INTERNÁ SMERNICA č. 81

IS - 81

Smernica pre používanie aktív so zreteľom na ochranu osobných údajov pre správcov informačného systému

Obsah

1. Účel smernice 3
2. Základné pojmy 3
3. Aktíva informačných technológií 4
4. Prevádzkové záznamy 5
5. Zálohovanie a archivovanie údajov 6
6. Autentizácia 6
7. Pracovné stanice 7
8. Prenosné zariadenia – notebooky 8
9. Mobilné zariadenia – tablety a smartfóny 8
10. Servery a ostatná IT technika v zabezpečených priestoroch 8
11. Antivírusová ochrana 9
12. Lokálna počítačová sieť 10
13. Prístup do siete Internet a mailová komunikácia 10
14. Vzdialený prístup do lokálnej počítačovej siete 11
15. Šifrovanie a kryptografické opatrenia 11
16. Manipulácia s médiami 11
17. Zásady práce s elektronickým podpisom a elektronickou pečaťou 12
18. Elektronická schránka 12
19. Premiestňovanie a likvidácia IT aktív 12
20. Zamestnanci externej organizácie 13
21. Záverečné ustanovenia 13

1. Účel smernice

1) Smernica upravuje práva a povinnosti všetkých zamestnancov Mesto Prievidza, Námestie slobody 14, 971 01 Prievidza (ďalej ako „Prevádzkovateľ“) v oblasti ochrany a bezpečnosti majetku, informácií a ďalších hodnôt, ktoré Prevádzkovateľ vlastní.

2. Základné pojmy

1) **Aktíva** – všetky hmotné i nehmotné hodnoty, ktoré Prevádzkovateľ vlastní alebo využíva a ktoré slúžia najmä na plnenie jeho úloh. Medzi hmotné aktíva patria najmä servery, počítače, počítačové siete, komunikačné zariadenia a ďalšie hmotné predmety vo vlastníctve organizácie. Medzi nehmotné aktíva patria najmä informačné systémy, pracovné postupy, know-how, údaje o zamestnancoch, ekonomické, finančné a obchodné údaje, majetkové a obdobné práva a ďalší nehmotný majetok.
2) **Aktíva informačných technológií (IT aktíva) –** všetky technické a softvérové prostriedky, ktoré slúžia na ukladanie, prenos a spracovanie osobných údajov v digitálnej podobe bez ohľadu na účel tohto spracovania.
3) **Autentizácia** – je nástroj, pomocou ktorého sa zabezpečuje prístup určených osôb k IT aktívu a zároveň zamedzuje prístup ostatným osobám k IT aktívu.
4) **Bezpečnostný incident** – situácia, stav, kedy môže dôjsť, dochádza alebo došlo k narušeniu existujúcej ochrany osobných údajov.
5) **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 podobne).
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) **Externá organizácia** – organizácia alebo spoločnosť vstupujúca do informačného systému za účelom jeho údržby alebo obnovy.
8) **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.
9) **Kryptovaná komunikácia** – dátová komunikácia zabezpečená kódom, kódovaný prenos dát, s použitím kryptografických opatrení, hesiel a bezpečnostných postupov.
10) **Likvidácia osobných údajov** – zrušenie osobných údajov rozložením, vymazaním alebo fyzickým zničením hmotných nosičov tak, aby sa z nich osobné údaje nedali reprodukovať.
11) **Mandátny certifikát** – kvalifikovaný certifikát pre elektronický podpis vydaný fyzickej osobe oprávnenej zo zákona alebo na základe zákona konať za inú osobu alebo orgán verejnej moci alebo v ich mene.

