Mesto Malacky, Radlinského 2751/1, 901 01 Malacky

Bezpečnostná smernica pre prácu s informačnými systémami mesta Malacky

Verzia:	0.1
Počet strán / príloh:	38/8
Dátum účinnosti:	01.06.2011
Vypracoval:	ATEMSEC, a.s.

Článok 1

Úvodné ustanovenie

1) Mesto Malacky (ďalej „mesto“) si uvedomuje dôležitosť informačných systémov verejnej správy (ISVS), ktoré prevádzkuje, význam údajov, ktoré sú v nich spracúvané, hodnotu majetku a technológií, ktoré používa pre svoju činnosť a povinnosť chrániť oprávnené záujmy mesta, štátu, zamestnancov a všetkých osôb, s ktorými prichádza do kontaktu. Z tohto dôvodu sa mesto a jeho orgány 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 a STN ISO/IEC 27002:2006.
2) Táto smernica je základným dokumentom pre všetkých vlastníkov aktív, používateľov a riadiacich pracovníkov informačnej bezpečnosti na všetkých úrovniach riadenia využívajúcich informačné systémy mesta a je záväzný pre všetkých používateľov výpočtovej techniky patriacej mestu Malacky.
3) Tento dokument upresňuje a aplikuje závery z bezpečnostnej politiky na konkrétne podmienky prevádzkovaných informačných systémov mesta. Obsahuje súhrn pravidiel, ktoré treba dodržiavať pre zachovanie dôvernosti, dostupnosti a integrity spracovávaných dát. Vymedzuje rozsah oprávnení a povinností riadiacich zamestnancov vykonávajúcich dohľad nad bezpečnosťou informačných systémov. Konkretizuje činnosť používateľov pri poruchách informačných systémov ako aj iných mimoriadnych situáciách a popisuje proces ich obnovy. Obsahuje zodpovednosť jednotlivých oprávnených osôb, spôsob identifikácie a autentizácie oprávnených osôb a princípy manipulácie s písomnosťami a ostatnými záznamami. Charakterizuje opatrenia proti škodlivým kódom, obsluhu zálohovacích zariadení a pod.
4) Bezpečnostná smernica je vytvorená na základe odporúčaní (tzv. „Best practices“) medzinárodných štandardov informačnej bezpečnosti ISO/IEC 27001:2005 Information security management. Specification with guidance for use, ISO/IEC 27002:2005 Information technology. Security technique. 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 Výnosu MF SR č. 312/2010 Z.z. a odporúčaní odvetvovej praxe. Smernica

vychádza aj s požiadaviek Zákona č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov.

Článok 2

Základné pojmy, definície a topológia siete

1) **Počítačová sieť LAN** (Local Area Network): je súhrn výpočtovej techniky, sieťových prvkov a softvérových aplikácií, prepojených za účelom potrieb mesta v oblasti výkonu verejnej správy, racionalizácie kancelárskych prác a elektronického prepojenia s ústrednými orgánmi štátnej správy SR, organizáciami verejnej správy, ako aj so zahraničnými partnermi. Sieť je tvorená štruktúrovanou kabelážou, ktorá prepája jednotlivé poschodia a pracoviská objektov, v ktorých sídlia príslušné orgány mesta (Mestský úrad a Mestská polícia). Počítačová sieť LAN je pripojená cez prístupový bod poskytovateľa služby na verejnú sieť Internet.
2) **Informačný systém:** je funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických a programových prostriedkov, ktoré sú súčasťou informačného systému.
3) **Informačná činnosť** je získavanie, poskytovanie a sprístupňovanie údajov, zhromažďovanie, spracúvanie, prenos, ukladanie, archivácia a likvidácia údajov; informačnú činnosť vykonáva mesto Malacky ako správca, resp. prevádzkovateľ informačného systému prostredníctvom procesov pokrývajúcich výkon jednotlivých úsekov správy.
4) **Výpočtová technika:** technické prostriedky informačných systémov, ktoré slúžia najmä na získavanie, zhromažďovanie, zaznamenávanie, usporadúvanie, premiestňovanie alebo prenos dát (napr. server, počítač, PDA, notebook, tlačiareň, skener, kopírovacie zariadenia).
5) **Výpočtová technika tretích strán:** technika, ktorá je vo vlastníctve a správe iného subjektu ako je mesto Malacky. (Do tejto skupiny patria aj súkromné technické prostriedky zamestnancov).
6) **Softvérové aplikácie:** programové prostriedky informačných systémov, ktoré slúžia najmä na získavanie, zhromažďovanie, zaznamenávanie, usporadúvanie, premiestňovanie alebo prenos dát (napr. editory, prehliadače, CG ISS a pod.).

7) **Sieťové prvky:** aktívne a pasívne technické prostriedky, ako napríklad: prepínač (switch), smerovač (router), firewall, prístupový bod pre bezdrôtové spojenie, kabeláž a pod.
8) **Server:** každá výpočtová technika, ktorá poskytuje svoj výkon, dátový priestor a služby cez počítačovú sieť viacerým používateľom (napr. súborový server, tlačový server, aplikačný server, databázový server, poštový server, WWW server).
9) **Používateľský účet:** (identifikácia) je súhrn údajov, ktoré jednoznačne identifikujú používateľa. Patrí medzi ne používateľské meno, heslo, prístupové práva a obmedzenia.
10) Používateľské meno: je reťazec znakov, ktorým sa používateľ jednoznačne identifikuje pre prihlásenie do siete.
11) **Meno počítača:** je reťazec znakov pre identifikáciu počítača, ktorý prideľuje správca siete resp. technický zamestnanec MsP.
12) **Prístupové práva:** umožňujú používateľovi využívať služby počítačovej siete tak, aby používal softvérové aplikácie a údaje, ktoré pre svoju prácu potrebuje. Obmedzovanie prístupových práv je snahou o elimináciu náhodného či úmyselného poškodenia počítača alebo počítačovej siete. Prístupové práva prideľuje používateľovi správca siete.
13) **Heslo:** umožňuje ochranu prístupu používateľa do počítačovej siete. Chráni pred neoprávneným prístupom do počítačovej siete cudzím používateľom.
14) **Monitorovanie siete:** je súbor kontrolných činností, pomocou ktorých správca siete kontroluje s akým softvérom používateľ pracuje, či má na prevádzanú prácu práva, či sa nepokúša o deštruktívnu činnosť alebo sa neusiluje svoje práva neoprávnene rozšíriť.
15) **Internet:** je celosvetová verejná počítačová sieť.
16) **Informačný systém www** (World Wide Web): je distribuovaný informačný systém vytvorený na báze architektúry klient – server, ktorý využíva možnosti techniky vyhľadávania informácie pomocou hypertextu. Získaná informácia môže mať formu textu, obrázka, videa či audia. Ak si používateľ vyberie označenú časť informácie, táto sa zobrazí, nezávisle od toho, na ktorom počítači v sieti sa informácia nachádza.
17) **Schránka elektronickej pošty:** je jedinečná e-mailová adresa zamestnanca slúžiaca na pracovnú elektronickú komunikáciu.
18) **Manažér informačnej bezpečnosti** (MIB): Zamestnanec MsÚ, ktorý zodpovedá za všetky aktivity týkajúce sa informačnej bezpečnosti a za celkový stav informačnej bezpečnosti mesta Malacky.

19) **Audítor informačnej bezpečnosti:** Zamestnanec MsÚ, ktorý je najvyššou kontrolnou zložkou informačnej bezpečnosti mesta Malacky.
20) **Správca siete:** zamestnanec MsÚ (informatik) vykonávajúci svoju činnosť podľa rozsahu určeného v pracovnej náplni. Je poverený správou počítačovej siete, sieťových prvkov, výpočtovej techniky a softvérových aplikácií MsÚ.
21) **Technický zamestnanec MsP:** zamestnanec Mestskej polície v Malackách (MsP) vykonávajúci svoju činnosť podľa rozsahu určeného v pracovnej náplni. Je poverený správou výpočtovej techniky a softvérových aplikácií MsP – mimo ISS. Opatrenia, ktoré realizuje vo všeobecnosti podľa tohto dokumentu správca siete, na pracovisku MsP ich vykonáva technický zamestnanec MsP – pokiaľ je to v tomto dokumente priamo uvedené (Čl. 5).
22) **Používateľ:** fyzická osoba (zamestnanec úradu alebo MsP), ktorá má legálny prístup do počítačovej siete mesta, internetu a má zriadenú vlastnú schránku elektronickej pošty.
23) **Sprostredkovateľ:** dodávateľská spoločnosť vrátane jej zamestnancov (tretia strana), podieľajúcich sa na poskytovaní služieb nevyhnutných pre chod informačných systémov, resp. počítačovej siete mesta.
24) **Nepovolaná osoba:** zamestnanec mesta, resp. cudzia osoba, ktorá nemá pridelené prístupové práva na vykonanie danej činnosti alebo operácie.
25) Bezpečnostný incident: nechcená alebo neočakávaná udalosť, pri ktorých existuje vysoká pravdepodobnosť narušenia integrity, dostupnosti alebo dôvernosti informačných systémov mesta Malacky. Za úmyselný bezpečnostný incident sa považuje cieľavedomé využitie zraniteľného miesta k spôsobeniu škôd/strát na aktívach informačného systému.
26) **Aktívum:** je softvérová aplikácia, výpočtová technika, poskytované služby, kvalifikované osoby, dobré meno a informácie (najmä osobné údaje), dokumentácia, zmluvy a iné skutočnosti, ktoré považuje mesto Malacky za citlivé.
27) **Mesto Malacky:** Mesto Malacky je na základe schváleného štatútu mesta Malacky v znení neskorších dodatkov samostatným územným samosprávnym a správnym celkom Slovenskej republiky združujúcim občanov, ktorí majú na jeho území trvalý pobyt a z pohľadu právnej formy je právnickou osobou (IČO: 00 304 913), ktorá za podmienok ustanovených zákonom samostatne hospodári s vlastným majetkom a s vlastnými príjmami.

