LENARTOV	SMERNICA STAROSTU OBCE LENARTOV	Číslo
		2/2013

Bezpečnostná smernica

Tieto zásady schválené: Uznesením č.

Vypracoval	Nová smernica/dodatok	Ruší smernicu/dodatok
Meno a priezvisko: Ing. Jana Bľandová		
Organizačný útvar/funkcia: starostka	**Platnosť:** **07.05.2013**	**Účinnosť:** 07.05.2013
Podpis:	**Dátum:** 07.05.2013	**Počet strán:** 1/13

Obsah

Hlava I.
Všeobecné ustanovenia

Čl. 1
Účel smernice

a) Smernica upravuje niektoré práva a povinnosti všetkých zamestnancov obce Lenartov (ďalej len obec), v oblasti ochrany a bezpečnosti majetku, informácií a ďalších hodnôt, ktoré obec vlastní.
b) Súčasťou smernice sú ustanovenia upravujúce bežné vzťahy zamestnancov, činnosť zamestnancov, povinnosti a práva v dobe ohrozenia obce, v dobe útoku na chránené hodnoty a záujmy obce a v dobe po odstránení hrozby alebo odvrátení útoku.

Čl. 2
Základné pojmy

a) Aktíva – sú všetky hmotné i nehmotné hodnoty, ktoré obec vlastní, alebo využíva a slúžia najmä na plnenie jeho služieb obyvateľstvu. Medzi hmotné aktíva patria najmä administratívne priestory, počítače, počítačové siete, komunikačné zariadenia a ďalšie hmotné premety vo vlastníctve obce. Medzi nehmotné aktíva patria pracovné postupy, know-how, údaje o zamestnancoch, ekonomické, finančné a obchodné údaje, majetkové a obdobné práva a ďalší nehmotný majetok. Medzi aktíva patria tiež osoby, ktoré sú v zamestnaneckom, obchodnom, majetkovom alebo inom obdobnom vzťahu k obce.
b) Hrozby – sú vplyvy okolia, iných osôb, zariadení a prostriedkov, ktoré úmyselne, alebo neúmyselne vplývajú na aktíva obce tak, že ich obec nemôže využívať, alebo inak ohrozujú oprávnené záujmy obce.
c) Bezpečnostné opatrenie – je súbor činností, zariadení a postupov, ktoré vykonáva obec na ochranu aktíva pred hrozbou. Rozlišujú sa proaktívne a reaktívne bezpečnostné opatrenia.
d) Proaktívne bezpečnostné opatrenie – je bezpečnostným opatrením, ktoré je vykonávané v dobe, kedy sa hrozba voči aktívu neuplatňuje (preventívne opatrenie) a jeho cieľom je hrozbu úplne odvrátiť (znemožniť jej na aktívum pôsobiť), alebo znížiť jej účinnosť tak, aby dopady na obec boli čo najnižšie.
e) Reaktívne bezpečnostné opatrenie – je opatrenie, ktoré sa vykonáva v dobe, keď sa hrozba realizuje a vplýva na konkrétne aktívum. Jeho cieľom je účinne zabrániť ďalšiemu pôsobeniu hrozby a tak minimalizovať jej účinky a zároveň vytvoriť predpoklady pre efektívne a skoré obnovenie aktíva a návrat do stavu pred pôsobením hrozby.
f) Bezpečnostný incident – je pôsobenie hrozby na aktívum a jej uplatnenie tak, že obce vznikajú škody bez ohľadu na ich rozsah a povahu.
g) Riziko – je odhad pravdepodobnosti možného pôsobenia konkrétnej hrozby na konkrétne aktívum (incidentu) vo vzťahu k predpokladanému dopadu na obec.
h) Riadenie rizika – je súbor organizačných a ekonomických rozhodnutí a opatrení, ktorých účelom je nájsť optimálny pomer medzi ekonomickou náročnosťou vynaloženého úsilia na proaktívne opatrenie a jeho odhadovaným efektom.
i) Prevádzkový záznam – je záznam o chode a činnosti technického prostriedku, organizačnej súčasti a pod. a to najmä ak sú považované za aktíva.
j) Povinná osoba - subjekty podľa zákona 275/2006 Z. z.
k) Externá organizácia – organizácia alebo spoločnosť vstupujúca do informačného systému za účelom jeho údržby alebo obnovy.

l) Mobilné zariadenia – považujú sa prostriedky spracovania ako sú notebooky, palmtopy, laptopy, smart karty a mobilné telefóny.

