá na schválenie primátorovi mesta,
f) zodpovedá za zapracovanie navrhovaných opatrení vyplývajúcich zo záverečnej správy auditu informačnej bezpečnosti,
g) iniciuje schvaľovací proces bezpečnostnej dokumentácie informačných systémov mesta,
h) iniciuje disciplinárne konanie a uplatnenie sankcií v prípade zistenia zdroja, ktorý spôsobil bezpečnostný incident v informačno-komunikačnom prostredí mesta,
i) vykonáva školenie používateľov informačných systémov mesta v oblasti informačnej bezpečnosti,
j) je zodpovedný za posudzovanie zmlúv s tretími stranami v otázkach bezpečnosti IKT, ktorých obsahom je implementácia nových informačných systémov mesta,
k) je formálne zodpovedný za schvaľovací proces zmien existujúcich a zavádzaných nových ISVS a IKT, a to za časť týkajúcej sa bezpečnostných požiadaviek na tretie strany.

3) **Aplikátori informačnej bezpečnosti** (správcovia siete, technický zamestnanci) – zamestnanci niektorého z orgánov mesta, ktorí zabezpečujú správu a údržbu zverených bezpečnostných mechanizmov, priebežné monitorovanie stavu informačnej bezpečnosti a podávanie správ o jeho stave MIB. Aplikujú bezpečnostné opatrenia pri vzniku bezpečnostných incidentov podľa stanovených pravidiel.

4) **Audítor informačnej bezpečnosti** – zamestnanec Mestského úradu v Malackách, ktorý je najvyššou kontrolnou zložkou informačnej bezpečnosti. Zodpovedá za kontrolu, posudzovanie implementácie, dodržiavanie bezpečnostnej politiky a dodržiavanie príslušných štandardov a dokumentov informačnej bezpečnosti na všetkých útvaroch, ako aj za zabezpečenie ostatných činností vykonávaných v rámci auditu stavu informačnej bezpečnosti. Predpokladom na vykonávanie funkcie audítor informačnej bezpečnosti je oprávnenie vykonávať interný audit systému manažérstva informačnej bezpečnosti na základe absolvovaného školenia. Audit systému manažérstva informačnej bezpečnosti

vykonáva jeden krát za rok, z ktorého robí zápis – Správa z interného auditu informačnej bezpečnosti. Je zodpovedný za vypracovanie a revíziu Metodiky vnútorného auditu informačnej bezpečnosti.

5) **Vlastník aktíva** - fyzická osoba (zamestnanec), zodpovedná za aktívum v jeho správe alebo za aktívum, ktoré primárne využíva jeho organizačná zložka. Zodpovedá za špecifikáciu požiadaviek na úroveň ochrany aktív, ktoré sú v jeho správe a implementáciu bezpečnostných opatrení v súlade s riadiacimi dokumentmi politiky informačnej bezpečnosti.

6) Za ochranu aktív mesta zodpovedajú všetci zamestnanci.

7) Za priebežnú kontrolu dodržiavania bezpečnostných opatrení na úrovni riadenia a implementácie a na operačnej úrovni zodpovedajú v rámci svojich kompetencií všetci zamestnanci s pridelenými bezpečnostnými úlohami a riadiaci zamestnanci.

8) Nedodržanie pravidiel a zásad stanovených na základe bezpečnostnej politiky a prijatých bezpečnostných opatrení bude posudzované ako porušenie pracovnej disciplíny podľa pracovného poriadku.

9) Všetci vedúci zamestnanci organizačných zložiek sú priamo v rámci svojej pôsobnosti zaviazaní zavádzať politiku informačnej bezpečnosti do každodennej praxe, podporovať a presadzovať zvyšovanie úrovne informačnej bezpečnosti mesta a prevádzkovaných ISVS. Vedúci zamestnanci organizačných zložiek zodpovedajú za to, že ich podriadení konajú v súlade s prijatými bezpečnostnými zásadami a všetky bezpečnostné procedúry v rámci ich oblasti zodpovednosti sú vykonávané správne a v súlade so všeobecnými záväznými právnymi predpismi a vnútornými organizačnými normami.

10) Všetci zamestnanci mesta (používatelia) sú povinní dodržiavať pravidlá vyplývajúce z vnútorných organizačných noriem. Zamestnanci zodpovedajú za všetky činnosti, ktoré vykonávajú v rámci svojej práce.

Článok 4

Správa politiky a kontrola jej dodržiavania

1) Dôležitou úlohou, ktorá je nevyhnutná pre kontinuálne zaistenie informačnej bezpečnosti, je udržiavanie bezpečnostnej politiky v aktuálnom stave preto sa vykonáva jej revízia raz ročne, resp. skôr a to v prípade:

a) významných organizačných a technických zmien infraštruktúry IKT,
b) zistenia nových, doteraz neuvažovaných rizík,
c) zvýšenia počtu hlásení bezpečnostných incidentov,
d) zmeny požiadaviek všeobecne záväzných právnych predpisov.

2) Všetky zmeny politiky informačnej bezpečnosti prebiehajú riadeným spôsobom a sú o nich vedené záznamy. Za riadenie a revízie politiky informačnej bezpečnosti zodpovedá manažér informačnej bezpečnosti. Politiku informačnej bezpečnosti schvaľuje primátor mesta ako interný záväzný dokument.

3) Kontrola dodržiavania politiky informačnej bezpečnosti a jej obsahovej náplne prebieha formou ročných interných (resp. externých) auditov informačnej bezpečnosti so zameraním na jednotlivé oblasti informačnej bezpečnosti.

Interné audity sa riadia podľa ***Metodiky vnútorného auditu informačnej bezpečnosti***.

