

Smernica

Bezpečnostná politika

Vypracovaná v zmysle Výnosu Ministerstva financií Slovenskej republiky č. 55/2014 Z.z.
o štandardoch pre informačné systémy verejnej správy, ktorá je zosúladená s

Nariadením Európskeho parlamentu a Rady (EÚ) č. 2016/679 (GDPR) a Zákonom č. 18/2018 Z.z. o ochrane
osobných údajov a o zmene a doplnení niektorých zákonov pri prevádzke informačných systémov

1. Všeobecné ustanovenia

Článok 1

Účel

Smernica upravuje niektoré práva a povinnosti všetkých zamestnancov ako aj niektorých zmluvných partnerov obce v oblasti ochrany informačných aktív – hlavne spracúvaných osobných a iných citlivých údajov v informačných systémoch (ďalej len „IS“), ďalej ochrany a bezpečnosti majetku, informácií a ďalších hodnôt, ktoré obec vlastní.

Bezpečnostná politika vychádza z výsledkov Analýzy bezpečnosti informačných aktív v IS a posúdenia rizík v Dokumentácii bezpečnostných opatrení na ochranu osobných údajov, ktoré rozširuje a dopĺňa tak, aby zodpovedali aj požiadavkám Výnosu Ministerstva financií Slovenskej republiky č. 55/2014 Z.z. o štandardoch pre informačné systémy verejnej správy.

Článok 2

Základné pojmy a skutočnosti

Osobné údaje – sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej len „dotknutá osoba“); identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby;

V podmienkach prevádzkovateľa sú to: všetky údaje o fyzických osobách, ktoré sú spracovávané v IS pre potreby najmä: matriky, evidencie obyvateľstva, evidencie miestnych daní a poplatkov, mzdovej evidencie a ostatných evidencií v rámci činností jednotlivých referátov obce.

Citlivé údaje – sú obchodné údaje, údaje o ekonomickej a finančnej situácii obce, know-how a všetky dokumenty týkajúce sa riadenia bezpečnosti a ochrany obce.

V podmienkach prevádzkovateľa sú to: údaje o pracovných rolách a prístupových oprávneniach používateľov IS.

Poverená osoba – každá fyzická osoba, ktorú prevádzkovateľ poveril spracovaním osobných údajov v jeho mene, pričom vykonal záznam o poverení v ktorom dokladuje, že súčasťou poverenia je oboznámenie poverenej osoby s Dokumentáciou bezpečnostných opatrení na ochranu osobných údajov prevádzkovateľa a Bezpečnostnou politikou prevádzkovateľa. Poverená osoba je prevzatím poverenia zaviazaná riadiť sa týmito dokumentami prevádzkovateľa ako aj príslušnými právnymi predpismi. Poverená osoba prichádza pri výkone svojej funkcie do styku s osobnými údajmi v rámci svojho pracovného pomeru, štátnozamestnaneckého pomeru, služobného pomeru, členského vzťahu, na základe poverenia, zvolenia alebo vymenovania, alebo v rámci výkonu verejnej funkcie a ktorá spracúva osobné údaje v rozsahu a spôsobom pri dodržaní zásad spracúvania osobných údajov v zmysle Nariadenia GDPR a Zák. č. 18/2018 Z.z.

V podmienkach prevádzkovateľa sú to: okrem štatutára obce najmä: zamestnanci, poslanci, členovia komisií, hlavný kontrolór.

Pre účely prevádzkovateľa sa poverené osoby definujú ako „poverené oprávnené osoby“, nakoľko prevádzkovateľ v poverení vymedzuje poverenej osobe okrem práv a povinností aj spracovateľské oprávnenia.

Poskytovanie osobných údajov – poskytovaním osobných údajov odovzdávanie osobných údajov oprávneným prijímateľom, ktorí ich ďalej spracúvajú.

V podmienkach prevádzkovateľa: napr. Daňový úrad, Sociálna poisťovňa, zdravotné poisťovne, Dátové centrum, ale tiež iní prevádzkovatelia IS, ku ktorým obec vystupuje vo vzťahu tzv. sprostredkovateľa: napríklad: IS JISHM, REGOB, CISMA a pod.