28) **Vedúci:** je nadriadený zamestnanca, na ktorého sa opatrenia podľa tohto dokumentu vzťahujú (vedúci oddelenia, prednosta MsÚ, náčelník MsP, primátor).
29) **Vstúpenie do počítača:** (vo vzťahu k čl. 4 ods. 8): je činnosť spojená s inštaláciou, konfiguráciou, výmenou, alebo údržbou počítača používateľa, resp. činnosť spojená s inštaláciou, konfiguráciou, aktualizáciou alebo zálohovaním softvérových aplikácii a dát uložených na tomto počítači.

Článok 3

Práva a povinnosti manažéra a audítora informačnej bezpečnosti

Manažér informačnej bezpečnosti:

1) zodpovedá za všetky aktivity týkajúce sa informačnej bezpečnosti a za celkový stav informačnej bezpečnosti informačných systémov mesta Malacky,
2) zodpovedá za metodické riadenie činností správcov siete, technických zamestnancov a sprostredkovateľov z pohľadu informačnej bezpečnosti,
3) zodpovedá za spracovanie, dopĺňanie a revíziu bezpečnostnej dokumentácie informačných systémov mesta,
4) zodpovedá za spracovanie dokumentu Analýza rizík ISVS pre daný kalendárny rok, ktorú predkladá podľa stanovených interných predpisov na schválenie primátorovi mesta,
5) zodpovedá za spracovanie dokumentu Správa o stave informačnej bezpečnosti mesta Malacky pre daný kalendárny rok, ktorú predkladá na schválenie primátorovi mesta,
6) zodpovedá za realizáciu, resp. implementáciu navrhovaných režimových a organizačných ochranných opatrení a za metodické riadenie realizácie technických ochranných opatrení vyplývajúcich zo záverečnej správy auditu informačnej bezpečnosti,
7) iniciuje schvaľovací proces bezpečnostnej dokumentácie informačných systémov mesta,
8) iniciuje disciplinárne konanie a uplatnenie sankcií v prípade zistenia zdroja, ktorý spôsobil úmyselný bezpečnostný incident v prostredí počítačovej siete mesta,
9) vykonáva školenie nových používateľov informačných systémov zamerané na ich práva a povinnosti vo vzťahu k bezpečnosti informačných systémov mesta,
10) zodpovedá za schvaľovací proces zmien existujúcich a zavádzaných nových ISVS a informačno-komunikačných technológií, a to hlavne za časť týkajúcej sa bezpečnostných požiadaviek na tretie strany.

Audítor informačnej bezpečnosti:

11) zodpovedá za kontrolu a dodržiavanie bezpečnostnej politiky informačných systémov mesta,
12) raz za rok vykonáva kontrolu dodržiavania informačnej bezpečnosti mesta (podľa Metodiky vnútorného auditu informačnej bezpečnosti),
13) na základe zistení z kontroly vypracováva Správu z interného auditu informačnej bezpečnosti, ktorú predkladá primátorovi.

Článok 4

Práva a povinnosti správcu počítačovej siete

Správca siete:

1) zodpovedá za prevádzku a údržbu zariadení (výpočtová technika, sieťové prvky), ktoré súvisia s prevádzkou počítačovej siete a za zariadenia umiestnené mimo budovy MsÚ, ako je: Turisticko-informačná kancelária v Inkubátore Malacky, n. o., Pálfiovský kaštieľ a vysunuté pracovisko v obchodnej organizácii Tekos Malacky, s.r.o.
2) zodpovedá za zaistenie maximálnej ochrany všetkých dát a informácií pred poškodením, zneužitím, stratou alebo neautorizovaným prístupom,
3) vytvára, prideľuje, modifikuje, ruší používateľské účty a vedie o nich záznamy (softvérové aplikácie v správe MsÚ),
4) má právo po dohode s príslušným vedúcim obmedziť alebo rozšíriť privilégia používateľov v ich prístupe k výpočtovej technike,
5) vykonáva inštaláciu výpočtovej techniky a softvéru, ich konfiguráciu, pripojenie počítačov k sieti a v prípade potreby manipuluje s jednotlivými časťami počítačovej siete,
6) pri nástupe nového zamestnanca, ktorý bude pracovať s výpočtovou technikou, na základe oznámenia (zaslaného písomne alebo elektronickou poštou) príslušného vedúceho, uskutoční základné poučenie a oboznámenie s pravidlami pre prácu v počítačovej sieti,
7) vykoná registráciu používateľa do počítačovej siete, stanoví používateľské práva a uskutočňuje ich údržbu na základe požiadavky (zaslanej písomne alebo elektronickou poštou) príslušného vedúceho,

8) zabezpečuje prevádzku a údržbu počítačov; má právo po predchádzajúcom upozornení vykonať potrebnú profylaktiku siete; má právo v rámci svojich právomocí a povinností požiadať o neodkladné prerušenie práce na všetkých zariadeniach v počítačovej sieti na dobu potrebnú na vykonanie nevyhnutných zásahov do systému siete; na požiadanie vedúceho má právo a povinnosť kedykoľvek v prípade potreby vstúpiť do počítača používateľa - o takomto zásahu následne vyhotoví protokol, kde budú uvedené kontrolné zistenia a všetky vykonané úkony. S protokolom následne oboznámi aj používateľa počítača – proti podpisu.
9) koordinuje činnosti pri poruchách siete, techniky alebo softvéru a vedie o tom záznamy; v prípade potreby riešenia stavu, ktorý neznesie odklad odpojí problémový segment siete tak, aby bola, pokiaľ je to možné, zachovaná funkčnosť siete,
10) zabezpečuje pravidelné zálohovanie dát pre možnosť ich obnovy v prípadoch neodstrániteľných porúch, a to systémové súbory serverov a databázové súbory; takisto zabezpečuje archiváciu dohodnutých dôležitých súborov z používateľských počítačov na vybraných médiách alebo do sieťového úložiska, a zodpovedá za dostatočnú kapacitu úložiska, v prípade mimoriadnej situácie sa bude riešiť zabezpečenie kapacity v priebehu čo najkratšej možnej doby,
11) sleduje prevádzku siete a internetového pripojenia, zodpovedá za ich technický stav, bezpečnosť a nepretržitú prevádzky schopnosť, odstraňuje zo systémov neoprávnene prebiehajúce programy a procesy,
12) zabezpečuje aktualizácie databáz antivírusového programu,
13) sleduje využitie serverového diskového priestoru používateľmi a zabezpečuje jeho dostatočnú kapacitu,
14) zodpovedá za vedenie evidencie (v elektronickej a tlačenej forme) o aktuálnom technickom a softvérovom vybavení siete (vrátane počítačov v správe MsÚ),
15) má právo a povinnosť v prípade požiadavky vedúceho monitorovať rozsah využívania internetu a zariadení výpočtovej techniky a o výsledku písomne informovať vedúceho; takisto má povinnosť, na základe písomnej požiadavky (alebo požiadavky zaslanej mailom) príslušného vedúceho, vykonať monitorovanie práce zamestnancov,
16) vedie evidenciu prvotne pridelených hesiel a ostatných prístupových kódov a v plnom rozsahu zodpovedá za ich prípadné zneužitie v dôsledku nedostatočnej ochrany uvedenej

evidencie, v prípade úniku prvotne prideleného hesla používateľa, ktorý si nezmenil toto heslo na vlastné, zodpovedá za jeho zneužitie používateľ,

17) je oprávnený v odôvodnených prípadoch s vedomím používateľa použiť softvérový prístup (VNC, RDP) na ľubovoľný počítač v lokálnej počítačovej sieti,
18) vykonáva sledovanie stavu dodržiavania licenčných zmlúv platných pre inštalovanie softvéru na prostriedkoch výpočtovej techniky, zodpovedá za dodržiavanie licenčnej politiky softvéru,
19) v prípade požiadavky vedúceho je povinný kontrolovať, vyhodnocovať a zálohovať logy prístupov a zmien do softvérových aplikácií (iba v prípade pokiaľ to aplikácia umožňuje),
20) je povinný bezodkladne oznámiť závažné bezpečnostné incidenty alebo podozrenie na ne manažérovi informačnej bezpečnosti,
21) spolupodieľa sa na periodických a náhodných kontrolách dodržiavania bezpečnosti informačného systému,
22) nie je oprávnený prevziať identitu používateľa bez jeho vedomia. Vo výnimočných alebo naliehavých prípadoch môže po dohode s vedúcim, zmeniť prihlasovacie heslo používateľa, vstúpiť do systému. O takomto zásahu následne vyhotoví protokol, kde budú uvedené kontrolné zistenia a všetky vykonané úkony. S protokolom neodkladne oboznámi i používateľa počítača – proti podpisu. Následne zabezpečí opätovné zadanie hesla týmto zamestnancom.
23) pri havárii alebo poruche informačného systému prijíma opatrenia na jeho urýchlenú obnovu,
24) nie je oprávnený prideliť inej osobe prístupové práva ekvivalentné právam vlastným
25) v druhej rade zodpovedá za prevádzku a správu technických zariadení zabezpečujúcich ochranu objektov (EZS) Mesta, ktoré nie sú v správe iného subjektu (napr. MsÚ, Pálfiovský kaštieľ,), v prvej rade zabezpečuje túto prevádzku určený správca budovy,
26) Pri akomkoľvek monitorovaní činnosti používateľa resp. siete je povinný správca siete resp. technický zamestnanec MsP vyhotoviť kontrolný list, v ktorom bude uvedené, na základe akého podnetu bude činnosť vykonaná, predchádzajúci súhlas vedúceho s vykonaním kontroly, aké bude zameranie a aké boli kontrolné zistenia. S výsledkom kontroly proti podpisu oboznámi vedúceho.