12) **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.
13) **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.
14) **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.
15) **Prevádzkovateľ** – subjekt, ktorý spracúva osobné údaje vo vlastnom mene, v tejto smernici je to Mesto Prievidza, Námestie slobody 14, 971 01 Prievidza .
16) **Realizujúca sa hrozba –** stav, kedy je aktívum hrozbou poškodzované alebo ničené, čo má za následok znefunkčnenie aktíva, alebo ohrozenie záujmov organizácie.
17) **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.
18) **USB zariadenie** – akékoľvek zariadenie pripojiteľné k USB rozhraniu a schopné prenosu dát cez toto rozhranie.
19) **Všeobecne použiteľný identifikátor** – trvalý identifikačný osobný údaj dotknutej osoby, ktorý zabezpečuje jej jednoznačnosť v informačných systémoch (zvyčajne rodné číslo).
20) **Zákon** – zákon č 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „Zákon“).

3. Aktíva informačných technológií

1) Správa IT aktív musí byť organizovaná tak, aby sa minimalizovala hrozba zneužitia postavenia administrátora.
2) Za ochranu údajov je zodpovedný ten správca IT aktíva, na ktorého technických prostriedkoch (pamäťových médiách) sú tieto údaje uložené. Na tento účel správca IT aktíva vykonáva nasledovné činnosti a úkony:
   a) vykonáva alebo zabezpečuje kopírovanie údajov na záložné médiá (zálohovanie údajov),
   b) vykonáva alebo zabezpečuje kopírovanie údajov na archívne médiá (archivovanie údajov),

c) vykonáva nastavenia prístupových práv k údajom tak, aby k nim mohli pristupovať len oprávnení používatelia,
d) inštaluje, spravuje a zabezpečuje také služby (aplikácie), ktoré umožnia zvýšenú ochranu osobných údajov šifrovaním alebo elektronickým podpisom.

3) Správca IT aktíva je zodpovedný za pravidelnú a včasnú aktualizáciu všetkých programových prostriedkov, ktorými sú najmä operačné systémy a ich súčasti, databázové systémy, používané aplikácie (najmä ak komunikujú po sieti), systémy antivírusovej ochrany a firewally.
4) Správca IT aktíva je povinný priebežne inštalovať všetky dostupné nové opravy softvérového aktíva, pokiaľ sa tým nenaruší bezproblémový chod a činnosť aktíva. O nainštalovaných opravách je povinný urobiť zápis, ktorý bude obsahovať dátum, kedy bola oprava nainštalovaná a zoznam nainštalovaných opráv. Pokiaľ takýto zápis, záznam, je dostupný v samotnom softvérovom aktíve, nevyžaduje sa vyhotovovať ďalší zápis. Minimálne raz za 6 mesiacov je správca IT aktíva povinný overiť, či neboli vydané nové verzie softvéru.
5) Zakazuje sa používanie programov, ktoré nemajú garanciu výrobcu o ich spoľahlivosti alebo neboli overené správcom IT aktíva v izolovanom prostredí, či neobsahujú nežiaduce funkcie a chyby. Overenie sa vykonáva tak, aby nemohlo dôjsť k ohrozeniu IT aktív, pričom sa musí preveriť najmä správanie programu v sieťovom prostredí vo vzťahu k údajom uloženým na pamäťovom médiu počítača.
6) Pri konfigurácii prostriedkov, programov a služieb správca IT aktíva dbá na to, aby sa používali len tie prostriedky, programy a služby, ktoré sú nevyhnutné pre plnenie pracovných úloh a potrieb Prevádzkovateľa. Zakazuje sa používanie programov, sieťových služieb a IT prostriedkov, ktoré nie sú potrebné pre výkon práce zamestnancov a plnenie ich úloh. Používané programy, služby a prostriedky musia byť konfigurované tak, aby k nim mali prístup len tí zamestnanci, ktorí tieto programy, služby a prostriedky potrebujú k svojej práci.
7) Správca IT aktíva vedie dokumentáciu o spravovanom aktíve, ktorá obsahuje všetky konfiguračné údaje, údaje o inštalovaných programoch, údaje o IP adresách, prihlasovacích menách a údaje o užívateľoch.

