Obecný úrad Lomnička
Lomnička 66
065 03 Podolínec

Smernica pre používanie IT aktív – pre zamestnancov

Obec Lomnička

Verzia:	01.42
Platné od:	
Stav dokumentu:	Finálny
Dôvernosť dokumentu:	Interný
Typ dokumentu:	Smernica pre používanie IT aktív – pre zamestnancov
Priorita:	štandardná

Autor dokumentu	e-mail	telefonický kontakt
CUBS plus, s.r.o.	kyber@cubsplus.sk oou@cubsplus.sk	0918/43 43 74 0903/608-164
Vlastník dokumentu	**e-mail**	**telefonický kontakt**
Obec Lomnička	obec@obeclomnicka.sk	0908 310 654 0948 164 202

Po zverejnení tohto dokumentu už nie sú všetky predchádzajúce verzie platné!
Po vytlačení a vytvorení lokálnych kópií sa dokument vyradí zo skupiny kontrolovaných dokumentov!

Obsah

1 ÚČEL SMERNICE

Smernica upravuje práva a povinnosti všetkých zamestnancov prevádzkovateľa základnej služby **obec Lomnička, IČO: 00330027, adresa: Obecný úrad Lomnička, Lomnička 66, 065 03 Podolínec**, (ďalej ako „PZS") v oblasti používania Informačno-komunikačných prostriedkov, ktoré PZS vlastní. Smernica slúži taktiež pre potreby naplnenia zákona NR SR č. 69/2018 Z. z. o kybernetickej bezpečnosti.

2 ZÁKLADNÉ POJMY

Z dôvodu lepšieho pochopenia princípov a postupov spojených s používaním IT aktív je nevyhnutné vymedziť si niekoľko základných pojmov, bez ktorých by táto problematika v podmienkach PZS nebola správne pochopená.

Bezpečnostný správca (manažér kybernetickej bezpečnosti) – je nezávislá zodpovedná osoba, ktorá riadi oblasť kybernetickej bezpečnosti, taktiež sa zaoberá riešením kybernetického bezpečnostného incidentu a má za úlohu zabezpečiť všetky postupy súvisiace s oznamovaním, odhaľovaním, analýzou a reakciou na kybernetický bezpečnostný incident.

Správca aktíva – je zamestnanec prevádzkovateľa, ktorému bol pridelený súbor aktív (mobilné telefóny, počítače, kamerový systém, aplikačné vybavenie a podobne) a ktorý je v prípade kybernetického bezpečnostného incidentu zodpovedný za pridelené aktívum a taktiež za definovanie nápravných opatrení v súčinnosti s manažérom kybernetickej bezpečnosti.

Aktíva informačných technológií (IT aktíva) — všetky technické a softvérové prostriedky, ktoré slúžia na ukladanie, prenos a spracúvame informácií v digitálnej podobe, bez ohľadu na účel tohto spracovania.

Aktíva operačných technológií (OT aktíva) - všetky technické a softvérové prostriedky, ktoré slúžia na signalizáciu / monitorovanie, meranie a reguláciu, riadenie / ovládanie a ochranu priemyselných technologických zariadení z rôznych oblastí a sektorov.

Autentizácia — je nástroj, pomocou ktorého sa zabezpečuje prístup určených osôb k IT aktívu a zároveň zamedzuje prístup ostatným osobám k IT aktívu.

Kybernetický bezpečnostný incident — situácia, stav, kedy môže dôjsť, dochádza alebo došlo k narušeniu existujúcej ochrany citlivých údajov.

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.).

Citlivé údaje — údaje, ktoré obsahujú osobné, ekonomické a iné údaje občanov a zamestnancov, údaje spadajúce pod osobitnú kategóriu osobných údajov v zmysle Nariadenia Európskeho parlamentu a Rady EÚ 2016/679 z 27 apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov a Zákona na ochranu osobných údajov č. 18/2018 Z. z.

Elektronická pečať — je informácia pripojená alebo inak logicky spojená s elektronickým dokumentom, obsahuje údaj, ktorý identifikuje pôvodcu pečate.

Elektronická schránka — štátom zriadené úložisko elektronických podaní prevádzkované Národnou agentúrou pre sieťové elektronické služby (NASES), slúžiace na prijímame elektronických podaní (žiadostí) od občanov, podnikateľov a iných inštitúcií a komunikáciu štátu a štátnych inštitúcií s organizáciami a podnikateľmi.

Hrozby vplyvy okolia, iných osôb, zariadení a prostriedkov, ktoré úmyselne alebo neúmyselne vplývajú na aktíva PZS tak, že ich organizácia nemôže využívať, alebo inak ohrozujú oprávnené záujmy PZS.

Kryptovaná komunikácia — dátová komunikácia zabezpečená kódom, kódovaný prenos dát s použitím kryptografických opatrení, hesiel a bezpečnostných postupov.

Likvidácia údajov — zrušenie údajov rozložením, vymazaním alebo fyzickým zničením hmotných nosičov tak, aby sa z nich údaje nedali reprodukovať.

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.

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.

Pracovná stanica — počítač určený na priame fyzické používanie používateľom.

