Interná smernica č. 1/2024
o kybernetickej bezpečnosti

Článok 1 - Úvodné ustanovenia

(1) Zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti sa do slovenského právneho poriadku transponuje smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (ďalej aj len „smernica“). Cieľom smernice, rovnako ako aj zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti (ďalej len „zákon“), je zaistiť ochranu informačných systémov a sietí pred narušením buď samotných technických zariadení, alebo údajov, ktoré sa v nich spracovávajú, alebo služieb, ktoré sa pomocou nich poskytujú.

(2) Informačný systém verejnej správy je v zmysle § 3 písm. k) druhého bodu zákona č. 69/2018 Z. z. zaradený medzi základné služby.

Článok 2 - Chránené priestory

(1) Chránená miestnosť je osobitne určená samostatná miestnosť, ktorá je stavebne alebo inak fyzicky oddelená od zvyšku chráneného priestoru alebo od nechránených priestorov, pričom slúži najmä na centralizovanie aktív a systematické uchovávanie osobných údajov v akejkoľvek elektronickej, písomnej alebo inej forme; za chránenú miestnosť môže byť považovaný aj osobitne zabezpečený odkladací priestor (napr. trezor, iné pevné uzamykateľné priestory); do chránenej miestnosti je regulovaný fyzický prístup zamestnancov a iných osôb a je vo zvýšenej miere zabezpečená prijatím vhodných technických bezpečnostných opatrení, realizovaných prostriedkami fyzickej povahy.

(2) Ochrana kancelárií:

a. označenie miestnosti – číselné označenie a spravidla pri kanceláriách aj označenie zamestnancov využívajúcich chránenú miestnosť titulom, menom, priezviskom a funkciou v organizácii,
b. počet vstupných dverí – každá chránená miestnosť má vlastné vstupné dvere,
c. konštrukcia dverí – pevné, uzamykateľné,
d. zabezpečenie vstupných dverí – pridelením kľúča,
e. zabezpečenie okien – okná nie sú zabezpečené zvýšenou mechanickou ochranou,
f. ochrana vstupu v pracovnej dobe – prístup je umožnený len príslušným pracovníkom, cudzie osoby môžu do miestnosti vstupovať len v sprievode,
g. bezpečnostné opatrenia – ochrana objektu, dostatočné zabezpečenie vstupu do chránených priestorov, obmedzenie prístupu do kancelárie iba pre konkrétneho zamestnanca.

(3) Ochrana serverovne:

a. označenie miestnosti – bez označenia,
b. počet vstupných dverí – jedny,
c. konštrukcia dverí – pevné, uzamykateľné,
d. zabezpečenie vstupných dverí – pridelením kľúča,
e. zabezpečenie okien – okná nie sú zabezpečené zvýšenou mechanickou ochranou,
f. zabezpečenie priestoru serverovne – požiarnym hasiacim prístrojom,
g. ochrana vstupu v pracovnej dobe – nepovolané osoby smú do serverovne vstupovať len v sprievode oprávnenej osoby,
h. bezpečnostné opatrenia – ochrana objektu, dostatočné zabezpečenie vstupu do chránených priestorov, obmedzenie prístupu do miestnosti len na nevyhnutný okruh oprávnených osôb a ďalších fyzických osôb zabezpečujúcich údržbu a technickú podporu v sprievode oprávnených osôb,
i. vlastní zamestnanci – iba správca informačných technológií bez obmedzenia,
j. upratovacia služba a návštevy – bez prístupu.

(4) Kontrola pohybu v chránených priestoroch:

a. vlastní zamestnanci – bez obmedzenia v rámci pridelených oprávnení a kľúčov od miestností, v ktorých vykonávajú pracovné činnosti,
b. zamestnanci externých dodávateľov – pohyb výlučne pod dohľadom povereného zamestnanca obce,
c. upratovacia služba – do niektorých chránených miestností môže byť zamietnutý prístup (napr. serverovňa),
d. správca budovy – iba na základe vopred oznámenej žiadosti a za prítomnosti povereného zamestnanca obce.

Článok 3 - Politika používania informačných technológií

(1) Správca informačných technológií (ďalej len „správca):

a. inštaluje systémové programy (predovšetkým operačné systémy),
b. manipuluje s diskovými médiami a tlačiarňami,
c. je zodpovedný za plnú prevádzkyschopnosť systémových prostriedkov a nástrojov,
d. na základe povolení zriaďuje nové používateľské kontá, prideľuje pre ne základné prístupové práva, preveruje oprávnenosť prístupových práv a používateľských kont a na základe povolenia ruší používateľské kontá. Pri prideľovaní prístupového práva sa uplatňuje nasledujúci postup:
    1. žiadosť – používateľ prostredníctvom starostu obce požiada o pridelenie prístupu;
    2. schválenie – starosta obce žiadosť schváli alebo zamietne;
    3. pridelenie prístupu – správca na základe pokynu od starostu obce pridelí prístup,