4. Prevádzkové záznamy

1) Ak je vedený prevádzkový záznam o činnosti a chode technického prostriedku alebo organizačnej súčasti, ktorá je aktívom so zvýšenou ochranou, je povinnosťou správcu tohto aktíva pravidelne vyhodnocovať tento záznam.
2) V prevádzkovom zázname musia byť zaznamenané všetky dôležité skutočnosti, ktoré môžu byť dôležité pre ochranu osobných údajov. O požadovanom obsahu prevádzkového záznamu musí byť zamestnanec, ktorý tento záznam vedie, poučený.
3) Prevádzkové záznamy sú bezpečnostným dokumentom.
4) Prevádzkovými záznamami sú najmä:
   a) prevádzkové záznamy o chode počítačov všetkých typov (napr. EventLog v OS MS Windows, syslog v systéme Linux),

b) prevádzkové záznamy o chode aplikácií a programov (napr. záznam o chode databázového servera),
c) prevádzkové záznamy o chode prvkov počítačovej siete (najmä smerovačov a firewall-ov),
d) prevádzkové záznamy z bezpečnostného systému fyzickej ochrany,
e) záznamy o vstupe do registratúrneho strediska,
f) záznamy o vstupe do miestnosti, kde sú umiestnené servery.

5. Zálohovanie a archivovanie údajov

1) Správca IT aktíva je povinný vykonávať zálohovanie a archiváciu podľa vypracovaného harmonogramu.
2) Médiá so záložnými údajmi musia byť uložené v inej miestnosti ako sa nachádza počítač, z ktorého boli záložné údaje vyhotovené.
3) Médiá s archívnymi údajmi musia byť uložené v inej budove ako sa nachádza počítač, z ktorého boli archivačné údaje vyhotovené. Pokiaľ nie je možné túto podmienku splniť, musia byť média s archívnymi údajmi uložené oddelene od médií so záložnými údajmi tak, aby sa v maximálnej možnej miere zamedzilo súčasnému zničeniu záložných aj archívnych médií v prípade živelnej pohromy alebo ich odcudzenia, či straty prekonaním jednej a tej istej prekážky.
4) Správca príslušného IT aktíva je povinný raz za šesť mesiacov otestovať funkčnosť záložného média a raz za rok funkčnosť archívneho média. Funkčnosť otestuje skopírovaním súborov z média alebo rozbalením komprimačných archívov.

6. Autentizácia

1) Správca IT aktíva, ktorý vyžaduje autentizáciu, stanoví autentizačné postupy a mechanizmy.
2) Pre autentizačné mechanizmy stanoví parametre, a to najmä vlastnosti hesiel. Stanoví dĺžku, štruktúru a expiračnú dobu hesiel.
3) Správca IT aktíva nesmie povoliť heslá kratšie ako 8 znakov; heslá musia obsahovať aspoň jeden neabecedný znak a ich expiračná doba nesmie byť dlhšia ako 12 mesiacov. Správca nesmie ako heslo použiť takú kombináciu znakov, ktorú by bolo možné priradiť k jeho osobe, akými sú napríklad meno používateľa a jeho rodinných príslušníkov napísané spredu či odzadu, telefónne číslo domov alebo na pracovisko a podobne.
4) Autentizačné prostriedky vydáva správca IT aktíva, ktorý o tom musí viesť evidenciu. Evidencia obsahuje údaje o autentizačných prostriedkoch, mená a podpisy zamestnancov, ktorým boli prostriedky vydané a dátum a čas výdaja a vrátenia.
5) Správca IT aktíva môže prideliť autentizačné údaje a prostriedky len zamestnancom Prevádzkovateľa alebo zamestnancom spoločnosti, ktorá robí údržbu daného aktíva.
6) Prístupové oprávnenia prideľuje používateľovi správca IT aktíva na základe požiadavky príslušného vedúceho zamestnanca. Tvoria ich prístupové meno, prístupové heslo a súbor nastavení, ktoré definujú povolené aktivity používateľa.
7) Prístupové oprávnenia sú prideľované podľa typu používateľa:
   a) administrátor – prístup k správe a údržbe aktíva; mal by to byť správca aktíva,

b) používateľ – prístup len k tým modulom aplikácie (aktíva), s ktorými bezprostredne pracuje,
c) externý používateľ – zamestnanec externej firmy, ktorá spravuje a udržiava danú aplikáciu (aktívum); prístup je kontrolovaný správcom aktíva alebo administrátorom, ak ho tým poveril správca aktíva.

