INTERNÁ SMERNICA č. 97

IS - 97

Smernica pre používanie aktív so zreteľom na ochranu osobných údajov pre zamestnancov

Obsah

1. Účel smernice

1) Smernica upravuje práva a povinnosti všetkých zamestnancov Mesto Prievidza, Námestie slobody 14, 971 01 Prievidza (ďalej ako „Prevádzkovateľ“) v oblasti používania informačno-komunikačných prostriedkov, ktoré Prevádzkovateľ vlastní.

2. Základné pojmy

1) **Aktíva informačných technológií (IT aktíva)** – všetky technické a softvérové prostriedky, ktoré slúžia na ukladanie, prenos a spracovanie informácií v digitálnej podobe, bez ohľadu na účel tohto spracovania.
2) **Autentizácia** – je nástroj, pomocou ktorého sa zabezpečuje prístup určených osôb k IT aktívu a zároveň zamedzuje prístup ostatným osobám k IT aktívu.
3) **Bezpečnostný incident** – situácia, stav, kedy môže dôjsť, dochádza alebo došlo k narušeniu existujúcej ochrany osobných údajov.
4) **Bezpečné vymazanie údajov** – vymazanie údajov na nosiči údajov tak, aby nemohlo dôjsť k ich opätovnému obnoveniu (napr. za použitia špeciálneho softvéru, viacnásobným prepisom disku a pod.).
5) **Dotknutá osoba** – je každá fyzická osoba, ktorej sa osobné údaje spracovávajú.
6) **Elektronická schránka** – štátom zriadené úložisko elektronických podaní prevádzkované Národnou agentúrou pre sieťové elektronické služby (NASES), slúžiace na prijímanie elektronických podaní (žiadostí) od občanov, podnikateľov a iných inštitúcií a komunikáciu štátu a štátnych inštitúcií s organizáciami a podnikateľmi**.**
7) **Hrozby** – vplyvy okolia, iných osôb, zariadení a prostriedkov, ktoré úmyselne alebo neúmyselne vplývajú na aktíva organizácie tak, že ich organizácia nemôže využívať, alebo inak ohrozujú oprávnené záujmy organizácie.
8) **Kryptovaná komunikácia** – dátová komunikácia zabezpečená kódom, kódovaný prenos dát s použitím kryptografických opatrení, hesiel a bezpečnostných postupov.
9) **Likvidácia osobných údajov** – zrušenie osobných údajov rozložením, vymazaním alebo fyzickým zničením hmotných nosičov tak, aby sa z nich osobné údaje nedali reprodukovať.
10) **Messaging –** je služba umožňujúca svojím používateľom sledovať, ktorí iní používatelia sú práve pripojení a podľa potreby im posielať správy, preposielať súbory medzi používateľmi a inak navzájom komunikovať.
11) **Oprávnená osoba** – je každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovnoprávneho vzťahu, služobného pomeru, členského vzťahu, na základe poverenia, zvolenia alebo vymenovania, alebo v rámci výkonu verejnej funkcie a ktorá spracúva osobné údaje v rozsahu a spôsobom určeným v poučení oprávnenej osoby o právach, povinnostiach a o zodpovednosti za ich porušenie (ďalej len „poučenie“). Oprávnená osoba zodpovedá za spracúvanie a náležitú ochranu osobných údajov v rozsahu svojej pracovnej činnosti.
12) **Osobné údaje** – údaje, týkajúce sa určenej alebo určiteľnej fyzickej osoby, pričom takou osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe všeobecne

použiteľného identifikátora, alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu, alebo sociálnu identitu.

