Interná smernica

o bezpečnostných štandardoch architektúry riadenia pre informačné systémy
Obce Herľany

Vymedzenie pojmov

Čl. 1

Použité pojmy a skratky

Na účely tejto smernice sa rozumie:

auditovateľnosť – schopnosť zistiť vybrané informácie o aktivitách subjektu.

autenticita – pravosť, nefalšovanosť, zhoda informácie so skutočnosťou. Napríklad zabezpečenie toho, že osoba je tým, za koho sa vydáva.

autorizácia – oprávnenie na prístup k aktívu, alebo na vykonávanie činnosti. Proces overovania, zisťovania prístupových práv.

autorizovaná osoba – osoba, ktorá má oprávnenie na prístup k aktívu alebo na vykonávanie činnosti.

bezpečnostná politika – tieto interné smernice „Bezpečnostná politika obce.....“.

bezpečnostné povedomie – základné pravidlá bezpečného vykonávania činností.

bezpečnosť – vlastnosť objektu alebo subjektu, ktorá určuje mieru jeho ochrany proti možným škodám. Taktiež stav, pri ktorom je riziko poškodenia aktív obmedzené na prijateľnú úroveň.

www - webová stránka, verejne on-line dostupné miesto na internete, sprístupňované prostredníctvom webového prehliadača a využívajúce protokol Hypertext Transfer Protocol (HTTP),

webovým sídlom - ucelený súbor webových stránok v správe jednej povinnej osoby podľa zákona; webové sídlo má pridelenú najmenej jednu doménu; webová stránka tvorí jednu vizuálnu obrazovku webového sídla, a to aj v prípade, ak je zložená z viacerých rámcov,

správcom obsahu - povinná osoba zodpovedná za správu obsahu webového sídla a na ňom zverejnené informácie; správca obsahu je zároveň správcom daného informačného systému verejnej správy,

technickým prevádzkovateľom - prevádzkovateľ informačného systému verejnej správy Obce Herľany podľa zákona, je ten, kto vykonáva činnosti určené správcom obsahu v súvislosti s technickou prevádzkou webového sídla,

aktívami - programové vybavenie, technické zariadenia, poskytované služby, kvalifikované osoby, dobré meno povinnej osoby a informácie, dokumentácia, zmluvy a iné skutočnosti, ktoré považuje povinná osoba za citlivé,

bezpečnostným incidentom - akýkoľvek spôsob narušenia bezpečnosti informačných systémov, ako aj akékoľvek porušenie bezpečnostnej politiky prevádzkovateľa a pravidiel súvisiacich s bezpečnosťou informačných systémov obce,

technickými komponentmi informačného systému verejnej správy - tie časti informačného systému verejnej správy a informačno-komunikačné technológie, ktoré nie sú určené na uchovávanie údajov, napríklad štruktúrovaná kabeláž, sieťové karty a zdroje,

zariadeniami informačného systému verejnej správy - tie časti informačného systému verejnej správy, ktoré môžu uchovávať údaje, napríklad pamäťové médiá a počítače vrátane prenosných počítačov,

súborom - postupnosť údajov v elektronickej forme, ktorá je označená názvom, informáciou o kapacite údajov a časovou značkou o jej poslednej zmene,

dátovým prvkom - jednotka údajov, ktorá je jednoznačne a nedeliteľne špecifikovaná prostredníctvom súboru atribútov,

dostupnosť – zabezpečenie prístupu k aktívam pre autorizovaných používateľov vtedy, keď je to potrebné.

dôvernosť – zaistenie toho, že k informáciám majú prístup len tie osoby, ktoré majú oprávnenie spracúvať osobné údaje a ktorí majú na to autorizáciu danú prevádzkovateľom.

hrozba – čokoľvek, čo môže spôsobiť škodu. Akcia alebo udalosť, ktorá môže ohroziť bezpečnosť aktíva.

IB – informačná bezpečnosť.

Informačná bezpečnosť – bezpečnosť informácií a všetkých ostatných aktív informačných technológií a informačných systémov. Informačná bezpečnosť je súčasťou celkovej bezpečnosti.

IS – Informačný systém / Informačné systémy.

Informačný systém – súbor technických a programových prostriedkov, záznamových médií, dát a personálu, ktoré spoločnosť používa na spracovanie informácií v určitej oblasti pôsobenia.

Integrita – neporušenosť, celistvosť, presnosť, kompletnosť.

IT – Informačné technológie.

LAN – Lokálna počítačová sieť (Local Area Network).

legislatíva – všeobecne záväzné predpisy a vnútorné predpisy Obce Herľany

opatrenia, bezpečnostné opatrenia, ochranné opatrenia – prax, postupy, alebo mechanizmy, ktoré znižujú bezpečnostné riziká.

osobné údaje – osobné údaje podľa zákona č. 18/2018 Z. z. o ochrane osobných údajov.

používateľ – osoba používajúca informácie patriace prevádzkovateľovi.

produkčný systém – systém nasadený v reálnej prevádzke prevádzkovateľa.

riziko – potenciálna možnosť, že daná hrozba využije zraniteľnosť aktív a spôsobí tak stratu alebo zničenie aktív.

správca – osoba, ktorá má na starosti správu, prevádzku, údržbu informačného systému.

spracúvanie informácií – akákoľvek manipulácia, spracúvanie, zmeny úpravy, doplnenia, vymazanie, uchovávanie, prezentácia, poskytovanie, prenos či ochrana informácií

Zamestnanec – osoba, ktorá má pracovnoprávny vzťah alebo iný obdobný vzťah s obcou Herľany.

IKT (ICT) - informačné a komunikačné technológie.

informačné a komunikačné technológie - zariadenie alebo systém (izolovaný alebo zapojený do siete), alebo subsystém zariadenia, ktoré sa používa na automatický zber, uchovávanie, narábanie, manažment, presun, riadenie, zobrazovanie, prepínanie, vzájomnú výmenu, prenos alebo prijímanie údajov alebo informácie. Medzi IKT patria počítače, ich pomocné zariadenia, softvér, firmvér, komunikačné linky a pod.