Článok 5
Riadenie informačnej bezpečnosti

1) Strategické ciele a zásady pre oblasť informačnej bezpečnosti vychádzajú z požiadaviek mesta, resp. jeho občanov a partnerov. Tieto požiadavky sú výsledkom troch činiteľov:
a) povinnosti mesta pôsobiť v súlade s legislatívou SR,
b) potreby ochrany záujmov mesta,
c) potreby riešenia rizík a bezpečnostných problémov, ktoré sú výsledkom meniaceho sa prostredia.

2) Dosiahnutie primeranej úrovne bezpečnosti pre jednotlivé hmotné a nehmotné aktíva mesta predpokladá plnenie stanovených cieľov v oblasti informačnej bezpečnosti a implementáciu primeraných bezpečnostných opatrení. Určenie primeraných bezpečnostných opatrení vyžaduje spracovanie analýzy a ohodnotenia rizík s prihliadnutím na stanovené požiadavky na informačnú bezpečnosť.

3) Akékoľvek riziko, ktoré nie je plne ošetrené implementovaným bezpečnostným mechanizmom, musí byť reportované vedeniu mesta. Tento proces umožní, aby zvyškové riziko zostalo v rámci akceptovateľných limitov.

4) Riziká pôsobiace na jednotlivé aktíva mesta sa analyzujú a hodnotia jeden krát za rok alebo v prípade potreby:

a) nového rozhodnutia o riadení rizík vzťahujúcich sa k základným funkciám mesta, napr. pri zmene priorít rozvoja, rozšírení oblastí kompetencií mesta podporovaných informačným systémom a pod.,
b) zosúladenia činnosti mesta s novými legislatívnymi a zmluvnými požiadavkami,
c) významnej zmeny architektúry informačného systému alebo významnej zmeny stratégie informačnej bezpečnosti,
d) určenia priorít a časových závislostí implementácie bezpečnostných opatrení,
e) výskytu nových hrozieb pôsobiacich na informačný systém,
f) výskytu zvýšeného množstva bezpečnostných incidentov.

5) Mesto Malacky deklaruje záujem postupovať pri riadení informačnej bezpečnosti podľa medzinárodne akceptovaných bezpečnostných noriem a štandardov.

6) Pre analýzu a ohodnotenie rizík sú navrhované štandardy pre kvalitatívnu analýzu rizík podľa ISO/IEC TR 13335 a ISO/IEC 27001. Odporúča sa detailný prístup analýzy rizík so zameraním sa najmä na kritické informačné systémy a procesy mesta a s nimi súvisiace hmotné a nehmotné aktíva.

7) Analýza a ohodnotenie rizík musí byť vykonané voči bezpečnostným požiadavkám a strategickým cieľom mesta v oblasti informačnej bezpečnosti s dôrazom na jej priority a nároky na dostupnosť, dôvernosť a integritu jednotlivých informačných systémov a procesov. Pri ohodnocovaní rizík musia byť zohľadnené aj bezpečnostné požiadavky vyplývajúce z všeobecne platných právnych predpisov, bezpečnostných štandardov a požiadaviek tretích strán.

8) Pre analýzu a ohodnotenie rizík procesov a informačných systémov mesta je vypracovaná ***Metodika manažmentu rizík pre oblasť informačnej bezpečnosti MsÚ Malacky***.

Článok 6

Zodpovednosť za informačnú bezpečnosť

1) Pre spoľahlivé a efektívne fungovanie SMIB je nevyhnuté vytvorenie a zavedenie organizačnej štruktúry, ktorá bude podporovať základné bezpečnostné funkcie.

2) Všetky role a pracovné funkcie musia mať vhodným spôsobom definované príslušné zodpovednosti a právomoci týkajúce sa informačnej bezpečnosti.

3) Organizácia informačnej bezpečnosti na mesto má tri úrovne:

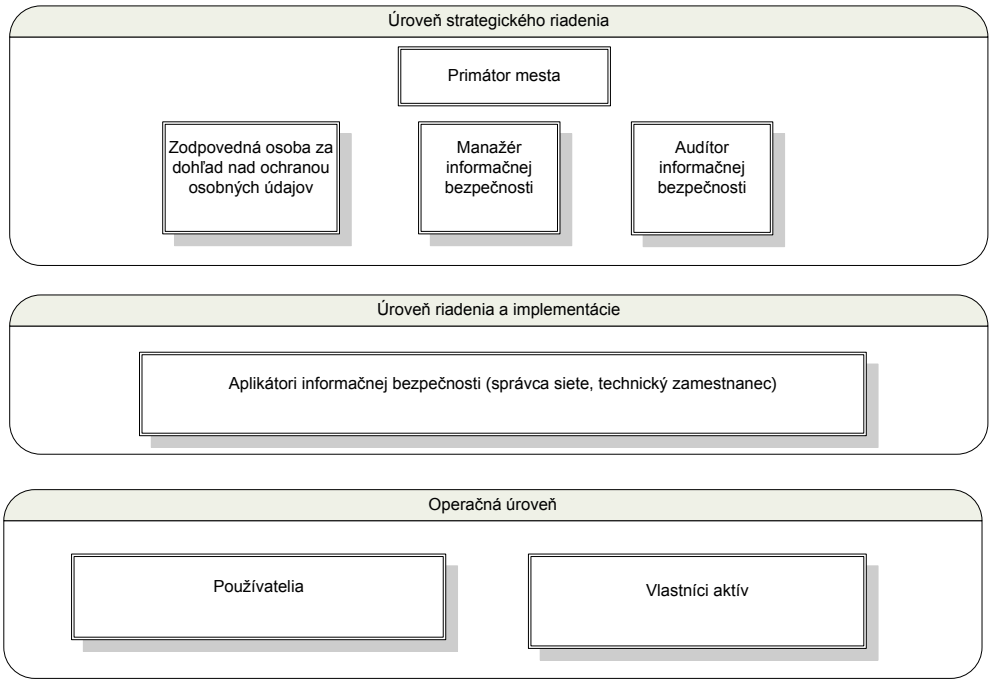
a) úroveň strategického riadenia, ktorou sú riešené koncepčné otázky týkajúce sa informačnej bezpečnosti a ktorá rozhoduje o riadení rizík a o implementácii globálnych bezpečnostných mechanizmov a opatrení,