13) **Poskytovanie osobných údajov** – odovzdávanie osobných údajov tretej strane, ktorá ich ďalej spracúva.
14) **Prevádzkovateľ** – subjekt, ktorý spracúva osobné údaje vo vlastnom mene, v tejto smernici je to Mesto Prievidza, Námestie slobody 14, 971 01 Prievidza .
15) **Realizujúca sa hrozba** – stav, kedy je aktívum hrozbou poškodzované alebo ničené, čo má za následok znefunkčnenie aktíva, alebo ohrozenie záujmov Prevádzkovateľa.
16) **Spracúvanie osobných údajov** – vykonávanie operácií alebo súboru operácií s osobnými údajmi, najmä ich získavanie, zhromažďovanie, šírenie, zaznamenávanie, usporadúvanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, premiestňovanie, využívanie, uchovávanie, blokovanie, likvidácia, ich cezhraničný prenos, poskytovanie, sprístupňovanie, alebo zverejňovanie.
17) **Sprístupňovanie osobných údajov** – oznámenie osobných údajov alebo umožnenie prístupu k nim príjemcovi, ktorý ich ďalej nespracúva.
18) **Sprostredkovateľ** – fyzická alebo právnická osoba poverená Prevádzkovateľom na základe písomnej zmluvy spracúvaním osobných údajov.
19) **Súhlas dotknutej osoby** – akýkoľvek slobodne daný súhlas so spracovaním osobných údajov, ktorý sa dá hodnoverne preukázať.
20) **Úrad** – v tomto dokumente je to Úrad na ochranu osobných údajov, ktorý je orgánom štátnej správy s celoslovenskou pôsobnosťou so sídlom v Bratislave, vykonávajúci nezávislý dozor nad ochranou osobných údajov a podieľajúci sa na ochrane základných práv a slobôd fyzických osôb pri spracúvaní ich osobných údajov.
21) **USB zariadenie** – akékoľvek zariadenie pripojiteľné k USB rozhraniu a schopné prenosu dát cez toto rozhranie.
22) **Všeobecne použiteľný identifikátor** – trvalý identifikačný osobný údaj dotknutej osoby, ktorý zabezpečuje jej jednoznačnosť v informačných systémoch (zvyčajne rodné číslo).
23) **Zákon** – zákon č. 18/2018 Z. z. o ochrane osobných údajov.
24) **Zodpovedná osoba** – osoba poverená výkonom dohľadu nad ochranou osobných údajov.
25) **Zverejňovanie osobných údajov** – publikovanie, uverejnenie alebo vystavenie osobných údajov na verejnosti prostredníctvom masovokomunikačných prostriedkov, verejne prístupných počítačových sietí, verejným vykonaním alebo vystavením diela, verejným vyhlásením, uvedením vo verejnom zozname, v registri alebo v operáte, ich umiestnením na úradnej tabuli alebo na inom verejne prístupnom mieste.

3. Autentizácia

1) Heslá pre prístup k IT aktívam musia maž dĺžku minimálne 8 znakov a obsahovať aspoň jeden neabecedný znak a ich expiračná doba nesmie byť dlhšia ako 12 mesiacov. Zamestnanec nesmie ako heslo použiť takú kombináciu znakov, ktorú by bolo možné priradiť k jeho osobe, akými sú napríklad meno zamestnanca a jeho rodinných príslušníkov napísané spredu či odzadu, telefónne číslo domov alebo na pracovisko a podobne.

2) Zamestnancom sa zakazuje zverejňovať alebo inej osobe vyzradiť svoje neverejné autentizačné údaje (heslá). Taktiež sa im zakazuje držanie záznamu hesiel (napr. na papieri, v softvérovom súbore, na prenosnom zariadení a pod.), ak takýto záznam nemôže byť bezpečne uložený a ak nebola metóda ich uchovania schválená. V prípade nedostupnosti zamestnanca môže k jeho údajom pristúpiť jeho priamy nadriadený v súčinnosti so správcom IT aktíva.
3) Zamestnanec je povinný chrániť pridelený autentizačný prostriedok (SmartCard alebo obdobný prostriedok) pred odcudzením a zničením a nesmie ho prenechať inej osobe. Ak zamestnanec autentizačný prostriedok už viac nepotrebuje, vráti ho správcovi IT aktíva, ktorý mu ho vydal.
4) Nedodržanie zásad používania hesla a autentizácie zamestnancom sa považuje za bezpečnostný incident.