e. zodpovedá za zálohovanie a archiváciu systémových a používateľských dát v zdieľanom priestore, za archív a vedenie evidencie záložných médií a ich bezpečné uloženie,
f. pravidelne kontroluje stav technických súčastí informačného systému,
g. raz týždenne nastavuje a kontroluje stav serverov,
h. podľa požiadaviek bezpečnostnej politiky nastavuje prístupové práva na aktívnych sieťových prvkoch a komunikačných zariadeniach,
i. pravidelne monitoruje stav siete pomocou programových nástrojov pre riadenie siete,
j. udržuje v aktuálnom stave informácie o topológii siete, aktívnych a pasívnych prvkoch, o ich parametroch a nastaveniach,
k. zriaďuje, eviduje a ruší kontá používateľov a skupín, pravidelne preveruje oprávnenosť používateľských kont, prípadne prístupových práv,
l. rieši havarijné stavy, obnovuje dáta, funkčnosť databáz a konzultuje neštandardné stavy s dodávateľskými firmami,
m. testuje a nasadzuje nové databázové softvéry, prípadne ich update a upgrade,
n. zálohuje databázy a kontroluje pravidelnosť a spoľahlivosť prevádzky z hľadiska obnovy databáz po poškodení dát a obnovy databáz k dátumu,
o. kontroluje v logovacích súboroch oprávnenosť vstupu do databázy (ochrana pred neoprávneným vstupom), zisťuje či bola prekonaná bezpečnostná brána a v prípade, že bola prekonaná, preveruje postup jej prekonania,
p. spolupracuje s ostatnými oddeleniami pri testovaní, výberovom konaní pre nový softvér. Tvorí a spolupodieľa sa na tvorbe návrhov smerníc, upresnení a školení súvisiacich s bezpečnosťou informačných systémov,
q. nastavuje bezpečnostné charakteristiky pre jednotlivé komponenty informačného systému vrátane komunikačných prvkov,
r. vyhodnocuje a spravuje kontrolné záznamy,
s. vykonáva bezpečnostné školenia používateľov,
t. kontroluje fyzickú bezpečnosť počítačového vybavenia a serverovne, archívnych médií a výstupných zariadení (tlačiarne, zapisovače, atď.),
u. kontroluje prístup k zariadeniam systému,
v. kontroluje bezpečné uloženie záložných médií a archívov,
w. kontroluje a spravuje systém prihlasovania užívateľov a stanovuje maximálnu dobu životnosti hesiel podľa bezpečnostnej politiky,
x. riadi a zabezpečuje päťročnú archiváciu súborov týkajúcich sa bezpečnostných záznamov operačného systému a dôležitých aplikácií,
y. analyzuje prieniky do informačných systémov, vytvára, optimalizuje a spravuje bezpečnostnú politiku,
z. odstraňuje technické poruchy a závady na zariadeniach IT a to buď svojpomocne, napr. výmenou súčiastky, časti dielu alebo celého dielu za nový v rámci záručných podmienok, alebo formou doručenia chybného zariadenia do príslušného servisného strediska alebo dohovoru o oprave cez dodávateľa daného zariadenia,
aa. realizuje technické prepojenia lokálnych počítačových sietí na súčastiach a pracoviskách,
bb. pripája zariadenia IT do elektrickej siete napájania a do počítačovej siete/prepája jednotlivé zariadenia IT medzi sebou,

cc. vykonáva previerku zariadení IT, ktoré podliehajú pravidelnému technickému auditu.

(2) Používateľ informačných technológií

a. používa počítač, operačný systém na ňom nainštalovaný, ako aj všetky aplikácie, na ktoré dostal oprávnenie,
b. prihlasuje sa do počítačovej siete a používa zdieľané súbory, databázy, aplikácie, tlačiarne, či iné zariadenia podľa práv, ktoré mu boli pridelené jeho priamym nadriadeným,
c. je preukázateľne poučený o povinnosti dodržiavať túto smernicu a riadiť sa ňou pri svojej práci,
d. riadi sa pokynmi správcu a obracia sa naňho v prípade závad, porúch a mimoriadnych situácií,
e. dbá na ochranu spracovávaných dát,
f. počítače a ostatné zariadenia informačných technológií používa výhradne na služobné účely vyplývajúce z jeho popisu pracovnej činnosti,
g. na iné účely použitia zariadení informačných technológií potrebuje písomný súhlas starostu obce,
h. je povinný chrániť prístupové heslá k informačnému systému, operačnému systému, pošte, vzdialenému prístupu a iným heslom chráneným prístupom,
i. zariadenia sú k perifériám zverené bez obmedzovania prístupu a bez obmedzenia internetu, pričom sa predpokladá, že používateľ si je po zaškolení vedomý rizík vyplývajúcich z používania tohto zariadenia,
j. technika obsahuje antivírový softvér, ktorý sa sám aktualizuje a aktualizácie operačného systému sa preberajú a inštalujú automaticky,
k. v prípade upozornenia používateľa na spustenie aktualizácie operačného systému, je nutné túto aktualizáciu v čo najbližšom možnom čase vykonať,
l. pri akejkoľvek zmene, týkajúcej sa používateľa, majúcej vplyv na používanie softvéru sa postupuje podaním novej žiadosti podľa odseku 1, písm. d).

(3) Používateľ internetu je zamestnanec prevádzkovateľa, ktorému bolo pridelené používateľské konto, resp. iným spôsobom umožnený prístup do celosvetovej počítačovej siete Internet.

(4) Používateľ intranetu je zamestnanec prevádzkovateľa, ktorému bolo pridelené používateľské konto a heslo, na základe ktorého mu bol umožnený prístup do vnútropodnikovej siete.

(5) Používateľom elektronickej pošty (e-mailu) je zamestnanec prevádzkovateľa, ktorému bolo pridelené používateľské konto na používanie elektronickej pošty.

(6) Používateľom elektronickej registratúry je zamestnanec prevádzkovateľa, ktorému bolo pridelené používateľské konto, na základe ktorého mu bolo umožnené používanie elektronickej registratúry.

(7) Za zamestnanca sa pre účely tejto smernice považujú všetci kmeňoví zamestnanci prevádzkovateľa, ale aj externí zamestnanci, ktorí majú

s prevádzkovateľom pracovnoprávny vzťah, prípadne iný zmluvný vzťah. Na vstup do informačného systému je každému pridelené prihlasovacie meno a heslo.