b) úroveň riadenia a implementácie bezpečnosti, ktorou sú metodicky riadené všetky oblasti informačnej bezpečnosti v rámci organizačných zložiek; na tejto úrovni je zabezpečená tvorba, údržba a presadzovanie metodiky informačnej bezpečnosti a tiež je zabezpečený návrh a implementácia konkrétnych bezpečnostných mechanizmov a opatrení,

c) úroveň prevádzky a realizácie, ktorá zabezpečuje každodennú prevádzku IS a realizáciu rutinných činností týkajúcich sa informačnej bezpečnosti podľa platných metodických postupov a štandardov.

4) V rámci jednotlivých úrovní organizácie riadenia informačnej bezpečnosti je zabezpečený aj výkon hodnotiacich a kontrolných činností.

5) Zaradenie jednotlivých článkov riadenia informačnej bezpečnosti do úrovní riadenia je zrejmé z obrázku 1.



Obrázok 1 Organizácia riadenia informačnej bezpečnosti v meste Malacky

Článok 6

Základné bezpečnostné úrovne ochrany, princípy a zásady

1) V nasledovných článkoch sú popísané zásady a princípy, ktoré je potrebné dodržiavať za účelom dosiahnutia základnej úrovne informačnej bezpečnosti. Jednotlivé zásady sú rozdelené do tematických celkov. Tieto zásady a princípy vychádzajú z bezpečnostných štandardov STN ISO/IEC27002.

Článok 7

Organizácia bezpečnosti

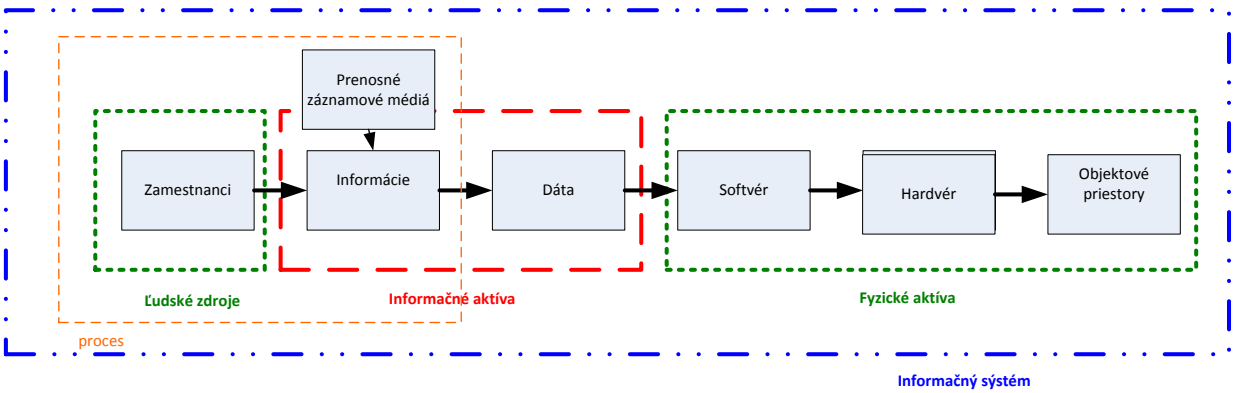
1) Informačná bezpečnosť musí byť organizačne riadená v súlade s v pravidlami stanovenými touto politikou informačnej bezpečnosti. Zodpovednosti za ochranu aktív a za vykonávanie špecifických procesov informačnej bezpečnosti musia byť jasne definované a zdokumentované. Pri ohodnocovaní a riadení rizík a návrhu bezpečnostných opatrení musí byť využívaná koordinovaná podpora všetkých zainteresovaných strán.
2) Pri výbere dodávateľov sa musia popri iných kritériách brať do úvahy aj záruky v oblasti informačnej bezpečnosti. Zmluvné vzťahy musia zohľadňovať platné, všeobecne záväzné právne predpisy SR a bezpečnostné požiadavky mesta v oblasti informačnej bezpečnosti.
3) Podmienky výkonu prác tretími stranami, ako aj príslušné bezpečnostné požiadavky musia byť zachytené v zmluve s treťou stranou. Pri návrhu a implementácií bezpečnostných opatrení v oblasti informačnej bezpečnosti musí byť kladený veľký dôraz nielen na ochranu spoločnosti pred tretími stranami, ale aj na ochranu oprávnených záujmov tretích strán, ktoré vstupujú s mestom do obchodných vzťahov.
4) Spôsob organizácie bezpečnosti ako aj účasť tretích strán sa riadi podľa ***Bezpečnostnej smernice pre prácu s informačnými systémami mesta Malacky***.

Článok 8

Klasifikácia a ohodnotenie kritickosti aktív informačných systémov

1) Informačným aktívom informačného systému sa rozumejú informácie resp. dáta, ktorým mesto priraďuje hodnotu, pre ktorú následne požaduje príslušný stupeň ochrany. Aktívami sú aj všetky časti informačného systému, ktoré slúžia najmä na získavanie, zhromažďovanie, zaznamenávanie, usporadúvanie, premiestňovanie alebo prenos dát. Ide o fyzické aktíva, softvérové aktíva a ľudské zdroje.