Čl. 3
Bezpečnostný správca

a) Za organizáciu bezpečnosti a ochrany všetkých aktív obce, za poznávanie hrozieb a rizík zodpovedá „Bezpečnostný správca“.
b) Bezpečnostný správca zodpovedá za:
   1. Vypracovanie a pravidelnú aktualizáciu „Bezpečnostného projektu“, pokiaľ je aktualizácia potrebná.
   2. Bezpečnú, plynulú a spoľahlivú prevádzku informačných systémov v ktorých sa spracovávajú osobné údaje.
   3. Zabezpečenie a organizáciu pravidelných školení zamestnancov ohľadom informačnej bezpečnosti a zaškolenie pracovníkov pri nástupe do zamestnania ohľadom zákona 428/2002 Z. z. o ochrane osobných údajov.
   4. Poučenie zamestnancov obce a tretích strán o svojich právach a povinnostiach predtým, ako získajú prístup k informačnému systému z titulu svojho pracovného zaradenia.

Čl. 4
Hrozby

a) Každý zamestnanec je povinný ohlásiť skutočnosti, ktoré by mohli indikovať zvýšenú pravdepodobnosť hrozby, alebo jej pôsobenie Bezpečnostnému správcovi alebo svojmu nadriadenému.
b) Bezpečnostný správca posúdi na základe indikovanej zmeny stavu hrozieb a na základe poslednej platnej verzie rizikovej analýzy, ktoré aktíva môžu byť hrozbou dotknuté. Bezpečnostný správca je povinný prijať okamžité opatrenia na odvrátenie alebo elimináciu hrozby.

Čl. 5
Bezpečnostné incidenty

a) Detekcia incidentov je súbor činností a opatrení vedúci k včasnému zisteniu bezpečnostného incidentu, resp. k včasnému zisteniu že hrozba pôsobí na niektoré aktívum obce.
b) Detekcia sa vykonáva nasledovným spôsobmi:
   1. Automatizovanými technickými prostriedkami – sú to napr. prostriedky hlásiace výskyt požiaru, snímače zisťujúce pohyb a pod.
   2. Automatickými informatickými (programovými) prostriedkami - sú to špecializované programy, ktoré vyhodnocujú prevádzkové záznamy a indikujú potenciálny incident.
   3. Sústavnou činnosťou zamestnancov – primeraná ostražitosť zamestnancov, najmä Správcov IT aktív a Bezpečnostného správcu a výkon kontrolnej činnosti.
c) Pri zistení incidentu musí byť o tomto informovaný Bezpečnostný správca. Na základe povahy incidentu a zasiahnutých aktív rozhodne bezpečnostný správca o zmene bezpečnostného režimu obce.
d) O každom bezpečnostnom incidente musí byť spracovaný záznam. Záznam spracúva Bezpečnostný správca. Každý zamestnanec je povinný poskytnúť Bezpečnostnému správcovi všetky podklady a údaje, ktoré potrebuje pre spracovanie záznamu o bezpečnostnom incidente.
e) Záznam o bezpečnostnom incidente musí obsahovať:

1. Dátum a čas kedy incident bol zistený, kedy skončil a ak je to možné zistiť aj kedy incident začal.
2. Opis spôsobu, ako bol incident zistený – uvedie sa najmä meno zamestnanca, ktorý incident ohlásil.
3. Dátum a čas, kedy bol zmenený bezpečnostný režim obce.
4. Chronologický opis priebehu incidentu, opis hrozieb ktoré sa realizovali a spôsob akým sa realizovali.
5. Zoznam dotknutých aktív, doklad o škodách a predpokladaná doba zotavenia.
6. Porovnanie s rizikovou analýzou Bezpečnostného projektu – doklad či bolo možné incident očakávať, či boli správne odhadnuté rizikové indexy a pod.
7. Opis prijatých opatrení – doklad kedy a kým boli prijaté, doklad o ich účinnosti a trvaní.
8. Návrh na prijatie opatrení pre zamedzenie recidívy incidentu, odhad pravdepodobnosti recidívy, záznam o úprave rizikovej analýzy Bezpečnostného projektu ak takúto úpravu bolo potrebné vykonať.
9. Zoznam opatrení a nariadení, ktoré boli porušené a mohli spôsobiť že incident nastal, zoznam zamestnancov ktorí tieto nariadenia porušili.