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

V podmienkach obce: sa na likvidáciu listín a fyzických nosičov údajov využíva skartovač.

Zverejňovanie osobných údajov – publikovanie, uverejnenie alebo vystavenie osobných údajov na verejnosti prostredníctvom masovokomunikačných prostriedkov, verejne prístupných počítačových sietí, verejným vykonaním alebo vystavením diela, verejným vyhlásením, uvedením vo verejnom zozname, v registri alebo v operáte, ich umiestnením na úradnej tabuli alebo na inom verejne prístupnom mieste.

V podmienkach obce: sa podľa potreby a na základe súhlasu dotknutých osôb zverejňujú audiovizuálne záznamy z rôznych kultúrno-spoločenských podujatí na obecnej internetovej stránke.

Účel spracúvania osobných údajov – účel spracúvania osobných údajov vopred určuje prevádzkovateľ v súvislosti s plnením svojich úloh, vymazaním alebo fyzickým zničením hmotných nosičov tak, aby sa z nich osobné údaje nedali reprodukovať.

V podmienkach obce: sa na likvidáciu listín a fyzických nosičov údajov využíva skartovač.

Informačný systém – v ktorom sa na vopred vymedzený alebo ustanovený účel systematicky spracúva alebo má spracúvať akýkoľvek usporiadaný súbor osobných údajov prístupných podľa určených kritérií bez ohľadu na to, či ide o informačný systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe; informačným systémom sa na účely tejto smernice rozumie aj súbor osobných údajov, ktoré sú spracúvané alebo pripravené na spracúvanie čiastočne automatizovanými alebo inými ako automatizovanými prostriedkami spracúvania.

V podmienkach prevádzkovateľa: je na základe určených účelov, rozsahu spracovaných osobných údajov a právneho základu spracúvania osobných údajov (osobitné zákony) prevádzkovateľom vymedzený zoznam informačných systémov (IS), ktoré môže prevádzkovateľ meniť podľa zmien v plnení svojich povinností, alebo zmien v účeloch.

O spracúvaní osobných údajov v jednotlivých IS a podľa jednotlivých účelov spracúvania vedie prevádzkovateľ záznamy o spracovateľských činnostiach.

Záznam o spracovateľských činnostiach prevádzkovateľa / zástupcu prevádzkovateľa

Tento záznam musí obsahovať najmenej tieto údaje:

Prevádzkovateľ / zástupca prevádzkovateľa

- a) identifikačné údaje a kontaktné údaje prevádzkovateľa, spoločného prevádzkovateľa, zástupcu prevádzkovateľa, ak bol poverený, a zodpovednej osoby,
- b) účel spracúvania osobných údajov,
- c) opis kategórií dotknutých osôb a kategórií osobných údajov,
- d) kategórie príjemcov vrátane príjemcu v tretej krajine alebo medzinárodnej organizácii,
- e) označenie tretej krajiny alebo medzinárodnej organizácie, ak prevádzkovateľ zamýšľa prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii a dokumentáciu o primeraných zárukách, ak prevádzkovateľ zamýšľa prenos podľa § 51 ods.1a 2, Zák. č.18 /2018 Z.z.

- narušenie spôsobené žiarením
- kompromitácia informácií
- technické zlyhanie
- nepovolené aktivity
- kompromitácia funkcií

V podmienkach prevádzkovateľa sú to hlavne hrozby:

- **možnosť úniku a zneužitia osobných údajov** nachádzajúcich sa v IS (ISO27005: kompromitácia informácií),
- **možnosť neoprávnenej manipulácie** s osobnými údajmi v IS (ISO27005: nepovolené aktivity)
- **nenávratné zničenie alebo poškodenie** osobných údajov v IS (ISO27005: fyzické poškodenie, prírodné udalosti, technické zlyhanie),
- **cieľené úmyselné zmeny, alebo vnášanie nepravých, neautentických údajov** do IS. (ISO27005: nepovolené aktivity)

Bezpečnostné opatrenia – sú činnosti, nariadenia a postupy, ktoré vykonáva prevádzkovateľ na ochranu aktív pred hrozbami. Rozlišujú sa na proaktívne (realizované preventívne pred možným uskutočnením hrozby s cieľom znemožniť hrozbe na aktíva pôsobiť – napr. antivírusové opatrenia) a reaktívne (realizované ako reakcia na už uskutočnenú hrozbu s cieľom zamedziť pôsobeniu hrozby a eliminovať dôsledky jej pôsobenia – teda uviesť aktíva do stavu pred začatím pôsobenia hrozby).