2) Ochrana všetkých aktív informačných systémov je založená na princípe vlastníctva. Pre každé aktívum musí byť určený jeho vlastník. Príklad procesu, informačného systému a jeho aktív je zobrazený na Obrázku 2.



Obrázok 2 Príklad blokovej schémy informačného systému

3) Všetky typy informačných aktív spracúvané, uchovávané alebo prenášané na mesto alebo v prevádzkovaných ISVS musia byť ohodnotené z pohľadu zabezpečenia ich dôvernosti, dostupnosti a integrity. Pre potreby klasifikácie a hodnotenie aktív musí byť vedený a udržiavaný inventárny zoznam všetkých aktív informačných systémov.

4) Klasifikácia a hodnotenie kritickosti všetkých hmotných a nehmotných aktív informačných systémov a procesov mesta sa riadi podľa ***Metodiky manažmentu rizík pre oblasť informačnej bezpečnosti MsÚ Malacky***. Výsledky inventarizácie, klasifikácie a hodnotenia kritickosti aktív, informačných systémov a procesov sú uvedené v dokumente ***Analýza rizík ISVS mesta Malacky*** vypracovanom pre daný rok.

Článok 9

Personálna bezpečnosť

1) Počas prijímacieho procesu musia byť primerane preverované schopnosti uchádzača plniť požadované pracovné činnosti a splnenie požiadaviek stanovených legislatívou.

2) Zamestnanci musia byť informovaní o svojich zodpovednostiach a právomociach týkajúcich sa bezpečnosti informácií bezprostredne po nástupe do zamestnania. Každý zamestnanec musí prejsť primeraným zácvikom týkajúcim sa pracovných postupov súvisiacich s informačnou bezpečnosťou a správneho používania informačných systémov, do ktorých bude mať povolený prístup. Spôsob školenia zamestnancov v rámci adaptačného obdobia manažérom informačnej bezpečnosti sa riadi podľa ***Bezpečnostnej smernice pre prácu s informačnými systémami mesta Malacky.*** Audítor informačnej bezpečnosti má oprávnenie vykonávať interný audit systému manažérstva informačnej bezpečnosti len na základe absolvovaného školenia pre interných audítorov systému manažérstva informačnej bezpečnosti. V prípade významných zmien v bezpečnostnej dokumentácii sú zamestnanci preškoľovaní manažérom informačnej bezpečnosti.

3) Každý zamestnanec, ktorý poruší povinnosť, bude postihovaný sankciami definovanými v Pracovnom poriadku.

4) Pri vzdelávaní a motivovaní zamestnancov v oblasti informačnej bezpečnosti má dôležitú úlohu vzdelávací program informačnej bezpečnosti, ktorého cieľom je zvyšovať zodpovednosť zamestnancov za aktíva mesta. Predmetom vzdelávania v oblasti informačnej bezpečnosti bude informovanie zamestnancov o prijatých opatreniach a súvisiacich postupoch.

Článok 10

Fyzická bezpečnosť a bezpečnosť prostredia

1) Priestor, v ktorom sa nachádzajú informačné systémy mesta, musí byť v neprítomnosti zamestnancov chránený primeraným bezpečnostným systémom. Tento systém musí byť realizovaný mechanicko-technickými, personálnymi a režimovými ochrannými opatreniami. Každá z týchto skupín opatrení plní v systéme svoju nezastupiteľnú úlohu. Zanedbanie alebo opomenutie niektorej z nich môže mať

za následok oslabenie alebo až znefunkčnenie celého ochranného systému. Je preto potrebné zabezpečiť v systéme zastúpenie všetkých skupín ochranných opatrení, kde pasívne prvky budú slúžiť na odradenie/spomalenie/zastavenie narušiteľa, aktívne prvky zabezpečia jeho detekciu, prvky fyzickej ochrany zaistia včasný zásah a zadržanie narušiteľa a prvky režimovej ochrany zabezpečia účinné a efektívne fungovanie uvedených opatrení.

Článok 11

Správa a prevádzka

1) Zodpovednosti a procedúry riadenia a prevádzky prostriedkov IS musia byť zdokumentované a udržiavané v aktuálnom stave. V prípadoch, kedy spracovanie informácií alebo prevádzky prostriedkov IS bude zverené tretej strane, musia byť prijaté primerané bezpečnostné opatrenia na zabezpečenie spracúvaných informácií. Na ochranu pred rizikom náhodného omylu používateľa systému musia byť navrhnuté a implementované vhodné bezpečnostné mechanizmy a kontrolné opatrenia. Ich cieľom bude obmedziť pravdepodobnosť vzniku omylu a zabezpečiť jeho odhalenie. Pre všetky dôležité prostriedky IS prevádzkované mestom musí byť vypracovaná dokumentácia v štandardizovanom formáte, ktorá bude aspoň obsahovať jednoznačnú identifikáciu systému, jeho popis a dokumentáciu konfigurácie, popis vzťahov a prepojení s inými prostriedkami a procesmi. Dokumentácia musí byť udržiavaná v aktuálnom stave. Dokumentácia k IS môže obsahovať dôverné alebo inak citlivé informácie. Preto je potrebné ju chrániť pred prezradením, krádežou, narušením alebo stratou. Musí byť stanovený spôsob vytvárania a uchovávania dokumentácie.
2) IT infraštruktúra pre prevádzkované IS musí byť navrhnutá tak, aby spĺňala požiadavky vlastníkov aktív na dostupnosť systémov a dôvernosť a integritu informácií v nich spracúvaných. Zálohovanie údajov umožňuje obnovu údajov a poskytovaných služieb v prípade nedostupnosti systému, zničenia alebo poškodenia údajov. Všetky dôležité údaje spracúvané v IS prevádzkovaných mestom musia byť zálohované a archivované.