f) Ak nastal bezpečnostný incident vedomou alebo nevedomou činnosťou zamestnanca, bude sankcionovaný podľa príslušných ustanovení zákonníka práce.

Čl. 6
Kontrolná činnosť

a) Kontrolná činnosť je súbor činností, ktorých úlohou je zisťovanie stavu bezpečnosti a ochrany aktív, stavu pripravenosti a účinnosti opatrení a výkon dozoru nad plnením tejto smernice.
b) Kontrolnú činnosť vykonáva bezpečnostný správca.
c) Každý zamestnanec je povinný poskytnúť všetky informácie, ktoré si kontrola vyžiada a sú vo vzťahu ku kontrolným úlohám.
d) Bezpečnostný správca je povinný zabezpečiť výkon kontrolnej činnosti, ktorej predmetom je ochrana a bezpečnosť najmenej 1x za rok.
e) Bezpečnostný správca má právo oboznámiť sa s výsledkami inej kontroly, ktorá bola vykonaná a ktorej predmetom nebolo zisťovanie stavu ochrany a bezpečnosti. Ak vo výsledkoch a záveroch kontroly sú skutočnosti, ktoré signalizujú alebo informujú o narušení bezpečnosti a ochrany je Bezpečnostný správca povinný uvedené informácie okamžite prešetriť formou ním samostatne vykonanej kontroly.

Čl. 7
Bezpečnostné režimy

g) Bezpečnostný režim je stav organizácie činnosti úradu alebo jeho časti, ktorý zodpovedá aktuálnemu ohrozeniu aktív.
h) Stupeň a rozsah bezpečnostného režimu určuje bezpečnostný správca na základe poznania aktuálneho stavu bezpečnosti a úrovne ohrozenia aktív.
i) Rozoznávajú sa nasledovné režimy:
   1. NORMÁLNY – normálny stav bežného chodu úradu, kedy nie je bezprostredne ohrozené žiadne aktívum,
   2. OHROZENIE – činnosť úradu nie je ničím zmenená, alebo ovplyvnená, ale úroveň ohrozenia niektorých 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, bezpečnostný správca vyhlási režim KRÍZA.

3. KRÍZA – činnosť úradu je zmenená následkom účinku niektorých hrozieb na aktíva úradu. 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 úradu. Počas tohto režimu je možné odpojiť časť úradu, alebo celý úrad 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, rekonštrukcii a náhrade poškodených aktív. Bezpečnostný správca navrhuje vedeniu úradu postup pri odstraňovaní škôd. Postup musí obsahovať stanovenie priorít, časovú postupnosť, technickú špecifikáciu opatrení na odstránenie škôd a odhad ekonomickej náročnosti. Bezpečnostný správca v súčinnosti so správcom IT je povinná dôkladne vyšetriť dôvody príčiny, a teda prečo došlo k realizácii hrozieb a škodám. Prechod do režimu NORMÁLNY je možný ak bol schválený postup odstránenia škôd, a ak je možné považovať stav úradu ako celku z bezpečnostného hľadiska za konsolidovaný

j) O zmene Bezpečnostného režimu musia byť ihneď vyrozumení všetci zamestnanci a osoby zodpovedné za výkon IT ochrany úradu.