Článok 4 - Používanie hardvéru

(1) Na pracoviskách prevádzkovateľa sa používa iba taký hardvér, ktorý je schválený starostom obce a je evidovaný v evidencii majetku obce.

(2) Akýkoľvek iný hardvér sa zakazuje používať.

(3) Zakazuje sa akýkoľvek zásah do hardvéru alebo jeho konfigurácie, jeho svojvoľné premiestňovanie, či výmena. Výkonom tejto činnosti je poverený správca.

(4) Používatelia, ktorým boli zverené alebo zapožičané prenosné notebooky, telefóny, prípadne akékoľvek iné zariadenia, sú povinní s nimi nakladať tak, aby nedošlo k ich strate, zneužitiu či krádeži, nesmú ich požičať, prenechať, odovzdať tretej osobe, či u tretej osoby takéto zariadenie založiť formou záložného práva.

(5) Poruchy hardvéru sa nahlasujú správcovi, ktorý sa okamžite, prípadne podľa dohody postará o nápravu, opravu alebo výmenu poruchového hardvéru.

(6) Kľúčové servery sú umiestnené v serverovni.

(7) Servery sú k elektrickému rozvodu pripájané cez UPS záložné zdroje.

(8) Na serveroch sa pravidelne vykonávajú aktualizácie operačného systému a programov.

(9) Kontrola dátových diskov aj antivírová kontrola sa vykonáva podľa plánu kontrol.

(10) Zálohovanie sa vykonáva v čase mimo pracovnej doby, prípadne v čase najnižšieho používania a to dvojúrovňovo. Prvá záloha sa ukladá na vnútorný disk servera, ale nie na disk, kde je umiestnená databáza IS. Druhá záloha sa vytvorí po ukončení zálohovania skopírovaním zálohy na archívne úložisko. Tým sa zároveň kontroluje jej použiteľnosť.

(11) Zálohy databáz informačného systému sa archivujú na samostatných offline diskoch.

(12) Zálohy databáz sa udržujú v archíve minimálne týždeň. Okrem toho sa archivuje aj niekoľko mesačných záloh.

Článok 5 - Používanie softvéru

(1) Pri práci s počítačom je zakázané pracovať s iným softvérom, než aký bol nainštalovaný, resp. schválený.

(2) Používateľ používa len taký softvér, na ktorého používanie má podľa schválenia nárok.

(3) Pri akejkoľvek zmene týkajúcej sa používateľa, ktorá má vplyv na používanie softvéru, je používateľ povinný požiadať starostu obce o vykonanie takejto zmeny.

(4) Po zakúpení softvér inštaluje správca, alebo zamestnanci dodávateľskej firmy za prítomnosti správcu.

(5) Poruchu softvéru sa nahlasujú správcovi. Ten sa okamžite, prípadne podľa dohody postará o nápravu poruchy softvéru.

(6) Na hardvérovom vybavení sa zakazuje používať, uchovávať alebo distribuovať akýkoľvek nelegálny softvér a iné nedovolené údaje.

Článok 6 - Používanie služieb internetu, intranetu a elektronickej pošty a registratúry

(1) Prevádzkovateľ používa alebo môže používať softvér a systémy, ktoré umožňujú monitorovať a zaznamenávať všetky použitia celosvetovej počítačovej siete Internet a elektronickej pošty. Systémy môžu zaznamenávať prístup na webové stránky, diskusné skupiny, použitie elektronickej pošty, prenos súborov medzi prevádzkovateľom a inými subjektami.

(2) Používateľ Internetu a elektronickej pošty musí vedieť, že prevádzkovateľ má právo v súlade s platnou legislatívou preverovať použitie týchto prístupov.

(3) Prevádzkovateľ má právo nariadiť kontrolu všetkých dát a akýchkoľvek súborov, ktoré sú uložené na lokálnych diskoch počítačov používateľov, alebo v ich domovských adresároch na serveroch prevádzkovateľa.

(4) Zakazuje sa zobrazovanie, archivovanie, uchovávanie, rozširovanie, spracovávanie alebo zaznamenávanie akéhokoľvek obrázku, či dokumentu s jednoznačným sexuálnym obsahom.

(5) Zakazuje sa používať elektronickú poštu na posielanie, preposielanie a rozširovanie pošty zábavného charakteru a charakteru, ktorý priamo nesúvisí s výkonom pracovnej činnosti.

(6) Prístup na Internet a elektronickú poštu sa nesmie vedome použiť na porušenie všeobecne záväzných právnych predpisov Slovenskej republiky alebo medzinárodných zmlúv, ktorými je Slovenská republika viazaná.

(7) Akýkoľvek softvér alebo súbor získaný prostredníctvom Internetu a uložený na lokálnej sieti prevádzkovateľa, alebo na lokálnom disku používateľa, sa stáva majetkom prevádzkovateľa. Všetky takéto súbory, dokumenty alebo softvér, sa môžu používať výhradne spôsobom, ktorý je v súlade s udelenými licenciami, autorskými

právami, resp. ich odsúhlasil správca a musia priamo súvisieť s pracovnými povinnosťami používateľa.

(8) Zakazuje sa získavanie a následné ukladanie zábavného softvéru alebo hier, videí, obrázkov a zvukových súborov z Internetu alebo prostredníctvom elektronickej pošty, hranie hier na Internete. Takisto sa zakazuje rozširovanie akéhokoľvek softvéru či údajov, ktoré sú majetkom prevádzkovateľa bez jeho predchádzajúceho písomného súhlasu.

(9) Používateľom Internetu a elektronickej pošty sa zakazuje využívať svetovú počítačovú sieť Internet a elektronickú poštu na zámerné rozširovanie akýchkoľvek vírusov, červov, trójskych koní alebo iného škodlivého softvéru. Takisto používateľ nesmie využiť či zneužiť prístup na Internet či elektronickú poštu na vyradenie, preťaženie alebo oklamanie akéhokoľvek počítačového systému alebo počítačovej siete a tým narušiť súkromie alebo bezpečnosť iného používateľa či spoločnosti.