3) Vytvárať prevádzkovú zálohu informačných systémov sa odporúča jedenkrát za deň v jednej kópií a archivačná záloha mesačne v dvoch kópiách, pričom každá je fyzicky uložená v inom objekte.

4) Pre všetky dôležité údaje spracúvané v IS musia byť spracované plány zálohovania a archivácie, ktoré vychádzajú z požiadaviek na dostupnosť a integritu týchto údajov. Všetka komunikácia medzi internými zabezpečenými a externými nezabezpečenými sieťami (napr. Internet) musí byť zabezpečená bezpečnostnou bránou. Prepojenie internej siete mesta so sieťami tretích strán musí byť schválené MIB po dôkladnej previerke bezpečného pripojenia. Bezpečnosť systémov nachádzajúcich sa v internej sieti voči narušeniu spôsobenému jej pripojením k externej sieti musí byť zaistená primeranými bezpečnostnými mechanizmami.

5) Všetky pracovné stanice a ostatné technické prostriedky IS musia byť chránené adekvátnymi a účinnými bezpečnostnými opatreniami na ochranu pred škodlivým softvérom a na jeho detekciu. Bezpečnostné mechanizmy na ochranu pred škodlivým softvérom musia byť pravidelne aktualizované.

6) Všetky fyzické aktíva musia byť udržiavané zaškoleným personálom. Ich opravu a servis môžu vykonávať len autorizovaní zamestnanci mesta, príp. zamestnanci tretích strán. Systém správy porúch bude navrhnutý a implementovaný takým spôsobom, aby bola zabezpečená detekcia, izolovanie, oprava a dokumentácia porúch prostriedkov IS. Zmluvy o údržbe musia zabezpečiť rýchlu a efektívnu podporu dodávateľa. Ak je to relevantné musia zmluvy o údržbe obsahovať dohody o dodržiavaní bezpečnostných požiadaviek spoločnosti a zmluvné záväzky dodávateľov týkajúce sa doby odozvy a realizácie opravy.

7) Správa a prevádzka informačných systémov sa riadi podľa ***Bezpečnostnej smernice pre prácu s informačnými systémami mesta Malacky*** .

Článok 12

Riadenie prístupu

1) Prístup k dôverným alebo inak citlivým údajom spracovávaným v IS môže byť povolený len na základe jednoznačnej identifikácie a autentifikácie používateľa. Autentifikácia používateľa sa vykonáva vhodných prostriedkom schválenými MIB.

Prístup do IS musí byť riadený kombináciou centralizovaného a voliteľného riadenia prístupu. V prípade centralizovaných IS musí byť aplikované centralizované riadenie prístupu, kde budú prístupové práva prideľované na základe prístupových profilov schválených ich vlastníkom a MIB. V prípade informácií spracúvaných na lokálnych pracovných staniciach môže byť aplikované aj voliteľné riadenie prístupu, kedy pravidlá a podmienky prístupu k údajom určuje ich vlastník. Každému používateľovi môže byť pridelený len taký rozsah prístupových práv, ktorý umožní plnenie pracovných úloh, a zároveň zabráni vykonávaniu iných neautorizovaných činností (princíp need to have). Zamestnancom, s ktorými bol rozviazaný pracovný pomer, musia byť v dostatočnom predstihu odobraté prístupové práva k dôležitým prostriedkom IS a k citlivým informačným aktívam. Musia byť vypracované predpisy upravujúce riadenie prístupových práv používateľov a administrátorov systémov a ich dodržiavanie musí byť kontrolované.

2) Všetky udalosti a aktivity súvisiace s bezpečnosťou (používanie IS, prístupy k dôverným alebo inak citlivým údajom a pod.) musia byť zaznamenávané, sledované a pravidelne vyhodnocované. Neautorizované, neúspešné prístupy alebo prístupy, ktoré sú v rozpore s pravidlami riadenia prístupu, musia byť ohlásené a vyšetrené. Musí byť zabezpečená nezávislosť sledovania auditných záznamov (je aplikované oddelenie rolí medzi osobami, ktoré kontrolu vykonávajú a ktorých aktivity sa sledujú).

3) Používanie mobilných technických prostriedkov spracovania informácií (notebooky, PDA, a pod.) v priestoroch ako aj mimo priestorov orgánov mesta podlieha schvaľovaciemu procesu. Na zabezpečenie bezpečnosti dôverných a inak citlivých informácií spracovávaných na mobilných technických prostriedkoch spracovania informácií mimo priestorov spoločnosti musia byť aplikované primerané bezpečnostné opatrenia. Mobilné technické prostriedky spracovania informácií môžu byť pripojené do počítačovej siete len po ich úspešnej identifikácií a autentifikácii. Prístup vzdialených používateľov k prostriedkom IS nachádzajúcich sa v dosahu sieti a v internej sieti musí byť autorizovaný oprávnenou osobou. Prístup môže byť umožnený až na základe overenia identity používateľa.

4) Riadenie prístupu do informačných systémov sa riadi ***podľa Bezpečnostnej smernice pre prácu s informačnými systémami mesta Malacky***.