II. ODDIEL

Bezpečnostná politika

Bezpečnostná politika určuje povinnosť zaistiť nenarušenie informačnej bezpečnosti KSK.

Čl. 2.

Definícia informačnej bezpečnosti

Informačná bezpečnosť je:
Súhrn opatrení prijatých na ochranu informácií a IKT systémov pred neoprávneným prístupom, použitím, zverejnením, poškodením, modifikáciou alebo zničením tak, aby sa zaistila dôvernosť, integrita a dostupnosť informácií.
Schopnosť IKT systému na danej úrovni spoľahlivosti odolávať náhodným udalostiam aj zámerným akciám a bezpečne prevádzkovať informačného systému obce Herľany, tak aby bola zabezpečená dostupnosť, autentickosť, integrita a dôvernosť uložených alebo prenášaných údajov a služieb poskytovanými alebo sprístupňovanými daným systémom.
Informačná bezpečnosť zahŕňa aj autorizáciu, autenticitu používateľov a auditovateľnosť aktivít používateľov a systémov.

Čl. 3.

Definícia bezpečnostnej politiky

Bezpečnostná politika je základný dokument Obce Herľany, ktorý vymedzuje štruktúru bezpečnostného manažmentu, zodpovednosť za ochranu informácií v organizácii, úroveň ochrany informácie.

Bezpečnostná politika je súbor pravidiel (smernice) a praktík (dokumentácie), ktoré špecifikujú alebo regulujú ako Obec Herľany poskytuje bezpečne informačné služby, tak aby chránil citlivé alebo kritické zdroje IS.

Čl. 4.

Poslanie bezpečnostnej politiky

Poslaním bezpečnostnej politiky je:

Spolu s ďalšími právnymi predpismi, dokumentmi a vnútornými predpismi Obce Herľany stanoviť stratégiu a konkrétne pravidlá bezpečného správania sa používateľov pri ich činnostiach v rámci Obce Herľany a činnosti obecného úradu.

Využívať všetky primerané, vhodné, praktické a efektívne bezpečnostné opatrenia pre ochránenie dôležitých procesov a aktív Obce Herľany za účelom dosiahnutia bezpečnostných cieľov obce Herľany.

Neustále sa snažiť o zlepšenie procesov a organizáciu práce pri práci s informačným systémom.

Chrániť a riadiť informačné aktíva Obce Herľany a obecného úradu a tým spôsobom umožniť dosiahnutie legislatívnych, zmluvných a morálnych povinností vrátane povinností ochrany osobných údajov.

Čl. 5.

Vecná a personálna pôsobnosť bezpečnostnej politiky

Bezpečnostná politika sa vzťahuje na aktíva Obce Herľany, ktoré priamo súvisia so spracovaním informácií. Je záväzná pre všetkých zamestnancov obce, zamestnancov obecného úradu ktorí vstupujú do informačných systémov obce a tretie osoby, ktoré prichádzajú do styku s aktívami obce. Tieto osoby sa zaviažu dodržiavať bezpečnostnú politiku.

Čl. 6.

Vyhlásenie vedenia obce o podpore bezpečnostnej politiky

Starosta obce vyhlasuje, že považuje predmetné aktíva a opatrenia na ich ochranu za veľmi dôležité a vyhlasuje, že dosiahnutiu bezpečnostných cieľov bude venovať trvalú pozornosť.
Starosta obce schvaľuje túto bezpečnostnú politiku, podporuje ju a realizuje kroky na jej presadzovanie prostredníctvom poverených zamestnancov.

Čl. 7.

Zodpovednosť za vypracovanie a aktualizáciu bezpečnostnej politiky

Za vypracovanie a aktualizáciu bezpečnostnej politiky zodpovedá team manažmentu bezpečnosti, ktorý menuje starosta obce Herľany. Na čele teamu je starosta Obce Herľany. Manažment bezpečnosti obce Herľany je kombinovaný team ktorého členmi sú:

- zástupca starostu,
- bezpečnostný manažér, ktorým je zodpovedná osoba,
- správca informačného systému,
- poslanec obecného zastupiteľstva,
- ďalšie osoby menované starostom obce.

Čl. 8.

Stanovenie pozície pre Manažment bezpečnosti obce

Manažment bezpečnosti obce je vytvorený na úrovni starostu.

Členmi teamu obce sú najmä: poslanci obecného zastupiteľstva.

Starosta obce; stojí na čele teamu.

Správca informačného systému informačnej bezpečnosti.

Zástupca starostu.

Poslanec obecného zastupiteľstva

Zodpovedná osobu, ktorá dozerá na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov obce.

Ďalšie osoby určené starostom obce.

Rozhodnutiami Manažmentu bezpečnosti obce sú povinní sa riadiť všetci zamestnanci obce, zamestnanci (ďalšie subjekty – Základná škola) ktorí sú dotknutí aktívami (pracujú na IS ktorý prevádzkuje obec), osoby ktoré pracujú s aktívami obce na základe osobitného poverenia (dodávatelia na základe zmluvy, atď.) a ďalšie dotknuté osoby.

Manažment bezpečnosti obce zodpovedá za:

- vypracovanie Interných bezpečnostných smerníc k zabezpečeniu informačnej bezpečnosti,
- aktualizáciu interných smerníc a bezpečnostných smerníc k zabezpečeniu informačnej bezpečnosti,
- kontrolu dodržiavania interných bezpečnostných smerníc a bezpečnostných smerníc k zabezpečeniu informačnej bezpečnosti,
- vypracováva bezpečnostné príkazy a odporúčania,
- presadzovanie informačnej bezpečnosti obce.

Starosta obce stojí na čele teamu obce. Zvoláva a riadi rokovanie teamu obce. Schvaľuje bezpečnostné smernice.