V podmienkach prevádzkovateľa: Obec má svoje technické a organizačné bezpečnostné opatrenia popísané v Dokumentácii bezpečnostných opatrení.

Bezpečnostný incident – je také pôsobenie hrozby na aktívum, pri ktorom obci na aktíve vzniká škoda.

V podmienkach prevádzkovateľa má bezpečnostné incidenty najmä tieto dopady:

- porušenie povinností stanovených nariadením č. **2016/679 EP a Rady EÚ** a zákonom č. 18/2018 Z. z. o ochrane osobných údajov a možné súvisiace sankcie,
- porušenie práv dotknutých osôb pri nezákonnom spracúvaní ich osobných údajov, alebo pri nedostatočnej ochrane ich osobných údajov v zmysle narušenia ich osobnej integrity, dôstojnosti, dobrého mena a podobne, ktorého dôsledkom môžu byť nielen sankcie regulačného orgánu, ale aj súdne spory s dotknutými osobami,
- možnosť výskytu úmyselných aktivít zameraných k zneužitiu osobných údajov,
- v prípade súčasného poškodenia alebo zničenia záložných kópií práca rekonštrukcia údajov (so zvýšenou pravdepodobnosťou chýb),
- v prípade poškodenia, zlyhania, alebo odcudzenia výpočtovej techniky omeškanie spracovania osobných údajov a nadväzujúcich činností,
- narušenie práce pracoviska, v prípade niektorých aplikácií práca rekonštrukcia údajov (nedostatočné, resp. žiadne údaje v listinnej forme),
- obmedzenie schopnosti pracoviska včas plniť svoje úlohy.

Riziko – Riziko je odhadom pravdepodobnosti možného pôsobenia konkrétnej hrozby na konkrétne aktívum vo vzťahu k predpokladanému dopadu na aktívum. Posudzuje sa veľkosť rizika pre každú identifikovanú hrozbu a každý IS samostatne s následným zhrnutím a identifikovaním najväčších rizík.

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 dozornému orgánu preukázať.

Zákonnosť spracúvania - spracúvanie osobných údajov je zákonné, ak sa vykonáva na základe aspoň jedného z týchto právnych základov:

- a) dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov aspoň na jeden konkrétny účel,
- b) spracúvanie osobných údajov je nevyhnutné naplnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo na vykonanie opatrenia pred uzatvorením zmluvy na základe žiadosti dotknutej osoby,
- c) spracúvanie osobných údajov je nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná,
- d) spracúvanie osobných údajov je nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby alebo inej fyzickej osoby,
- e) spracúvanie osobných údajov je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi,
- f) spracúvanie osobných údajov je nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany okrem prípadov, keď nad týmito záujmami prevažujú záujmy alebo práva dotknutej osoby vyžadujúce si ochranu osobných údajov, najmä ak je dotknutou osobou dieťa. Tento právny základ sa nevzťahuje na spracúvanie osobných údajov orgánmi verejnej moci pri plnení ich úloh.

Článok 5

Správa aktív

Aktíva prevádzkovateľa sa na účely tejto smernice členia do nasledujúcich skupín:

- aktíva s vysokou ochranou - sú to tie aktíva, ktorých poškodenie alebo strata by ohrozila záujmy obce v plnom rozsahu,
- aktíva so zvýšenou ochranou – sú tie aktíva, ktorých poškodenie alebo strata by čiastočne ohrozili záujmy obce,
- aktíva obvyklej ochrany – sú to aktíva, ktorých individuálne poškodenie alebo strata spôsobia ľahko odstrániteľnú škodu alebo neohrozia záujmy obce.

Zaradenie predmetu alebo skutočnosti medzi aktíva vykonáva BS.