8) Oprávnenie prideľovať autentizačné údaje a prostriedky udelí Prevádzkovateľ správcovi IT aktíva v rozhodnutí o pridelení správy aktíva.
9) Začiatok, zmenu alebo ukončenie pracovného pomeru zamestnanca oznámi príslušný vedúci oddelenia, alebo útvaru správcovi IT aktíva, ktorý vydáva autentizačné údaje a prostriedky.
10) Personálne oddelenie musí zabezpečiť navrátenie pridelených zariadení a navrátenie informačných aktív, odstránenie informácií oprávnenej osoby z pridelených zariadení a odovzdanie výsledkov práce v súvislosti s informačnými systémami. Pre naplnenie tejto úlohy musia byť vytvorené dostatočné podmienky v pracovnej zmluve, zmluvách s externými pracovníkmi a v zmluvách s tretími stranami zaväzujúcimi sa k mlčanlivosti a k súčinnosti pri vykonaní týchto úloh.

7. Pracovné stanice

1) Správca IT aktíva zodpovedá za pripojenie pracovnej stanice do lokálnej počítačovej siete Prevádzkovateľa, inštaláciu operačného systému a všetkého ostatného programového vybavenia.
2) Na pracovných staniciach musí byť nainštalovaný informačný systém, na ktorý je zabezpečená podpora výrobcu. Správca IT aktíva je povinný zabezpečiť pravidelnú aktualizáciu operačného systému a ostatného programového vybavenia pracovných staníc.
3) Správca IT aktíva zabezpečí inštaláciu len takých programových prostriedkov, ktoré zamestnanec potrebuje ku svojej práci. Prístupové práva nastaví tak, aby zamestnanec nemohol na pracovnej stanici meniť žiadne programové vybavenie, a tiež meniť konfiguráciu programového vybavenia.
4) Správca IT aktíva odovzdá nainštalovanú pracovnú stanicu používateľovi, ktorý prevzatie potvrdí podpisom na preberacom protokole.
5) Pri odovzdaní nainštalovanej pracovnej stanice je správca IT aktíva povinný poučiť používateľa o zásadách bezpečnej práce s pracovnou stanicou v prostredí lokálnej počítačovej siete a v prostredí Internetu. Zamestnanec preberajúci pracovnú stanicu podpíše záznam o poučení.
6) Na pracovných staniciach, na ktorých sa nepoužívajú prenosné USB zariadenia, správca IT aktíva zabezpečí zablokovanie USB portov. Správca aktíva eviduje zoznam pracovných staníc, na ktorých je zablokované a zakázané používanie prenosných USB zariadení. Tento zoznam schvaľuje Prevádzkovateľ.
7) Na pracovných staniciach, na ktorých je povolené používanie prenosných USB zariadení, zabezpečí správca IT aktíva automatickú kontrolu USB zariadení antivírusovým programom.

8. Prenosné zariadenia – notebooky

1) Pred odovzdaním zariadenia zamestnancovi je správca IT aktíva povinný nainštalovať na zariadenia softvér na antivírusovú ochranu, kryptovanie a šifrovanie citlivých údajov, osobných údajov a softvér pre riadenie šifrovaného prístupu do lokálnej siete Prevádzkovateľa, ak to zamestnanec z titulu svojich pracovných povinností potrebuje alebo ak si to vyžaduje zabezpečenie primeranej ochrany osobných údajov.
2) Správca IT aktíva je povinný pri odovzdávaní zariadenia poučiť príslušných zamestnancov o dodatočných rizikách vyplývajúcich z tohto druhu mobilnej práce a o opatreniach, ktoré sú potrebné na prácu s prenosnými zariadeniami.
3) Správca IT aktíva je povinný zabezpečiť na prenosných zariadeniach (notebookoch), ak je to z hľadiska uložených údajov potrebné, kryptované partície pevného disku alebo kryptované adresáre. Správca IT aktíva musí poučiť používateľa zariadenia o tom, že citlivé údaje a osobné údaje bude ukladať vo svojom notebooku len na kryptovanú partíciu alebo do kryptovaného adresára.

