Obecný úrad Lomnička
Lomnička 66
065 03 Podolínec

Smernica pre používanie IT aktív – pre správcov informačných systémov

Obec Lomnička

Verzia:	01.42
Platné od:	
Stav dokumentu:	Finálny
Dôvernosť dokumentu:	Interný
Typ dokumentu:	Smernica pre používanie IT aktív – pre správcov IS
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 — 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.

Aktíva informačných technológií (IT aktíva) — všetky technické a softvérové prostriedky, ktoré slúžia na ukladanie, prenos a spracúvanie 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.

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 — 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.

Externá organizácia — organizácia alebo spoločnosť vstupujúca do Informačného systému za účelom jeho údržby alebo obnovy.

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.

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 prevádzkovateľa.

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

3 AKTÍVA INFORMAČNÝCH TECHNOLÓGIÍ A OPERAČNÝCH TECHNOLÓGIÍ

1) Správa IT/OT aktív musí byť organizovaná tak, aby sa minimalizovala hrozba zneužitia postavenia administrátora.

2) Za ochranu údajov je zodpovedný ten správca IT/OT aktíva, na ktorého technických prostriedkoch (pamäťových médiách) sú tieto údaje uložené. Na tento účel správca IT/OT 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 údajov šifrovaním alebo elektronickým podpisom.

3) Správca IT/OT 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 firewall.
4) Správca IT/OT 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/OT aktíva povinný overiť, či neboli vydané nové verzie softvéru.
5) Zakazuje sa používame programov, ktoré nemajú garanciu výrobcu o ich spoľahlivosti alebo neboli overené správcom IT/OT aktíva v izolovanom prostredí, či neobsahujú nežiadúce funkcie a chyby. Overenie sa vykonáva tak, aby nemohlo dôjsť k ohrozeniu IT/OT aktív, pričom sa musí preveriť najmä správame programu v sieťovom prostredí vo vzťahu k údajom uloženým na pamäťovom médiu počítača.
6) Pri konfigurácii prostriedkov, programov a služieb správca IT/OT aktíva dbá na to, aby sa používali len tle prostriedky, programy a služby, ktoré sú nevyhnutné pre plnenie pracovných úloh a potrieb Prevádzkovateľa. Zakazuje sa používanie programov, sieťových služieb a IT/OT 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/OT 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 citlivých 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 miestnosti, kde sú umiestnené servery.

5 ZÁLOHOVANIE A ARCHIVOVANIE ÚDAJOV

1) Správca IT/OT 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/OT aktíva Je povinný raz za šesť mesiacov otestovať funkčnosť záložného média a raz za rok funkčnosť archívneho médiá. Funkčnosť otestuje skopírovaním súborov z média alebo rozbalením komprimovaných archívov.

6 AUTENTIZÁCIA

1) Správca IT/OT 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 3 mesiace. 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/OT 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/OT 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/OT 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/OT aktíva v rozhodnutí o pridelení správy aktíva.
9) Začiatok, zmenu alebo ukončenie pracovného pomeru zamestnanca oznámi príslušný vedúci oddelenia alebo útvaru správcovi IT/OT aktíva, ktorý vydáva autentizačné údaje a prostriedky.
10) Personálne oddelenie musí zabezpečiť navrátenie pridelených zariadení a navrátene informačných aktív, odstránenie informácií oprávnenej osoby z pridelených zariadení a odovzdane 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/OT 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/OT 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/OT aktíva odovzdá nainštalovanú pracovnú stanicu používateľovi, ktorý prevzatie potvrdí podpisom na preberacom protokole.

5) Pri odovzdaní nainštalovanej pracovnej stanice je správca IT/OT 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 používame prenosných USB zariadení. Tento zoznam je definovaný v internej smernici.
7) Na pracovných staniciach, na ktorých je povolené používame 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 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 citlivých 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 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 verne 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 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.

11 SERVERY A OSTATNÁ IT/OT TECHNIKA V ZABEZPEČENÝCH PRIESTOROCH

1) Servery a ostatná IT/OT technika, ktorá spracováva alebo uchováva 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/OT 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 evidencií 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/OT technike, ktorá spracováva alebo uchováva údaje mimo pracovných staníc tak, ako keby mal zriadenú serverovňu.

12 ANTIVÍRUSOVÁ OCHRANA

1) Správca IT/OT 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/OT aktíva je povinný venovať zvýšenú pozornosť tomu, aby škodlivý kód nebol zavedený počas výkonu pohotovostných procedúr alebo procedúr údržby.
3) Správca IT/OT aktíva je povinný zabezpečiť inštaláciu a pravidelnú aktualizáciu antivírusových detekčných a nápravných softvérov na prehliadame počítačov, serverov a médií na rutinnej báze.