Zodpovedná osoba ako manažér informačnej bezpečnosti:

- iniciuje kroky na zaistenie súladu so všeobecne záväznými právnymi predpismi SR v oblasti informačnej bezpečnosti,
- koordinuje monitorovanie informačnej bezpečnosť obce,
- zabezpečuje súlad interných aktov s právnymi normami a príslušnými smernicami,

- dozerá nad ustanoveniami zmlúv, kde musí byť zakotvenie dodržiavanie ochrany osobných údajov, ich štandardov a usmernení,
- zabezpečuje súlad bezpečnostnej politiky so zákonom č. 18/2018 Z.z.,
- zabezpečuje aby bezpečnostné opatrenia a interná úprava boli v súlade so zákonom č. 18/2018 Z.z. Zabezpečujú úpravu príslušných smerníc a dokumentov,
- zabezpečuje oboznámenie zamestnancov a tretie osoby s ochranou osobných údajov, zvlášť so zákonom č. 18/2018 Z.z. o ochrane osobných údajov.

Starosta obce

Zabezpečuje plnenie BP v oblasti personálnej bezpečnosti, najmä:

Príchod a odchod zamestnanca, alebo tretej osoby na pracoviská kde sa spracúvajú osobné údaje.

Zabezpečuje súlad interných noriem so všeobecnými právnymi normami v personálnej oblasti.

Čl. 9.

Presadzovanie bezpečnostnej politiky

Bezpečnostná politika je presadzovaná na všetkých úrovniach riadenia obce. Procesy súvisiace s realizáciou bezpečnostnej politiky koordinuje zodpovedná osoba ako manažér informačnej bezpečnosti. Za súlad každého aktíva s bezpečnostnou politikou a súvisiacimi predpismi zodpovedá správca daného aktíva.

Čl. 10.

Bezpečnostné smernice

Bezpečnostné smernice sú vnútorné predpisy obce, ktoré upravujú požiadavky na bezpečnosť aktív a vybrané zásady informačnej bezpečnosti. Vypracúva ich manažér informačnej bezpečnosti v rámci teamu Manažmentu bezpečnosti obce a vydáva ich starosta obce. Nedodržanie bezpečnostných smerníc sa považuje za porušenie bezpečnostnej politiky. Ak nie je uvedené inak, za ich aplikáciu zodpovedajú správcovia príslušných aktív.

Čl. 11.

Bezpečnostné príkazy

Bezpečnostné príkazy sú vnútorné predpisy, ktoré majú jednorazový charakter. Vypracúva ich zodpovedná osoba ako manažér informačnej bezpečnosti za účelom prevencie aktuálnych bezpečnostných hrozieb alebo pri potrebe prijatia konkrétnych bezpečnostných opatrení. Vydáva ich starosta obce. Ich nedodržanie sa považuje za

porušenie bezpečnostnej politiky. Ak nie je uvedené inak, za ich aplikáciu zodpovedajú správcovia príslušných aktív.

Čl. 12.

Bezpečnostné odporúčania

Bezpečnostné odporúčania sú dokumenty, ktoré vydáva zodpovedná osoba ako manažér informačnej bezpečnosti za účelom sumarizovania vybraných zásad informačnej bezpečnosti. Nepodliehajú ďalšiemu schvaľovaniu. Ich dodržiavanie je odporúčané.

Čl. 13.

Súlad so zákonnými požiadavkami

Bezpečnostná politika obce musí byť v súlade so všeobecne záväznými právnymi predpismi, vnútornými predpismi obce a jej zmluvnými záväzkami. Súlad bezpečnostnej politiky s právnymi normami zabezpečuje starosta, Manažment bezpečnosti a zodpovedná osoba.

Čl. 14.

Požiadavky na informačný systém obce

Bezpečnostná politika a príslušné interné smernice k ochrane osobných údajov obce spolu so všeobecne záväznými právnymi predpismi určujú požiadavky na informačné systémy verejnej správy obce.

Čl. 15.

Bezpečnostná dokumentácia informačnej bezpečnosti

Obsahom smerníc sú detailnejšie rozpracované bezpečnostné pravidlá a postupy. Sú to najmä tieto dokumenty:

- Analýza rizík informačnej siete obce,
- Smernica o používaní informačných systémov obce,
- Smernica o prideľovaní, modifikácii a rušení užívateľských prístupov do informačnej siete obce
- Smernica o zálohovaní a archivácií dát nachádzajúcich sa v informačnej sieti obce,
- Smernica o prevádzke informačnej siete obce,
- Katalóg služieb informačnej siete obce,
- Evidencia informačných systémov s osobnými údajmi.

Správcovia aktív sú povinní viesť dokumentáciu ku správe aktív a priebežne ju aktualizovať.

Manažér informačnej bezpečnosti vedie, aktualizuje, určuje umiestnenie a prístupové práva k tejto dokumentácii v elektronickej forme.

Čl. 16.

Bezpečnostné ciele

Určenie bezpečnostných cieľov Obce Herľany z hľadiska informačnej bezpečnosti.

Cieľom bezpečnosti spracovania osobných údajov v obci Herľany je najmä:

- **prevencia;** zaistenie adekvátnej ochrany aktív, aby sa v maximálnej možnej miere predchádzalo bezpečnostným incidentom,
- **pripravenosť;** zaistenie schopnosti efektívne reagovať na bezpečnostné incidenty, minimalizovať ich dopad a čas potrebný na obnovu činnosti informačných a komunikačných systémov po bezpečnostných incidentoch,
- **udržateľnosť;** dosiahnutie, udržiavanie a rozširovanie stanovenej bezpečnostnej úrovne v oblasti informačnej bezpečnosti
- **zabezpečiť kontinuitu činností bez zbytočných prerušení.**

V súvislosti s týmto cieľmi je potrebné ďalej:

- zabezpečiť ochranu aktív,
- zachovanie dôvernosti, integrity a dostupnosti informácií,
- dostupnosť aktív oprávneným používateľom,
- chrániť aktíva obce pred zneužitím,
- umožniť realizáciu VZN obce, uznesení zastupiteľstva, úloh starostu obce a ďalších zamestnancov obce.
- chrániť dobré meno obce,
- umožniť realizáciu rozvojových projektov obce,
- udržiavať súlad s legislatívou týkajúcou sa informačnej bezpečnosti,
- zvyšovať bezpečnostné povedomie zamestnancov obce.