9. Mobilné zariadenia – tablety a smartfóny

1) Mobilný internet sa pridelí zamestnancom, ktorých zaradenie a charakter práce si vyžaduje operatívne pripájanie sa k Internetu mimo pracoviska. Mobilný internet sa pridelí zamestnancovi na základe písomnej požiadavky a s písomným súhlasom príslušného vedúceho pracovníka.
2) Správca IT aktíva eviduje zoznam mobilných zariadení, z ktorých je možné pripojiť sa do vnútornej lokálnej siete prevádzkovateľa.
3) Každé mobilné zariadenie musí byť zabezpečené antivírusovým programom a ochranou proti malvérom.
4) Pre riziká, ktoré vplývajú z používania mobilných zariadení, je potrebné vykonať podporné bezpečnostné opatrenia zahrňujúce:
   a) registráciu mobilných zariadení,
   b) požiadavky na verzie softvéru pre mobilné zariadenia a pre aplikáciu záplat,
   c) obmedzenia pripojenia k informačných službám,
   d) riadenie prístupov,
   e) zakázanie, vymazanie alebo uzatvorenie na diaľku,
   f) zálohovanie.

10. Servery a ostatná IT technika v zabezpečených priestoroch

1) Servery a ostatná IT technika, ktorá spracováva alebo uchováva osobné údaje mimo pracovných staníc, musí byť zabezpečená pred zneužitím alebo poškodením, umiestnená do osobitnej a uzamykateľnej miestnosti (serverovni), s potrebným technickým, klimatickým a bezpečnostným vybavením.

2) Pokiaľ sú okná serverovne prístupné z ulice alebo iného verejne dostupného miesta, sú na prvom nadzemnom poschodí alebo sú inak ľahko dostupné, je potrebné ich zabezpečiť mrežou alebo fóliou proti rozbitiu.
3) Serverovňa musí byť vybavená snímačom pohybu, zatopenia a protipožiarnym snímačom.
4) V priestoroch serverovne je zakázané skladovať horľavé materiály. Pred vstupom do serverovne musí byť dostupný hasiaci prístroj, ktorý je vhodný pre hasenie IT techniky.
5) Serverovňa musí byť zabezpečená pred neoprávneným prístupom. Vstup do serverovne je možný len pre poučených zamestnancov, ktorí zabezpečujú chod a servis zariadení umiestnených v serverovni. Ostatné osoby môžu vstupovať do serverovne len v prítomnosti poučenej osoby oprávnenej k vstupu do serverovne alebo s jej súhlasom. Vstup všetkých osôb do serverovne je potrebné zaevidovať do knihy evidencie vstupov.
6) V knihe evidencii vstupov musí byť zaznamenané: meno osoby vstupujúcej do serverovne, dátum a čas pobytu v serverovni, meno osoby, ktorá sprístupnila vstup do serverovne nepoučenej osobe a účel pobytu osoby v serverovni.
7) Pokiaľ prevádzkovateľ nemá zriadenú osobitnú miestnosť, t. j. serverovňu, je povinný zabezpečiť prístup k serverom a ostatnej IT technike, ktorá spracováva alebo uchováva osobné údaje mimo pracovných staníc tak, ako keby mal zriadenú serverovňu.