Hlava II.
Osobitné ustanovenia o niektorých aktívach

Čl. 8
Aktíva informačných technológií

a) Aktívami informačných technológií (IT aktíva) sa rozumejú všetky technické a softvérové prostriedky, ktoré slúžia na ukladanie, prenos a spracovanie informácií v digitálnej podobe bez ohľadu na účel tohto spracovania. Správu IT aktív má na starosti správca IT aktív.
b) Správa IT aktíva musí byť organizovaná tak, aby sa minimalizovala hrozba zneužitia postavenia administrátora.
c) Za ochranu údajov je zodpovedný ten správca IT aktíva na ktorého technických prostriedkoch (pamäťových médiách) sú tieto údaje uložené. K tomuto účelu vykonáva nasledovné činnosti úkony:
   1. Vykonáva, alebo zabezpečuje, kopírovanie údajov na záložné médiá (zálohovanie údajov).
   2. Vykonáva, alebo zabezpečuje, kopírovanie údajov na archívne médiá (archivovanie údajov).
   3. Vykonáva nastavenia prístupových práv k údajom tak, aby k nim mohli pristupovať len oprávnení používatelia.
   4. Inštaluje, spravuje a zabezpečuje také služby (aplikácie), ktoré umožnia zvýšenú ochranu údajov šifrovaním, alebo elektronickým podpisom.
d) Správca IT aktíva 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.
e) Správca IT aktíva je povinný pribežne inštalovať všetky dostupné nové opravy softvérového aktíva, pokiaľ sa tým nenaruší bezproblémový chod a činnosť aktíva.
f) Zakazuje sa používanie neovereného kódu. Pod pojmom neoverený kód sa rozumie taký program, ktorý nemá garanciu výrobcu o jeho spoľahlivosti, alebo nebol overený správcom IT aktíva v izolovanom prostredí či neobsahuje nežiaduce funkcie a chyby. Overenie sa vykonáva tak, aby nemohlo dôjsť k ohrozeniu aktív obce a musí sa preveriť najmä správanie programu v sieťovom prostredí a vo vzťahu k údajom uloženým na pamäťovom médiu počítača.
g) Pri konfigurácii prostriedkov, programov a služieb správca IT aktíva dbá na to, aby sa používali len tie prostriedky, programy a služby, ktoré sú nevyhnutné pre plnenie pracovných úloh a potrieb 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 svoje práci.
h) Správca IT aktíva vedie dokumentáciu o spravovanom aktíve, ktorá obsahuje všetky konfiguračné údaje, údaje o inštalovaných programoch, údaje o adresách a menách a údaje o užívateľoch.

Čl. 9
Zálohovanie a archivovanie údajov

a) Správca IT aktíva je povinný vykonávať zálohovanie a archiváciu všetkých informačných systémov obce a dôležitých údajov na počítačoch.
b) Médiá so záložnými údajmi musia byť uložené v inej miestnosti, než sa nachádza počítač z ktorého boli záložné údaje vyhotovené.
c) Médiá s archívnymi údajmi musia byť uložené v inej budove, než sa nachádza počítač z ktorého boli záložné údaje vyhotovené.
d) Správca IT aktíva 1 x za 6 mesiacov otestuje funkčnosť jedného zálohovacieho média a 1 x ročne vykoná test obnovenia zo zálohovacieho média a otestuje funkčnosť jedného archivačného média.

Čl. 10
Autentizácia

a) Správca IT aktíva, ktoré vyžaduje autentizáciu stanoví autentizačné postupy a mechanizmy.
b) Pre autentizačné mechanizmy stanoví parametre a to najmä vlastnosti hesiel. Stanoví dĺžku, štruktúru a expiračnú dobu hesiel.
c) Správca nesmie povoliť heslá kratšie ako 6 znakov, heslá musia obsahovať aspoň jeden neabecedný znak a ich expiračná doba nesmie byť dlhšia ako 12 mesiacov. Správca nesmie ako heslo použiť takú kombináciu znakov, ktorú by bolo možné priradiť k jeho osobe, akými sú napríklad meno používateľa a jeho rodinných príslušníkov napísané spredu či odzadu, telefónne číslo domov alebo na pracovisko a podobne.
d) Zakazuje sa zverejňovať, alebo inej osobe vyzradiť neverejné autentizačné údaje (heslá). Taktiež sa zakazuje držanie záznamu hesiel (napr. na papieri, v softvérovom súbore alebo prenosnom zariadení) ak takýto záznam nemôže byť bezpečne uložený a ak nebola metóda ich uchovania schválená.
e) Správca IT aktíva môže prideliť autentizačné údaje a prostriedky len zamestnancom obce alebo zamestnancom externej firmy ktorá robí údržbu daného aktíva.
1. Prístupové oprávnenia prideľuje používateľovi správca IT aktíva na základe požiadavky vedúceho základného organizačného útvaru alebo osobitného útvaru. Tvoria ich prístupové meno, prístupové heslo a súbor nastavení, ktoré definujú povolené aktivity používateľa.
f) Prístupové oprávnenia sú prideľované podľa typu používateľa :
   1. Administrátor – prístup k správe a údržbe aktíva, mal by to byť správca IT aktíva.
   2. Používateľ - prístup len k tým modulom aplikácie (aktíva) s ktorými bezprostredne pracuje.
   3. Externý používateľ – zamestnanec externej firmy, ktorá spravuje a udržiava danú aplikáciu (aktívum), prístup je kontrolovaný správcom IT aktív.
g) Personálne oddelenie oznámi skončenie pracovného pomeru zamestnanca Bezpečnostnému správcovi, ktorý o tom informuje všetkých správcov IT aktív, ktorým vydal oprávnenie prideľovať autentizačné údaje a prostriedky. Správcovia sú potom povinní zabezpečiť včasné odobratie autentizačných prostriedkov a znemožnenie prístupu k aktívam.