Článok 13

Vývoj a údržba

1) Všetky časti prevádzkovaných IS musia byť vyvíjané v súlade s legislatívnymi požiadavkami, formálnymi metodickými postupmi a bezpečnostnými požiadavkami politiky informačnej bezpečnosti. Všetky bezpečnostné požiadavky a opatrenia týkajúce sa vyvíjaného systému musia byť schválené MIB. Počas celého procesu vývoja musia byť do vývoja zapojení okrem špecialistov z oblasti informačných technológií, aj špecialisti zodpovední za informačnú bezpečnosť a koncoví používatelia. Prostredia na vývoj a testovanie systémov a produkčné prostredie musia byť fyzicky aj logicky oddelené. Systémy alebo ich časti sa môžu nasadiť do ostrej prevádzky až po ich otestovaní a akceptácii špecialistami z oblasti informačných technológií, informačnej bezpečnosti a koncovými používateľmi. Na testovanie môžu byť použité len databázy, ktoré neobsahujú osobné údaje. Pri zabezpečovaní vývoja tretími stranami musia byť podmienky výkonu prác tretími stranami, ako aj bezpečnostné požiadavky zachytené v zmluve s treťou stranou.

2) Zamestnanci ani externí dodávatelia nesmú svojvoľne zasahovať do konfigurácie prevádzkovaných systémov, všetky realizované zmeny musia byť autorizované vlastníkom systému. Všetky požiadavky a rozhodnutia o zmene musia byť realizované dokumentovaným spôsobom, všetky významné realizované zmeny musia byť evidované. Zmeny prostriedkov IS musia byť predmetom formálneho zmenového konania. Výber nových prostriedkov IS musí byť vykonaný na základe stanovených akceptačných kritérií, ktorých súčasťou musia byť aj bezpečnostné požiadavky. Účel a použitie nových prostriedkov IS musia byť schválené MIB. Implementácii nových prostriedkov IS alebo akejkoľvek aktivite ovplyvňujúcej existujúce prostriedky IS musí predchádzať analýza rizík za účelom zistenia dopadu prípadných zmien na úroveň prevádzkovaných služieb a na bezpečnosť ostatných prostriedkov IS. V prípade identifikácie rizík musia byť navrhnuté a implementované primerané bezpečnostné opatrenia.

3) Vývoj a údržba informačných systémov sa riadi podľa ***Bezpečnostnej smernice pre prácu s informačnými systémami mesta Malacky.***

Článok 14

Hlásenie a reakcia na bezpečnostné incidenty

1) Všetky podozrenia alebo detegované pokusy narušenia bezpečnosti a bezpečnostné slabiny, ktoré môžu mať za následok vznik bezpečnostného incidentu a nefunkčnosť prostriedkov IS, musia byť ihneď ohlásené. Povinnosť hlásenia bezpečnostných udalostí majú všetci zamestnanci mesta a tretie strany. O hláseniach bezpečnostných incidentov a o ich riešení musí byť vedená evidencia. V rámci evidovania bezpečnostných incidentov musia byť zavedené mechanizmy umožňujúce kvalifikovať a monitorovať typy, rozsahy a náklady incidentov a nefunkčností. Tieto informácie musia byť použité na identifikáciu opakujúcich sa incidentov alebo nefunkčností s vážnym dopadom a pri návrhu dodatočných bezpečnostných opatrení. O všetkých závažných bezpečnostných incidentoch musí byť bezodkladne informovaný MIB. Pre hlásenie a reakciu na bezpečnostné incidenty musia byť vypracované predpisy. Postup reakcie na významné a opakujúce sa bezpečnostné incidenty musí byť zdokumentovaný vo forme inštrukcií. V rámci procesu vzdelávania a metodického riadenia musia byť zamestnanci inštruovaní o správaní sa v prípade zistenia bezpečnostného incidentu. V primeranom rozsahu musia byť o procedúrach hlásenia bezpečnostných incidentov upovedomené aj tretie strany. Musí byť zavedený formálny disciplinárny proces pre tých zamestnancov, ktorí porušili bezpečnostné opatrenia a procedúry mesta.
2) Hlásenie a reakcia na bezpečnostné incidenty sa riadi podľa ***Bezpečnostnej smernice pre prácu s informačnými systémami mesta Malacky***.

Článok 15

Riadenie kontinuity činností

1) Na obnovu funkčnosti dôležitých IS prevádzkovaných mestom, v prípade krízovej situácie musia byť vypracované a nepretržite udržiavané plány zachovania kontinuity činností. Plány zachovania kontinuity činností pozostávajú z havarijných procedúr

popisujúcich priamu reakciu na incident s cieľom minimalizovať jeho následky a obnovu základných funkcií a činností IS, procedúr na obnovu funkčnosti, zameraných na úplnú obnovu funkčnosti IS do stavu pred incidentom. Stratégia obnovy musí byť prehodnocovaná v minimálne ročnom intervale. Plány zachovania kontinuity činností musia byť kontrolované a testované v minimálne ročnom intervale alebo po každej významnej zmene v prostredí. Dodávatelia sieťových služieb musia byť zmluvne zaviazaní poskytovať dohodnutú úroveň kvality služieb.

Článok 16

Zabezpečenie súladu

1) Všetky požiadavky definované všeobecne záväznými právnymi predpismi SR aplikovateľnými v rámci mesta musia byť sledované a všetky špecifické opatrenia a zodpovednosti z hľadiska plnenia zákonných požiadaviek dokumentované. Pre zabezpečenie súladu so zákonnými požiadavkami musia byť prijaté náležité opatrenia.