Čl. 17.

Hodnotenie dosiahnutia bezpečnostných cieľov

Bezpečnostný cieľ je dosiahnutý, ak aplikovaním bezpečnostných opatrení je zabezpečené potlačenie, zníženie zistených rizík na požadovanú úroveň.
Požadovaná úroveň akceptácie rizík je daná analýzou rizík. Analýza rizík je súčasťou manažmentu rizík.
Vyhodnocovanie plnenia bezpečnostných opatrení na základe prijatých bezpečnostných smerníc bude dosahované vnútornou, alebo externou kontrolou -

auditom informačného systému obce. Výsledky auditov budú pravidelne vyhodnocované Manažmentom bezpečnosti obce.
Priebežné hodnotenie nasadenia opatrení na aktíva obce je zabezpečované evidenciou bezpečnostných incidentov a ich ohodnotenie z pohľadu dopadu na určené bezpečnostné ciele.

Čl. 18.

Požadovaná úroveň informačnej bezpečnosti

Požadovaná úroveň informačnej bezpečnosti je vtedy, keď:

- miera ohrozenia chránených aktív si nevyžaduje prijímanie mimoriadnych opatrení,
- na elimináciu hrozieb je postačujúca normálna činnosť pri prevádzkovaní informačného systému obce, ktorá vyplýva z interných smerníc,
- je výrazom nastavenej hodnoty veľkosti akceptovateľného rizika,
- ak aktívum spĺňa všetky naň kladené bezpečnostné požiadavky

Bezpečnostné požiadavky sú požiadavky definované:

- legislatívou,
- bezpečnostnou politikou k štandardnej ochrane osobných údajov,
- posúdením vplyvu na ochranu osobných údajov,
- bezpečnostnými príkazmi,
- inou príslušnou dokumentáciou týkajúcou sa informačnej bezpečnosti daného aktíva (prevádzkové predpisy, havarijné plány, požiarno-poplachové smernice,...)

Stanovenie veľkosti akceptovateľného rizika chránených aktív je dané analýzou a manažmentom rizík, ktoré tvoria samostatný dokument. Dosiahnutie primeranej úrovne bezpečnosti aktív obce je zabezpečené manažmentom rizík.

Čl. 19.

Manažment rizík

Manažment rizík je sústavná činnosť vykonávaná za účelom dosahovania primeranej úrovne bezpečnosti aktív obce. Je riadená manažérom informačnej bezpečnosti. Pozostáva z analýzy a riadenia rizík. Spôsob vykonávania manažmentu rizík je v kompetencii starostu obce.

Štandardom pre manažment rizík pre oblasť informačnej bezpečnosti je implementácia systému riadenia a monitorovania rizík v súvislosti s informačným

systémom obce, a to najmä podľa relevantných technických noriem a pravidelného zbierania relevantných údajov súvisiacich s rizikami.

Čl. 20.

Analýza rizík

Analýza rizík je procesom v ktorom sa identifikujú bezpečnostné riziká, ktoré je potrebné kontrolovať alebo akceptovať.
Analýza rizík zahŕňa analýzu:

- aktív,
- hrozieb,
- zraniteľností,
- určenie potenciálnych rizík.

Analýza rizík sa vykonáva aj mimo priestorov obce a obecného úradu. Ide o priestory v ktorých sa nachádzajú informačné aktíva obce, kde prebieha spracovanie – vkladanie údajov do informačnej siete obce, alebo do informačnej siete, kde je obec poverená jeho správou.
Analýza rizík sa musí vykonať aj pri mobilných IKT. (Napr. prenosné počítače používané mimo úradu.)

V prípade závislosti informačného systému obce na informačnom systéme verejnej správy je povinnosťou vykonať aj analýzu rizík a analyzovanie procesov obce, ktoré sú podstatné pre plnenie činnosti obce z hľadiska ich závislosti na informačných systémoch verejnej správy. Musia sa určiť procesy, ktoré nemôžu prebiehať v prípade výpadku alebo obmedzenia funkčnosti príslušných informačných systémov verejnej správy; tieto procesy sú kritickými procesmi.
Analýze rizík kritických procesov sa musí venovať osobitná pozornosť. Kritické procesy sú procesy, kde v prípade zlyhania procesu dôjde k znefunkčneniu časti, alebo celku informačného systému potrebného na výkon samosprávnych funkcií obce. Kritické procesy informačného systému určí Manažment bezpečnosti obce.

Z analýzy rizík vyplynú činnosti, ktoré je potrebné realizovať na zvýšenie bezpečnosti aktív (riadenie rizík). Nezávisle od tejto činnosti správcovia aktív musia samostatne zabezpečovať bezpečnosť svojich aktív. Správcovia spravujú zverené aktíva na základe prijatej bezpečnostnej politiky, opatrení a smerníc, technickej dokumentácie.

Čl. 21.
Riadenie rizík

Analýza rizík je východiskom pre proces riadenia rizík. Proces riadenia rizík pozostáva z:

- určenia celkovej stratégie analýzy a riadenia rizík vhodnej pre obec v súlade s politikou informačnej bezpečnosti obce,

- výber bezpečnostných opatrení pre jednotlivé aktíva, ako reakcia na výsledky analýzy rizík,
    - správa rizika – aplikácia, úprava alebo vylepšenie bezpečnostných opatrení,
    - vyhnutie sa riziku, alebo prenos rizika – prenesenie zodpovednosti za riziko alebo zmena konceptu riešenia,
    - akceptovanie rizika – akceptovanie aktuálneho stavu bez zmeny.
- formulovanie bezpečnostnej politiky informačného systému obce a v prípade potreby aktualizovanie globálnej politiky bezpečnosti obce,
- vytvorenie bezpečnostných projektov systémov a plánov (smerníc) pre implementovanie bezpečnostných opatrení, založených na schválených politikách bezpečnosti systémov. Plán bezpečnosti informačného systému obce bude súčasťou schvaľovaného ročného rozpočtu.