Osobitné povinnosti pre správcu siete ohľadom prístupu na počítače v sieti v správe MsP

1) Na základe oficiálnej žiadosti náčelníka MsP (poslanej písomne alebo elektronickou poštou na adresu správcu siete) je správca siete povinný nainštalovať antivírusový softvér a umožniť z PC MsP prístup do počítačovej siete mesta, a to v rozsahu: prístup do siete Internet, spracovávanie elektronickej pošty, prístup do systému ISS.
2) Správca siete v spolupráci s technickým zamestnancom MsP na základe žiadosti náčelníka MsP (poslanej písomne alebo elektronickou poštou na adresu správcu siete) zabezpečí vytvorenie používateľských účtov a modifikáciu ich prístupových práv v doméne MsÚ.
3) Správca siete bez predchádzajúcej dohody náčelníka s nadriadeným správcu nezabezpečuje inštaláciu, nastavenia (napr. správa používateľských účtov) a aktualizáciu žiadneho softvéru umiestneného na počítačoch v správe MsP, s výnimkou vyššie uvedených úkonov, v súlade s bodmi 2) a 4) v článku 5.
4) Správca siete bez predchádzajúcej dohody náčelníka s nadriadeným správcu nezabezpečuje technickú prevádzku žiadnej výpočtovej techniky v správe MsP.

Nakoľko správca siete má nadštandardné prístupové práva do softvérových aplikácií, resp. domény, vyplývajúce z náplne jeho práce, je povinný pristupovať do týchto systémov len v nevyhnutnom rozsahu a zároveň je povinný zachovať mlčanlivosť o skutočnostiach, o ktorých sa dozvedel pri výkone svojho zamestnania, a ktoré v záujme zamestnávateľa nemožno oznamovať iným osobám. Porušenie tejto zásady je považované za závažné porušenie pracovnej disciplíny hrubým spôsobom a bude posudzované v zmysle platných interných predpisov.

Článok 5

Práva a povinnosti technického zamestnanca MsP

Technický zamestnanec MsP:

1) zodpovedá za prevádzku a údržbu zariadení v správe MsP (výpočtová technika, sieťové prvky),

2) vykonáva inštaláciu, konfiguráciu a aktualizáciu technických a programových prostriedkov informačných systémov MsP,
3) zodpovedá za zaistenie maximálnej ochrany všetkých dát a informácií uložených na zariadeniach v správe MsP pred poškodením, zneužitím, stratou alebo neautorizovaným prístupom,
4) vytvára, prideľuje, modifikuje, resp. ruší používateľské účty a vedie o nich záznamy (softvérové aplikácie v správe MsP),
5) na základe usmernenia náčelníka MsP obmedzuje alebo rozširuje privilégia používateľov v ich prístupe k výpočtovej technike,
6) informuje manažéra informačnej bezpečnosti o skutočnostiach, ktoré sú v rozpore so všeobecne záväznými právnymi predpismi alebo internými predpismi v oblasti informačnej bezpečnosti,
7) je povinný bezodkladne oznámiť závažné bezpečnostné incidenty alebo podozrenie na ne správcovi siete, resp. manažérovi informačnej bezpečnosti,
8) spolupodieľa sa na periodických a náhodných kontrolách dodržiavania bezpečnosti informačného systému,
9) pri havárii alebo poruche informačného systému prijíma opatrenia na jeho urýchlenú obnovu.
10) zodpovedá za vedenie evidencie (v elektronickej a tlačenej forme) o aktuálnom technickom a softvérovom vybavení pracoviska MsP,
11) v prípade požiadavky vedúceho je povinný kontrolovať, vyhodnocovať a zálohovať logy prístupov a zmien do softvérových aplikácií (iba v prípade pokiaľ to aplikácia umožňuje),

Vo vzťahu k technickej a administratívnej podpore pracoviska MsP sa vzťahujú na technického zamestnanca MsP aj niektoré ďalšie oprávnenia a povinnosti v kompetencii správcu siete (napr. vytváranie, rušenie a zmena prístupových práv, aktualizovanie a uloženie administrátorských prístupových hesiel, centrálne zálohovanie dát, licenčná politika a ochrana autorských práv, ochrana proti škodlivému kódu, monitorovanie práce používateľov na základe požiadavky vedúceho, vzdialený prístup (VNC, RDP), atď.).

Článok 6

Práva a povinnosti správcu www stránok

Správca www stránok (webmaster):

1) zabezpečuje prevádzku www stránky mesta (www.malacky.sk) na internete po administratívnej stránke,
2) preberá materiály na technologické spracovanie pre internet,
3) koordinuje technické spracovanie jednotlivých dokumentov podľa platnej metodiky prípravy www stránok v predpísanom štandardnom formáte, na základe Výnosu Ministerstva financií SR č. 312/2010 Z. z. o štandardoch pre informačné systémy verejnej správy,
4) iniciuje rozvoj internetových stránok mesta,
5) udeľuje a zabezpečuje prístup určených zamestnancov MsÚ a MsP do redakčného systému web stránok mesta,
6) vedie dokumentáciu týkajúcu sa spracovania web stránok mesta.

Článok 7

Práva a povinnosti používateľa výpočtovej techniky

Používateľ:

1) sa zaväzuje, že bude počítačovú sieť používať len spôsobom, ktorý nenaruší prácu ostatných používateľov alebo chod zariadení zabezpečujúcich prevádzku siete,
2) má právo používať všetky služby počítačovej siete v rozsahu potrebnom na plnenie svojich pracovných povinností, má právo používať internet a elektronickú komunikáciu pri dodržaní pravidiel súvisiacich s týmito činnosťami,
3) smie používať len ten používateľský účet, ktorý mu bol pridelený, používateľ sa nesmie snažiť žiadnym spôsobom o získanie prístupu iného používateľa, nesmie maskovať identitu počítačového účtu ani počítača, ktorý používa,
4) vykonáva svoju činnosť len na jemu pridelených, resp. povolených (napr. pri vzdialenom prístupe) prostriedkoch výpočtovej techniky a výlučne pod jemu prideleným používateľským účtom,
5) zodpovedá v plnej miere za všetky preukázané škody vzniknuté v dôsledku zneužitia jeho účtu zavineného nedbalou manipuláciou s prístupovými kódmi alebo ich

poskytnutím inej osobe, alebo v dôsledku nedodržania iných ustanovení v týchto pravidlách,

6) nesmie používať prostriedky výpočtovej techniky na získanie neautorizovaného prístupu ku vzdialeným počítačom.
7) je povinný sledovať zaplnenie diskového priestoru v jemu zverenom počítači a v prípade nedostatku tohto priestoru (pri poklese voľného priestoru na pracovnom disku pod cca 500 MB) konzultovať jeho zvýšenie či uvoľnenie so správcom siete, resp. technickým zamestnancom MsP.
8) je povinný neodkladne oznámiť všetky zistené bezpečnostné incidenty, poruchy výpočtovej techniky alebo softvérových aplikácií správcovi siete resp. technickému zamestnancovi MsP telefonicky alebo prostredníctvom elektronickej pošty,
9) nesmie úmyselne vykonávať činnosti, ktoré majú vážny dopad na činnosť výpočtovej techniky (napr. periférne zariadenia) a počítačovej siete. Medzi ne patrí:
   a) neodborná manipulácia s časťami počítačovej siete,
   b) inštalácia nových, resp. rekonfigurácia už existujúcich komponentov alebo softvérových aplikácií,
10) nesmie dať k dispozícii svoj používateľský účet a umožniť tak jeho využívanie inej osobe bez súhlasu nadriadeného, správcu siete, resp. technického zamestnanca MsP,
11) nesmie obchádzať technické a organizačné bezpečnostné opatrenia a využívať prípadné nedostatky v bezpečnosti siete, zistené nedostatky je povinný neodkladne oznámiť správcovi siete,
12) nesmie zámerne vykonávať činnosti, ktoré predstavujú plytvanie s počítačovými zdrojmi na úkor ostatných používateľov, pričom medzi tieto činnosti patrí: posielanie hromadných e-mailových správ (s výnimkou pracovných), tlač zbytočných alebo súkromných výstupov, zvyšovanie dátovej záťaže siete (napr. používanie peer-to-peer sietí, sťahovanie objemných dát z internetu, ktoré nesúvisia s pracovnou činnosťou, resp. s update počítača), nepovolené hranie počítačových hier a iné nepovolené využívanie zverenej výpočtovej techniky a softvéru,
13) nesmie do priestoru počítačovej siete umiestniť informácie porušujúce práva inej osoby, hanlivého, sexuálneho, rasovo, nábožensky alebo národnostne urážlivého charakteru, takisto nesmie takéto informácie vytvárať či posielať elektronickou poštou,

14) nesmie čítať, kopírovať, meniť alebo mazať dáta iných používateľov bez ich vedomia, nesmie neoprávnene kopírovať a distribuovať žiadne časti operačných systémov, aplikačných programov a údajov z databáz,
15) môže prenášať dôležité alebo citlivé údaje (osobné údaje, obchodné, poštové, resp. bankové tajomstvo – v elektronickej alebo tlačenej forme) mimo pracovísk mesta Malacky (napr. emailom, na pamäťových diskoch, notebookoch, atď.), iba na základe súhlasu prednostu mestského úradu alebo náčelníka mestskej polície. Dôležité alebo citlivé dáta sa v elektronickej forme môžu prenášať iba v zašifrovanej forme (na základe školenia správcom siete, resp. technickým zamestnancom MsP a po dodaní softvérovo-technického zabezpečenia),
16) musí sa riadiť platnou licenčnou politikou softvéru,
17) má právo požiadať o konzultáciu so správcom siete, resp. technickým zamestnancom MsP, ohľadom používanej výpočtovej techniky a softvérových aplikácií v pracovných dňoch podľa aktuálne platného časového rozvrhu správcu siete resp. technického zamestnanca MsP, v prípade nevyhnutnej potreby na základe požiadavky poslanej písomne alebo elektronickou poštou, aj v inom čase,
18) zodpovedá spoločne s príslušnými vedúcimi podľa svojej pôsobnosti za obsah informácií zverejňovaných na internete,
19) je povinný spolupracovať pri akejkoľvek kontrolnej alebo audítorskej činnosti súvisiacej s manažérstvom informačnej bezpečnosti informačných systémov vyplývajúcej z bezpečnostnej politiky alebo inej bezpečnostnej dokumentácie,
20) musí mať základné znalosti práce so súbormi a adresármi v prostredí operačného systému MS Windows; vytváranie, premenovanie, mazanie a presúvanie súborov medzi CD, DVD, externým HDD, USB flash pamäťami, diskami pracovnej stanice a počítačovej siete sa predpokladá ako základná požiadavka na splnenie uložených pracovných úloh,
21) má povinnosť zálohovať, resp. archivovať agendu na svojom počítači resp. na inom úložisku dát v periodicite, ktorú mu stanoví vedúci,
22) využívanie počítačovej siete pre iné činnosti než sú uvedené v pravidlách musia byť dopredu schválené vedením MsÚ, MsP alebo správcom počítačovej siete.