Čl. 11
Osobné údaje

a) Osobné údaje a personálne údaje môžu byť ukladané a prenášané len zabezpečeným spôsobom.
b) Zabezpečenie personálnych údaj sa vykonáva nasledovnými opatreniami:
   1. Dokumenty na papieri a na pamäťových médiách musia byť ukladané v kovovej uzamykateľnej skrini, ktorá je umiestnená v uzamykateľnej miestnosti. Vstup do tejto miestnosti je povolený len vedúcemu personálneho oddelenia a ním určeným zamestnancom.
   2. Prenášanie papierových dokumentov s personálnymi údajmi je možné len v uzavretých a nepriehľadných schránkach alebo obaloch.
   3. Prenášanie digitálnych dokumentov sieťou, emailom, alebo na médiách je možné vykonávať len v zašifrovanej podobe.
   4. Miestnosti v ktorých sa spracúvajú osobné údaje musia byť v neprítomnosti zamestnanca uzamknuté. Okná miestností musia byť opatrené žalúziami, ktoré znemožnia odpozeranie údajov. Ak sa miestnosť nachádza na prízemí, musia byť okná opatrené mrežami. Miestnosti musia byť vybavené zábranným opatrením, ktorá zamedzí neoprávneným osobám nahliadať do dokumentov a na obrazovky počítačov, alebo odcudziť média a dokumenty. Obrazovky počítačov musia byť umiestnené tak, aby nepovolané osoby z nich nemohli prečítať osobné údaje.
   5. Zakazuje sa zhotovovať (tlačiť) dokumenty s osobnými údajmi na iných zariadeniach než na zariadeniach, ktoré sú umiestnené v zabezpečených priestoroch.
   6. Zakazuje sa ponechávanie dokumentov s osobnými údajmi v tlačových zariadeniach napr. kopírkach, tlačiarňach alebo faxoch bez dozoru.

Čl. 12
Ekonomické údaje

a) Ekonomickými údajmi sú všetky údaje o ekonomike a financiách obce, údaje o obchode, marketingu a obchodných partneroch. Do skupiny ekonomických údajov sa zaraďujú aj údaje o know-how a technologické informácie.
b) Ochrana ekonomických údajov sa vykonáva rovnakým spôsobom ako ochrana osobných údajov, okrem šifrovania.
c) O potrebe zašifrovania ekonomických údajov rozhoduje Bezpečnostný správca.

Čl. 13
Fyzická ochrana

a) Každý zamestnanec je zodpovedný za fyzickú bezpečnosť svojho pracoviska a zverených mu pracovných prostriedkov. Pri odchode z pracoviska je povinný uzamknúť pracovisko, uzavrieť okná a prekontrolovať zariadenia či nemôžu spôsobiť požiar alebo inú haváriu. Ak zamestnanec nemôže túto povinnosť splniť oznámi to ihneď svojmu nadriadenému, alebo Bezpečnostnému správcovi.
b) Umiestnenie aktív musí byť vykonané tak, aby sa účinne zabránilo ich odcudzeniu alebo fyzickému poškodeniu.
c) Bezpečnostný správca môže rozdeliť obecný úrad a pod obec patriace budovy na bezpečnostné zóny a určiť, ktoré osoby môžu do týchto zón vstupovať. Pre zamedzenie vstupu nepovolaných osôb do bezpečnostných zón prijme účinné opatrenia.