Zamestnanci používajúci aktívum so zvýšenou a vysokou ochranou sú povinní oznámiť správcovi tohto aktíva akúkoľvek skutočnosť, o ktorej sa domnievajú, že by mohla byť hrozbou pre dané aktívum.

Za ochranu a správu aktív obvyklej ochrany sú zodpovední zamestnanci, ktorí za tieto aktíva prevzali hmotnú zodpovednosť alebo im boli zverené do používania.

Aktívum sa môže používať len na ten účel, ktorý je deklarovaný v inventári aktív. Iné dočasné použitie je možné len so súhlasom BS.

Bezpečnostný správca pravidelne, najmenej jedenkrát za rok, zvoláva poradu Správcov aktív.

Článok 6

Kontrolná činnosť

Úlohou kontrolnej činnosti je zisťovanie stavu bezpečnosti a ochrany informačných technológií, stavu pripravenosti a účinnosti opatrení a výkon dozoru nad plnením tejto smernice.

V podmienkach obce kontrolnú činnosť vykonáva Bezpečnostný správca (BS) nasledovne:

- každý pracovník – poverená oprávnená osoba – používateľ IS je povinný poskytnúť BS všetky informácie o ktoré pri výkone prehliadky, alebo kontroly žiada a sú vo vzťahu k predmetu prehliadky alebo kontroly,
- prehliadkou, ktorú BS vykonáva popri výkone svojich obvyklých pracovných povinností a vedie o jej zisteniach záznam v prevádzkovom denníku,
- kontrolou podľa schváleného plánu kontrol, resp. nenaplánovanou kontrolou, ktorých cieľom je preveriť dodržiavanie tejto smernice u konkrétneho pracovníka – oprávnenej osoby – používateľa IS, alebo viacerých takýchto osôb. O kontrole Bezpečnostný správca vykoná záznam, v ktorom uvedie predmet kontroly, dátum a čas, kedy bola kontrola vykonaná, kto kontrolu vykonal a zistené skutočnosti; ak sa kontrolou zistí porušenie tejto smernice, všeobecne záväzných predpisov, alebo iných interných nariadení obce, predloží BS správu o kontrole starostovi obce. Správa o výsledkoch kontroly musí obsahovať:
 - a) chronologický opis priebehu kontrolnej činnosti,
 - b) zoznam zistených nedostatkov,
 - c) odporúčané opatrenia.
- každý pracovník – poverená oprávnená osoba – používateľ IS je povinný poskytnúť BS všetky informácie o ktoré pri výkone prehliadky, alebo kontroly žiada a sú vo vzťahu k predmetu prehliadky alebo kontroly.

i) zoznam opatrení a nariadení, ktoré boli porušené a mohli spôsobiť že incident nastal, zoznam osôb ktoré tieto nariadenia porušili,

- ak nastal bezpečnostný incident vedomou alebo nevedomou činnosťou oprávnenej osoby, bude sankcionovaná podľa príslušných ustanovení Zákonníka práce a Pracovného poriadku.

Článok 8

Bezpečnostné režimy

Bezpečnostný režim je stav organizácie činnosti obce alebo jej časti, ktorý zodpovedá aktuálnemu ohrozeniu aktív prevádzkovateľa.

Stupeň a rozsah bezpečnostného režimu určuje BS alebo Správca IT na základe poznania aktuálneho stavu bezpečnosti a úrovne ohrozenia aktív prevádzkovateľa.

Rozoznávajú sa nasledovné režimy:

1. normálny – normálny stav bežného chodu prevádzkovateľa, kedy nie je bezprostredne ohrozené žiadne aktívum,

2. ohrozenie - činnosť prevádzkovateľa nie je ničím zmenená alebo ovplyvnená, ale úroveň ohrozenia niektorého aktíva je zvýšená (zvýšená je pravdepodobnosť realizácie niektorej hrozby), čo vyžaduje monitorovanie tohto stavu a prijatie ďalších proaktívnych opatrení. Opatrenia sa prijímajú na základe aktuálneho poznania stavu hrozieb, ktorý je indikovaný najmä analýzou obsahu prevádzkových záznamov alebo výskytom bezpečnostných incidentov, ktoré síce bezprostredne nevyžadovali zmenu bezpečnostného režimu, ale dôsledky incidentu mohli spôsobiť zvýšenie pravdepodobnosti výskytu a realizácie niektorej z hrozieb. Po prijatí opatrení sa odhadne ich účinnosť, znovu sa posúdi úroveň rizika a rozhodne sa o prijatí ďalších opatrení, alebo o prechode do režimu „**normálny**“. Ak sa zistí, že aj napriek prijatým opatreniam došlo k realizácii hrozby a dochádza k poškodzovaniu alebo ničeniu aktív obce, vyhlási sa režim „**kríza**“.