Článok 8

Práva a povinnosti vedúceho

Vedúci má, okrem práv a povinností uvedených v článku 7, tieto práva a povinnosti:

1) má právo písomne resp. mailom požiadať o nastavenie zdieľania diskového priestoru na určených sieťových počítačoch na príslušnom pracovisku,
2) má právo v odôvodnených prípadoch písomne resp. mailom požiadať o monitorovanie práce jednotlivých počítačov v sieti na pracovisku,
3) má právo určiť používateľom povinnosť zálohovať, resp. archivovať vybraný typ agendy na vybranom počítači v rámci svojho pracoviska, prípadne po dohode so správcom siete resp. technickým zamestnancom MsP v sieťovom úložisku alebo na vybrané médiá,
4) má právo rozhodnúť o sprístupnení vybraného počítača tretej osobe v prípade dlhodobej neprítomnosti zamestnanca alebo v prípade inej mimoriadnej udalosti, o čom musí bezodkladne písomne, resp. mailom informovať správcu siete, resp. technického zamestnanca MsP,
5) má právo určovať zodpovedných používateľov v rámci pracoviska a úroveň nastavenia ich prístupových práv k aplikáciám prevádzkovaných v počítačovej sieti alebo na počítačoch v rámci príslušného pracoviska,
6) má právo rozhodovať o rozmiestnení výpočtovej techniky na pracovisku,
7) má právo po konzultácii so správcom www stránok, rozhodovať o zaradení materiálov v elektronickej forme na internetový server,
8) V prípade príchodu, resp. odchodu nového zamestnanca na pracovisko má právo vystaviť žiadosť o pridelenie, resp. odobratie prostriedkov výpočtovej techniky, o inštaláciu softvérových aplikácií, o vytvorenie, resp. zrušenie používateľských účtov.

Článok 9

Zásady pre tvorbu hesiel

1) Autorizácia používateľa môže byť viac úrovňová. Na každej úrovni je vhodné používať iné heslo.
2) Používateľ je povinný pracovať iba pod používateľským účtom, ktoré mu bolo pridelené. Správca siete, resp. technický zamestnanec MsP môže povoliť používanie skupinového používateľského účtu.

3) Používateľ je povinný nastaviť silné heslá pre prihlásenie do softvérovej aplikácie.
4) Silné heslá musia spĺňať príslušné atribúty: minimálna dĺžka 5 znakov, obsahujú veľké písmeno, malé písmeno, špeciálny znak alebo číslicu. Silné heslá nesmú obsahovať meno a ani žiadny regulárny slovný výraz.
5) Silné heslá nie je potrebné používať len v tom prípade, pokiaľ jeden používateľský účet využíva viacero oprávnených používateľov (napr. strážna služba MsP),
6) Používateľ je povinný zapamätať si prístupové heslá a nezapisovať ich na rôzne médiá (napr. post-it, poznámkový blok).
7) Všetky heslá sú považované za dôvernú informáciu, preto sa zakazuje:
   a) poskytovať prístupové heslo telefonicky alebo e-mailom,
   b) poskytovať prístupové heslo v prieskumných dotazníkoch,
   c) poskytovať prístupové heslo spolupracovníkom pri dlhodobej neprítomnosti,
   d) používať prístupové heslá využívané v rámci informačných systémov mesta Malacky (napr. CG ISS), v externých systémoch na súkromné účely.
8) Používateľ je povinný pri zadávaní prístupového hesla zabezpečiť, aby nedošlo k odčítaniu hesla z klávesnice.
9) V prípade pokiaľ používateľ zdieľa pracovisko s inými zamestnancami, ktorí nie sú oprávnení používať jemu pridelený počítač, je povinný pri opustení pracoviska sa odhlásiť zo systémov tak, aby nebol týmto neoprávneným osobám umožnený prístup.
10) Používateľ je povinný po prvotnom prihlásení do systému si zmeniť svoje prístupové používateľské heslo.
11) Používateľ je povinný meniť prístupové heslá v pravidelných intervaloch, najneskôr raz za 6 mesiacov.
12) Používateľ je povinný podozrenie na kompromitáciu prístupového hesla nahlásiť správcovi siete, resp. technickému zamestnancovi MsP, alebo je povinný si ho sám zmeniť.
13) Správca siete je povinný:
   a) nastaviť pracovnú stanicu, resp. server na používanie šetriča obrazovky s aktivovanou ochranou heslom pri obnovení pracovnej činnosti po 5 minútach nečinnosti,
   b) nastaviť prístupové práva a prvotné prístupové heslo do operačného systému,

c) pokiaľ to softvérová aplikácia umožňuje, zapnúť obmedzené logovanie bezpečnostných incidentov - odporúčajú sa tri neúspešné pokusy o autorizáciu do systému,

d) viesť a vyhodnocovať auditný záznam o jednotlivých prihláseniach do softvérovej aplikácie (pokiaľ to systém umožňuje),

e) diskrétnou formou a adresne oznámiť prvotné prednastavené prístupové heslá do aplikácie používateľovi,

f) viesť aktuálny zoznam oprávnených používateľov softvérových aplikácií.

Všetky aktuálne administrátorské prístupové heslá do softvérových aplikácií MsÚ musia byť uložené v zapečatenej obálke. Za aktualizáciu zoznamu je zodpovedný správca siete. Zapečatená obálka musí byť uložená v trezore. Na pracovisku MsP zodpovedá za aktualizáciu zoznamu hesiel technický zamestnanec MsP. Kópia je uložená v PC náčelníka v zaheslovanej forme.

Článok 10

Prideľovanie, modifikácia a rušenie prístupových práv

1) Zavedenie a zrušenie používateľských účtov do informačných systémov mesta sa realizuje na základe pracovnoprávnych vzťahov - vznik, zmena a ukončenie pracovného pomeru resp. iného obdobného pracovného vzťahu.
2) V prípade príchodu nového, resp. odchodu používateľa má vedúci oprávnenie vystaviť žiadosť o pridelenie, resp. odobratie prostriedkov výpočtovej techniky a žiadosť o vytvorenie, resp. zrušenie prístupových práv do softvérových aplikácií.
3) Žiadosť musí byť poslaná písomne alebo elektronickou poštou správcovi siete, resp. technický zamestnanec MsP, pričom žiadosť musí obsahovať titul, meno a priezvisko používateľa, pracovné zaradenie, zoznam softvérových aplikácií, prípadne ich modulov s ktorými bude zamestnanec pracovať. Úroveň prístupových práv a v prípade vytvárania prístupu do ISS aj rodné číslo zamestnanca (príloha 1).
4) Správca siete zodpovedá za prideľovanie, modifikáciu, resp. rušenie prístupových práv používateľov v doméne MsÚ a používateľov softvérových aplikácií, prostredníctvom

ktorých sa zabezpečuje výkon úloh súvisiacich s agendou MsÚ, alebo agendou MsÚ spoločne s agendou MsP.

5) Technický zamestnanec MsP zodpovedá za prideľovanie, modifikáciu, resp. rušenie prístupových práv používateľov softvérových aplikácií, prostredníctvom ktorých sa zabezpečuje výkon úloh súvisiacich výlučne s agendou MsP.
6) Webmaster zodpovedá za prideľovanie, modifikáciu, resp. rušenie prístupových práv do webového sídla mesta Malacky (www.malacky.sk).
7) Podpisom žiadosti o zrušenie prístupových práv dáva vedúci zároveň súhlas na zrušenie všetkých používateľských účtov a uložených dát odchádzajúceho zamestnanca.
8) Pred ukončením pracovného pomeru správca siete resp. technický zamestnanec MsP prevezme prostriedky výpočtovej techniky od používateľa a za jeho prítomnosti ho skontroluje.
9) V prípade potreby je používateľ oprávnený požiadať o zmenu už pridelených prístupových práv priamo správcu siete, resp. technického zamestnanca MsP bez súhlasu vedúceho. V praxi takáto požiadavka predstavuje: zmenu prístupového hesla, pridelenie oprávnenia tlačiť na sieťovej tlačiarni, update softvéru alebo inštalácia ovládača.
10) V prípade pokiaľ proces vytvorenia/rušenia prístupových práv je v kompetencií sprostredkovateľa, správca siete je povinný neodkladne ho informovať o danej požiadavke.
11) V prípade dlhodobej neprítomnosti zamestnanca (viac ako 4 týždne) a na žiadosť vedúceho, správca siete, resp. technický zamestnanec MsP zablokuje jeho používateľský účet.
12) Používateľ nesmie používať pridelené prístupové práva na inú činnosť, ako je stanovená jeho pracovnou zmluvou, náplňou práce, pracovným alebo funkčným zaradením. Používateľ nesmie poskytnúť svoj používateľský účet neoprávnenej osobe.
13) Pokiaľ používateľ získa privilegovaný stav, ktorý mu nebol udelený, je povinný túto skutočnosť bezprostredne oznámiť manažérovi informačnej bezpečnosti, ktorý je povinný vykonať záznam o tomto bezpečnostnom incidente (Príloha 7) a oznámiť túto skutočnosť správcovi siete, resp. technickému zamestnancovi MsP. Správca siete, resp. technický zamestnanec MsP je povinný neodkladne zrušiť tento privilegovaný stav. V prípade pokiaľ používateľ získa neoprávnený privilegovaný stav, v dôsledku úmyselnej činnosti správcu

siete, resp. technického zamestnanca je manažér informačnej činnosti povinný informovať vedúceho.