4. Fyzická bezpečnosť

1) Každý zamestnanec je zodpovedný za fyzickú bezpečnosť svojho pracoviska a zverených pracovných prostriedkov. Pri odchode z pracoviska je povinný uzamknúť pracovisko, uzavrieť okná a prekontrolovať zariadenia, či nemôžu spôsobiť požiar alebo inú haváriu. Ak zamestnanec nemôže túto povinnosť splniť, ihneď to oznámi svojmu nadriadenému.
2) Vstup do všetkých objektov Prevádzkovateľa prostredníctvom osobitných kľúčov a ďalších zabezpečovacích prvkov majú určení vedúci zamestnanci, upratovačky a zamestnanci, ktorých schválilo vedenie Prevádzkovateľa.
3) Evidenciu kľúčov, prístup a manipuláciu s nimi vedie poverený zamestnanec Prevádzkovateľa. Náhradné kľúče sa uchovávajú v uzamknutej skrinke. Prípadnú stratu kľúčov sú zamestnanci povinní ihneď oznámiť zamestnancovi, ktorý zodpovedá za ich evidenciu. Náhradné kľúče sa vydávajú len po zaevidovaní straty a po jej objasnení, o čom sa spíše zápis. Získavať kľúče od kancelárií, ktoré nie sú pracoviskom zamestnanca, je zakázané. Požičiavať kľúče od kancelárií v rámci príslušného oddelenia možno len so súhlasom vedúceho oddelenia. Oprávnené osoby, ktoré môžu vstupovať do všetkých alebo dopredu určených priestorov prostredníctvom zapožičaných kľúčov, sú vedené v evidencii kľúčov s určením priestorov, do ktorých majú oprávnený vstup.

5. Pracovné stanice

1) Zamestnanec je povinný používať zverené pracovné stanice len na pracovné účely. Porušenie tohto ustanovenia sa považuje za bezpečnostný incident.
2) Z pridelenej pracovnej stanice zamestnanec pristupuje iba k tým informačným systémom a sieťovým službám, ku ktorým má právo a povinnosť pristupovať na základe jeho pracovnej zmluvy a náplne.
3) Zamestnancom sa neodporúča využiť funkcionalitu na automatické zapamätanie hesla, najmä ak ide o heslo k zvlášť dôležitým informačným systémom.
4) Zamestnanec nesmie používať pracovnú stanicu alebo iné prostriedky a nástroje k pokusom o získanie neautorizovaného prístupu do zabezpečených systémov v rámci LAN a Internetu.

5) Zamestnanec môže na pracovných staniciach používať výlučne len programové vybavenie nainštalované správcom aktíva počítačov, resp. nainštalované s jeho preukázateľným súhlasom. Zamestnanec nemôže na pracovnej stanici meniť žiadne programové vybavenie, a tiež nemôže meniť konfiguráciu programového vybavenia.
6) Zamestnanec nemôže vytvárať a distribuovať kópie programového vybavenia inštalovaného na pracovnej stanici.
7) Zamestnanec je pred opustením pracoviska povinný ukončiť prácu s aplikačným programovým vybavením, odhlásiť sa zo siete a operačného systému a dohliadnuť na vypnutie pracovnej stanice.
8) Pri krátkodobej neprítomnosti môže zamestnanec nahradiť odhlásenie sa zo systému a vypnutie pracovnej stanice spustením šetriča obrazovky s heslom, resp. uzamknutím obrazovky.
9) Je zakázané pripájať vlastné zariadenia (napr. notebooky, tablety, tlačiarne a pod.) do siete Prevádzkovateľa, a taktiež povoliť pripojenie cudzej osoby do siete Prevádzkovateľa bez vedomia správcu IT aktíva. Taktiež sa zamestnancom zakazuje používať nekryptované USB zariadenia na prenos osobných údajov. Prenos osobných údajov mimo budovu Prevádzkovateľa alebo ďalšie priestory Prevádzkovateľa prostredníctvom externých pamäťových médií je možný len v zašifrovanej podobe alebo médiami kryptovanými silným heslom. Porušenie tohto bodu sa považuje za bezpečnostný incident.