(10) Vyjadrovať sa v mene prevádzkovateľa, alebo jeho súčastí do akýchkoľvek diskusných skupín môžu len zamestnanci, ktorí sú riadne poverení komunikáciou s médiami. Ostatní používatelia Internetu a elektronickej pošty sa môžu zúčastňovať na diskusiách a fórach v priebehu pracovnej doby, ak sa to vzťahuje na ich odbornú činnosť, ale v tom prípade vystupujú ako jednotlivci vo vlastnom mene a sú povinní informovať ostatných zúčastnených, že nie sú oprávnení vystupovať v mene prevádzkovateľa, alebo jeho súčastí. Pri účasti v týchto diskusiách a fórach je používateľ Internetu a elektronickej pošty povinný zdržať sa akýchkoľvek politických, náboženských, rasových prejavov, prejavov neznášanlivosti a prejavov urážajúcich ľudskú dôstojnosť, či prejavov týkajúcich sa trestnej činnosti.

(11) Používateľ Internetu, intranetu a elektronickej pošty nesmie zverejňovať údaje a dôverné informácie o prevádzkovateľovi. Používatelia Internetu a elektronickej pošty môžu počas obednej alebo inej prestávky, alebo po pracovnej dobe využívať prístup na Internet a elektronickú poštu pre prieskum alebo prezeranie informačných zdrojov nesúvisiacich s náplňou práce len so súhlasom starostu obce a za predpokladu, že budú dodržané všetky ustanovenia tejto smernice. Porušenie tohto ustanovenia je závažným porušením pracovnej disciplíny a môže mať za následok okamžité skončenie pracovného pomeru zamestnanca.

(12) Prevádzkovateľ je v zmysle príslušných zákonných ustanovení povinný poskytnúť orgánom činným v trestnom konaní všetky dostupné záznamy, týkajúce sa prístupu na Internet, intranet a elektronickú poštu príslušného používateľa Internetu a elektronickej pošty.

(13) Používateľ Internetu a elektronickej pošty sa musí riadiť všeobecne záväznými právnymi predpismi, autorským právom, či obchodnými značkami.

(14) Používateľ elektronickej registratúry má vlastný účet do registratúry a heslo s ktorým sa prihlasuje do systému.

(15) Zamestnanec podateľne má právo prezerať, skenovať a archivovať všetku prijatú poštu.

Článok 7 - Narušenie technicko-softvérovej bezpečnosti

(1) Správca zabezpečuje správu, údržbu, servis a ďalšie činnosti spojené s prevádzkovaním informačného systému, rieši všetky požiadavky obsluhy, prijíma informácie o poruchách aj bezpečnostných incidentoch.

(2) Zamestnanec pri podozrení z narušenia bezpečnosti zvereného počítača alebo v prípade výskytu bezpečnostného incidentu upovedomí o tejto skutočnosti správcu a spolupracuje s ním na náprave alebo riešení incidentu.

(3) Pri odstraňovaní porúch kľúčových komponentov informačného systému je správca oprávnený vyhlásiť technickú odstávku na nevyhnutný čas potrebný na odstránenie poruchy.

(4) Bezpečnosť databáz a aplikácií zabezpečuje správca v spolupráci s poverenými pracovníkmi jednotlivých pracovísk.

(5) Riešenie nepredvídaných udalostí informačného systému je štandardne zabezpečené správcom informačných technológií počas pracovnej doby 7.00 – 13.00.

(6) V prípade nepredvídanej situácie je správca oprávnený (podľa možnosti po predchádzajúcom upozornení používateľov) vyhlásiť technickú odstávku systému na nevyhnutný čas, potrebný pre riešenie udalosti.

(7) Riešenie každého bezpečnostného incidentu musí byť správcom primerane zdokumentované. Dokumentuje sa predovšetkým príčina vzniku incidentu (pokiaľ je známa), dôsledky, všetky opatrenia prijaté pri riešení incidentu a ich účinnosť, ako aj zistené nedostatky v existujúcom pláne pre prípad nepredvídanej situácie.

(8) Priority pri riešení bezpečnostného incidentu:

a. bezodkladné obnovenie bežnej prevádzky informačného systému aspoň v núdzovom režime, zabezpečenie ochrany údajov, zachovanie dôkazového materiálu nevyhnutného na ďalšiu analýzu príčin vzniku bezpečnostného incidentu,
b. zistenie príčin, ktoré viedli k vzniku bezpečnostného incidentu,
c. určenie zodpovednosti za vznik bezpečnostného incidentu a vyvodenie dôsledkov,
d. zovšeobecnenie zistených skutočností a návrh opatrení na zabránenie opakovanému výskytu bezpečnostného incidentu.

(9) Preventívne opatrenia:

a. správca alebo poverená externá dodávateľská firma sú povinní pravidelne vykonávať základnú preventívnu kontrolu kľúčových komponentov informačného systému (testovanie systému, odstránenie nepotrebných súborov, posúdenie rýchlosti zapĺňania pamäťovej kapacity, množstvo a vek životnosti médií používaných na zálohovanie, previerka na výskyt nových programov v systéme, vyčistenie komponentov systému a podobne). Na tento účel je možné vyhlásiť odstávku systému na nevyhnutne potrebnú dobu. Termín odstávky sa stanoví tak, aby čo najmenej narušil bežnú činnosť používateľov. O tomto termíne sa používatelia oboznámia s dostatočným predstihom;
b. správca je povinný pravidelne vykonávať základnú preventívnu kontrolu zameranú na preverenie funkčnosti komponentov nevyhnutných pre riešenie nepredvídaných situácií (zariadenie pre zálohovanie a obnovu údajov, médiá so záložnými kópiami údajov a programov, záložné zdroje, aktuálnosť zálohovaných prístupových hesiel a ďalších uchovávaných parametrov systému);
c. správca pomáha používateľom na jednotlivých pracoviskách riešiť problémy, ktoré sa objavia pri práci so systémom. V prípade opakovaného výskytu problémov z dôvodu nedostatočnej kvalifikácie, resp. schopností užívateľa pracovať s informačným systémom, je správca oprávnený upozorniť starostu obce na zistené nedostatky a potrebu nápravy.