Realizujúca sa hrozba — stav, kedy je aktívum hrozbou poškodzované alebo ničené, čo má za následok znefunkčnenie aktíva alebo ohrozenie záujmov PZS.

USB zariadenie — akékoľvek zariadenie pripojiteľné k USB rozhraniu a schopné prenosu dát cez toto rozhranie.

Kybernetický bezpečnostný incident - akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému, obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby, vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo ohrozenie bezpečnosti informácií.

3 AUTENTIZÁCIA

1) Heslá pre prístup k IT aktívam musia mať dĺžku minimálne 8 znakov a musia obsahovať aspoň jeden neabecedný znak a ich expiračná doba nesmie byť dlhšia ako 3 mesiace. 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 kybernetický 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.
2) Ak zamestnanec nemôže túto povinnosť splniť, ihneď to oznámi svojmu nadriadenému alebo bezpečnostnému správcovi.
3) Vstup do všetkých objektov Prevádzkovateľa prostredníctvom osobitných kľúčov a ďalších zabezpečovacích prvkov majú určení vedúci zamestnanci, upratovačky a zamestnanci, ktorých schválilo vedenie PZS.
4) Evidenciu kľúčov, prístup a manipuláciu s nimi vedie poverený zamestnanec PZS. Náhradné kľúče sa uchovávajú v uzamknutej skrinke. Prípadnú stratu kľúčov sú zamestnanci povinní ihneď oznámiť zamestnancovi, ktorý zodpovedá za ich evidenciu, alebo bezpečnostnému správcovi. 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 vedenia. 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. Kľúčový režim PZS sa riadi dokumentom s názvom Kľúčový poriadok.

5 PRACOVNÉ STANICE

1) **Zamestnanec je povinný používať zverené pracovné stanice len na pracovné účely. Porušenie tohto ustanovenia sa považuje za kybernetický 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 získame 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 alebo vedenia PZS.
10) **Zakazuje sa používanie vlastných USB kľúčov a vynášanie citlivých údajov na nich. Porušenie tohto bodu sa považuje za kybernetický bezpečnostný Incident.**

6 NOTEBOOKY A PRÁCA S CITLIVÝMI ÚDAJMI

1) Zamestnanec je povinný mať notebook zabezpečený heslom. Pokiaľ má na notebooku 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 e-mailom.
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 ako aj mobilného zariadenia – smartfónu alebo tabletu obsahujúceho citlivé údaje sa považuje za kybernetický bezpečnostný incident.**
7) Zamestnanec je zodpovedný za fyzickú ochranu zvereného zariadenia pred krádežou, stratou alebo poškodením.
8) Zamestnancom sa neodporúča využiť funkcionalitu na automatické zapamätanie hesla, najmä ak ide o heslo k zvlášť dôležitým aplikáciám a e-mailom.
9) Pri práci s citlivými údajmi na zariadení, musí byť na zariadení prevádzkovaný aktualizovaný antivírusový nástroj.
10) Zamestnanec je povinný oddeľovať pracovné a súkromné aktivity, pri ktorých sa zariadenie používa. Pre používanie zariadenia pre pracovné aktivity a prácu s citlivými údajmi je zamestnanec povinný využívať softvérovú podporu na zabezpečenie primeranej ochrany citlivých údajov. Prístup k spracovávaným citlivým údajom na zariadení musí byť zamedzený iným osobám alebo automatizovaným prostriedkom šifrovaním a autentizáciou.
11) Zamestnanec si pri práci s citlivými údajmi na takomto zariadení musí byť vedomý rizika, ktoré vyplýva z práce na neznámych a nezabezpečených WiFi sieťach a za prenos citlivých údajov cez takéto siete preberá plnú zodpovednosť.
12) Pokiaľ zamestnanec uchováva na zariadení citlivé údaje, je povinný tieto údaje uchovávať v zašifrovanej časti pamäťového média, SD karty alebo pamäti zariadenia.
13) **Krádež alebo strata mobilného zariadenia sa považuje za kybernetický bezpečnostný incident.**

7 PRAVIDLÁ VZDIALENÉHO PRÍSTUPU DO POČÍTAČOVEJ SIETE

1) Pokiaľ sa zamestnanec pripája na diaľku na súkromnom počítači, musia na ňom byť zapnuté automatické aktualizácie softvéru. Minimálne pre operačný systém, internetový prehliadač a antivírový program.
2) Všetky (pracovné aj súkromné) počítače, pracovné stanice, tablety, mobilné zariadenia alebo notebooky musia byť chránené antivírovým programom.
3) Do aplikácií, ktoré zabezpečujú vzdialený prístup do siete zamestnávateľa, nesmú byť zapamätané prihlasovacie údaje, najmä heslá. Je potrebné vždy pri každom vzdialenom prístupe zadávať prihlasovacie údaje.