V procese riadenia rizík predkladá bezpečnostný manažér Manažmentu bezpečnosti obce zistené neakceptovateľné riziká s návrhom opatrení na ich elimináciu. Súčasťou návrhu je aj analýza nákladov na realizovanie bezpečnostných opatrení.

Za proces riadenia rizík zodpovedá bezpečnostný manažér a príslušní správcovia aktív. Správcom aktíva môže byť aj užívateľ, ktorý ma pridelené prenosné informačno-komunikačné zariadenie.

Čl. 22

Monitorovanie rizík

Monitorovanie rizík a následné vyhodnocovanie výsledkov musí prebiehať v pravidelných intervaloch, napr. aj formou auditov a testov aplikovaných opatrení. Evidencia a hodnotenie záznamov o informačnej bezpečnosti slúžia ako podklad pre pravidelné preskúmanie fungovania systému. Systém monitorovania rizík je súčasťou bezpečnostnej politiky obce. Monitorovanie rizík denne vykonávajú príslušní správcovia aktív.

Čl. 23
Definícia aktív

Za aktíva sa považujú najmä informácie a prostriedky, ktoré zabezpečujú ich zber, spracovanie, uchovávanie, ochranu a prezentáciu. Aktívami sú najmä:

- **fyzické aktíva;** HW, komunikačné prostriedky, infraštruktúra NN siete, LAN, WAN...
- **informácie/dáta;** dokumenty, bázy dát, súbory,..
- **softvér;** operačné systémy**,** aplikačné programové vybavenie, **...**

- **poskytovanie služieb;** servisné činnosti, poskytovanie infraštruktúry, poskytovanie webových služieb,....,
- **ľudia**; zamestnanci, občania, ...
- **nehmotné hodnoty;** imidž, dobré meno,....

Manažment rizík obsahuje podrobnú analýzu aktív od ktorých závisí činnosť informačného systému obce, alebo ktoré závisia od činnosti informačného systému obce. Aktíva ktoré sú pre obec kritické musia byť zvlášť vyznačené s jasnou definíciou hrozieb a zásad ich ochrany. Kritické aktíva sú tie, ktoré sú nevyhnutné pre zabezpečenie chodu úradu, plnenie úloh vyplývajúcich zo všeobecne platných právnych noriem, prijatých uznesení Zastupiteľstvom obce, úloh starostu obce, plnenie zmlúv a ďalšie. Zaradenie aktív medzi kritické posudzuje manažér informačnej bezpečnosti obce.
Analýzu aktív vykonáva Manažment bezpečnosti obce po predložení bezpečnostným manažérom na základe bezpečnostných cieľov.

Čl. 24

Zodpovednosť za bezpečnosť aktív

Za bezpečnosť každého aktíva zodpovedá jeho správca, prípadne garant aktíva. Analýza aktív obsahuje priradenie aktív ku organizačnej zložke obce, ktorá za tieto aktíva zodpovedá. Katalóg služieb obsahuje zoznam aktív, kde je ďalej uvedené meno a funkčné zadelenie správcu a garanta aktíva. Správcu, resp. garanta určuje starosts písomnou formou. Tento dokument odovzdá manažérovi bezpečnosti obce.
Za dodržiavanie bezpečnostnej politiky v rámci svojej činnosti zodpovedajú zamestnanci obce a všetky tretie osoby na základe zmluvných vzťahov s obcou.

Čl. 25

Bezpečnostné pozície v informačnom systéme obce

Na plnenie bezpečnostnej politiky a zabezpečenie informačnej bezpečnosti sú určené tieto kategórie bezpečnostných pozícií:

- Manažér informačnej bezpečnosti – starosta obce. Zodpovedá za nastavenie a dodržiavanie
- Správcovia siete. Na základe zmluvného vzťahu to môže byť aj menovaná osoba dodávateľa.
- Gestori aplikácií - Spravidla sú to vedúci zamestnanci jednotlivých pracovísk, alebo nimi poverení zamestnanci.
- Používatelia - (osoba ktorá používa informačný systém obce) zamestnanec, občan,....

Čl. 26

Bezpečnostné audity

Dodržiavanie bezpečnostných požiadaviek sa overuje najmä interným auditom informačnej bezpečnosti.

(1) Interné audity.

Interné audity koordinuje, alebo vykonáva najmä manažér informačnej bezpečnosti, ktorý môže byť zároveň interným audítorom. Manažér informačnej bezpečnosti, alebo starosta obce môžu poveriť aj zamestnanca úradu obce na vykonanie interného auditu časti informačného systému obce.

Správcovia a garanti aktív poskytujú pri interných auditoch potrebnú súčinnosť.

Manažér informačnej bezpečnosti, interný audítor má za týmto účelom právo na prístup k potrebným informáciám, ktoré sa týkajú bezpečnosti aktív obce.

Audit pozostáva najmä z kontroly plnenia bezpečnostných požiadaviek, vykonateľnosť nastavených opatrení kladených na príslušné aktíva.

Výsledkom auditu je správa ktorá má spravidla obsahovať:

- rozsah overenia bezpečnosti,
- použité štandardy,
- kto vykonal audit,
- zoznam zistených nedostatkov s odôvodnením, prečo daná skutočnosť je chápaná ako nedostatok,
- odporúčania na odstránenie zistených nedostatkov,
- vyjadrenie k stavu bezpečnosti auditovaného aktíva s uvedením obmedzení a výhrad, ktoré negatívne ovplyvnili priebeh a výsledok auditu,
- stanovisko obecného zastupiteľstva a starostu k správe o výsledku auditu.

Správca aktíva je povinný poznatky získané auditmi využiť na prípravu korekčných a preventívnych opatrení zabezpečujúcich, že bezpečnosť informačného systému obce bude stále na požadovanej úrovni.

Interné audity sa vykonávajú minimálne raz za rok pri kritických aktívach informačného systému obce, alebo po aplikovaní, modifikácii bezpečnostných opatrení. Cieľom auditu je vyhodnotiť účinnosť aplikovaného opatrenia.

(2) Záznamy z auditov a protokolovanie.