(10) Prístup do priestorov centrálneho servera má len správca a starosta obce, ostatné osoby sa môžu v týchto priestoroch zdržiavať len so súhlasom správcu alebo starostu obce.

(11) V prípade, že sa na pracovnej ploche používateľa zobrazí varovanie, že sa na zariadení nachádza vírus, používateľ nesmie toto varovanie ignorovať. V prípade zavírenia pevného disku, USB kľúča a pod., používateľ túto skutočnosť bezodkladne oznámi správcovi, prípadne po konzultácii s ním vykoná antivírové čistenie príslušného pamäťového média. V prípade objavenia vírusu v prijatej elektronickej pošte používateľ o tejto udalosti bezodkladne upovedomí správcu. V žiadnom prípade zavírenú elektronickú poštu neposiela inému adresátovi, a na svojej pracovnej stanici ju uchová len dočasne a len na žiadosť správcu (na účely ďalšej analýzy prieniku vírusu do systému).

(12) Používateľ pracovnej stanice zaznamená a ohlási správcovi každú odchýlku od bežnej činnosti pracovnej stanice, predovšetkým nasledovné udalosti:

a. hlásenia chýb operačného systému a aplikácií, s ktorými používateľ pracuje (presný prepis chybového hlásenia) spolu so stručným popisom situácie (vykonávaných akcií), počas ktorej sa toto hlásenie vyskytlo,
b. problémy s technickými zariadeniami pracovnej stanice spolu s popisom situácie, počas ktorej k problémom došlo (popis akcií, zadávaných údajov alebo viditeľných javov, ktoré predchádzali, resp. nasledovali výskyt problému).

(13) Používateľ pri práci na vlastnej pracovnej stanici alebo pri dočasnom používaní pracovnej stanice pridelenej inému užívateľovi zaznamená a bezodkladne ohlási správcovi a pridelenému používateľovi pracovnej stanice každú udalosť, ktorá by mohla indikovať porušenie bezpečnosti informačného systému, predovšetkým však nasledovné udalosti:

a. výskyt vírusu (prepis varovného hlásenia),
b. únik údajov s informáciou, aké informácie unikli, kam a ako,
c. odcudzenie médií s údajmi z pracovnej stanice,
d. odcudzenie technických zariadení pracovnej stanice,
e. neoprávnený zásah do technických zariadení pracovnej stanice,
f. neoprávnený zásah do programového vybavenia pracovnej stanice (vrátane výskytu nových súborov alebo adresárov na disku pracovnej stanice) alebo do nastavenia jeho parametrov (napr. nastavené zdieľanie disku alebo adresárov pracovnej stanice).

(14) Používatelia sú povinní spolupracovať so správcom pri objasňovaní príčin výskytu bezpečnostných problémov, aby mohli byť následne vykonané opatrenia, ktoré môžu v budúcnosti zabrániť výskytu podobnej situácie.

(15) Používateľ internetu, intranetu, elektronickej pošty a elektronickej registratúry je povinný zachovávať mlčanlivosť o informáciách získaných zo zdrojov prevádzkovateľa. Porušenie tohto ustanovenia je závažným porušením pracovnej disciplíny a môže mať za následok okamžité skončenie pracovného pomeru zamestnanca.

Článok 8 - Preventívne opatrenia proti narušeniu technicko-softvérovej bezpečnosti

(1) Preventívne opatrenia proti havárií informačného systému spôsobené technickou chybou niektorého komponentu centrálneho počítača (serveru):

a. zabezpečenie záložných zdrojov s automatickým vypnutím počítača,
b. monitorovanie činnosti serverov, kontrola chybových hlásení,
c. používanie hot swap diskových polí,
d. zabezpečenie dostatku finančných prostriedkov na obnovu informačného systému (podľa možnosti obmieňať server každých päť rokov),
e. zachovávanie pravidla: novší server sa stáva hlavným, starší záložným,
f. zálohovanie údajov.

(2) Preventívne opatrenia proti vírusovej infiltrácii:

a. zabezpečenie antivírovej ochrany,
b. inštalácia len autorizovaných programov oprávnenými zamestnancami,
c. preverovanie cudzích nosičov (CD, DVD, USB disky...),
d. nepripájanie nepreverených počítačov do LAN bez vedomia správcu,
e. odpájanie nepoužívaných pasívnych rozvodov od aktívnych prvkov LAN,

f. mazanie nevyžiadaných e-mailových príloh bez otvárania,
g. sledovanie aktuálneho diania na LAN a v sieti internet.

(3) Preventívne opatrenia proti neautorizovanému vstupu z internetu:

a. zákaz spúšťania programov z prostredia internetu nepodpísaných certifikačnou autoritou,
b. zákaz sťahovania neautorizovaných programov z prostredia internetu,
c. kontrola a vyhodnocovanie log súborov firewallu, routerov, antivírového programu a pod.,
d. zabezpečenie súborovej integrity operačných systémov a obnovy poškodených alebo infikovaných údajov zo záloh,
e. zvýšenie bezpečnosti firewallov,
f. nastavenie šifrovaných prenosov v LAN,
g. pre prípadný prístup z internetu do lokálnej siete používať výhradne zabezpečenú VPN,
h. inštalácia doplnkových programov, ktoré eliminujú možnosť napadnutia počítača.