11. Antivírusová ochrana

1) Správca IT aktíva je povinný zabezpečiť inštaláciu a pravidelnú aktualizáciu antivírusových detekčných a nápravných softvérov na kontrolu a ochranu počítačov, notebookov, tabletov, smartfónov, serverov a médií na rutinnej báze. Antivírusové kontroly musia zhŕňať:
   a) kontrolu všetkých súborov na elektronických alebo optických médiách, ako aj súborov prijatých prostredníctvom počítačovej siete z hľadiska prítomnosti škodlivého kódu ešte pred používaním,
   b) kontrolu príloh elektronickej pošty a stiahnutých súborov z hľadiska výskytu škodlivého kódu ešte pred spustením; táto kontrola by sa mala vykonávať na rozličných miestach, napr. na elektronických poštových serveroch, pracovných staniciach a pri vstupe do siete prevádzkovanej Prevádzkovateľom,
   c) kontrolu pred nevyžiadanou poštou – spamom,
   d) kontrolu webových stránok z hľadiska výskytu škodlivého kódu.
2) Správca IT aktíva je povinný venovať zvýšenú pozornosť tomu, aby škodlivý kód nebol zavedený počas výkonu pohotovostných procedúr alebo procedúr údržby.
3) Správca IT aktíva je povinný zabezpečiť inštaláciu a pravidelnú aktualizáciu antivírusových detekčných a nápravných softvérov na prehliadanie počítačov, serverov a médií na rutinnej báze.
4) Správca IT aktíva zabezpečí, ak je to potrebné, za účelom zníženia nebezpečenstva vniknutia vírusu, vypnutie automatického zavádzania USB, CD, DVD a iných externých zariadení, tzv. “Autorun”.

12. Lokálna počítačová sieť

1) Správca IT aktíva zodpovedá za prevádzku lokálnej siete, jej technický rozvoj, dátovú bezpečnosť a dodržiavanie pravidiel pripojenia do siete. Zaisťuje používanie, chod a servis centrálnych sieťových serverov (DNS, FireWall, DHCP a pod.).
2) Správca IT aktíva je povinný viesť plán sieťových a káblových prepojení a pravidelne ho aktualizovať. Definuje používateľom oprávnenia na prístup k zariadeniam a službám, ktoré sú súčasťou ním spravovanej lokálnej počítačovej siete. Za týmto účelom je povinný evidovať aktuálny zoznam MAC a IP adries všetkých pripojených zariadení.
3) Správca IT aktíva inštaluje a konfiguruje VPN a WiFi klienta používateľom a v zmysle Čl. 6 prideľuje autentifikačné prostriedky.
4) Správca IT aktíva je povinný v zmysle Čl. 4 sledovať prevádzkové záznamy sieťových zriadení a pravidelne ich vyhodnocovať.
5) Správca IT aktíva je povinný upozorniť bez zbytočného odkladu vedenie Prevádzkovateľa na zistené bezpečnostné incidenty a tieto incidenty zdokumentovať.
6) V prípade lokalizácie incidentu z vnútra lokálnej počítačovej siete je správca IT aktíva povinný zariadenie spôsobujúce incident, bezodkladne od lokálnej počítačovej siete odpojiť.
7) V prípade incidentu z Internetu, ktorý by mohol mať za následok spôsobenie škody na zariadeniach v lokálnej počítačovej sieti, je správca IT aktíva povinný odpojiť celú lokálnu počítačovú sieť od Internetu, a to do doby, kým sa incident neprešetrí a neprijmú sa primerané opatrenia.