6. Notebooky a práca s osobnými a citlivými údajmi

1) Zamestnanec je povinný mať notebook zabezpečený heslom. Pokiaľ má na notebooku osobné alebo citlivé údaje, je povinný tieto údaje uchovávať v zašifrovanej časti disku a na notebooku prevádzkovať aktualizovaný antivírusový nástroj.
2) Zamestnancom sa neodporúča využiť funkcionalitu na automatické zapamätanie hesla, najmä ak ide o heslo k zvlášť dôležitým informačným systémom a emailom.
3) Zamestnancom sa zakazuje používať neznáme nezabezpečené WiFi siete na pripojenie do Internetu.
4) Pri pripojení do lokálnej počítačovej siete je zamestnanec povinný zabezpečiť zálohovanie údajov uložených na zariadeniach.
5) Zamestnanec je zodpovedný za fyzickú ochranu notebooku pred krádežou, stratou alebo poškodením.
6) Krádež alebo strata notebooku sa považuje za bezpečnostný incident.

7. Mobilné zariadenia – smartfóny a tablety a práca s osobnými a citlivými údajmi

1) Zamestnanec je zodpovedný za fyzickú ochranu zvereného zariadenia pred krádežou, stratou alebo poškodením.
2) Zamestnancom sa neodporúča využiť funkcionalitu na automatické zapamätanie hesla, najmä ak ide o heslo k zvlášť dôležitým informačným systémom a emailom.
3) Pri práci s osobnými a citlivými údajmi na zariadení, musí byť na zariadení prevádzkovaný aktualizovaný antivírusový nástroj.

4) Zamestnanec je povinný oddeľovať pracovné a súkromné aktivity, pri ktorých sa zariadenie používa. Pre používanie zariadenia pre pracovné aktivity, prácu s osobnými údajmi, zamestnanec je povinný využívať softvérovú podporu na zabezpečenie primeranej ochrany osobných údajov. Prístup k spracovávaným osobným údajom na zariadení musí byť zamedzený iným osobám alebo automatizovaným prostriedkom šifrovaním a autentizáciou.
5) Zamestnanec si pri práci s osobnými údajmi na takomto zariadení musí byť vedomý rizika, ktoré vyplýva z práce na neznámych a nezabezpečených WiFi sieťach a za prenos osobných údajov cez takéto siete preberá plnú zodpovednosť.
6) Pokiaľ uchováva zamestnanec na zariadení osobné alebo citlivé údaje, je povinný tieto údaje uchovávať v zašifrovanej časti pamäťového média, SD karte, alebo pamäti zariadenia.
7) Krádež alebo strata mobilného zariadenia sa považuje za bezpečnostný incident.

8. Antivírusová ochrana

1) Ak sa na pracovnej stanici používateľa zobrazí varovanie, že sa na disku alebo prenosnom médiu nachádza vírus alebo iný škodlivý kód, zamestnanec nesmie toto varovanie ignorovať. Ak zavírené prenosné médium patrí inému subjektu, používateľ ho označí ako zavírené a vráti ho majiteľovi. Prípadné zavírenie vlastného pevného disku alebo prenosného média používateľ bezodkladne oznámi správcovi aktíva počítačov a počítačovej siete, resp. po konzultácii s ním odstráni vírus z príslušného pamäťového média.
2) Objavenie vírusu v prijatej elektronickej pošte používateľ bezodkladne oznámi správcovi aktíva počítačov a počítačovej siete. V žiadnom prípade zavírenú elektronickú poštu neposiela inému adresátovi a na svojej pracovnej stanici ju uschová len dočasne a len na žiadosť správcu aktíva počítačov a počítačovej siete (na účely ďalšej analýzy prieniku vírusu do systémov pracoviska).