3. kríza - činnosť prevádzkovateľa je zmenená následkom účinku niektorých hrozieb na aktíva obce. Vyžaduje sa prijatie účinných reaktívnych opatrení na odvrátenie hrozby a minimalizáciu škôd. Tento režim sa vyhlasuje, ak bol zistený výskyt realizujúcej sa niektorej hrozby na aspoň jedno IT aktívum (server alebo informačný systém), na ktorom sa spracovávajú osobné alebo citlivé údaje. Pod pojmom realizujúca sa hrozba, sa rozumie taký stav, kedy je aktívum hrozbou poškodzované alebo ničené, čo má za následok znefunkčnenie aktíva alebo ohrozenie záujmov obce. Počas tohto režimu je možné odpojiť časť prevádzkovateľa alebo celého prevádzkovateľa od internetu, nariadiť vypnutie počítačov a serverov alebo ich odpojenie od počítačovej siete. Po odvrátení hrozby sa prechádza do režimu „**zotavenie**“.

4. zotavenie - špeciálny režim po „**krízovom**“ režime, kedy dochádza ku konsolidácii činnosti prevádzkovateľa, rekonštrukcii a náhrade poškodených aktív. Navrhuje sa vedeniu postup pri odstraňovaní škôd. Postup musí obsahovať stanovenie priorít, časovú postupnosť, technickú špecifikáciu opatrení na odstránenie škôd a odhad ekonomickej náročnosti. BS v súčinnosti so Správcom IT je povinný dôkladne vyšetriť dôvody príčiny, a teda prečo došlo k realizácii hrozieb a škodám. Prechod do režimu „**normálny**“ je možný, ak bol schválený postup

Článok 10

Havarijné plánovanie

Havarijne plánovanie je súbor činností na zabezpečenie čo najvyššej dostupnosti údajov a ich ochrana pre zničením alebo poškodením.

V prípade výpadku pracovnej stanice je Správca IT povinný po identifikácii problému zabezpečiť:

- opravu alebo výmenu chybného dielu PC,
- náhradný PC,
- reinštaláciu alebo inštaláciu OS a konfiguráciu z inštalačných médií,
- inštaláciu klientskych aplikácií z inštalačných médií,
- inštaláciu antivírusového programu,
- nastavenie prístupových práv,
- v prípade neodkladnosti prístup k informačným systémom z inej funkčnej pracovnej stanice.

V prípade výpadku servera je Správca IT povinný po identifikácii problému zabezpečiť:

- opravu servera v servisnej organizácii alebo náhradný server,
- inštaláciu hardware a jeho fyzické pripojenie do počítačovej siete,
- inštaláciu príslušného operačného systému servera,
- zo záložných kópií obnovenie systémových a konfiguračných súborov,
- inštaláciu antivírusového programu a spustenie aktualizácie,
- inštaláciu IS a obnovenie dát z najmladších záložných médií.

V prípade výpadku sieťového prepojenia je Správca IT povinný po identifikácii problému zabezpečiť:

- opravu alebo výmenu chybného aktívneho alebo pasívneho prvku počítačovej siete,
- obnovenie konfiguračného nastavenia zariadenia,
- otestovanie jednotlivých sieťových prepojení.

S postupmi pri haváriách, poruchách a mimoriadnych situáciách, ktoré sledujú efektívnu obnovu systému, je potrebné oboznámiť všetkých vedúcich zamestnancov.