(4) Technické narušenie alebo zlyhanie bezpečnosti zariadenia v informačnom systéme (pamäť počítača, procesor, CD/DVD, harddisk, WiFi zariadenie...) je nutné nahlásiť správcovi.

(5) Dôležité aktívne prvky siete je nutné chrániť záložnými zdrojmi elektrickej energie so stabilizátorom sieťového napätia kvôli ochrane pred poruchami napájania.

(6) Preventívne opatrenia pred poruchami aktívnych prvkov siete:

a. monitorovanie činnosti,
b. zabezpečenie dostatočnej kapacity,
c. pripájanie prostredníctvom záložného zdroja,
d. zabezpečenie dostatočnej ochrany pred nepovolaným prístupom.

(7) Ako preventívne opatrenie pred poruchou pasívnej časti siete premeriavať kabeláž, zásuvky a konektory.

(8) Preventívne opatrenia na ochranu pred haváriou databáz:

a. sledovanie konfiguračných súborov,
b. monitorovanie a včasná reakcia na hlásenia programov,
c. denná kontrola chybových hlásení aplikácií a databázy.

(9) Preventívne opatrenia na ochranu pred haváriou aplikácií:

a. sledovanie hlásení aplikácií a zaznamenávanie postrehov používateľov,
b. sledovanie konfiguračných súborov,
c. monitorovanie a včasná reakcia na hlásenia,
d. denná kontrola chybových hlásení aplikácií.

(10) Preventívne opatrenia na ochranu pred haváriou pracovných staníc:

a. používanie výhradne autorizovaných programov,
b. inštalácia antivírových programov,
c. inštaláciu nových programov smie vykonať len správca,
d. používatelia nesmú zasahovať do konfiguračných súborov,
e. chybové hlásenia sú používatelia povinní hlásiť správcovi,
f. záloha dát na určené média,
g. za zálohy, prevádzku a bezpečnosť zodpovedá používateľ.

(11) Preventívne opatrenia proti mimoriadnym udalostiam spôsobeným vplyvom zvyškových rizík:

a. zabezpečenie niekoľkonásobných záložných kópií,
b. kontrola splnenia protipožiarnych opatrení,
c. kontrola osôb pri vstupe do priestorov prevádzkovateľa,
d. inštalácia elektronického zabezpečovacieho systému, bezpečnostných mreží, dverí,
e. zabezpečenie overenia osôb pri vstupe do chránených priestorov,
f. v prípade vyradenia aktív informačných systémov z činnosti zvolať krízový štáb,
g. koordinácia činnosti podľa bezpečnostných záverov,
h. aktivácia záložného pracoviska,
i. kontrola úplnosti systému na záložnom pracovisku,
j. spustenie záložnej prevádzky,
k. odstránenie škody na pôvodnom pracovisku,
l. po obnovení funkčnosti vrátenie činnosti na pôvodné pracovisko,
m. v prípade napadnutia len časti aktív informačného systému presunúť aktíva do vyhovujúcich priestorov, inštalovať záložné databázy a pripojenia, ak sú nutné, spustiť prevádzku,
n. po odstránení dôsledkov vrátiť činnosť do stavu pred udalosťou.

Článok 9 - Všeobecné pravidlá bezpečnosti informačných technológií

(1) Používateľ je oprávnený pracovať s počítačom, softvérom a údajmi potrebnými pre výkon jeho činnosti iba v súlade s pridelenými právami a oprávneniami.

(2) Je zakázané poskytovať tretím osobám špecifické informácie o používateľoch informačného systému, ktoré by mohli byť zneužité pre neoprávnený prístup k údajom a programom, najmä identifikácie a autentifikácie, rozsah oprávnení a práv a heslá používateľov.

(3) Každý používateľ má pridelené svoje prihlasovacie meno a heslo, ktoré musí zachovať v tajnosti. Tieto mená a heslá pomáhajú stanoviť osobnú zodpovednosť. Zakazuje sa spoločné používanie prihlasovacích mien a hesiel viacerými používateľmi. V prípade nebezpečia prezradenia je potrebné heslo okamžite zmeniť.

(4) Používateľ je plne zodpovedný za svoje heslo, nesmie byť ľahko uhádnuteľné, alebo odvoditeľné. V prípade zabudnutia hesla, si používateľ v súčinnosti so správcom dohodne vytvorenie nového hesla.

(5) V záujme zaistenia bezpečnosti svojich počítačov, počítačových sietí a softvérového vybavenia majú zamestnanci nainštalované rôzne programy (napr. firewall, proxy server, antivírusové prostriedky), monitorovacie systémy pre Internet a elektronickú poštu a bezpečnostné systémy. Zamestnancom sa zakazuje vyraďovať z činnosti, narúšať, prekonávať alebo obchádzať ktorékoľvek bezpečnostné zariadenie alebo systém.

(6) Svojvoľné zapájanie sieťových prvkov ako WiFi router, mobilný internet a pod., ktoré neboli písomne schválené správcom, sa považuje za hrubé porušenie pracovnej disciplíny a napĺňa podľa zákona podstatu kybernetického útoku. Prevádzkovateľovi vzniká povinnosť takýto incident nahlásiť Najvyššiemu bezpečnostnému úradu, ktorý ho následne prešetrí.

(7) Sieťové prvky je oprávnený inštalovať, konfigurovať a zapájať správca, alebo poverená firma za prítomnosti správcu.