Správcovia aktív majú v zmysle prevádzkových smerníc využívať auditné a protokolovancie schopností serverov, sietí a aplikácií na zaznamenávanie detailov všetkých relevantných udalostí.
Pravidelné prezeranie auditných záznamov zabezpečuje bezpečnostný manažér a správca siete. Tieto záznamy musia byť pravidelne vyhodnocované. V prípade

detekcie neautorizovaných aktivít musia príslušní správcovia bezodkladne vykonať vhodné nápravné opatrenia.

(3) Manažér bezpečností po vyhodnotení auditných správ je povinný, v prípade kritických procesov, navrhnúť opatrenia na odstránenie nedostatkov Manažmentu bezpečnosti obce. V ostatných prípadoch je povinný prijať opatrenie ktoré musia správcovia aktív realizovať neodkladne.

(4) Auditné správy a protokoly je potrebné archivovať v zmysle smernice „Správa registratúry“ a Smernice o zálohovaní, archivovaní a obnove.

Čl. 27

Zálohovanie dát

Zálohovanie dát je základným bezpečnostným opatrením pre zabezpečenie prevádzky informačného systému obce. Je základným prvkom v pláne obnovy činností informačného systému a sietí.

Rozdelenie dát podľa dôležitosti:

(1) citlivé dáta; môžu spôsobiť hmotnú aj nehmotnú škodu pri ich strate alebo poškodení, prípadne môže ich znehodnotenie narušiť prebiehajúci alebo uzavretý proces,

- osobné údaje, osobitná kategória citlivých údajov, ktoré sa spracúvajú v informačnom systéme obce, kde musí byť zabezpečené nakladanie s údajmi podľa zákona č. 18/2018 Z. z. o ochrane osobných údajov,

(2) dáta potrebné pre prípravu dokumentov v rozhodovacom procese; (textové súbory, prezentácie, tabuľky...) ich stratou nevznikne hmotná, ani nehmotná škoda, ale môže sa spomaliť alebo narušiť rozhodovací proces,

(3) ostatné dáta; nevznikne hmotná, ani nehmotná škoda, nemôže sa spomaliť ani narušiť rozhodovací proces.

V rámci ochrany údajov sa vo všeobecnosti zálohujú všetky citlivé údaje kategórie 1. Dáta kategórie 2 sa zálohujú na podnet vlastníka dát. Údaje 3. kategórie sa nezálohujú.
Pre proces zálohovanie je dôležité umiestnenie údajov. Dáta kategórie 1. a 2. musia byť umiestnené na serveroch.
Aplikačné programové vybavenie, databázy, používateľské dáta na serveroch, programové komponenty, konfigurácie, a iné dáta potrebné na fungovanie serverov musia byť zálohované tak, aby v prípade zničenia originálnych dát tieto bolo možné obnoviť zo zálohy. Dáta musia byť zálohované na úložisku, ktoré je fyzicky oddelené od úložiska originálnych dát.
Dáta užívateľov IS, ktorí majú dáta na lokálnych diskoch personálnych počítačov sa systémovo nezálohujú (3. kategória dát). Za uchovanie týchto dát plne zodpovedajú sami užívatelia.

Systémová záloha je záloha riadená zálohovacím systémov a ktorá sa vykonáva automatizovane (smernica o zálohovaní) podľa stanovených kritérií a je aplikovaná na príslušné aktíva informačného systému obce.
Podľa prevádzkových potrieb sa môžu vykonávať mimoriadne zálohy dát v časti informačného systému, podľa požiadaviek správcov aktív.
Za zálohovanie dát zodpovedajú správcovia aktív ktorí stanovujú požiadavky na vytváranie záloh.
Za vykonávanie systémových záloh je zodpovedný správca informačnej siete, ktorého určí manažér informačnej bezpečnosti. Správca zabezpečí nastavenie systému zálohovania na základe informácií, ktoré doň vkladajú a aktualizujú jednotliví správcovia aktív.
Proces zálohovania obsahuje Smernica o zálohovaní, archivovaní a obnove.

Čl. 28

Typy záloh

Zálohy rozdeľujeme na:

(1) Prevádzkové; denné, týždenné, systémové zálohy.

(2) Archivačné; systémová, alebo individuálna záloha vykonaná za účelom archivácie dát.

Archivačné zálohy sa vykonávajú najmä po ukončení uceleného informačného procesu. Napr. ukončenie projektu, ročná účtovná uzávierka v EIS, spisová agenda na prelome rokov, modifikácia informačného systému obce, alebo významná zmena informačného systému obce jeho časti, a pod.

Čl. 29

Plán obnovy

Manažment bezpečnosti obce zabezpečí vypracovanie plánov na obnovu činnosti nefunkčných, poškodených alebo zničených kritických informačných systémov obce.
Plán obnovy je súčasťou Smernice o zálohovaní, archivovaní a obnove.
Za vypracovanie zodpovedá manažér informačnej bezpečnosti.

Čl. 30

Monitorovanie bezpečnosti

Monitorovanie bezpečnosti sa vykonáva nepretržite použitím príslušných opatrení. Pre každý softvér, ktorého novoobjavená zraniteľnosť by mohla spôsobiť závažný bezpečnostný incident musí byť zabezpečená aplikácia bezpečnostných záplat v primeranom čase. Ak toto nie je zabezpečené automaticky, správca softvéru je

povinný sledovať informácie o novoobjavených zraniteľnostiach príslušného softvéru a bezpečnostné záplaty aplikovať manuálne.

Čl. 31

Zoznam dokumentov na zaistenie informačnej bezpečnosti

Systém riadenia informačnej bezpečnosti je vymedzený, zhmotnený písomnou dokumentáciou, ktorá ho definuje a opisuje.

Tento systém dokumentov tvorí:

(1) Bezpečnostná politika obce (tento dokument).

(2) Analýza a manažment rizík.

(3) Riadenie bezpečnosti pri projektovaní a vývoji. Obsahuje:

   a. Bezpečnosť projektových prác.

   b. Bezpečnosť vývoja SW.

   c. Bezpečnosť testovania.

   d. Môžu sa využiť vlastné pravidlá, alebo je potrebné prijať bezpečnostné pravidlá dodávateľa informačného systému obce, ktoré je potrebné odsúhlasiť v rámci zmluvy.

