245/2018

OBEC JESENSKÉ
Sobotská č. 10, 980 02 Jesenské

Smernica č. 1/2018
o bezpečnostných štandardoch architektúry riadenia pre informačné systémy obce Jesenské

	Vypracoval	Schválil
Meno a priezvisko	Tibor Borbás	Mgr. Gabriel Mihályi
Funkcia	Prednosta OcÚ	Starosta obce
Smernica je určená pre	Všetkých zamestnancov obce Jesenské	
Dátum	24.05.2018	24.05.2018
Podpis		

OBSAH SMERNICE

Interná smernica

o bezpečnostných štandardoch architektúry riadenia pre informačné systémy obce Jesenské

I. ODDIEL

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 – interná smernica „Bezpečnostná politika obce Jesenské", prípadne iné interné predpisy a dokumenty.

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) alebo Hypertext Transfer Protocol over Secure Sockets Layer (HTTPs),

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 Jesenské podľa zákona, je ten, kto vykonáva činnosti určené správcom obsahu v súvislosti s technickou

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 Jesenské

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.

Čl. 5

Vecná a personálna pôsobnosť bezpečnostnej politiky

Bezpečnostná politika sa vzťahuje na aktíva obce, 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. Na čele teamu je Mgr. Gabriel Mihályi – starosta obce. Manažment bezpečnosti obce je kombinovaný team ktorého členmi sú:

- Starosta obce,
- Prednosta obecného úradu,
- 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

1. Manažment bezpečnosti obce je vytvorený na úrovni starostu.

2. Členmi teamu obce sú:

- Starosta obce – stojí na čele teamu.
- Správca informačného systému informačnej bezpečnosti.
- Prednosta obecného úradu.
- Poslanec obecného zastupiteľstva - .....
- Zodpovedná osobu, ktorá dozerá na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov obce.
- Ďalšie osoby určené starostom obce.

3. Rozhodnutiami Manažmentu bezpečnosti obce sú povinní sa riadiť všetci zamestnanci obce, zamestnanci (školské zariadenia a KomPaS s.r.o.), 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.

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

1. 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.

2. Správcovia aktív sú povinní viesť dokumentáciu ku správe aktív a priebežne ju aktualizovať.
3. Manažér informačnej bezpečnosti vedie, aktualizuje, určuje umiestnenie a prístupové práva k tejto dokumentácii v elektronickej forme.

2. 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,...)

3. 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

1. 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.

2. 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

1. 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.

2. 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.
3. Analýza rizík sa musí vykonať aj pri mobilných IKT. (Napr. prenosné počítače používané mimo úradu.)

4. 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.
5. 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

- **ľudia**; zamestnanci, občania, ...
- **nehmotné hodnoty;** imidž, dobré meno,....

2. 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.
3. Analýzu aktív vykonáva Manažment bezpečnosti obce po predložení bezpečnostným manažérom na základe bezpečnostných cieľov.

Čl. 24

Zodpovednosť za bezpečnosť aktív

1. 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.
2. 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.
- Správcovia siete.
- Gestori aplikácií - Spravidla sú to vedúci zamestnanci jednotlivých pracovísk, alebo nimi poverení zamestnanci.
- Používatelia - (osoba ktorá používa informačný systém obce) zamestnanec, občan, a pod.

Čl. 26

Bezpečnostné audity

1. Dodržiavanie bezpečnostných požiadaviek sa overuje najmä interným auditom informačnej bezpečnosti.

Interné audity

2. 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.

3. Správcovia a garanti aktív poskytujú pri interných auditoch potrebnú súčinnosť.

2. Rozdelenie dát podľa dôležitosti:

a) 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,

b) 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,

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

3. 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.
4. 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.
5. 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.
6. 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.
7. Podľa prevádzkových potrieb sa môžu vykonávať mimoriadne zálohy dát v časti informačného systému, podľa požiadaviek správcov aktív.
8. Za zálohovanie dát zodpovedajú správcovia aktív ktorí stanovujú požiadavky na vytváranie záloh.
9. 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.
10. Proces zálohovania obsahuje Smernica o zálohovaní, archivovaní a obnove.

Čl. 28
Typy záloh

1. Zálohy rozdeľujeme na:
   a. Prevádzkové; denné, týždenné, systémové zálohy.
   b. Archivačné; systémová, alebo individuálna záloha vykonaná za účelom archivácie dát.

2. 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.

- Sledovanie stavu a vývoj bezpečnosti. (monitorovanie sieťovej infraštruktúry, monitorovanie činnosti ľudí).
- Budovanie bezpečného povedomia.
- 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:

- Názov dokumentu.
- Kým bol vypracovaný.
- Kedy bol vypracovaný.
- Kedy bol aktualizovaný a dôvod aktualizácie.
- Verzia dokumentu.
- Kedy bol schválený, platný a účinný.

Čl. 33

Revízia bezpečnostnej politiky

1. 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 revíziu Bezpečnostnej politiky.
2. Revízia bezpečnostnej politiky sa vykonáva minimálne raz ročne, alebo v prípadoch ak sa zmení akákoľvek časť podporujúca niektorý zo základných procesov organizácie.
3. 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

1. 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.
2. 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).
3. Realizáciu a dodržiavanie schválenej bezpečnostnej politiky priebežne monitoruje Manažment bezpečnosti obce, osobitne manažér informačnej bezpečnosti.
4. 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.

3. Porušenie schválenej bezpečnostnej politiky rieši individuálne Manažment bezpečnosti obce, ktorý zároveň stanovuje postihy za nedodržanie bezpečnostnej politiky.
4. 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.
5. 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

1. 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.

2. 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.
3. Realizácia opatrení z tohto postupu sa realizuje tak, že nadriadený zamestnanec potvrdí vykonanie opatrení.
4. 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

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

a) prípadné obmedzenie vo vzťahu k bývalému zamestnancovi, ktorým je najmä mlčanlivosť a obmedzenie na výkon činností po istú dobu po ukončení zamestnania,

b) navrátenie pridelených zariadení IT, ktorými sú najmä počítače, pamäťové médiá, čipové karty a navrátenie informačných aktív, ktorými sú najmä programy, dokumenty a údaje,

c) odstránenie informácií obce zo zariadení pridelených zamestnancovi, ktorými sú najmä počítače, notebooky, pamäťové médiá a ďalšie mobilné elektronické zariadenia,

d) zrušenie prístupových práv v informačných systémoch verejnej správy,

e) odovzdanie výsledkov práce v súvislosti s informačnými systémami obce, ktorými sú najmä programy vrátane dokumentácie a vlastné elektronické dokumenty.

2. 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.

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

4. 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.

Čl. 41
ZÁVEREČNÉ USTANOVENIE

Táto smernica nadobúda platnosť od 25.5.2018.

V Jesenskom, dňa 24.05.2018

OBEC JESENSKÉ 4

Mgr. Gabriel Mihályi
Starosta obce Jesenské