13. Prístup do siete Internet a mailová komunikácia

1) Správca IT aktíva v súčinnosti s vedením zabezpečuje výber blokovaných stránok. V prípade zistenia prenosu veľkého objemu dát nesúvisiacich s pracovnou činnosťou zamestnanca, má správca IT aktíva právo zakázať a znemožniť užívateľovi prístup do Internetu.
2) Správca IT aktíva pridelí zamestnancovi pri nástupe do zamestnania emailovú adresu v tvare: meno.priezvisko@prevádzkovateľ.sk. Pri existencii duplicitného mena a priezviska pridelí emailovú adresu v tvare: meno.priezvisko.pracovisko@prevadzkovatel.sk.
3) Údaje prenášané elektronickou poštou musia byť chránené tak, aby bola čo najlepšie zaistená ich dôvernosť, integrita a aby bolo možné preukázanie autorstva. Odporúča sa elektronickú poštu šifrovať a digitálne podpisovať.
4) Veľkosť posielanej elektronickej pošty je obmedzená. Konkrétne parametre sú stanovené takto:
   a) veľkosť poštovej schránky 200 MB a 5000 emailov,
   b) veľkosť jednej poštovej správy je do 20 MB,
   c) veľkosť prílohy sa započítava do veľkosti poštovej správy.
5) Správca IT aktíva zabezpečí nastavenie poštového klienta a hesla na počítači zamestnanca.
6) Správca IT aktíva na podnet zamestnanca alebo jeho priameho nadriadeného rieši problémy s odosielaním a prijímaním pošty, so zabudnutím hesla a s nefunkčnosťou emailovej adresy.

14. Vzdialený prístup do lokálnej počítačovej siete

1) Prácou na diaľku sa označuje každá forma práce z prostredia mimo kancelárie, vrátane netradičných pracovných prostredí.
2) Vzdialený prístup do lokálnej siete musí byť chránený šifrovaním.
3) Vzdialený prístup je možné realizovať len pripojením sa na virtuálnu pracovnú plochu počítača zamestnanca.
4) Zariadenie, z ktorého sa zamestnanec vzdialene pripája, musí byť zabezpečené antivírusovým programom a ochranou proti malvérom.

15. Šifrovanie a kryptografické opatrenia

1) Metódy šifrovania na prenos médií a prideľovanie kryptografických kľúčov (certifikátov) pre pripojenie do vnútornej sieťovej infraštruktúry riadi správca IT aktíva, v súčinnosti s vedením Prevádzkovateľa.
2) Kryptografický kľúč generuje na základe žiadosti schválenej štatutárom, alebo prednostom MsÚ. Túto skutočnosť zaznamená do zoznamu pridelených kryptografických kľúčov, pričom zaznamená dátum exspirácie kryptografického kľúča.
3) Správca IT aktíva zabezpečuje:
   a) distribúciu určeným používateľom vrátene toho, ako má byť kľúč aktivovaný,
   b) obnovu kľúčov, ktoré sa stratili alebo poškodili,
   c) zničenie kľúčov,
   d) zaznamenávanie a audit aktivít týkajúcich sa riadenia kľúčov,
   e) generovanie a získavanie certifikátov verejných kľúčov.
4) Technické prostriedky na šifrovanie USB zariadení, notebookov a mailovej komunikácie určí správca IT aktíva. Tieto prostriedky rozdistribuuje jednotlivým zamestnancom prostredníctvom vedúcich jednotlivých odborov a zabezpečí ich zaškolenie. Každý zamestnanec zodpovedá za to, že ním používané USB zariadenie, notebook a mail bude pre účely spracovania a prenosu osobných údajov zabezpečený predpísanými kryptovacími prostriedkami. Inštaláciu týchto prostriedkov zabezpečuje správca IT aktíva.
5) Zamestnanci, ktorí prenášajú osobné údaje na USB zariadeniach, notebookoch a prostredníctvom mailovej komunikácie, sú povinní tieto údaje šifrovať pridelenými technickými prostriedkami. Nedodržanie tohto nariadenia sa považuje za bezpečnostný incident.

16. Manipulácia s médiami

1) Obsahy akýchkoľvek opakovateľne použiteľných médií, ktoré majú byť odnesené z organizácie, musia byť zmazané, ak už nie sú ďalej potrebné.
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 z organizácie vyniesol.

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.
5) Informácie, ktoré majú byť uchované dlhšie, ako je doba životnosti média, na ktorom sú uložené (na základe špecifikácie výrobcu), musia byť uložené aj na inom mieste, aby sa tak predišlo ich strate spôsobenej nečitateľnosťou média.
6) Médiá obsahujúce elektronické dokumenty musia byť zlikvidované bezpečne a spoľahlivo, napr. spálením, rozrezaním alebo hĺbkovým vymazaním dát, ak nemajú byť použité pre iný účel.