(8) Súbory, ktoré obsahujú citlivé (dôverné) údaje, musia byť pri akomkoľvek prenose prostredníctvom Internetu zašifrované. V tomto smere bude používateľovi nápomocný správca.

(9) Pri opustení pracoviska je potrebné vylúčiť akúkoľvek možnosť neoprávneného prístupu tretích osôb k dátam a manipulácie s nimi. V prípade, že používateľ, či správca zistí pokus o narušenie bezpečnosti, týkajúce sa ochrany dát, je povinný takémuto pokusu podľa svojich schopností a možností zabrániť a okamžite o tom informovať starostu obce.

(10) V prípade prítomnosti zástupcu servisnej alebo dodávateľskej firmy je starosta obce povinná určiť zamestnanca, ktorý bude zodpovedný za dohľad nad dodržiavaním ustanovení tejto smernice zo strany zástupcov servisných alebo dodávateľských firiem.

(11) V prípade poruchy zariadenia informačných technológií, ktoré by mohlo obsahovať dáta, musí správca pred odovzdaním tohto zariadenia do opravy odstrániť všetky možné médiá, na ktorých by sa mohli nachádzať údaje (pevné disky, CD, DVD média a pod.).

(12) Ak je poškodený pevný disk, správca je povinný dať zástupcovi servisnej firmy podpísať čestné prehlásenie o mlčanlivosti, ktoré bude súčasťou zmluvy, prípadne objednávky.

(13) Bez predchádzajúceho písomného súhlasu správcu je zakázané poskytovať v akejkoľvek forme akékoľvek údaje, dáta, databázy či prehľady o informačných systémoch iným osobám a organizáciám.

(14) Správca zabezpečí inštaláciu, prevádzku a priebežnú aktualizáciu antivírusového systému pre všetky počítače, ktoré používajú zamestnanci prevádzkovateľa.

(15) Každý bezpečnostný incident, ktorý sa vyskytne na hardvéri, softvéri alebo zariadeniach počítačovej siete, musí byť okamžite ohlásený podľa jeho povahy správcovi. Dokumentáciu o všetkých bezpečnostných incidentoch, ktoré sa vyskytli sa vedú v denníku incidentov.

(16) Správca bez predchádzajúceho informovania starostu obce nepoverí osobu ani firmu na vstup do priestorov. Akýkoľvek pokus o vstup, s odvolaním sa na informačné technológie bez predchádzajúceho informovania zo strany správcu, sa považuje za bezpečnostný incident.

(17) Pri podozrení na takúto skutočnosť je to zamestnanec povinný okamžite hlásiť ako pokus o bezpečnostný incident starostovi obce aj správcovi.

(18) Všeobecne platí, že všetko, čo nie je výslovne povolené – je zakázané!

Článok 10 - Práca s citlivými a osobnými dátami

(1) Všetci zamestnanci sú povinní manipulovať s dátami a dátovými nosičmi obsahujúcimi citlivé informácie tak, aby sa nedostali do rúk nepovolaných osôb. Porušenie tohto ustanovenia je závažným porušením pracovnej disciplíny a môže mať za následok okamžité skončenie pracovného pomeru zamestnanca.

(2) Zásady spracúvania údajov sú základnými mantinelmi, v rámci ktorých sa konkrétne spracúvanie osobných údajov fyzickej a právnickej osoby posudzuje a vykonáva. Cieľom zásad spracúvania údajov je vykonávanie spracúvania údajov tak, aby boli rešpektované práva dotknutých osôb a aby spracúvaním údajov nedochádzalo k porušovaniu práva na zachovanie ľudskej dôstojnosti alebo k iným neoprávneným zásahom do práva na ochranu súkromia. Patria medzi ne:

a. zásada zákonnosti – osobné a citlivé údaje možno spracúvať len zákonným spôsobom a tak, aby nedošlo k porušeniu základných práv dotknutej osoby,
b. zásada obmedzenia účelu – údaje sa môžu získavať len na konkrétne určený, výslovne uvedený a oprávnený účel a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmto účelom,
c. zásada minimalizácie osobných údajov – spracúvané údaje musia byť primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú,
d. zásada správnosti – údaje spracúvané na určitý účel musia byť správne, presné a podľa potreby aktualizované tak, aby sa zabezpečilo, že sa údaje, ktoré sú nesprávne bezodkladne vymažú alebo opravia,

e. zásada minimalizácie uchovávania – údaje musia byť uchovávané, kým je to potrebné na účel, na ktorý sa údaje spracúvajú,
f. zásada integrity a dôvernosti – údaje musia byť spracúvané spôsobom, ktorý prostredníctvom primeraných technických a organizačných opatrení zaručuje primeranú bezpečnosť údajov vrátane ochrany pred neoprávneným a nezákonným spracúvaním údajov, náhodnou stratou, výmazom, alebo poškodením,
g. zásada zodpovednosti – prevádzkovateľ je zodpovedný za dodržiavanie základných zásad spracúvania osobných údajov, za súlad spracúvania osobných údajov so zásadami spracúvania osobných údajov a je povinný tento súlad so zásadami spracúvania osobných údajov na požiadanie preukázať príslušnému úradu,
h. cezhraničný prenos údajov do tretej krajiny, ktorá nezaručuje primeranú úroveň ochrany údajov, možno uskutočniť, ak dotknutá osoba pred jeho uskutočnením poskytla písomný súhlas s vedomím, že tretia krajina nezaručuje primeranú úroveň ochrany údajov. Súhlas musí obsahovať názov krajiny, do ktorej bude uskutočnený prenos údajov, ako aj upozornenie, že táto krajina nezaručuje primeranú úroveň ochrany údajov.