14) Správca siete je povinný mať prehľad o všetkých používateľoch v systémoch, o ich právomociach a dĺžke prístupu.

15) Manažér informačnej bezpečnosti je povinný mať prehľad o všetkých dodávateľoch softvérových aplikácií.

Článok 11

Zálohovanie dát

1) Používateľ je povinný:
   a) niesť zodpovednosť za informácie uložené na lokálnom disku, ktoré sám vytvoril,
   b) stanoviť si maximálnu dobu periodicity zálohovania,
   c) zálohovať súbory, ktoré vytvára, resp. modifikuje a ich zároveň ukladá na lokálny disk pracovnej stanice, pričom použije na to prioritne službu softvérového vybavenia, s ktorým pracuje,
   d) nenechávať dôležité alebo citlivé dáta (obsahujúce: osobné údaje, obchodné, poštové, resp. bankové tajomstvo) na verejne prístupných dátových úložiskách,
   e) osobné údaje neukladať v nezabezpečenej forme na prenosné záznamové média,
   f) vykonávať pravidelnú údržbu a čistenie dát,
   g) mať uložené len tie dáta, ktoré môžu byť potrebné k výkonu práce,
   h) prenosné zálohovacie médiá s „citlivými“ údajmi ukladať v uzamykateľnej skrini, zásuvke, resp. trezore, mimo priestorov, v ktorých sú spracovávané zálohované údaje.
2) Za centrálne zálohovanie databáz s údajmi IS CG ISS je zodpovedný správca siete.
3) Zálohovacie médiá centrálneho zálohovania musia byť uložené tak, aby boli okamžite k dispozícii v prípade potreby obnovenia dát, avšak musia byť ukladané mimo priestorov, v ktorých sú spracovávané zálohované údaje.
4) Všetky zálohovacie a inštalačné média musia byť uložené tak, aby nedošlo k neoprávnenej manipulácií, poškodeniu záznamu, predovšetkým nesmú byť vystavované pôsobeniu silného magnetického poľa (v blízkosti mobilného telefónu, reproduktora

akustického zariadenia, elektrického transformátora), teplotným extrémom, vlhkosti a prašnosti.

5) Test funkcionality zálohovacích médií a obnovy systému zo zálohy vykonáva správca siete, resp. technický zamestnanec MsP, a to minimálne 1 x za rok, pričom o ňom vedie záznam (Príloha 8).

Článok 12

Zásady pre používanie elektronickej komunikácie

1) Používanie elektronickej komunikácie je prípustné len na plnenie pracovných povinností, ktorých rozsah upresňuje príslušný vedúci.
2) Každý používateľ má právo na jedno e-mailové konto. V prípade pridelenia generickej e-mailovej adresy môže mať aj viac ako jednu adresu.
3) Generická alebo ďalšia e-mailová adresa sa prideľuje na základe požiadavky vedúceho zaslanej písomne alebo e-mailom.
4) Každému používateľovi je pri nástupe do zamestnania pridelená, na základe požiadavky vedúceho poslanej písomne alebo elektronickou poštou, e-mailová adresa v tvare meno.priezvisko@malacky.sk. Pri existencii duplicitného mena a priezviska dvoch alebo viacerých zamestnancov v rámci MsÚ má adresa tvar meno.priezvisko.poradovecislo@malacky.sk. Štruktúra e-mailovej pracovnej adresy je stanovená záväzne výnosom Ministerstva financií SR 312/2010 Z. z. o štandardoch pre informačné systémy verejnej správy a v nadväznosti na zákon 275/2006 Z. z. o informačných systémoch verejnej správy.
5) V prípade e-mailovej schránky zriadenej pred rokom 2011, ostáva používateľovi táto pridelená aj naďalej v tvare priezvisko@malacky.sk, resp. priezvisko.m@malacky.sk, a to pre potreby zachovania časovej kontinuity elektronickej komunikácie a v nej obsiahnutých informácií.
6) Používateľ je povinný používať elektronickú komunikáciu len na legálne účely. Obsah dát odosielaných v rámci počítačovej siete MsÚ a internetu nesmie byť v rozpore s dobrými mravmi.
7) Používateľ je povinný rešpektovať zákaz posielania reťazových, reklamných, poplašných a hromadných e-mailových správ, s výnimkou pracovných informačných správ. Posielanie

nevyžiadaných správ, tzv. SPAM, je v SR zakázané, viď §3 ods. 6 zákona č. 147/2001 Z. z. o reklame a zmenách.

8) Používateľ je povinný v prípade prijatia podozrivých e-mailových správ túto skutočnosť neodkladne hlásiť správcovi siete, resp. technickému zamestnancovi MsP a nesmie tieto správy otvárať či posielať iným používateľom.
9) Používateľ v plnej miere zodpovedá za stratu dát pri nedodržaní uvedených zásad.

Článok 13

Zásady pre používanie internetu

1) Používateľ má právo pre plnenie pracovných povinnosti využívať internet.
2) Je zakázané navštevovať stránky s pornografickou, warezovou, hackerskou a inou tematikou odporujúcou dobrým mravom, okrem odôvodnených prípadov (napr. MsP).
3) Je zakázané vedome prenášať vírusy alebo iné potenciálne škodlivé kódy.
4) Pri komunikácii s inými sieťami je potrebné dodržiavať pravidlá, ktoré platia v týchto sieťach.
5) Je prísne zakázané neoprávnene prenikať do vzdialených počítačových stredísk alebo sietí akýmkoľvek spôsobom.
6) Používateľ je povinný riadiť sa týmito zásadami a nesie plnú zodpovednosť za prípadnú škodu spôsobenú nedodržaním týchto pravidiel a zásad.

Článok 14

Prístup do siete pomocou vzdialeného prístupu

1) Správca siete, resp. technický zamestnanec MsP môže vytvoriť používateľom v prípade nevyhnutnej potreby vzdialený prístup do LAN siete mesta Malacky (napr. prístup do CG ISS), pričom tento prístup musí byť realizovaný prostredníctvom zabezpečenej virtuálnej privátnej siete (VPN).
2) O vzdialený prístup musí požiadať prednosta mestského úradu alebo náčelník mestskej polície, a to písomne alebo elektronickou poštou (príloha 1). Žiadosť musí obsahovať dôvod vytvorenia vzdialeného prístupu a dobu počas ktorej má byť zrealizovaný.

3) Rovnaký postup podľa bodu 1) a 2) sa uplatňuje aj v prípade požiadavky na vzdialený prístup v rámci LAN siete mesta Malacky (napr. za účelom monitoringu činností používateľov).
4) V prípade monitoringu činností používateľov cez vzdialený prístup, musí byť o tejto činnosti oboznámený monitorovaný používateľ.
5) Tým, že pracovné stanice, z ktorých sa vytvára vzdialený prístup do LAN siete mesta Malacky, sa nachádzajú v nezabezpečenom priestore, za ich "čistotu" zodpovedajú používatelia, ktorí musia mať na svojich pracovných staniciach nainštalované aktuálne bezpečnostné programy, záplaty, antivírové, antispamové a anti-spywarové ochrany a zároveň tieto stanice nesmú obsahovať vírusy, trójske kone , červy, hackerské programy a ďalší škodlivý kód, ktorý môže ohroziť sieť.

Článok 15

Hlásenie bezpečnostných incidentov

1) Bezpečnostný incident je jedna z nechcených alebo neočakávaných udalostí, pri ktorých existuje vysoká pravdepodobnosť narušenia integrity, dostupnosti alebo dôvernosti informačných systémov mesta Malacky. Ide hlavne o:
   a) porušovanie zásad bezpečnostnej politiky informačných systémov mesta Malacky,
   b) získanie neoprávneného privilegovaného stavu alebo prístupových práv,
   c) odopretie služby (prístup na Internet, e-mail, vzdialený prístup),
   d) problémy s prihlásením do domény alebo do softvérovej aplikácie,
   e) výrazné zníženie výkonnosti počítača,
   f) nezmyselné hlásenia,
   g) opakované výstražné hlásenia o prítomnosti škodlivého kódu,
   h) zvýšený počet doručenej nevyžiadanej pošty – spamu,
   i) samovoľné spúšťanie niektorých aplikácií,
   j) porušenie stanov fyzickej a objektovej bezpečnosti,
   k) strata prideleného prostriedku výpočtovej techniky,
   l) neoprávnený zásah do výpočtovej techniky.
2) V prípade vzniku bezpečnostného incidentu je používateľ povinný nahlásiť túto skutočnosť správcovi siete, resp. technickému zamestnancovi MsP.

3) V prípade bezpečnostného incidentu s priamym dopadom na chod orgánu mesta alebo bezpečnostného incidentu s nepriamym, resp. dodatočným dopadom na chod mesta, je správca siete, resp. technický zamestnanec MsP, povinný informovať manažéra informačnej bezpečnosti, ktorý vykoná záznam o bezpečnostnom incidente (Príloha 7).
4) V prípade riešenia bezpečnostného incidentu je správca siete, resp. technický zamestnanec MsP povinný sa riadiť postupom uvedeným v článku Havarijný plán a plán kontinuity činností, resp. iným dokumentom zaoberajúcim sa riadením kontinuity činností, resp. havarijným plánovaním.