3. Osobné údaje prevádzkovateľa

Článok 11

Zabezpečenie osobných údajov

Každá poverená oprávnená osoba (pracovník, volený zástupca, používateľ IS), ktorá príde do styku s osobnými údajmi, musí byť v poverení oboznámená s príslušnými právnymi normami (Nariadenie GDPR, Zákon č.18/2018 Z.z.) o ochrane osobných údajov. Toto oboznámenie musí byť v súlade a v rozsahu s jeho pracovnou náplňou, alebo volenou funkciou. Oboznámenie vykonáva BS, určená Zodpovedná osoba, alebo iná prevádzkovateľom poverená osoba. O oboznámení musí byť vykonaný záznam.

Osobné údaje môžu byť spracovávané a prenášané len zabezpečeným spôsobom.

- údaje nemohli byť známe tejto neoprávnenej osobe a zabrániť tomu, aby táto neoprávnená osoba mohla prísť do styku s týmito osobnými údajmi.
- oprávnená osoba kontroluje a overuje správnosť a aktuálnosť osobných údajov po ich získaní a zaradení v informačnom systéme osobných údajov,
 - poverená oprávnená osoba vykonáva spracovateľské operácie len so správnymi, úplnými a podľa potreby aktualizovanými osobnými údajmi vo vzťahu k účelu spracúvania,
 - nesprávne a neúplné osobné údaje je oprávnená osoba povinná bez zbytočného odkladu opraviť alebo doplniť. Nesprávne a neúplné osobné údaje, ktoré nemožno opraviť alebo doplniť tak, aby boli správne a úplné je povinná blokovať, kým sa rozhodne o ich likvidácii,
 - pred získaním osobných údajov od dotknutej osoby je oprávnená osoba povinná oboznámiť ju s názvom a sídlom obce, účelom spracúvania osobných údajov, rozsahom spracúvania osobných údajov, predpokladanom okruhu tretích strán pri poskytovaní osobných údajov alebo príjemcov pri sprístupňovaní osobných údajov, forme zverejnenia, ak sa osobné údaje zverejňujú a tretie krajiny, ak sa predpokladá alebo je zrejmé, že sa do týchto krajín uskutoční cezhraničný prenos osobných údajov,
 - poverená oprávnená osoba je povinná poučiť dotknutú osobu o dobrovoľnosti alebo povinnosti poskytnutia osobných údajov a o existencii jej práv,
 - poverená oprávnená osoba je povinná zabezpečiť preukázateľný súhlas na spracúvanie osobných údajov dotknutej osoby v IS prevádzkovateľa, ak sa spracúvanie osobných údajov nevykonáva podľa iného právneho základu.
 - získavať osobné údaje nevyhnutné na dosiahnutie účelu spracúvania kopírovaním, skenovaním alebo iným zaznamenávaním úradných dokladov na nosič informácií je možné len vtedy, ak to osobitný zákon výslovne umožňuje bez súhlasu dotknutej osoby alebo na základe písomného súhlasu dotknutej osoby, ak je to nevyhnutné na dosiahnutie účelu spracúvania,
 - poverená oprávnená osoba je povinná chrániť prijaté dokumenty a súbory pred stratou, poškodením, zneužitím, odcudzením, neoprávneným sprístupnením, poskytnutím alebo inými nepripustnými formami spracúvania,
 - oprávnená osoba je povinná vykonať likvidáciu osobných údajov, ktoré sú súčasťou už nepotrebných pracovných dokumentov (napr. rôzne pracovné súbory, pracovné verzie dokumentov v listinnej podobe) rozložením, vymazaním alebo fyzickým zničením hmotných nosičov tak, aby sa z nich osobné údaje nedali reprodukovať; to neplatí vo vzťahu k osobným údajom, ktoré sú súčasťou obsahu registratúrnych záznamov obce.

Každá osoba je zodpovedná za fyzickú bezpečnosť svojho pracoviska, jemu zverených aktív a všetkých pracovných prostriedkov. Pri odchode z pracoviska je povinná uzamknúť pracovisko, uzavrieť okná a prekontrolovať zariadenia, či nemôžu spôsobiť požiar alebo inú haváriu. Ak nemôže túto povinnosť splniť, oznámi to ihneď svojmu nadriadenému alebo BS.