(3) Likvidácia osobných a citlivých údajov:

a. po skončení účelu spracovania údajov je potrebné tieto osobné údaje zlikvidovať, pokiaľ osobitný zákon nenariaďuje inak,
b. dokumenty v listinnej podobe, obsahujúce osobné a citlivé údaje, možno uchovávať po dobu určenú na ich uchovanie, v zmysle registratúrneho poriadku prevádzkovateľa. Po ukončení doby uchovania je potrebné tieto dokumenty zlikvidovať,
c. údaje, ktoré sú v informačnom systéme spracúvané v elektronickej podobe, vrátane údajov na pamäťových médiách, ako napríklad pevné disky, USB kľúče, DVD, CD, veľkokapacitné externé pevné disky, sa uchovávajú v tejto podobe len na nevyhnutne potrebnú dobu, ktorá je určená účelom informačného systému. Po jej uplynutí sa bezpečným spôsobom likvidujú tak, aby údaje nebolo možné obnoviť,
d. pamäťové médiá, vrátane diskov v serveroch a pracovných staniciach, ktoré boli použité na uloženie osobných a citlivých údajov v elektronickej podobe, musia byť pred svojim trvalým vyradením upravené tak, aby z nich nebolo možné obnoviť osobné údaje, ktoré na nich boli zapísané. Oddelenie informatiky, archívu a registratúry v koordinácii s príslušným odborom to zabezpečí prepísaním celého pamäťového média náhodnými údajmi alebo fyzickým zničením pamäťového média.

(4) Mlčanlivosť:

a. používateľ je povinný zachovávať mlčanlivosť o osobných a citlivých údajoch, ktoré spracúva,
b. povinnosť mlčanlivosti trvá aj po ukončení spracúvania osobných a citlivých údajov,

c. povinnosť mlčanlivosti neplatí, ak je to nevyhnutné, na plnenie úloh súdu a orgánov činných v trestnom konaní podľa osobitného zákona.

(5) Minimálne bezpečnostné zásady:

a. získavať na základe svojho pracovného zaradenia len nevyhnutné údaje výlučne na vopred ustanovený účel,
b. spracúvať jedine také údaje, ktoré sú nevyhnutne potrebné na dosiahnutie cieľa spracovania,
c. spracúvať údaje len v priestoroch na to určených,
d. o preprave osobných a citlivých údajov v písomnej forme alebo na pamäťových médiách mimo týchto priestorov môže rozhodnúť jedine príslušný vedúci zamestnanec; v takom prípade musí byť zabezpečená ochrana, dôvernosť, dostupnosť a integrita prepravovaných údajov,
e. oznámiť príslušnému vedúcemu zamestnancovi a zodpovednej osobe každý bezpečnostný incident (napríklad podozrenie na únik osobných a citlivých údajov, neoprávnené zasahovanie do osobných a citlivých údajov) a oznámiť každé zistenie o nedostatočnej účinnosti existujúcich bezpečnostných opatrení prijatých na ochranu osobných a citlivých údajov,
f. chrániť údaje v listinnej alebo elektronickej podobe pred stratou, poškodením, zneužitím, odcudzením, neoprávneným sprístupnením, poskytnutím, alebo inými neprípustnými formami spracúvania,
g. umožniť vstup do miestnosti, v ktorej oprávnená osoba spracúva osobné a citlivé údaje neoprávneným osobám (napríklad upratujúci personál, servisní zamestnanci, návštevy...) až po zabezpečení ochrany údajov najmä uzatvorením dokumentov v elektronickej podobe, zatvorením spisového materiálu v listinnej podobe,
h. využiť všetky dostupné prostriedky na zabezpečenie údajov pred prístupom neoprávnenej osoby (napríklad uchovávanie dokumentov v uzamknutých častiach nábytku, uzamykanie miestnosti počas dočasnej neprítomnosti…),
i. používateľ je povinný dodržať ďalšie postupy upravené poučením, touto smernicou, iným vnútorným predpisom prevádzkovateľa, zákonom alebo iným všeobecne záväzným právnym predpisom,
j. pokiaľ používateľ nebol poučený k spracúvaniu osobných a citlivých údajov pred začatím jeho spracovania alebo z poučenia iných vnútorných predpisov prevádzkovateľa jej nie je zrejmé, ako má plniť vyššie pomenované úlohy, je povinná o tejto skutočnosti informovať svojho nadriadeného a spracovanie údajov obmedziť len na úlohy, ktoré sú jej zrejmé,
k. pri automatizovanom spracúvaní osobných a citlivých údajov používať programové vybavenie, ktoré vyžaduje meno a heslo používateľa,
l. údaje, ktoré sa spracúvajú automatizovaným spôsobom je potrebné pravidelne zálohovať,
m. údaje je v závislosti od ich citlivosti potrebné pseudonymizovať a šifrovať,
n. na všetkých vstupoch do automatizovaného informačného systému je nevyhnutné používať antivírovú ochranu,
o. priestory určené pre spracúvanie osobných a citlivých údajov musia byť zamknuté mimo pracovnej doby, aj pri dočasnej pracovnej neprítomnosti oprávnenej osoby,

p. všetci zamestnanci musia byť poučení o povinnostiach súvisiacich s ochranou osobných a citlivých údajov,
q. písomné dokumenty sa archivujú v uzamykateľných skriniach,
r. používať transparentný systém zaznamenávania bezpečnostných incidentov,
s. zamestnanci musia nepotrebné elektronické dokumenty likvidovať zmazaním zo softvérového aj hardvérového zariadenia a písomné dokumenty likvidovať skartovaním.

Článok 11 - Spoločné a záverečné ustanovenia

(1) Táto smernica nadobúda účinnosť od 01. 01. 2025.

(2) Schválené starostom obce Lukovištia 31. 12. 2024.