9. Prístup do siete Internet a mailová komunikácia

1) Každý zamestnanec, ktorému bol umožnený prístup do siete Internet, je povinný rešpektovať nasledovné zásady:
   a) využívať prístup do siete Internet len v súlade so svojou pracovnou náplňou,
   b) dodržiavať etické zásady a zdržiavať sa činností, ktoré by mohli viesť k poškodeniu dobrého mena prevádzkovateľa alebo k iným škodám,
   c) prípadný prenos osobných údajov cez Internet zabezpečiť šifrovaním, ak nie je zamestnanec schopný prenos takto zabezpečiť, nie je prípustné ho uskutočniť,
   d) zakazuje sa preberať zo siete Internet nelegálny obsah (softvér, súbory chránené autorskými právami a pod.). Preberanie spustiteľných programov je povolené len po konzultácii so správcom aktíva počítačov a počítačovej siete,
   e) odporúča sa neukladať heslá na disku počítača.
2) Zamestnanec je povinný používať elektronickú poštu len v súlade so svojou pracovnou náplňou.
3) Zamestnanec je povinný zabezpečiť správne adresovanie príjemcu mailovej správy a na prenos správ používať všeobecne dané dátové štandardy.

4) Pri posielaní osobných údajov je zamestnanec povinný použiť kryptovanú komunikáciu.
5) Zamestnanec je oprávnený používať elektronickú poštu len na pracovné účely; obsah dát odosielaných v rámci lokálnej siete a cez Internet nesmie byť v rozpore s dobrými mravmi.
6) Je zakázané používať elektronickú poštu na súkromné účely.
7) Zamestnanci nesmú posielať alebo dovoliť posielať v mene Prevádzkovateľa žiadne e-maily, prílohy alebo uverejnenia na internetovú stránku bez autorizácie vedúcim zamestnancom, ktorý je oprávnený robiť rozhodnutia v mene Prevádzkovateľa a Prevádzkovateľa reprezentovať.
8) Zamestnanci nesmú posielať e-maily, ktoré by mohli poškodiť dobré meno Prevádzkovateľa alebo jeho vzťahy s klientmi, alebo ktoré môžu priviesť klientov Prevádzkovateľa do omylu.
9) Zamestnancom sa zakazuje posielať reťazové a hromadné e-maily, reklamné správy a pod., pokiaľ takouto činnosťou nebude zamestnanec poverený svojim nadriadeným alebo to nebude mať v náplni práce.
10) Zakazuje sa používanie messengerov, výnimky povoľuje oprávnený vedúci a správca IT aktíva.

Porušenie ustanovení tohto článku sa považuje za bezpečnostný incident.

10. Šifrovanie a kryptografické opatrenia

1) Zamestnanci, ktorí prenášajú osobné dáta na USB zariadeniach, notebookoch a prostredníctvom mailovej komunikácie, sú povinní tieto dáta šifrovať pridelenými technickými prostriedkami. Nedodržanie tohto nariadenia sa považuje za bezpečnostný incident.
2) Kryptografické opatrenia sa môžu použiť na dosiahnutie rôznych cieľov informačnej bezpečnosti ako napr.:
   a) dôvernosti: použitím šifrovania informácií na ochranu citlivých a kritických informácií či uložených alebo prenášaných,
   b) integrity/pôvodnosti: použitím elektronického podpisu alebo správy o pôvodnosti kódu na overenie pôvodnosti, alebo integrity uloženej, alebo prenášanej citlivej, alebo kritickej informácie.

11. Manipulácia s médiami

1) Obsahy akýchkoľvek opakovateľne použiteľných médií, ktoré majú byť odnesené z priestorov Prevádzkovateľa, musia byť zmazané, ak už nie sú ďalej potrebné. Zmazanie je potrebné spraviť formou bezpečného vymazania. Za zmazanie zodpovedá pracovník, ktorý povolil odnos médií z priestorov Prevádzkovateľa.
2) Pre všetky médiá s citlivými a osobnými údajmi odnášané z priestorov Prevádzkovateľa je potrebné urobiť autorizáciu a vykonať záznam o vynesení, pričom tento záznam musí obsahovať dátum, typ média, aké dáta sú uložené na médiu, dôvod vynesenia a kto médium vyniesol z organizácie.
3) Na prenos médií je potrebné použiť spoľahlivé prostriedky transportu alebo kuriéra.
4) Všetky médiá s osobnými a citlivými údajmi musia byť uložené v bezpečnom, chránenom prostredí, podľa špecifikácie výrobcu.

