Obec HRUŠOV

IČO:00328308

Bezpečnostný projekt obce HRUŠOV
na ochranu osobných údajov

V Hrušove dňa 20,júna 2014

Starosta obce Hrušov schvaľuje tento bezpečnostný projekt vypracovaný na základe zákona č. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

V Hrušove 20. júna 2014

Gabriel PARTI
starosta obce

Obsah

Osoby zodpovedné za ochranu osobných údajov

p. Gabriel PARTI, starosta obce (štatutárny orgán)

p. Ing.Katarína ZSEBIKOVÁ, osoba zodpovedná za ochranu osobných údajov za Obecný úrad Hrušov

p. Attila POGÁNY, osoba zodpovedná za Hospodársku činnosť OcÚ Hrušov.

Úvod

V súlade s § 20 zákona NR SR č. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov vydávam tento bezpečnostný projekt, ktorým definujem primerané technické, organizačné a personálne opatrenia na zabezpečenie bezpečnosti osobných údajov pred ich prípadným odcudzením, stratou, poškodením, neoprávneným prístupom, zmenou a rozširovaním.

Bezpečnostný projekt vymedzuje rozsah a spôsob technických, organizačných a personálnych opatrení potrebných na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti.

Bezpečnostný projekt je spracovaný v súlade so základnými pravidlami bezpečnosti informačného systému vydanými bezpečnostnými štandardmi, právnymi predpismi a medzinárodnými zmluvami, ktorými je Slovenská republika viazaná.

Vymedzenie základných pojmov

Všeobecné

systém ochrany osobných údajov
- predstavuje súhrn prostriedkov, metód, činností opatrení a zariadení, ktoré vo svojom komplexe pôsobia k zamedzeniu úniku osobných údajov alebo ich vyzradeniu, zneužitiu pred nepovolanými osobami.

aktíva
- sú hmotné a nehmotné objekty, ktoré sú súčasťou chráneného systému, pričom ich narušením dochádza k strate dôvernosti, dostupnosti a integrity, alebo až k strate predmetu ochrany.

bezpečnostná politika
- je súhrn zákonov predpisov, nariadení a pravidiel, podľa ktorých sa chráni, distribuuje a riadi prístup k informáciám. Bezpečnostná politika stanovuje spôsob a vykonáva opatrenia pre ochranu skutočností. Pre vzťah medzi subjektom a objektom predstavuje súhrn pravidiel, predpisov a nariadení, podľa ktorých určuje vzájomné pôsobenie. Súčasťou bezpečnostnej politiky je i personálna bezpečnosť

osobný údaj
- osobnými údajmi sú údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, pričom takou osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu a ich význam treba chrániť pred zneužitím, poškodením, zničením, stratou alebo odcudzením

objekt
- je pasívna časť", ktorá prijíma, spracúva, prenáša, ukladá informáciu. Prístup k objektu znamená oboznamovanie sa s informáciami, ktoré obsahuje. Objekt môže byť sektor na disku, záznam na magnetofónovej páske, časť operačnej pamäti, externé nosiče informácií

subjekt
- je aktívna časť. Môže ňou byt' osoba, proces ,zariadenie, ktoré zabezpečuje tok informácií medzi objektmi a spôsobuje zmenu stavu systému

zdroj
-je čas, informácie, objekty alebo procesy, ktoré sú použité alebo spotrebované pri spracovaní informácii

dôveryhodný výpočtový systém
- je systém, ktorého organizačné, technické a programové vybavenie a bezpečnostné opatrenia sú na takej úrovni, že dovoľuje bezpečne pracovať s informáciami

chránený systém
-je tvorený jednotlivými objektmi, pre ktoré je definovaný určitý stupeň ochrany

elektronická zabezpečovacia signalizácia
- je systém elektronických prostriedkov určených k fyzickej ochrane a technickej ochrane určených priestorov a aktív pred nepovolaným vniknutím, narušením, požiarom a iným vplyvom, ktoré môžu spôsobiť poruchu systému

elektronická požiarna signalizácia
- je systém elektronických prostriedkov určených k ochrane priestorov a aktív pred požiarom