Čl. 14
Pracovné stanice

a) Zamestnanec je povinný používať zverené pracovné stanice len na pracovné účely. Porušenie tohto ustanovenia sa považuje za bezpečnostný incident.
b) Zamestnanec môže na pracovných staniciach používať výlučne len programové vybavenie nainštalované správcom IT aktíva, resp. nainštalované s jeho preukázateľným súhlasom. Zamestnanec nemôže na pracovnej stanici meniť žiadne programové vybavenie a tiež nemôže meniť konfiguráciu programového vybavenia s výnimkou zmien, s ktorými sa mení vzhľad pracovného prostredia.
c) Zamestnanec nemôže vytvárať a distribuovať kópie programového vybavenia inštalovaného na pracovnej stanici.
d) Zamestnanci pred opustením pracoviska sú povinní ukončiť prácu s aplikačným programovým vybavením, odhlásiť sa zo siete a operačného systému a dohliadnuť na vypnutie pracovnej stanice.
e) Pri krátkodobej neprítomnosti môže zamestnanec nahradiť odhlásenie sa zo systému a vypnutie pracovnej stanice, spustením šetriča obrazovky s heslom resp. jej uzamknutím.
f) Zamestnanci sú povinní vykonávať základnú údržbu pracovnej stanice (čistenie povrchu obrazovky, klávesnice, myši..). Odstraňovanie nepotrebných súborov dátových adresárov a pomocných adresárov operačného systému (Kôš, Temp, Temporary Internet Files...) prípadne spustenie programov určených na údržbu (scandisk, defragmentácia...) vykonávajú zamestnanci v spolupráci so správcom IT aktíva.
g) Zamestnanci sú povinní po inštalácii novej verzie programového vybavenia po dobu minimálne jedného týždňa venovať zvýšenú pozornosť činnosti systému a kontrolovať správnosť výsledkov jeho práce. Prípadne odchýlky od požadovaného stavu sú povinní čo najúplnejšie zdokumentovať a bezodkladne ohlásiť správcovi IT aktíva.
h) Zakazuje sa pripájať do siete obce vlastné zariadenia (napr. notebooky, PDA, tlačiarne a pod.) a taktiež povoliť pripojenie cudzej osoby do siete obce bez vedomia Bezpečnostného správcu. Taktiež sa zamestnancom zakazuje používať vlastné USB kľúče. Porušenie tohto bodu sa považuje za bezpečnostný incident.

Čl. 15
Mobilné zariadenia

a) Pridelenie jednotlivých mobilných zariadení okrem mobilných telefónov riadi správca IT aktíva.
b) Pred odovzdaním zariadenia zamestnancovi je správca IT aktíva povinný nainštalovať na zariadenia softvér na antivírovú ochranu, kryptovanie a šifrovanie citlivých údajov a softvér pre riadenie šifrovaného prístupu do lokálnej siete obce, ak to zamestnanec z titulu svojich pracovných povinností potrebuje.
c) Správca IT aktíva je povinný zabezpečiť aby zariadenie pri pripojení do lokálnej siete úradu automaticky od zálohovalo citlivé a osobné údaje.
d) Zamestnanec je zodpovedný za fyzickú ochranu zariadenia pred krádežou alebo poškodením.
e) Krádež mobilného zariadenia sa považuje za bezpečnostný incident.