(4) Riadenie bezpečnosti pri budovaní informačného systému obce. Obsahuje:

   a. Pravidlá pre výber komponentov.

   b. Pravidlá pre posudzovanie zmien komponentov počas prevádzky.

(5) Riadenie bezpečnosti pri prevádzke.

   a. Manažment konfigurácií a zmien.

   b. Kapacitný manažment.

   c. Technická dokumentácia.

   d. Údržba HW.

   e. Monitorovanie bezpečnostne relevantných zmien.

   f. Auditné záznamy a protokolovanie.

   g. Bezpečnostné testovanie.

   h. Riadenie médií.

   i. Zabezpečené vymazanie pamätí.

j. Oddelenie povinností.

k. Správne používanie SW.

l. Riadenie zmien SW.

m. Archivácia, zálohovanie a obnova dát.

n. Ošetrovanie bezpečnostných incidentov.

(6) Havarijné plánovanie.

(7) Sledovanie stavu a vývoj bezpečnosti. (monitorovanie sieťovej infraštruktúry, monitorovanie činnosti ľudí).

(8) Budovanie bezpečného povedomia.

(9) Audit a preskúmavanie. (audit súvisiaci s ochranou osobných údajov, HW, SW, IS...)

Čl. 32

Vedenie dokumentácie na zaistenie informačnej bezpečnosti

Bezpečnostný manažér vedie dokumentáciu na zaistenie informačnej bezpečnosti v štruktúrovanej forme podľa predchádzajúceho bodu, kde eviduje najmä:

(1) Názov dokumentu.

(2) Kým bol vypracovaný.

(3) Kedy bol vypracovaný.

(4) Kedy bol aktualizovaný a dôvod aktualizácie.

(5) Verzia dokumentu.

(6) Kedy bol schválený, platný a účinný.

Čl. 33

Revízia bezpečnostnej politiky

Bezpečnostná politika sa upraví vždy, keď sa zmení akákoľvek časť podporujúca niektorý zo základných procesov obce (strategický smer, bezpečnostné ciele, štruktúra IT, štruktúra obecného úradu, aktíva a ich štruktúra atď.). Na vykonanie revízie vydá pokyn starosta ako manažér informačnej bezpečnosti, ktorý zabezpečí v súčinnosti s Manažmentom bezpečnosti obce reviziu Bezpečnostnej politiky.
Revízia bezpečnostnej politiky sa vykonáva minimálne raz ročne, alebo v prípadoch ak sa zmení akákoľvek časť podporujúca niektorý zo základných procesov organizácie.

Dôvodom na vykonanie mimoriadnej revízie môžu byť aj navrhované opatrenia pri zistených nedostatkoch z interného, alebo externého auditu, alebo šetrenia bezpečnostného incidentu na kritické aktíva informačného systému obce.

Čl. 34

Zabezpečenie realizácie a dodržiavania schválenej bezpečnostnej politiky

Realizácia a dodržiavanie schválenej bezpečnostnej politiky je zabezpečená systémom riadenia informačnej bezpečnosti ktorý je vymedzený a zhmotnený písomnou dokumentáciou uvedenou v tomto dokumente, resp. prílohách k tomuto dokumentu.
Dodržiavať tento a všetky nadväzné (podriadené) dokumenty je povinná každá osoba vstupujúca, alebo využívajúca informačný systém obce. Jedná sa najmä o zamestnancov obce a tretie osoby (dodávatelia, osoby s osobitným pracovno-právnym vzťahom).
Realizáciu a dodržiavanie schválenej bezpečnostnej politiky priebežne monitoruje Manažment bezpečnosti obce, osobitne manažér informačnej bezpečnosti.
Zabezpečiť a kontrolovať dodržiavanie bezpečnostnej politiky musí každý zamestnanec, ktorý zároveň zodpovedá za všetky činnosti vykonávané v procesoch obce týkajúcich sa bezpečnostnej politiky a informačnej bezpečnosti.

Čl. 35

Personálna bezpečnosť

Všetci zamestnanci obce a osoby, ktoré vykonávajú činnosti pre obec vyplývajúce zo zmluvných záväzkov (ďalej len „tretie osoby“) a prichádzajú do styku s aktívami obce z pohľadu informačnej bezpečnosti, musia byť poučení o schválenej bezpečnostnej politike obce a o povinnostiach z nej vyplývajúcich.
Poučenie musí byť vykonané pred vykonávaním činností vyplývajúcich zo zmluvných záväzkov, alebo z pracovnej zmluvy.
Povinnosti vyplývajúce z bezpečnostnej politiky obce a z pracovného zaradenia zamestnanca musia byť uvedené v jeho pracovnej zmluve, alebo musia byť vydané písomnou formou najbližším priamym nadriadeným zamestnancovi.
Poučenie musí byť preukázateľne dokladované. Dokument o poučení musí obsahovať prehlásenie, že poučovaný bude dodržiavať schválenú bezpečnostnú politiku. Podľa druhu vykonávaných činností musia byť ďalej oboznámení aj o ďalších interných smerniciach a nariadeniach v ktorých sa zabezpečuje ochrana osobných údajov.
Za poučenie zodpovedá **a vykonáva** ho v pracovno-právnom vzťahu zodpovedná osoba, v prípade tretích strán osoba uvedená v zmluve ako osoba oprávnená jednať vo veciach technických a pod., prípadne vedúci zamestnanec z ktorého podnetu, alebo kde predmet zmluvy sa vykonáva.
Dokument o poučení musí byť doručený manažérovi informačnej bezpečnosti ktorý ho zaeviduje.