Odborné

zadávateľ úlohy
-je orgán alebo organizácia, ktorá podľa platných predpisov požaduje spracovanie informácii, obsahujúce osobné údaje, pomocou technických prostriedkov

užívateľ
- je orgán alebo organizácia, ktorá využíva informácie z výsledkov spracovania pre vlastnú odbornú činnosť a riadenie. Táto organizácia zodpovedá za vydanie a dodržiavanie smerníc, režimových opatrení, pre ochranu osobných údajov subjektami. Užívateľom je osoba ktorá je v priamej interakcii s technickými prostriedkami

riešiteľ
- je subjekt, ktorý spracúva projektovú úlohu. Spracovateľom môže byt' právnická alebo fyzická osoba, ktorá na zmluvnom základe vypracúva bezpečnostnú, programovú, projektovú a prevádzkovú dokumentáciu k ochrane osobných údajov

bezpečnostný pracovník
- je subjekt určený vedúcim organizácie k obhospodarovaniu prevádzkových systémov určených pre ochranu a spracúvanie osobných informácii. Vykonáva kontroly v oblasti dodržiavania zásad manipulácie, ukladania, spracovania, prenášania a archivovania osobných informácii

kontrolný záznam (audit)
je súbor údajov, ktoré poskytujú prehľad o činnosti a aktivitách subjektu na technických prostriedkoch

dôvernosť
-je súhrn opatrení k ochrane aktíva pred nepovolaným prístupom

integrita
- je charakteristika systému z hľadiska presnosti a komplexnosti zabezpečenia informácii a zabezpečenia programového vybavenia

dostupnosť
- je charakteristika systému z hľadiska oprávneného prístupu k utajovaným informáciám.

Bezpečnostný zámer

Bezpečnostný zámer vymedzuje základné bezpečnostné ciele, ktoré je potrebné dosiahnuť na ochranu informačného systému pred ohrozením jeho bezpečnosti.
Obsahuje súhrn objektov, subjektov, metód, opatrení, prostriedkov, a procesov slúžiacich k minimalizácii narušenia chránených aktív.
Definuje úrovne bezpečnosti:

- Globálna
- Informačná
- Počítačová

Základné bezpečnostné ciele

Obsahujú formuláciu základných bezpečnostných cieľov.

1. Zabezpečiť ochranu osobných údajov pred odcudzením, stratou, poškodením, neoprávneným prístupom, zmenou a rozširovaním.
2. Minimalizovať riziká pri prevádzke informačného systému pred napadnutím aktív.
3. Zabezpečiť kontinuitu činností v informačnom systéme v prípade narušenia.
4. Zabezpečiť ochranu aktív.
5. Zabezpečiť ohodnotenie o ošetrenie rizík.
6. Stanoviť rovnováhu medzi akceptovateľnými stratami a jednorázovými a ročnými nákladmi.
7. Zabezpečiť realizáciu preventívnych opatrení.
8. Zabezpečiť pripravenosť na aktívny prístup pri riešení akéhokoľvek narušenia.
9. Analyzovať možnosti napadnutia.
10. Stanoviť úrovne bezpečnosti.

Úrovne bezpečnosti

1. <u>Globálna bezpečnosť</u>

Patria sem všetky opatrenia slúžiace k zabezpečeniu všeobecnej bezpečnosti, pôsobiace na všetky druhy aktív. (technologické zariadenia, prevádzky, objekty, HIM, NIM, zamestnanci, financie..)

Špecifikácia globálnych opatrení.

- Protipožiarne smernice
- Organizačné opatrenia
- Návrh rozpočtu obsahujúci financovanie bezpečnosti
- Personálne opatrenia

2. Informačná a komunikačná bezpečnosť
Zahrňuje bezpečnostné opatrenia týkajúce sa informačného systému ako celku. K aktívam patria dokumenty, komunikačné linky, internet, mobilné telekomunikačné zariadenia.

3. Počítačová bezpečnosť
Zahrňuje aktíva ako sú počítačové servre, pracovné stanice, pamäťové médiá, operačné systémy, aplikácie, databázy.

Bezpečnostné opatrenia

Formulujú minimálne požadované bezpečnostné opatrenia.
Bezpečnostná politika obce Hrušov je súhrn:

- organizačných
- technických
- personálnych

opatrení, ktoré zabezpečujú ochranu dôverných skutočností v jeho pôsobnosti .