Poverené oprávnené osoby (pracovníci, volení zástupcovia) sú povinní zachovávať mlčanlivosť o osobných údajoch, s ktorými prídu do styku. Tie nesmú využiť ani pre osobnú potrebu a bez súhlasu štatutára obce ich nesmú zverejniť, nikomu poskytnúť a ani sprístupniť.

4. Prostriedky informačných technológií

Článok 13

Správca informačných technológií

Správcom informačných technológií (ďalej tiež „SIT“) a IT aktív je zamestnanec obce – oprávnená osoba, alebo externý špecialista (pracovník externej organizácie s ktorou má obec zmluvný vzťah, poverený správou informačných technológií.

Správa informačných technológií musí byť organizovaná tak, aby sa minimalizovala hrozba zneužitia postavenia administrátora.

Za ochranu údajov uložených na prostriedkoch informačných technológií je zodpovedný Správca IT, ktorý k tomuto účelu vykonáva nasledovné činnosti:

- vykonáva kopírovanie údajov na záložné médiá (zálohovanie údajov),
- vykonáva kopírovanie údajov na archívne médiá (archivovanie údajov),
- vykonáva nastavenia prístupových práv k údajom tak, aby k nim mohli pristupovať len oprávnené osoby – oprávnení používateľa IS,
- inštaluje, spravuje a zabezpečuje také služby (aplikácie), ktoré umožnia zvýšenú ochranu údajov,

Správca IT je zodpovedný za pravidelnú a včasnú aktualizáciu všetkých programových prostriedkov tak, aby boli včas odstraňované chyby v týchto softvérových prostriedkoch, ktorými sú najmä operačné systémy a ich súčasti, databázové systémy, používané aplikácie (najmä ak komunikujú po sieti), systém antivírusovej ochrany a firewally.

Správca IT je povinný priebežne nainštalovať všetky dostupné nové opravy softvérového vybavenia, pokiaľ sa tým nenaruší bezproblémový chod a činnosť. Najmenej raz za 3 mesiace je Správca IT povinný overiť, či neboli vydané nové verzie softvéru.

Zakazuje sa používanie neovereného kódu. Pod pojmom neoverený kód sa rozumie taký program, ktorý nemá garanciu výrobcu o jeho spoľahlivosti alebo nebol overený Správca IT v izolovanom prostredí, či neobsahuje nežiaduce funkcie a chyby. Overenie sa vykonáva tak, aby nemohlo dôjsť k ohrozeniu osobných údajov obce a musí sa preveriť najmä správanie programu v sieťovom prostredí a vo vzťahu k údajom uloženým na pamäťovom médiu počítača.

Pri konfigurácii prostriedkov, programov a služieb Správca IT dbá na to, aby sa používali len tie prostriedky, programy a služby, ktoré sú nevyhnutné pre plnenie pracovných úloh a potrieb zamestnancov obce. Zakazuje sa používanie programov, sieťových služieb a IT prostriedkov, ktoré nie sú potrebné pre výkon práce zamestnancov a plnenie ich úloh. Používané programy, služby a prostriedky musia byť konfigurované tak, aby k nim mali prístup len tí zamestnanci, ktorí tieto programy, služby a prostriedky potrebujú k svojej práci.