Článok 16

Spôsob, forma a periodicita výkonu kontrolných činností zameraných na dodržiavanie bezpečnosti informačného systému

1) Manažér informačnej bezpečnosti stanoví plán kontrol na dodržiavanie bezpečnostných smerníc.
2) O kontrole zameranej na dodržiavanie bezpečnosti informačného systému musí byť spísaný protokol, ktorý môže slúžiť ako podklad pre spracovanie dokumentu Analýza rizík ISVS.
3) So zmenami vykonanými po kontrole musia byť oboznámení kontrolovaní používatelia.
4) Kontrolu vykonáva 1 x ročne Manažér informačnej bezpečnosti v spolupráci so správcom siete, resp. technickým zamestnancom MsP.
5) Vykonáva sa kontrola nastavenia bezpečnostných parametrov počítačov a počítačovej siete. Pri vykonávaní kontroly bezpečnostných parametrov počítačov, zodpovední sú povinní skontrolovať funkčnosť a aktuálnosť antivírusového, prípadne antispamového resp. antispywaroveho programu a činnosť firewallu. Je potrebné kontrolovať používané služby (Napr. MSN Messenger v MS Windows XP) a taktiež, či je nastavená pravidelná aktualizácia bezpečnostných záplat operačného systému. Pri kontrole pracovnej stanice je potrebné zistiť, či sa nepoužíva nelicencovaný softvér, programy pre komunikáciu, prípadne softvér pre zdieľanie a sťahovanie súborov z rôznych voľných serverov (napr. DC++, Kazaa a pod.).
6) Vykonáva sa kontrola dodržiavania bezpečnosti v oblasti prístupových hesiel. Zodpovední sú povinní náhodne kontrolovať používanie silných hesiel do softvérových aplikácií. Ďalej

sú povinní kontrolovať prístupové heslo do BIOSu a stav blokovania bootovania z periférií pracovných staníc. Sú povinní kontrolovať používanie hesiel šetričov obrazovky a odhlasovanie sa zo systému aj pri krátkodobej neprítomnosti používateľa. V prípade nedodržiavania používania hesiel alebo silných hesiel z dôvodu neoboznámenia sa s informačnou bezpečnostnou politikou je potrebné zistiť príčinu tohto nedostatku a používateľa predbežne oboznámiť s bezpečnostnými opatreniami pri správe prístupových hesiel.

7) Vykonáva sa kontrola nastavenia prístupových práv. Zodpovední sú povinní náhodne kontrolovať či úroveň udeleného prístupu zodpovedá pracovnému účelu a či sú prístupové práva používateľov funkčné.
8) Vykonáva sa kontrola manipulácie a uloženia prenosných záznamových médií. Zodpovední sú povinní kontrolovať, či boli nepoužívané prenosné pamäťové médiá, likvidované bezpečne a spoľahlivo. Ďalej sú povinní kontrolovať uloženie prenosných pamäťových médií, ktoré majú byť uložené tak, aby k nim mali prístup iba oprávnené osoby a zabránilo sa ich zneužitiu.
9) Vykonáva sa kontrola zálohovania dát. Zodpovední sú povinní kontrolovať, či sú zálohy a archívy všetkých dát vykonávané pravidelne a kde sú ukladané. Zálohy musia byť označené a má byť kontrolovaná ich funkčnosť.
10) Nedostatky, ktoré boli zistené pri kontrole je potrebné neodkladne odstrániť.

Článok 17

Ochranné opatrenia v oblasti fyzickej a objektovej bezpečnosti

1) Prostriedky výpočtovej techniky musia byť fyzicky chránené pred neautorizovaným fyzickým prístupom. Musia byť umiestnené tak, aby vplyvom okolia nedošlo k neúmyselnému poškodeniu alebo k ich poruche.
2) Používateľ má zakázané otvárať kryty prostriedkov výpočtovej techniky, meniť ich hardvérovú konfiguráciu alebo akýmkoľvek iným spôsobom do nich fyzicky zasahovať.
3) Tlačové výstupy s „citlivými“ dátami sa zakazuje nechávať ležať na centrálnych tlačiarňach, kopírovacích strojoch alebo skeneroch.
4) Dokumenty v papierovej forme s „citlivými“ dátami nenechávať voľne položené na stoloch, aby nebol k údajom voľný prístup neoprávnenej osoby.

5) Kľúče od uzamykateľných skríň, miestností a trezorov, v ktorých sú uložené dokumenty v papierovej forme alebo pamäťové médiá, resp. elektronický kľúč s „citlivými“ dátami, majú v stálej držbe iba oprávnené osoby, alebo sú uložené v zalepenej obálke v uzamykateľnej skrini u prednostu mestského úradu alebo náčelník mestskej polície.
6) Dokumenty v papierovej forme obsahujúce osobné údaje je potrebné ukladať do uzamykateľných skríň, miestností alebo trezora.
7) Počas dlhodobej neprítomnosti oprávnenej osoby sa zakazuje nechávať kľúče od skríň, miestností, resp. trezorov v zámkovom systéme.
8) Mimo pracovnej doby je potrebné vstup do objektu a ostatné otvárateľné vstupné otvory (napr. okná, dvere) uzatvárať/uzamykať.
9) Priestor prístupný verejnosti možno monitorovať pomocou videozáznamu len na účely verejného poriadku a bezpečnosti a odhaľovania kriminality. Monitorovaný priestor musí byť zreteľne označený ako monitorovaný.
10) Vyhotovený záznam možno využiť len na účely trestného konania alebo konania o priestupkoch.
11) Ak vyhotovený záznam kamerovým sledovacím systémom priestoru prístupného verejnosti nie je využitý na účely trestného konania alebo konania o priestupkoch, musí byť zlikvidovaný najneskôr v lehote siedmich dní odo dňa nasledujúceho po dni, v ktorom bol záznam vyhotovený, ak osobitný zákon neustanovuje inak.
12) Za správu záznamov a bezpečnosť kamerového systému MsÚ zodpovedá správca budovy.
13) Za správu záznamov a bezpečnosť Mestského kamerového systému zodpovedá technický zamestnanec MsP.
14) Do priestorov serverovne má prístup výhradne správca siete. Iné osoby (napr. audítor, kontrolór, sprostredkovateľ) majú prístup do priestorov serverovne iba za sprievodu oprávnenej osoby, ktorá rozhodne o oprávnenosti požiadavky o vstup.
15) Priestory serverovní musia byť klimatizované a chránené pred priamym slnečným žiarením.
16) Kritické prostriedky výpočtovej techniky a sieťové prvky, ktorých výpadok môže mať za následok stratu dostupnosti, musia byť chránené pred výpadkami elektrickej energie a inými elektrickými anomáliami.

Článok 18

Údržba zariadení a likvidácia záznamových médií

1) Prostriedky výpočtovej techniky musia byť správne udržiavané, aby sa zaistila ich nepretržitá dostupnosť a integrita.
2) Prostriedky výpočtovej techniky musia byť udržiavané podľa dodávateľom odporúčaných servisných intervalov a špecifikácií. Musia sa vykonávať záznamy o všetkých poruchách a o každej opravárenskej údržbe. Záznam o poruchách a údržbe vykoná správca siete, resp. technický zamestnanec MsP.
3) Používateľom sa zakazuje vykonávať opravy a servis technických prostriedkov. Opravy a servis môže vykonávať, resp. zabezpečovať len správca siete, resp. technický zamestnanec MsP.
4) Do prostriedkov výpočtovej techniky, ktoré sú v záručnej lehote, sa nesmie zasahovať vôbec, pokiaľ nebolo s dodávateľom výpočtovej techniky dohodnuté inak.
5) V prípade vzniku požiadavky na údržbu prostriedkov výpočtovej techniky je používateľ povinný požiadať e-mailom alebo telefonicky správcu siete, resp. technického zamestnanca MsP.
6) Čistenie povrchu prostriedkov výpočtovej techniky od prachu je v kompetencii používateľa. Vnútorné čistenie zariadení môže vykonávať len správca siete, resp. technický zamestnanec MsP - minimálne 1 x za rok.
7) Používateľ je povinný vykonávať základnú údržbu pridelenej výpočtovej techniky - vyčistenie povrchu pracovnej stanice, obrazovky monitora a klávesnice (na základe školenia správcom siete, resp. technickým zamestnancom MsP a po dodaní materiálno-technického zabezpečenia).
8) Používateľ nesmie znižovať životnosť výpočtovej techniky hrubým zaobchádzaním (fyzickou silou) a jej znečisťovaním (napr. jedlom, nápojmi).
9) Používateľ je zodpovedný za likvidáciu už nepotrebných alebo poškodených pamäťových médií, resp. je zodpovedný za ich odovzdanie správcovi siete alebo technickému zamestnancovi MsP, ktorý ich zlikviduje.
10) Likvidácia záznamových médií musí prebiehať tak, aby sa uložené informácie stali nečitateľnými a nemohli byť zneužité inou neoprávnenou osobou (formátovaním pomocou skartovačky dát alebo fyzickým znehodnotením).

Článok 19

Bezpečnosť technických prostriedkov mimo priestorov MsÚ a MsP

1) Použitie akýchkoľvek mobilných prostriedkov výpočtovej techniky mimo priestorov MsÚ a MsP musí byť povolené správcom siete, resp. technickým zamestnancom MsP. Mobilné prostriedky zahŕňajú všetky formy notebookov, organizátorov a externých záznamových médií (napr. USB, externý HDD).
2) Dátové úložiská mobilných prostriedkov výpočtovej techniky (napr. notebook, USB kľúč) používaných mimo priestorov MsÚ a MsP musia byť šifrované.
3) Poskytovaná bezpečnosť musí byť rovnaká, ako pre prostriedky výpočtovej techniky v rámci pracovísk mesta používané na ten istý účel, berúc do úvahy riziká práce v externom prostredí.
4) Mobilné technické prostriedky nesmú byť ponechané nestrážené na verejných miestach a musia byť nosené ako príručná batožina.
5) Používateľ musí dodržiavať inštrukcie výrobcu pre používanie výpočtovej techniky (napr. ohľadne vystavenia silným elektromagnetickým poliam, prevádzkové podmienky ako teplota, vlhkosť prostredia, a pod.).
6) Počas služobných ciest je potrebné mať prenosné prostriedky stále pod kontrolou, nesmú sa nechávať v otvorenom aute alebo podávať ako batožina v lietadle.