Čl. 36

Poučenie o právach a povinnostiach pred vstupom do informačného systému obce

Zamestnanci obce a tretia strana musia byť poučení o svojich právach a povinnostiach predtým, ako získajú prístup k informačnému systému obce, v prípade rozdielnych práv a povinností pre rôzne informačné systémy obce sa poučenie zopakuje a jeho obsah sa primerane upraví.
Poučenie musí byť preukázateľne dokladované. Dokument o pouční musí obsahovať prehlásenie, že poučovaný bude dodržiavať uvedené povinnosti.. Podľa druhu vykonávaných činností musia byť ďalej oboznámení aj o ďalších interných smerniciach a nariadeniach. Poučenie vykonáva bezpečnostný manažér. V prípade prístupov do APV správcovia aplikácií, alebo garant aplikácie.
Dokument o poučení musí byť doručený manažérovi informačnej bezpečnosti na evidenciu. Doklad o poučení slúži ako podklad pre zriadenie prístupu.

Čl. 37

Postihy

Nedodržanie schválenej bezpečnostnej politiky môže byť kvalifikované u zamestnancov ako porušenie pracovnej disciplíny a v tom prípade budú vyvodené opatrenia v zmysle zákonníka práce.
V prípade nedodržania bezpečnostnej politiky, alebo niektorého zo súvisiacich predpisov zo strany dodávateľa, môžu byť uplatnené postihy v zmysle zmluvy, kde tieto postihy musia byť taxatívne uvedené.
Porušenie schválenej bezpečnostnej politiky rieši individuálne Manažment bezpečnosti obce, ktorý zároveň stanovuje postihy za nedodržanie bezpečnostnej politiky.
Nedodržiavanie bezpečnostnej politiky je povinný neodkladne hlásiť každý zamestnanec starostovi v prípade, že takéto porušenie zistí. Dodržiavanie bezpečnostnej politiky je povinný vyžadovať a kontrolovať každý vedúci zamestnanec.
V prípade bezpečnostného incidentu, alebo ak je to potrebné na primerané zaistenie bezpečnosti aktíva, môže byť používateľovi odobraný prístup k aktívu z podnet Manažmentu bezpečnosti obce, alebo manažéra informačnej bezpečnosti.

Čl. 38

Nahlasovanie bezpečnostných incidentov

Zamestnanci, používatelia a tretie osoby sú povinní oznamovať bezpečnostné incidenty informačného systému obce manažérovi informačnej bezpečnosti a starostovi obce.

Čl. 39

Postup pri zahájení pracovného pomeru

Pri uzavretí pracovného pomeru zamestnanca, alebo tretej osoby v zmysle zmluvy, je povinnosť postupovať tak, aby uvedeným postupom sa zabezpečilo:

- najmä oboznámenie sa s bezpečnostnou politikou a ďalšími právnymi normami, internými smernicami a nariadeniami, podľa charakteru práce,
- pridelenie IT, ktorými sú najmä počítače, pamäťové médiá, čipové karty, identifikačné karty a pridelenie informačných aktív, ktorými sú najmä programy, dokumenty a údaje,
- zavedenie prístupových práv v informačných systémoch obce.

Za vykonanie všetkých opatrení uvedených v smernici a v tomto dokumente zodpovedá v pracovno-právnom vzťahu nadriadený vedúci pracovník, v prípade tretích strán osoba uvedená v zmluve ako osoba oprávnená jednať vo veciach technických a pod., prípadne vedúci zamestnanec z ktorého podnetu, alebo kde predmet zmluvy sa vykonáva.
Realizácia opatrení z tohto postupu sa realizuje tak, že nadriadený zamestnanec potvrdí vykonanie opatrení.
Formulár s potvrdeným postupom musí byť doručený manažérovi informačnej bezpečnosti. Po splnení týchto opatrení, môže zamestnanec, alebo tretia osoba reálne vykonávať pracovné činnosti, ktoré mu vyplývajú z pracovného zaradenia, alebo zmluvy.

Čl. 40

Postup pri ukončení pracovného pomeru

Pri ukončení pracovného pomeru zamestnanca, alebo tretej osoby v zmysle zmluvy, je povinnosť postupovať tak, aby uvedeným postupom sa zabezpečilo:

1. prípadné obmedzenie vo vzťahu k bývalému zamestnancovi, ktorým je najmä mlčanlivosť a obmedzenie na výkon činností po istú dobu po ukončení zamestnania,
2. navrátenie pridelených zariadení IT, ktorými sú najmä počítače, pamäťové médiá, čipové karty a navrátenie informačných aktív, ktorými sú najmä programy, dokumenty a údaje,
3. odstránenie informácií obce zo zariadení pridelených zamestnancovi, ktorými sú najmä počítače, notebooky, pamäťové médiá a ďalšie mobilné elektronické zariadenia,
4. zrušenie prístupových práv v informačných systémoch verejnej správy,
5. odovzdanie výsledkov práce v súvislosti s informačnými systémami obce, ktorými sú najmä programy vrátane dokumentácie a vlastné elektronické dokumenty.

Za vykonanie všetkých opatrení uvedených v smernici a v tomto dokumente zodpovedá v pracovno-právnom vzťahu nadriadený vedúci pracovník, v prípade tretích strán osoba uvedená v zmluve ako osoba oprávnená jednať vo veciach technických a pod., prípadne vedúci zamestnanec z ktorého podnetu, alebo kde predmet zmluvy sa vykonáva.

Realizácia opatrení z tohto postupu sa realizuje formulárom, kde nadriadený zamestnanec, správca aktíva, prípadne garant aplikácie potvrdia vykonanie opatrení.

Formulár s potvrdeným postupom musí byť doručený manažérovi informačnej bezpečnosti na evidenciu. Po splnení týchto opatrení, pre porušenie právnych povinností pri ochrane osobných údajov môže byť so zamestnancom rozviazaný pracovný pomer a jeho konanie v rozpore so zákonom č. 18/2018 Z.z. o ochrane osobných údajov oznámené Úradu na ochranu osobných údajov. V prípade tretej strany môžu byť potvrdené vykonané práce, dodanie tovaru alebo služieb. Pri porušení ochrany osobných údajov sa bude po ukončení zmluvného vzťahu postupovať ako u zamestnanca.

V Herľanoch, dňa 02. 01. 2019

Ing. Slavomír Rusnák v. r.

starosta Obce Herľany