Článok 16

Riadenie prístupových práv

- SIT pre aktíva ktoré vyžadujú autentizáciu, stanoví autentizačné postupy a mechanizmy,
- pre autentizačné mechanizmy SIT stanoví parametre, a to najmä vlastnosti hesiel: dĺžku, štruktúru a expiračnú dobu,
- SIT nesmie povoliť heslá kratšie ako 8 znakov, heslá musia obsahovať aspoň jeden neabecedný znak a ich expiračná doba nesmie byť dlhšia ako 1 rok.
- zakazuje sa zverejňovať, alebo neoprávnenej osobe akýmkoľvek spôsobom sprístupniť vyzradiť neverejné autentizačné údaje (heslá).
- zakazuje držanie záznamu hesiel (napr. na papieri, v nešifrovanom softvérovom súbore) ak takýto záznam nemôže byť bezpečne uložený. Oprávnená osoba je povinná chrániť autentizačný prostriedok jemu zverený.
- SIT môže prideliť autentizačné údaje a prostriedky len oprávneným osobám obce, alebo externým špecialistom zmluvnej externej organizácie, ktorá robí údržbu daného aktíva.
- prístupové oprávnenia prideluje používateľovi IS SIT na základe požiadavky SB, resp. štatutára obce. Tvoria ich prístupové meno, prístupové heslo a súbor nastavení, ktoré definujú povolené aktivity používateľa (užívateľská rola),
- používateľ IS sa nesmie žiadnymi prostriedkami pokúšať získať prístupové práva alebo privilegovaný stav, ktorý mu nebol pridelený SIT,
- pokiaľ používateľ IS v dôsledku chyby programových alebo technických prostriedkov získa privilegovaný stav, ktorý mu nebol udelený alebo mu prístupové práva nebol pridelené, je povinný túto skutočnosť neodkladne oznámiť SIT,
- po skončení pracovného pomeru oprávnenej osoby - používateľa IS je SIT povinný odobrať odchádzajúcemu zamestnancovi jeho prihlasovacie údaje a zmeniť ich tak, aby sa mu znemožnil ďalší prístup,
- prístupové oprávnenia sú pridelované 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 – externý špecialista externej organizácie, ktorá spravuje a udržiava danú aplikáciu (aktívum), prístup je kontrolovaný správcom aktíva alebo administrátorom, ak ho tým poveril SIT,
- SIT je povinný preveriť používateľské prístupové práva minimálne raz za rok,
- nedodržanie zásad používania hesla a autentizácie zamestnancom sa považuje za bezpečnostný incident.

- 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 prevádzkovej obcou.

- kontrolu pred nevyžiadanou poštou – Spamom,

- kontrolu webových stránok z hľadiska výskytu škodlivého kódu,

SIT je povinný venovať zvýšenú pozornosť tomu, aby škodlivý kód nebol zavedený počas výkonu pohotovostných procedúr alebo procedúr údržby.

V prípade, že sa na pri práci oprávnenej osoby – používateľa IS zobrazí na pracovnej ploche varovanie, že sa na disku alebo prenosnom médiu nachádza vírus alebo iný škodlivý kód, oprávnená osoba nesmie toto varovanie ignorovať. V prípade, že vírus obsahujúce prenosné médium patrí inému subjektu, oprávnená osoba toto označí ako „obsahujúce vírus“ a vráti majiteľovi. V prípade infikovania vlastného pevného disku alebo prenosného média, oprávnená osoba túto skutočnosť bezodkladne oznámi SIT.

Článok 19

Prístup do siete internet a mailová komunikácia

Každá oprávnená osoba, ktorej bol umožnený prístup do siete internet, je povinná rešpektovať nasledovné zásady:

- prístup do siete internet využívať predovšetkým v súlade so svojou pracovnou náplňou,

- dodržiavať etické zásady a zdržiavať sa činností, ktoré by mohli viesť k poškodeniu dobrého mena obce,

- komunikácia v internete spravidla nie je chránená pred „odpočúvaním“. V prípade potreby prenosu osobných údajov je nevyhnutné tieto pred prenosom zabezpečiť šifrovaním. Ak nie je oprávnená osoba schopná prenos takto zabezpečiť, nie je prípustné ho uskutočniť,

- je zakázané zo siete internet preberať nelegálny obsah (softvér, súbory chránené autorskými právami a pod.). Preberanie spustiteľných programov je povolené len po konzultácii so SIT,

- Výber blokových stránok bude v kompetencii SIT na základe bezpečnostnej analýzy.

- oprávnená osoba je povinná zabezpečiť správne adresovanie príjemcu mailovej správy a na prenos správ používať všeobecne dané dátové štandardy,

- v prípade posielania citlivých a osobných údajov je povinný použiť kryptovanú komunikáciu za použitia kryptovacieho kľúča, ktorý mu bol na požiadanie vydaný BS,

5. Záverečné ustanovenia

Článok 21

Účinnosť smernice

Bezpečnostná smernica nadobúda účinnosť dňom 25.05.2018

Na túto smernicu sa nevzťahuje povinnosť zverejnenia v zmysle zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám v znení neskorších predpisov.

V MANOLE dňa: 25.05.2018

.....

Meno, priezvisko, podpis:
(štatutár prevádzkovateľa)