Článok 20

Ochranné opatrenia v oblasti dodávky služieb tretími stranami

1) Prístup do počítačovej siete môže byť umožnený aj zamestnancom zmluvného partnera tretej strany, avšak iba ak si to vyžaduje ich činnosť vo vzťahu k mestu.
2) Tretím stranám sa povoľuje vzdialený prístup do počítačovej siete, resp. softvérovej aplikácie len v prípade, pokiaľ sú jeho podmienky jednoznačne definované zmluvným vzťahom, resp. špecifickým dokumentom (napr. smernica).
3) Všetci sprostredkovatelia (dodávatelia) musia rešpektovať a dodržiavať politiku informačnej bezpečnosti mesta a dodržiavať diskrétnosť ako jednu z definovaných obchodných podmienok.

4) Servisný personál sprostredkovateľa musí vykonávať všetky údržbové a servisné aktivity pod dohľadom správcu siete, resp. technickým zamestnancom MsP, a zároveň musí podpísať prehlásenie o dodržiavaní informačnej bezpečnosti mesta Malacky (Príloha 2), ktorého kópiu eviduje manažér informačnej bezpečnosti.
5) Zmluva medzi sprostredkovateľom informačno-komunikačných technológií, resp. softvérových aplikácií a mestom by mala podľa potreby a možností zahŕňať nasledujúce bezpečnostné požiadavky:
   a) záväzok, že ponúkaný produkt je plne v súlade s požiadavkami na štandardy pre informačné systémy verejnej správy podľa platného výnosu daného ministerstva (MF SR),
   b) záväzok dodávateľa dodržiavať bezpečnostnú politiku informačnej bezpečnosti mesta,
   c) záväzok poučiť svojich zamestnancov o ich povinnostiach a kompetenciách vo vzťahu k mestu,
   d) meno kontaktnej osoby a jeho zástupcu sprostredkovateľa, kontaktné údaje minimálne v rozsahu: adresa, tel. číslo, e-mail, fax,
   e) meno zodpovednej osoby za mesto, jej kontaktné údaje, a to minimálne v rozsahu: adresa, tel. číslo, e-mail, fax (budúci správca IS),
   f) záručný a pozáručný servis (update softvérových aplikácií, update bezpečnostných záplat, časové lehoty dodávky),
   g) technické a bezpečnostné požiadavky pre vzdialený prístup sprostredkovateľa (štandardne sa neodporúča - je prípadne potrebné priamo uviesť že sa zakazuje, resp. povoľuje),
   h) v prípade vývoja novej softvérovej aplikácie, stanoviť podmienky jej testovania pred zavedením do prevádzky (preberací protokol by mal obsahovať správu z výsledkov testovania), stanoviť čas testovania,
   i) v prípade vývoja novej softvérovej aplikácie, uviesť klauzulu o neimplikovaní programového kódu („skryté“ funkcie), ktorý môže byť samostatnou aplikáciou alebo môže byť súčasťou iného programu, a ktorý umožňuje skrytý neoprávnený prístup do aplikácie,
   j) v prípade vývoja novej softvérovej aplikácie vyžadovať podrobnú analýzu potrebných a nepotrebných funkcií, ktoré je vhodné požadovať blokovať,

k) v prípade vývoja novej softvérovej aplikácie žiadať možnosti logovania prihlásení do systému a obsahových zmien používateľmi,

l) v prípade vývoja novej softvérovej aplikácie stanoviť minimálnu hierarchiu rolí a prístupov,

m) hardvérové a softvérové požiadavky na prevádzku,

n) v prípade outsourcingu služieb poskytovania dátového úložiska je potrebné uviesť: forma a periodicita zálohy a archivácie ukladaných údajov, miesto ukladania záznamových médií (trezor, uzamykateľná ohňovzdorná skriňa),

o) v prípade outsourcingu služieb vytvárania a rušenia prístupových práv do softvérovej aplikácie je potrebné uviesť: postup vytvárania/rušenia práv, požiadavky na štruktúru a zmenu prístupového hesla,

p) spôsob dodávky a aktualizácie administrátorskej, používateľskej a prevádzkovej dokumentácie (architektúra, konfigurácie a väzby),

q) možnosti odstúpenia od zmluvy v prípade nedodržania bezpečnostných požiadaviek.

6) Správca siete resp. technický zamestnanec MsP je zodpovedný aj za kontrolu splnenia bezpečnostných požiadaviek uvedených v zmluve. O príprave zmluvy so sprostredkovateľom musí byť informovaný manažér informačnej bezpečnosti, ktorý musí mať kópiu finálnej verzie predmetnej zmluvy alebo aspoň jej častí týkajúcich sa bezpečnostných požiadaviek na sprostredkovateľa.

Článok 21

Havarijný plán a plán kontinuity činností

Popis havárie	Postupy na zabezpečenie stavu obnovy
Havárie IS spôsobené technickou chybou niektorého komponentu servera	Pri výpadku servera presmerovať prevádzku na záložný server. Aktualizovať dáta na záložnom serveri z poslednej zálohy hlavného servera. Presmerovať aplikácie a používateľov na záložný server. Odstrániť poruchu na hlavnom serveri. Po odstránení poruchy presmerovať prevádzku na hlavný server. Ukončiť prácu na hlavnom serveri. Previesť zálohu dát. Aktualizovať dáta na hlavnom serveri z poslednej zálohy na záložnom serveri. Presmerovať aplikácie a používateľov na hlavný server. Prípadne pokiaľ nie je k dispozícii záložný server, musia byť používatelia informovaní o predpokladanej dobe odstávky.
Porucha napájania, strata dodávky elektrickej energie	V čase výpadku sa musia automaticky aktivovať záložné zdroje a po stanovenom čase maximálne 1 hodiny sa musí previesť automatický shutdown všetkých serverov. Po nábehu elektrickej energie je potrebné zabezpečiť spustenie serverov a prekontrolovať ich funkčnosť v čo najkratšom čase.
Porucha aktívnych prvkov siete	Vymeniť chybnú časť.
Porucha v pasívnej časti siete	Opraviť, prípadne vymeniť chybnú časť.

Porucha servera spôsobená vírusom, neautorizovaným programom	Odpojiť každého používateľa. Spustiť antivírový program s aktuálnou databázou známych vírusov. Detekovať spôsob narušenia. Odstrániť príčinu poruchy. Opraviť narušenú funkčnosť. Opätovne skontrolovať systém antivírovým programom. Prekontrolovať všetky pracovné stanice fyzicky pripojené aj nepripojené do LAN. Nájsť zdroj infiltrácie a zabezpečiť jeho eliminovanie. Znovu spustenie systému a pripojenie používateľov.
Porucha prostriedkov demilitarizovanej zóny	Odpojiť LAN od prostriedkov demilitarizovanej zóny. Vyhľadať príčinu nefunkčnosti. Odstrániť príčinu výmenou častí, inštalovaním aktualizácií, výmenou celku. Preveriť prostriedky firewallu, prekladu adries a proxy. Po otestovaní funkčnosti pripojiť LAN.
Havária databáz	Zo zálohy inštalovať databázu na hlavný server.
Havária aplikácie	Nainštalovať novšiu verziu aplikácie. Konzultovať chyby s dodávateľom.
Porucha mail servera	Vymeniť chybnú časť. Aktualizovať softvér V prípade výmeny disku previesť inštaláciu zo zálohy.

Porucha pracovných staníc	Technická chyba: Zabezpečiť opravu chybnej časti. Softvérová chyba: Identifikovať príčinu. Obnoviť súbory zo zálohy, alebo preinštalovať operačný systém. Aktualizovať antivírusovú ochranu.

Článok 22

Školenie

1) Každý zamestnanec využívajúci výpočtovú techniku je povinný po nástupe do zamestnania absolvovať školenie o zásadách riadenia informačnej bezpečnosti vyplývajúcej z bezpečnostnej politiky a o spôsobe používania softvérových aplikácií. A zároveň je povinný podpísať vyhlásenie o dodržiavaní vyššie uvedených zásad pri nástupe do zamestnania do 1 mesiaca od nástupu – Prehlásenie oprávnenej osoby o dodržiavaní informačnej bezpečnosti mesta Malacky (príloha 6).
2) Školenie vykonáva Manažér informačnej bezpečnosti.

Článok 23

Spoločné ustanovenia

Porušenie ustanovení Bezpečnostnej smernice pre prácu s informačnými systémami mesta Malacky možno v opodstatnených prípadoch kvalifikovať ako závažné porušenie pracovnej disciplíny (s výnimkou ustanovení, v ktorých je explicitne určená závažnosť porušenia). O ďalšom postupe sa rozhodne na základe platného pracovného poriadku.

Účinnosť od .....

V Malackách dňa

Príloha č.1 Pridelenie, zmena konfigurácie, odovzdanie prostriedkov výpočtovej techniky, inštalácia softvérových aplikácií a pridelenie, zrušenie prístupových práv

Vec: Pridelenie, zmena konfigurácie, odovzdanie prostriedku výpočtovej techniky, inštalácia softvérových aplikácií a pridelenie, zrušenie prístupových práv

Zamestnanec:			
Titul:	Priezvisko:	Meno:	
Zamestnaný od:	Kód oddelenia:	Kancelária:	
Osobné číslo:	Rodné číslo (pre CG ISS):	Tel. klapka:	

Nadriadený:			
Titul:	Priezvisko:	Meno:	Funkcia:

Druh požiadavky	☐ **Zriadenie**	☐ **Zmena**	☐ **Zrušenie**

Technické prostriedky:	
Stručný popis :	

Informačný systém/softvérová aplikácia	Zriadenie	Odobratie	Dátum od:

V prípade odobratia prostriedkov výpočtovej techniky, resp. odinštalovania softvérových aplikácia, resp. zrušenia používateľských účtov nadriadený zabezpečil pracovné údaje a dáta, ktoré sa vykonaním daného úkonu môžu zneprístupniť alebo stratiť.