4) K informačnému systému (pracovná stanica, mobilné zariadenie, notebook a podobne), použitému na vzdialené pripojenie by mal mať prístup len zamestnanec, ktorý vzdialene pristupuje do siete zamestnávateľa.
5) Vzdialené pripájanie sa musí uskutočniť cez softvér, ktorý ma zabezpečenú komunikáciu medzi klientami ako napríklad TemViewer, Desktop Anywhere alebo iné. Je možné taktiež použiť privátny VPN tunel.
6) Pre pripájanie tretích strán ako napríklad správa informačných systémov, cloudových služieb, mailových služieb, vzdialenú správu softvérového vybavenia, je potrebné zabezpečiť, aby každý prístup bol zaznamenaný systémom a prevádzkovateľ základnej služby bol o takomto prístupe upovedomený.
7) Ak je možné, odporúča sa na vzdialené pripájanie použiť dvoj faktorovú autentifikáciu.

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 E-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 PZS alebo k iným škodám,
   c) prípadný prenos citlivých 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 e-mailovej správy a na prenos správ používať všeobecne dané dátové štandardy.
4) Pri posielaní citlivých 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 PZS žiadne e-maily, prílohy alebo uverejnenia na internetovú stránku bez autorizácie vedúcim zamestnancom, ktorý je oprávnený robiť rozhodnutia v mene PZS a jeho reprezentovať.
8) Zamestnanci nesmú posielať e-maily, ktoré by mohli poškodiť dobré meno PZS alebo jeho vzťahy s klientmi, alebo ktoré môžu priviesť klientov PZS 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.
11) **Porušenie ustanovení tohto článku sa považuje za kybernetický bezpečnostný incident.**

10 ŠIFROVANIE A KRYPTOGRAFICKÉ OPATRENIA

1) Zamestnanci, ktorí prenášajú citlivé údaje na USB zariadeniach, notebookoch a prostredníctvom e-mailovej komunikácie, sú povinní tieto dáta šifrovať pridelenými technickými prostriedkami. **Nedodržanie tohto nariadenia sa považuje za kybernetický bezpečnostný incident.**
2) Prenos citlivých údajov mimo budovu prevádzkovateľa alebo ďalšie priestory prevádzkovateľa prostredníctvom externých pamäťových médií je možný len v zašifrovanej podobe alebo médiami kryptovanými silným heslom.
3) 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 PZS, musia byť zmazané, ak už nie sú ďalej potrebné. Zmazanie je potrebné spraviť formou bezpečného vymazania. Za zmazanie zodpovedá zamestnanec, ktorý povolil odnos médií z priestorov PZS.
2) Pre všetky médiá s citlivými údajmi odnášané z priestorov PZS 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 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 PZS 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 PZS alebo ním poverení zamestnanci.
3) Zamestnanec je oprávnený podpísať dokument v mene PZS 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 PZS, je povinný zdržať sa podpisovania a bezodkladne požiadať o zrušenie mandátneho certifikátu. O tejto skutočnosti je povinný oboznámiť vedenie PZS.
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 PZS.

13 ELEKTRONICKÁ SCHRÁNKA

1) Do elektronickej schránky má prístup štatutár PZS 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 PZS 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 osoba používa zverené zariadenia na plnenie svojich úloh, musí tieto informačné aktíva vrátiť PZS alebo ním poverenej osobe zodpovednej za prevzatie zverených zariadení. O takomto odovzdaní sa vykoná písomný záznam 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), svoje meno a podpis.
2) Pred ukončením pracovnej zmluvy alebo inej zmluvy, na základe ktorej sa osoba - zamestnanec - stal oprávnenou osobou a používa e-mailové schránky pridelené PZS, je táto osoba povinná prehlásiť, že e-mailové správy, ktoré boli v jej používaní, sú služobného charakteru a môžu sa používať pre potreby prevádzkovateľa.
   Prehlásenie by malo byť súčasťou odovzdávacieho protokolu alebo výstupného listu. Povinnosťou odchádzajúceho zamestnanca je odstrániť z e-mailovej schránky správy,

ktoré nemajú služobný charakter. Na správy v e-mailových schránkach odchádzajúceho zamestnanca bude Prevádzkovateľ nahliadať ako na správy bezvýhradne prináležiace PZS.

3) Po ukončení pracovnej zmluvy alebo inej zmluvy, na základe ktorej sa osoba - zamestnanec - stal 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 osobitnom tlačive alebo ako súčasť výstupného listu.
4) Po ukončení pracovnej zmluvy alebo inej zmluvy, na základe ktorej sa osoba – zamestnanec - stal oprávnenou osobou a má zverené kľúče, alebo iné prístupy do priestorov PZS (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 PZS, prípadne na personálnom oddelení. O odovzdaní je potrebné spraviť záznam na osobitnom tlačive alebo ako súčasť výstupného listu.

15 ZÁVEREČNÉ USTANOVENIA

1) Táto smernica nadobúda platnosť dňom jej podpisu a účinnosť od 1.5.2024.
2) Prevádzkovateľ je povinný s touto smernicou oboznámiť všetkých zamestnancov.

Obecný úrad Lomnička
Lomnička 66
065 03 Podolínec

Zoznam osôb, ktoré boli oboznámené so Smernicou pre používanie IT aktív - pre zamestnancov

P.č.	Meno a priezvisko	Funkcia	Dátum	Podpis
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				