Čl. 16
Antivírová ochrana

a) V prípade, že sa na pracovnej stanici používateľa zobrazí varovanie, že sa na disku alebo prenosnom médiu nachádza vírus alebo iný škodlivý kód, používateľ nesmie toto varovanie ignorovať. V prípade, že zavírené prenosné médium patrí inému subjektu, používateľ ho označí ako zavírené a vráti majiteľovi. V prípade zavírenia vlastného pevného disku alebo prenosného média, používateľ túto skutočnosť bezodkladne oznámi správcovi IT aktíva, prípadne po konzultácii s ním odstráni vírus z príslušného pamäťového média.
b) V prípade objavenia vírusu v prijatej elektronickej pošte používateľ bezodkladne o tejto udalosti upovedomí správcu IT aktíva. V žiadnom prípade zavírenú elektronickú poštu neposiela inému adresátovi a na svojej pracovnej stanici ju uschová len dočasne a len na žiadosť správcu IT aktíva (na účely ďalšej analýzy prieniku vírusu do systémov pracoviska.).
c) Správca IT aktíva je povinný zabezpečiť inštaláciu a pravidelnú aktualizáciu antivírusových detekčných a nápravných softvérov na prehliadanie počítačov, serverov a médií na rutinnej báze. Vykonávané kontroly musia zhŕňať:
   1. Kontrolu všetkých súborov na elektronických alebo optických médiách, ako aj súborov prijatých prostredníctvom počítačovej siete z hľadiska prítomnosti škodlivého kódu ešte pred používaním.
   2. Kontrolu príloh elektronickej pošty a siahnutých súborov z hľadiska výskytu škodlivého kódu ešte pred spustením, táto kontrola by sa mala vykonávať na rozličných miestach, napr. na elektronických poštových serveroch, pracovných staniciach a pri vstupe do siete prevádzkovanej obcou.
   3. Kontrolu pred nevyžiadanou poštou – Spamom.
   4. Kontrola webových stránok z hľadiska výskytu škodlivého kódu.
d) Správca IT aktíva je povinný venovať zvýšenú pozornosť tomu aby škodlivý kód nebol zavedený počas výkonu pohotovostných procedúr alebo procedúr údržby.

Čl. 17
Prístup do siete internet a mailová komunikácia

a) Každý zamestnanec, ktorému bol umožnený prístup do siete internet je povinný rešpektovať nasledovné zásady:
   1. Prístup do siete internet využívať predovšetkým v súlade so svojou pracovnou náplňou.
   2. Dodržiavať etické zásady a zdržiavať sa činností, ktoré by mohli viesť k poškodeniu dobrého mena pracoviska alebo k iným škodám.
   3. Komunikácia v internete spravidla nie je chránená pred “odpočúvaním“. V prípade potreby prenosu osobných údajov je nevyhnutné tieto údaje pred prenosom zabezpečiť šifrovaním. Ak nie je zamestnanec schopný prenos takto zabezpečiť, nie je prípustné ho uskutočniť.
   4. Je zakázané zo siete internet preberať nelegálny obsah (softvér, súbory chránené autorskými právami a pod.). Preberanie spustiteľných programov je povolené len po konzultácii so správcom IT aktíva.
b) Výber blokovaných stránok bude v kompetencii správcu IT aktív na základe webovej analýzy. V prípade veľkého prenosu objemu dát nesúvisiacich s pracovnou činnosťou zamestnanca vyplývajúceho z výsledkov webovej analýzy, má pravo správca aktív IT zakázať a znemožniť užívateľovi prístup do internetu.

c) Zamestnanec je povinný používať elektronickú poštu len v súlade so svojou pracovnou náplňou.
d) V prípade svojej dlhodobej neprítomnosti na pracovisku zamestnanec zabezpečí funkciu automatickej odpovede na prichádzajúci e-mail, kde presne uvedie obdobie svojej neprítomnosti, poprípade osobu, ktorá ho zastupuje s uvedením kontaktu.
e) Zamestnanec je povinný zabezpečiť správne adresovanie príjemcu mailovej správy a na prenos správ používať všeobecne dané dátové štandardy stanovené vo výnose Ministerstva financií 312/2010 o štandardoch vo verejnej správe. Zakazuje sa posielanie súborov v prílohách iných ako:
    1. textových súborov .rtf, .html, .htm, .xhtml, .pdf, .odt, .txt
    2. grafických súborov .gif, .png, .jpg, .jpeg, .jpe, .jfif, .jfi, .jif, .tif, .tiff, .swf, .svg
    3. audio a video súborov .mpg, .mpeg, .mp4, .mp3, .ogg, .oga, .ogv, .ogx, .wav, .aiff
    4. súborov s kompresiou .zip, .tar, .gz