12. Zásady práce s elektronickým podpisom a elektronickou pečaťou

1) Na podpisovanie elektronických dokumentov v mene Prevádzkovateľa elektronickým podpisom sa musí použiť výlučne kvalifikovaný elektronický podpis s mandátnym certifikátom (ďalej len „*kvalifikovaný mandátny certifikát*“) alebo kvalifikovaný systémový certifikát.
2) Elektronicky podpisovať dokumenty kvalifikovaným mandátnym certifikátom môže len štatutár Prevádzkovateľa alebo ním poverení zamestnanci.
3) Zamestnanec je oprávnený podpísať dokument v mene Prevádzkovateľa len prostredníctvom kvalifikovaného systémového certifikátu, okrem prípadov, kedy je poverený štatutárom na podpisovanie prostredníctvom kvalifikovaného mandátneho certifikátu.
4) Zamestnanec, ktorému bol vydaný kvalifikovaný mandátny certifikát, v prípade zániku jeho oprávnenia podpisovať v mene Prevádzkovateľa, je povinný zdržať sa podpisovania a bezodkladne požiadať o zrušenie mandátneho certifikátu. O tejto skutočnosti je povinný oboznámiť vedenie Prevádzkovateľa.
5) Správca IT aktíva zodpovedá za vyhotovenie certifikátu a za bezpečné uloženie a ochranu údajov potrebných k vyhotoveniu kvalifikovaného systémového certifikátu.
6) V prípade, že sa ktorýkoľvek zamestnanec dozvie o skutočnostiach, ktoré by mohli znamenať, že údaje potrebné na vyhotovenie kvalifikovaného mandátneho certifikátu alebo kvalifikovaného systémového certifikátu boli kompromitované, je povinný túto skutočnosť oznámiť správcovi IT aktíva, ktorý bezodkladne zabezpečí zrušenie platnosti príslušného certifikátu. O tejto skutočnosti bezodkladne oboznámi aj vedenie Prevádzkovateľa.

13. Elektronická schránka

1) Do elektronickej schránky má prístup štatutár Prevádzkovateľa alebo ním poverení zamestnanci.
2) Na prístup do schránky je potrebné mať elektronický občiansky preukaz s čipom, bezpečnostný osobný kód (BOK) a mať v počítači nainštalované aplikácie eID klienta, ovládač čítačky čipových kariet či aplikáciu pre kvalifikovaný elektronický podpis s mandátnym certifikátom.
3) Zriadenie prístupov do jednotlivých priečinkov elektronickej schránky zabezpečuje správca IT aktíva na návrh vedenia Prevádzkovateľa. Nastavuje možnosti disponovať s priečinkami schránky, čítať a zmazať správy, presúvať a nahrávať správy, vytvárať a zmazať podpriečinky a nastavovať v nich pravidlá.
4) Poverení zamestnanci majú povinnosť prijímať a kontrolovať elektronicky doručované správy každý deň. Obsah správ sú povinní bezodkladne distribuovať na oddelenie dotknuté touto správou. Prevzatie obsahu správy musí byť potvrdené podpisom, obdobne ako je to u doporučenej poštovej zásielky. Pokiaľ je to potrebné, treba obsah správy vytlačiť a v tlačenej forme distribuovať ako doporučenú listovú zásielku.