Článok 17

Ochrana informačných systémov verejnej správy

1) Na úseku ochrany osobných údajov sa mesto Malacky vo všeobecnosti zaväzuje zosúladiť svoje informačné systémy s bezpečnostnými štandardy podľa výnosu Ministerstva financií z 9. júna 2010 č. 312/2010 o štandardoch pre informačné systémy verejnej správy (výnos MF SR). Zaväzuje sa spracovať komplexnú bezpečnostnú dokumentáciu vymedzujúcu rozsah a spôsob technických, organizačných a personálnych opatrení potrebných na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačné systémy verejnej správy, a to z hľadiska narušenia ich bezpečnosti, spoľahlivosti a funkčnosti. Spracovaná bezpečnostná dokumentácia musí byť v súlade s bezpečnostnými štandardmi výnosu MF pre architektúru riadenia (štandardy pre riadenie informačnej bezpečnosti realizované vypracovaním a implementáciou bezpečnostnej politiky, štandardy pre personálnu bezpečnosť, štandardy pre manažment rizík informačnej bezpečnosti a štandardy pre kontrolný mechanizmus riadenia informačnej bezpečnosti) a pre

minimálne technické zabezpečenie (štandardy pre ochranu proti škodlivému kódu, štandardy pre sieťovú bezpečnosť, štandardy pre fyzickú bezpečnosť a bezpečnosť prostredia, štandardy pre aktualizáciu softvéru, štandardy pre monitorovanie a manažment bezpečnostných incidentov, štandardy pre periodické hodnotenie zraniteľností, štandardy pre zálohovanie, štandardy pre fyzické ukladanie záloh, štandardy pre riadenie prístupu aktualizáciu informačno-komunikačných technológii a s štandardy pre účasť tretej strany).

Článok 18

Ochrana osobných údajov

1) Na úseku ochrany osobných údajov sa mesto vo všeobecnosti zaväzuje dodržiavať práva jednotlivca na ochranu súkromia definované v Ústave Slovenskej republiky v ústavnom zákone, ktorým bola prijatá Listina základných ľudských práv a slobôd, v Občianskom zákonníku, v oznámení č. 49/2001 Z. z., ktorým bol prijatý Dohovor o ochrane jednotlivcov pri automatizovanom spracúvaní osobných údajov (Dohovor Rady Európy č. 108), v Zákonníku práce a v Trestnom zákone. Osobitne na úseku ochrany osobných údajov sa spoločnosť bude riadiť v zmysle zákona č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov. Tento zákon je priamym rozpracovaním požiadaviek Smernice Európskeho parlamentu a Rady č. 95/46/EC. Vo svojich ustanoveniach upravuje ochranu osobnosti a ukladá, že za bezpečnosť osobných údajov zodpovedá sám prevádzkovateľ IS a to tým, že ich chráni pred náhodným ako aj nezákonným poškodením, zničením, náhodnou stratou, zmenou, nedovoleným prístupom alebo sprístupnením. Na tento účel je povinný prijať primerané technické, organizačné a personálne opatrenia, a to vo forme bezpečnostného projektu informačného systému. Jeho vypracovanie zákon podmieňuje prepojením IS na verejne prístupnú počítačovú sieť alebo prevádzkovaním IS v počítačovej sieti, ktorá je prepojená na verejne prístupnú počítačovú sieť. Zámerom tohto ustanovenia je sprísniť podmienky spracovávania najmä tých osobných údajov, ktoré patria medzi osobitné kategórie osobných údajov (napr. rodné číslo, zdravotné záznamy) a sú vystavené možným hrozbám pri spracovávaní v prostredí, ktoré je prepojené do siete Internet.

2) Ochrana osobných údajov sa riadi podľa ***Bezpečnostného projektu informačných systémov na ochranu osobných údajov***.

Článok 19

Ochrana listového tajomstva

1) Mesto sa zaväzuje dodržiavať listové tajomstvo vyplývajúce z Listiny základných práv a slobôd, v ktorej sa uvádza, že nikto nesmie porušiť listové tajomstvo ani tajomstvo iných písomností a záznamov, či už uchovávaných v súkromí alebo zasielaných poštou alebo iným spôsobom s výnimkou prípadov a spôsobom, ktoré ustanoví zákon. Rovnako sa zaručuje tajomstvo správ podávaných telefónom, telegrafom alebo iným podobným zariadením.

Článok 20

Ochrana súkromia proti nevyžiadaným správam

1) Vo vzťahu k súkromiu našich klientov, dodávateľov a sprostredkovateľov sa mesto zaväzuje plniť všetky náležitosti, ktoré jej vyplývajú z príslušných zákonov a vykonávajúcich vyhlášok. Ide hlavne o zákon č. 610/2003 Z.z. o elektronických komunikáciách v znení neskorších predpisov, ktorý vychádza z direktívy EÚ. Okrem uvedeného zákona, problematiku nevyžiadanej pošty rieši aj zákon o reklame (zákon NRSR č. 147/2001 Z. z. o reklame v znení neskorších predpisov) a zákon o elektronickom obchode (zákon NRSR č. 22/2004 Z. z. o elektronickom obchode).

Článok 21

Bezpečnosť informačných systémov poskytovateľov dátového priestoru

1) Mesto sa zaväzuje dodržiavať zásady poskytovania elektronických komunikačných sietí a služieb upravujúce zákon č. 610/2003 Z. z. o elektronických komunikáciách. Organizáciám pôsobiacim v tejto sfére, zákon okrem iného ukladá povinnosť prijať zodpovedajúce technické a organizačné opatrenia na ochranu bezpečnosti svojich sietí a služieb. Tieto opatrenia s ohľadom na stav techniky a náklady na realizáciu musia zabezpečiť úroveň bezpečnosti, ktorá je primeraná existujúcemu riziku. V prípade poskytovania elektronických služieb vo vzťahu k mestu ide hlavne o

poskytovanie: pripojenia do komunikačných sietí (iba prenos dát), tzv. proxy, čo znamená dočasné uloženie dát (napr. za účelom rýchleho pripojenia do siete Internet), dátového priestoru (napr. web hosting) a poskytovanie sieťových nástrojov (napr. na vyhľadávanie v Internete). Spoločnosť sa zaväzuje dodržiavať zásady týkajúce sa zodpovednosti poskytovateľov elektronických služieb. V rámci EÚ túto problematiku rieši smernica Európskeho parlamentu a Rady 2000/31/ES o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, a to najmä o elektronickom obchode (smernica o elektronickom obchode), ktorá bola aplikovaná v zákone NR SR č. 22/2004 Z. z. o elektronickom obchode v znení neskorších predpisov.