    Komunikácia v iných formátoch (napríklad MS Office .doc, .docx, .xls, .xlsx, .pps, .ppt,…) je možná len po obojstrannej dohode a vzájomnom súhlase. Žiadny subjekt nie je oprávnený požadovať komunikáciu v týchto formátoch. Zakazuje sa posielať súbory typu .exe, .com, .bat, .scr, a pod.
f) V prípade posielania citlivých a osobných údajov je povinný použiť kryptovanú komunikáciu za použitia kryptovacieho kľúča, ktorý mu bol na požiadanie vydaný Bezpečnostným správcom.
g) Používať elektronickú poštu len na legálne účely, obsah dát odosielaných v rámci siete úradu a cez internet nesiem byť v rozpore s dobrými mravmi.
h) Je zakázané používanie elektronickej pošty na súkromné účely.
i) Rešpektovať zákaz posielať reťazové a hromadné e-maily, reklamné správy a pod.
j) Pravidelne vykonávať údržbu vlastnej elektronickej posty (zálohovanie správ, mazanie, zhutňovanie a pod.).
k) Zakazuje sa používanie messengerov, výnimky sa uskutočnia len na základe povolenia nadriadeného a správcu IT aktíva.
l) Porušenie ustanovení tohto článku sa považuje za bezpečnostný incident.

Čl. 18
Manipulácia s médiami

a) Obsahy akýchkoľvek opakovateľne použiteľných médií, ktoré majú byť odnesené z organizácie, musia byť zmazané, ak už nie sú ďalej potrebné.
b) Pre všetky médiá s citlivými a osobnými údajmi odnášané z organizácie je potrebné urobiť autorizáciu a vykonať záznam o vynesení. Pričom tento záznam musí obsahovať dátum, typ média, aké dáta sú uložené na médiu, dôvod vynesenia a kto médium vyniesol z organizácie.
c) Všetky média s osobnými a citlivými údajmi musia byť uložené v bezpečnom, chránenom prostredí, podľa špecifikácie výrobcu.
d) Informácie, ktoré majú byť uchované po dobu dlhšiu ako je doba životnosti média, na ktorom sú uložené (na základe špecifikácie výrobcu) musia byť uložené aj na inom mieste, aby sa tak predišlo strate spôsobenej nečitateľnosťou média
e) Média ktoré nie sú už potrebné sa musia bezpečne a spoľahlivo zlikvidovať.

Čl. 19
Zamestnanci externej organizácie

a) Prístup zamestnancov externej organizácie zriaďuje správca IT aktíva na základe schválenia Bezpečnostným správcom. Bezpečnostný správca si vedie zoznam povolených prístupov k jednotlivým aktívam.

b) Správca vydá zamestnancovi externej organizácie prístupové heslo a práva podľa článku 10 tejto smernice.
c) Správca IT aktíva je povinný zabezpečiť bezpečný šifrovaný prístup zamestnanca tretej strany k jeho aktívu.
d) Zamestnanci externej organizácie sú povinný pred prihlásením k IT aktívu o tejto skutočnosti oboznámiť správcu IT aktíva buď prostredníctvom mailu alebo telefónom. Na základe tohto oznámenia im správca IT aktíva povolí pripojenie. Po skončení údržby alebo inej činnosti zamestnancom externej organizácie, správca IT aktíva zruší možnosť pripojenia.
e) Bezpečnostný správca je povinný poučiť zamestnancov externej organizácie o ochrane a mlčanlivosti ohľadom osobných a citlivých údajov. Táto skutočnosť by mala byť zakomponovaná do zmluvy s externou organizáciou.

Čl. 20
Záverečné ustanovenia

a) Táto smernica nadobúda platnosť dňom jej podpisu a účinnosť od .....2013.
b) Bezpečnostný správca je povinný s touto smernicou oboznámiť všetkých zamestnancov.
c) Na túto smernicu sa nevzťahuje povinnosť zverejnenia v zmysle zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám v znení neskorších predpisov.

Schválené dňa xx.xx.xxx

_____
Starosta obce