Podpis nadriadeného: dňa:

Podpis zamestnanca: dňa:

Príloha č.2 Prehlásenie zamestnanca dodávateľskej spoločnosti o dodržiavaní informačnej bezpečnosti mesta Malacky

Mesto Malacky, Radlinského 2751/1, 901 01 Malacky

Poučenie o dodržiavaní informačnej bezpečnosti mesta Malacky

(Meno, priezvisko, ČOP fyzickej osoby)

(Názov spoločnosti v OR, IČO)

bol/a poučený/á o právach a povinnostiach vo vzťahu ochrane informačných systémov Mesta Malacky

- Pracovník dodávateľskej spoločnosti je povinný dodržiavať zásady Bezpečnostnej politiky informačných systémov mesta Malacky a zásady vyplývajúce z Bezpečnostnej smernice pre prácu s informačnými systémami mesta Malacky.
- V prípade zistenia nechcených alebo neočakávaných udalostí (bezpečnostných incidentov), pri ktorých existuje vysoká pravdepodobnosť narušenia integrity, dostupnosti alebo dôvernosti informačných systémov mesta Malacky, je povinný hlásiť túto skutočnosť osoba, ktorá je uvedená v zmluve ako kontaktná alebo zodpovedná osoba.
- Je povinný zachovávať mlčanlivosť o skutočnostiach, o ktorých sa dozvedel pri výkone zamestnania na orgánoch mesta Malacky, a ktoré v záujme mesta Malacky nemožno oznamovať iným osobám (§81 písm. e zákona č. 311/2001 Z.z. Zákonník práce v znení neskorších predpisov a §18 ods. 2 zákona č.428/2002 Z.z.).
- Povinnosť mlčanlivosti pracovníka dodávateľskej spoločnosti trvá aj po zániku zmluvného vzťahu dodávateľa a mesta Malacky.
- Povinnosť mlčanlivosti neplatí, ak je to nevyhnutné na plnenie úloh orgánov činných v trestnom konaní a vo vzťahu k Úradu pre ochranu osobných údajov pri plnení jeho úloh.
- Pracovník dodávateľskej spoločnosti je zodpovedný za škodu, ktorú spôsobil zavineným porušovaním povinnosti pri plnení pracovných úloh alebo v priamej súvislosti s ním (§ 179 až 185 Zákonníka práce).

Poučeniu som porozumel/a v celom rozsahu a svojim podpisom to potvrdzujem.

V Malackách dňa .....

....

poučená osoba konateľ dodávateľskej spoločnosti

Príloha č.3

PERIODICKÁ KONTROLA BEZPEČNOSTI ISVS

♦

KONTROLA NASTAVENIA BEZPEČNOSTNÝCH PARAMETROV PRACOVNÝCH STANÍC A POČÍTAČOVEJ SIETE

♦

Obsah vykonávanej kontroly: funkčnosť a aktuálnosť antivírusového, antispamového resp. antispywaroveho programu a činnosť personálneho firewallu. Kontrola aktualizácie bezpečnostných záplat operačných systémov pracovných staníc. Kontrola používania nelicencovaného softvéru.

Názov pracovnej stanice v sieti	Meno a pracovná pozícia používateľa	Zistený stav	Odporúčané opatrenia	Dátum realizácie odporúčaných doplňujúcich opatrení

Dátum vykonanej kontroly:
Kontrolu vykonali: **Manažér informačnej bezpečnosti:** **Správca siete:**

Príloha č.4

PERIODICKÁ KONTROLA BEZPEČNOSTI ISVS

♦

KONTROLA DODRŽIAVANIA BEZPEČNOSTI V OBLASTI PRÍSTUPOVÝCH HESIEL A PRÁV

♦

Obsah vykonávanej kontroly: používanie silných hesiel do informačných a operačných systémov, prístupové heslá do BIOSov a stav blokovania bootovania systému z periférií pracovných staníc. Používanie hesiel šetričov obrazovky a odhlasovanie sa zo systému aj pri krátkodobej neprítomnosti používateľa. Kontrola či úroveň udeleného prístupu zodpovedá pracovnému účelu a či sú prístupové práva používateľov funkčné.

Názov pracovnej stanice v sieti	Meno a pracovná pozícia používateľa	Zistení stav	Odporúčané opatrenia	Dátum realizácie odporúčaných doplňujúcich opatrení

Dátum vykonanej kontroly:
Kontrolu vykonali: **Manažér informačnej bezpečnosti:** **Správca siete:**

Príloha č. 5

PERIODICKÁ KONTROLA BEZPEČNOSTI ISVS

♦

KONTROLA MANIPULÁCIE A ULOŽENIA PRENOSNÝCH PAMÄŤOVÝCH MÉDIÍ A KONTROLA ZÁLOHOVANIA DÁT

♦

Obsah vykonávanej kontroly: či boli používané prenosné pamäťové médiá likvidované bezpečne a spoľahlivo (spálením alebo inou technológiou). Kontrola uloženia prenosných pamäťových médií, tak aby k nim mali prístup iba oprávnené osoby a zabránilo sa ich zneužitiu. Kontrola či sú zálohy všetkých dát vykonávané pravidelne a kde sú ukladané.

Názov pracovnej stanice v sieti	Meno a pracovná pozícia používateľa	Zistení stav	Odporúčané opatrenia	Dátum realizácie odporúčaných doplňujúcich opatrení

Dátum vykonanej kontroly:

Kontrolu vykonali **Manažér informačnej bezpečnosti:** **Správca siete:**

Príloha č.6 Prehlásenie oprávnenej osoby o dodržiavaní informačnej bezpečnosti mesta Malacky

Mesto Malacky, Radlinského 2751/1, 901 01 Malacky

Poučenie o dodržiavaní informačnej bezpečnosti mesta Malacky

(Meno, priezvisko, ČOP fyzickej osoby)

bol/a poučený/á o právach a povinnostiach vo vzťahu ochrane informačných systémov Mesta Malacky

- Oprávnená osoba je povinná dodržiavať zásady Bezpečnostnej politiky informačných systémov mesta Malacky a s ňou súvisiacej bezpečnostnej dokumentácie (hlavne Bezpečnostná smernica pre prácu s informačnými systémami mesta Malacky).
- Oprávnená osoba je povinná zachovávať mlčanlivosť. Povinnosť mlčanlivosti o skutočnostiach, o ktorých sa dozvedela pri výkone zamestnania, a ktoré v záujme zamestnávateľa nemožno oznamovať iným osobám vyplýva z §81 písm. e zákona č. 311/2001 Z.z. Zákonník práce v znení neskorších predpisov a §18 ods. 2 zákona č.428/2002 Z.z.
- Povinnosť mlčanlivosti trvá aj po zániku funkcie oprávnenej osoby alebo po skončení jej pracovného pomeru, štátnozamestnaneckého pomeru alebo obdobného pracovného vzťahu.
- Povinnosť mlčanlivosti neplatí, ak je to nevyhnutné na plnenie úloh orgánov činných v trestnom konaní a vo vzťahu k Úradu pre ochranu osobných údajov pri plnení jeho úloh.
- Porušenie povinnosti zachovávať mlčanlivosť je sankcionovateľné podľa §-u 49 zákona 428/2002 Z.z.., ako aj podľa §-u 178 Trestného zákona (Neoprávnené nakladanie s osobnými údajmi) a §-u 257 a/ Trestného zákona (Poškodenie a zneužitie záznamu na nosiči informácií).
- Na základe Zákonníka práce oprávnená osoba je povinná hospodáriť riadne s prostriedkami, ktoré jej zveril zamestnávateľ a chrániť jeho majetok pred poškodením, stratou, zničením a zneužitím.
- Oprávnená osoba bola poučená o spôsobe využívania všetkých informačných systémov, ktoré bude využívať v rámci svojej pracovnej náplne.

Poučeniu som porozumel/a v celom rozsahu a svojim podpisom to potvrdzujem.

V Malackách dňa .....

.....	.....
poučená osoba	manažér informačnej bezpečnosti

Príloha č.7 Záznam o vzniku bezpečnostného incidentu

ZÁZNAM O VZNIKU BEZPEČNOSTNÉHO INCIDENTU

Bezpečnostný incident bol spôsobený nasledujúcim zdrojom rizika:

Čas, spôsob reakcie a kto ju vykonal:

Následok bezpečnostného incidentu:

Dátum: Spracoval (meno, priezvisko, pozícia):

Navrhované opatrenia na elimináciu pravdepodobnosti vzniku tohto bezpečnostného incidentu v budúcnosti:

Dátum: Navrhol (meno, priezvisko, pozícia): .....

Časový plán na zavedenie navrhovaných opatrení:

Dátum: Navrhol (meno, priezvisko, pozícia): .....
Dátum: Schválil (meno, priezvisko, pozícia): .....
Za zavedenie opatrení je zodpovedný (meno, priezvisko, pozícia): .....

Záznam o preskúmaní, či implementované opatrenia spĺňajú očakávania:

Dátum: Vykonal (meno, priezvisko, pozícia): .....

Príloha č.8 Záznam o vykonaní testu obnovy IS z prevádzkovej zálohy

Dátum obnovy: Test vykonal (meno, priezvisko, pozícia): .....

Dátum zálohy: Zálohu vykonal (meno, priezvisko, pozícia): .....

Typ média:

Miesto uloženia média:

Názov softvérovej aplikácie/informačného systému:

Rozsah obnovovaných dát:

Popis spôsobu obnovy:

Vzniknuté problémy pri obnove dát:

Navrhované opatrenia:

Dátum: Navrhol (meno, priezvisko, pozícia): .....

Záznam o preskúmaní, či implementované opatrenia spĺňajú očakávania:

Dátum: Vykonal(meno, priezvisko, pozícia): .....