14. Ukončenie pracovného alebo obdobného pomeru oprávnenej osoby, zamestnanca

1) Pred ukončením pracovnej zmluvy alebo inej zmluvy, na základe ktorej sa osoba - zamestnanec stáva oprávnenou osobou a táto používa zverené zariadenia na plnenie svojich úloh, musí tieto informačné aktíva vrátiť Prevádzkovateľovi alebo ním poverenej osobe zodpovednej za prevzatie zverených zariadení. O takomto odovzdaní sa vykoná „Písomný záznam o odovzdaní zverených zariadení“ na osobitnom tlačive alebo ako súčasť výstupného listu s kompletným zoznamom odovzdaných aktív. Vlastník zvereného zariadenia je zodpovedný za kompletnosť odovzdaných zariadení. Odovzdanie zvereného zariadenia môže byť realizované aj potvrdením preberajúceho o odovzdaní na tlačive, v ktorom bolo potvrdené prevzatie zariadenia. Preberajúci uvedie dátum prevzatia, stav zariadenia (prípadné jeho nedostatky) a svoje meno a podpis.
2) Pred ukončením pracovnej zmluvy alebo inej zmluvy na základe ktorej sa osoba - zamestnanec stáva oprávnenou osobou a používa e-mailové schránky pridelené Prevádzkovateľom, je táto oprávnená osoba povinná prehlásiť, že mailové správy, ktoré boli v jej používaní, sú služobného charakteru a môžu sa používať pre potreby prevádzkovateľa. Prehlásenie je súčasťou „Písomného záznamu o odovzdaní zverených zariadení“ alebo výstupného listu. Povinnosťou odchádzajúceho zamestnanca je odstrániť z mailovej schránky správy, ktoré nemajú služobný charakter. Na správy v e-mailových schránkach odchádzajúceho zamestnanca bude Prevádzkovateľ nahliadať ako na správy bezvýhradne prináležiace Prevádzkovateľovi.
3) Po ukončení pracovnej zmluvy alebo inej zmluvy, na základe ktorej sa osoba - zamestnanec stáva oprávnenou osobou a má pridelené prístupové práva do operačných a informačných systémov (OS a IS), je povinný príslušný správca IS bezodkladne odobrať tieto prístupové práva ich deaktiváciou. Pokyn na odobratie prístupových práv dáva personálne oddelenie a ich odobratie potvrdzuje správca na „Písomnom zázname o odovzdaní zverených zariadení“ alebo na výstupnom liste.
4) Po ukončení pracovnej zmluvy alebo inej zmluvy ,na základe ktorej sa osoba - zamestnanec stáva oprávnenou osobou a má zverené kľúče, alebo iné prístupy do priestorov Prevádzkovateľa (dochádzkové karty, čipy na prístup do priestorov a iné oprávnenia pre vstup do priestorov), je povinná táto osoba odovzdať kľúče alebo iné prístupy do priestorov Prevádzkovateľa Prevádzkovateľovi, prípadne na personálnom oddelení. O odovzdaní je potrebné spraviť záznam v „Písomnom zázname o odovzdaní zverených zariadení“ alebo na výstupnom liste.
5) Písomný záznam o odovzdaní zverených zariadení alebo výstupný list má obsahovať:
   a) meno, priezvisko a funkcia oprávnenej osoby končiacej pracovný alebo obdobný pomer s dátumom ukončenia pracovného alebo obdobného pomeru,
   b) zoznam zverených prostriedkov (zariadenia, kľúče, vstupné karty, prístupy do OS a IS),
   c) zoznam odovzdaných prostriedkov a ich nedostatkov,
   d) meno, priezvisko, dátum a funkcia osoby, ktorej boli odovzdané zverené zariadenia,
   e) meno, priezvisko, dátum a funkcia osoby, ktorá zrušila prístupy do OS a IS,

f) prehlásenie oprávnenej osoby končiacej pracovný pomer potvrdené podpisom, že mailové správy, ktoré boli v jej používaní sú služobného charakteru a môžu sa používať pre potreby prevádzkovateľa.

15. Záverečné ustanovenie

1) Vedúci oddelení Prevádzkovateľa sú povinní s touto smernicou oboznámiť všetkých zamestnancov.
2) Táto smernica nadobúda platnosť dňom jej podpisu a účinnosť od 01.10.2018.

	Vypracoval	**Posúdil**	**Schválil**
Meno a priezvisko	Ing. Ivan Kotrík	MVDr. Norbert Turanovič	JUDr. Katarína Macháčková
Funkcia	vedúci referátu informatiky	prednosta MsÚ	primátorka mesta
Dátum	15.09.2018	15.09.2018	15.09.2018
Podpis			