4) Správca IT/OT aktíva zabezpečí, ak je to potrebné, za účelom zníženia nebezpečenstva vniknutia vírusu, vypnutie automatického zavádzania USB, CD, DVD a iných externých zariadení, tzv. "Autorun".

13 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 aktuálnej smernice prideľuje autentifikačné prostriedky.
4) Správca IT aktíva je povinný v zmysle článku 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.

14 PRÍSTUP DO SIETE INTERNET A E-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 unikátnu emailovú adresu.
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 a to:
   a) veľkosť poštovej schránky je obmedzená nastavením mailového servera,
   b) veľkosť jednej poštovej správy je obmedzená nastavením mailového servera,
   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.

15 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 a musí byť použitá dvojfaktorová autentifikácia.
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.

16 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 bezpečnostným správcom. 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 získavame 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 citlivých údajov zabezpečený predpísanými kryptovacími prostriedkami. Inštaláciu týchto prostriedkov zabezpečuje správca IT aktíva.

5) Zamestnanci, ktorí prenášajú citlivé 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.

17 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.
2) Pre všetky médiá s citlivými 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 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.

18 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 bezpečnostného správcu.
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 uložene a ochranu údajov potrebných k vyhotoveniu kvalifikovaného systémového certifikátu.
5) Rovnako správca IT aktíva zodpovedá za platnosť údajov potrebných na vyhotovenie kvalifikovaného systémového certifikátu.

19 ELEKTRONICKÁ SCHRÁNKA

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

20 PREMIESTŇOVANIE A LIKVIDÁCIA IT AKTÍV

1) Pri premiestňovaní IT/OT aktíva zaznamená správca IT/OT aktíva, kedy a ku komu bolo IT/OT aktívum premiestnené, účel premiestnenia a dátum vrátenia aktíva do pôvodných priestorov.
2) Pri premiestnení IT/OT aktíva do servisu alebo inej organizácie, kde bude mimo dosahu zamestnancov Prevádzkovateľa, je potrebné, ak Je to možné, odstrániť z pevného disku všetky údaje, prípadne urobiť hĺbkové sformátovane 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/OT aktíva rozhoduje správca IT/OT aktíva, pričom o tejto skutočnosti informuje vedenie Prevádzkovateľa a urobí záznam o likvidácii aktíva
4) Ak likvidované IT/OT aktívum obsahuje pevný disk alebo iné úložisko s citlivými údajmi, je správca IT/OT aktíva povinný, ak je to možné, tieto údaje neobnoviteľne zlikvidovať. Nedodržanie tejto zásady sa považuje za bezpečnostný incident.

21 ZAMESTNANCI EXTERNEJ ORGANIZÁCIE

1) Prístup zamestnancov externej organizácie zriaďuje správca IT/OT aktíva na základe schválenia Prevádzkovateľom správca IT/OT aktíva vedie zoznam povolených prístupov k jednotlivým aktívam.
2) Správca IT/OT aktíva zriadi zamestnancovi externej organizácie prístupové práva podľa tejto smernice.
3) Správca IT/OT aktíva Je povinný zabezpečiť bezpečný šifrovaný prístup zamestnanca tretej strany k jeho aktívu.
4) Zamestnanci externej organizácie sú povinní pred prihlásením k IT/OT aktívu o tejto skutočnosti informovať správcu IT/OT aktíva buď prostredníctvom mailu alebo telefonicky k tejto povinnosti musí byť externá organizácia zmluvne zaviazaná. Na základe tohto oznámenia im správca IT/OT aktíva povolí pripojenie. Po skončení údržby alebo inej činnosti zamestnancom externej organizácie, správca IT/OT aktíva zruší možnosť pripojenia.

5) Správca IT/OT aktíva je povinný poučiť zamestnancov externej organizácie, ktorí prichádzajú do styku s citlivými údajmi, o ich ochrane a o povinnosti zachovávať mlčanlivosť. Táto skutočnosť musí byť uvedená v príslušnej zmluve s takouto externou organizáciou.

22 ZÁVEREČNÉ USTANOVENIA

1) Táto smernica nadobúda platnosť dňom jej podpisu a účinnosť od 1.5.2024.
2) Prevádzkovateľ je povinný s touto smernicou oboznámiť zamestnancov informatiky alebo správy IT/OT a vedenie Prevádzkovateľa.

Obecný úrad Lomnička
Lomnička 66
065 03 Podolínec

Zoznam osôb, ktoré boli oboznámené so Smernicou pre používanie IT aktív pre správcov informačných systémov

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