Článok 22

Trestno-právna zodpovednosť za porušenie bezpečnosti informačných systémov

1) Mesto Malacky si uvedomuje a berie na seba trestno-právnu zodpovednosť za porušenie bezpečnosti informačných systémov. Ide hlavne o porušovanie autorských práv používaním a predávaním nelegálnych kópií softvéru, výrobkov nelegálnych kópií hudobných alebo filmových diel pomocou počítača. Mesto sa zaväzuje, že bude dodržiavať všetky náležitosti vyplývajúce z aplikovania Dohovoru o počítačovej kriminalite č. 185/2001, vydaný Radou Európy dňa 23. novembra 2001 do právnych predpisov SR. Mesto, sa zaväzuje dodržiavať zásady týkajúce sa autorských práv vyplývajúcich zo zákona č. 618/2003 Z.z. o autorskom práve a právach súvisiacich s autorským právom v znení neskorších predpisov (autorský zákon).

Článok 23

Ochrana obchodného tajomstva

1) Mesto sa zaväzuje chrániť obchodné tajomstvo definované Obchodným zákonníkom, t.j. všetky skutočnosti obchodnej, výrobnej alebo technickej povahy majúce skutočnú alebo potenciálnu materiálnu či nemateriálnu hodnotu, nie sú v príslušných obchodných kruhoch bežne dostupné, majú byť podľa vôle tretej strany utajené.
2) Mesto sa zaväzuje taktiež plniť si svoje povinnosti a zodpovednosti pri aplikácii zákona č. 211/2000 Z.z o slobodnom prístupe k informáciám v znení neskorších predpisov.

Článok 24

Bezpečnosť informačných systémov vo vzťahu k technickým normám a štandardom

3) V oblasti bezpečnosti informačných systémov sa mesto zaväzuje prijať všetky náležitosti súvisiace so zavádzaním systému manažérstva informačnej bezpečnosti (SMIB). Táto implementácia bude realizovaná podľa štandardov STN ISO/IEC 27001 a STN ISO/IEC 17799:2005. Tento štandard sa opiera o prvky integrovaného systému riadenia IMS (Instructional Management Systems), ktoré sú známe zo systémov riadenia kvality podľa ISO 9001.

Článok 25

Audit stavu informačnej bezpečnosti

1) Základom zvyšovania úrovne informačnej bezpečnosti je vykonávanie hodnotiacich a kontrolných činností. Základným takýmto procesom je audit stavu informačnej bezpečnosti, ktorý vykonáva audítor informačnej bezpečnosti. Cieľom auditu stavu informačnej bezpečnosti je:
   a) Overovanie a posudzovanie efektívnosti implementácie, udržiavania a dodržiavania bezpečnostnej politiky navrhnutých bezpečnostných mechanizmov a opatrení a ostatných riadiacich dokumentov SMIB.
   b) Posúdenie miery zhody s požiadavkami schválených bezpečnostných štandardov a zhody s ostatnými identifikovanými požiadavkami týkajúcimi sa informačnej bezpečnosti.
   c) Poskytnutie primeranej istoty o tom, že informačná bezpečnosť je na primeranej úrovni.
   d) Overiť splnenie legislatívnych požiadaviek.
2) Auditná činnosť môže prebiehať formou interných alebo externých auditov so zameraním na jednotlivé oblasti informačnej bezpečnosti. Interné a externé audity sa riadia schváleným plánom auditov. Z auditu musí byť vypracovaný audítorská správa obsahujúca nedostatky zistené auditom a navrhované opatrenia, zodpovednosti a termíny ich realizácie.

Článok 26

Záverečné ustanovenia

1) Akékoľvek zmeny a doplnenia tejto politiky je možné vykonať iba písomne, pri dodržaní postupu pre vydávanie vnútorných organizačných noriem.

2) Bezpečnostná politika ISVS mesta Malacky nadobúda účinnosť dňom jej vydania.

Primátor mesta Malacky

Príloha č. 1 Bezpečnostná dokumentácia ISVS mesta Malacky

Smernice mesta Malacky

Názov dokumentu	Číslo dokumentu	Aktualizácie
Bezpečnostná politika ISVS mesta Malacky	V procese schvaľovania	-
Bezpečnostná smernica pre prácu s informačnými systémami mesta Malacky	V procese schvaľovania	-

Bezpečnostné projekty, plány, metodiky, príručky a manuály

Názov dokumentu	Rok vypracovania
Metodika manažmentu rizík pre oblasť informačnej bezpečnosti mesta Malacky	2011
Metodika vnútorného auditu informačnej bezpečnosti	2011
Analýza rizík ISVS MsÚ Malacky 2011	2011
Analýza rizík ISVS MsP Malacky 2011	2011
Bezpečnostný projekt informačných systémov na ochranu osobných údajov	2011
Bezpečnostná politika pre prístup k vzdialenej správe a databáze MsÚ (Corageo)	2011