17. 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) Pridelenie kvalifikovaného systémového certifikátu pre zamestnanca Prevádzkovateľa zabezpečuje správca IT aktíva na návrh štatutára.
3) Správca IT aktíva vedie register kvalifikovaných mandátnych certifikátov, ktoré boli vydané zamestnancom Prevádzkovateľa. Súčasťou registra sú okrem údajov o zamestnancoch, ktorým bol kvalifikovaný mandátny certifikát pridelený aj technické údaje o certifikátoch a najmä údaj o vzniku a zániku mandátneho certifikátu.
4) Správca IT aktíva zodpovedá za vyhotovenie certifikátu a za bezpečné uloženie a ochranu údajov potrebných k vyhotoveniu kvalifikovaného systémového certifikátu.
5) Rovnako správca IT aktíva zodpovedá za platnosť údajov potrebných na vyhotovenie kvalifikovaného systémového certifikátu.

18. Elektronická schránka

1) Správca IT aktíva zabezpečuje zriadenie prístupov do jednotlivých priečinkov elektronickej schránky na návrh štatutára. Nastavuje možnosti disponovať s priečinkami schránky, čítať a zmazať správy, presúvať a nahrávať správy, vytvárať a zmazať podpriečinky a nastavovať v nich pravidlá.

19. Premiestňovanie a likvidácia IT aktív

1) Pri premiestňovaní IT aktíva zaznamená správca IT aktíva, kedy a ku komu bolo IT aktívum premiestnené, účel premiestnenia a dátum vrátenia aktíva do pôvodných priestorov.
2) Pri premiestnení IT aktíva do servisu alebo inej organizácie, kde bude mimo dosahu zamestnancov Prevádzkovateľa, je potrebné, ak je to možné, odstrániť z pevného disku

všetky osobné údaje, prípadne urobiť hĺbkové sformátovanie pevného disku. V prípade, že je uzatvorená zmluva o mlčanlivosti s externou servisnou firmou, je možné premiestnenie aktíva aj s nezmazaným pevným diskom.

3) O likvidácii IT aktíva rozhoduje správca IT aktíva, pričom o tejto skutočnosti informuje vedenie Prevádzkovateľa a urobí záznam o likvidácii aktíva.
4) Ak likvidované IT aktívum obsahuje pevný disk alebo iné úložisko s citlivými alebo osobnými údajmi, je správca IT aktíva povinný, ak je to možné, tieto údaje neobnoviteľne zlikvidovať. Nedodržanie tejto zásady sa považuje za bezpečnostný incident.

20. Zamestnanci externej organizácie

1) Prístup zamestnancov externej organizácie zriaďuje správca IT aktíva na základe schválenia Prevádzkovateľom. Správca IT aktíva vedie zoznam povolených prístupov k jednotlivým aktívam.
2) Správca IT aktíva zriadi zamestnancovi externej organizácie prístupové práva podľa Čl. 6 tejto smernice.
3) Správca IT aktíva je povinný zabezpečiť bezpečný šifrovaný prístup zamestnanca tretej strany k jeho aktívu.
4) Zamestnanci externej organizácie sú povinní pred prihlásením k IT aktívu o tejto skutočnosti informovať správcu IT aktíva buď prostredníctvom mailu alebo telefonicky. K tejto povinnosti musí byť externá organizácia zmluvne zaviazaná. Na základe tohto oznámenia im správca IT aktíva povolí pripojenie. Po skončení údržby alebo inej činnosti zamestnancom externej organizácie, správca IT aktíva zruší možnosť pripojenia.
5) Správca IT aktíva je povinný poučiť zamestnancov externej organizácie, ktorí prichádzajú do styku s osobnými údajmi, o ochrane osobných a citlivých údajov a o povinnosti zachovávať mlčanlivosť. Táto skutočnosť musí byť uvedená v príslušnej zmluve s takouto externou organizáciou.

21. 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			