1. Špecifikácia organizačných opatrení a spôsob ich využitia

Organizačné opatrenia predstavujú zákonné normy, predpisy a nariadenia, podľa ktorých sa riadi činnosť určených pracovísk pre spracúvanie, ukladanie, manipuláciu, archiváciu a skartáciu osobných údajov.

Požiadavky na organizačné opatrenia
Zabezpečenie aktív pomocou organizačných opatrení, ktorými sú organizované pracovné činnosti a postupy pri zabezpečovaní globálnej, informačnej a počítačovej bezpečnosti.
Organizačné opatrenie obsahujú:

- Definovanie organizačnej štruktúry
- Rozdelenie kompetencií
- Určenie pracovných a bezpečnostných postupov
- Organizačné opatrenia

Základnú normu tvorí organizačný poriadok obce Hrušov.
Starosta obce menuje krízový štáb (havarijný tím), ktorý zabezpečí kontinuitu činností v prípade narušenia informačného systému, mimoriadnej udalosti, živelnej pohromy a inej nepredvídanej situácie.
Pre krízový štáb musí byť zrejmé:

- Personálne obsadenie
- Hierarchia tímov, podriadenosť a zodpovednosť
- Spôsob komunikácie
- Prerozdelenie úloh medzi členmi tímov
- Krízový štáb má právomoci vydávať rozhodnutia

2. Špecifikácia technických opatrení a spôsob ich využitia

Technické opatrenia predstavujú všetky určené technické prostriedky (aktíva), určené pre spracúvanie, manipuláciu, archiváciu a skartáciu dôverných skutočností a všetky prostriedky a metódy ochrany určených technických prostriedkov.
Používanie technických prostriedkov pre spracúvanie osobných informácii je povolené iba osobám oprávneným oboznamovať sa s osobnými informáciami.
Technické prostriedky, sú využívané zásadne zamestnancami, ktorí majú tieto prostriedky pridelené. Zamestnanca zodpovedného za výpočtovú techniku určí starosta obce Hrušov.

Technickými prostriedkami na účely zákona NR SR č. 122/2013 Z. z. v znení neskorších predpisov sú :

1. **Výpočtová technika** - ktorou sa zabezpečuje vytváranie, spracovávanie, tlač a uchovávanie dát a informácii. Výpočtovú techniku tvorí komplex zariadení (technické a programové vybavenie, periférne zariadenia a podobne) a ich vzájomné prepojenie telekomunikačnými systémami a počítačovými sieťami a dátové nosiče (diskety, pásky, CD disky a pod.)
2. **Zariadenie na vyhotovenie písaného textu** - písacie stroje mechanické, elektrické - elektronické, tlačiarne pri osobných počítačoch a severoch, rozmnožovacie stroje.

a) Písaný text vyhotovený na mechanickom písacom stroji je originál. Kópie sa vytvárajú pomocou indigového papiera. Použitý indigový papier, ktorým sa vytvorili kópie osobných písaných textov musí byt' uložený, a manipulovať s ním sa musí, ako s písomnosťou obsahujúcou osobné údaje. Pre prácu s originálmi a kópiami platia všeobecne záväzné predpisy vyhlášky.

b) Písacie stroje elektrické sú zariadenia obdobné ako písacie stroje mechanické, pričom niektoré funkcie sú na elektrický pohon. Pre prácu s nimi platí bod a).

c) Písacie stroje elektronické pracujú na báze elektronických prvkov, majú pamäťový prvok, digitálny displej, alebo s možnosťou prepojenia na osobný počítač. Ostatné prvky obdobné ako u písacích strojov elektrických. Pre prácu s nimi platí bod a) a technické podmienky ako na počítačoch.

d) Tlačiarne sú periférne zariadenia výpočtovej techniky, na priame vytváranie tlačených dokumentov.

Rozmnožovacie zariadenia slúžia na vytváranie verných kópii z originálov.
Telekomunikačné systémy a siete slúžia na prenos informácií na diaľku. Vo vedeniach môžu byt' prepojené optickou cestou, alebo pomocou elektromagnetických vĺn.
Dátové nosiče sú médiá, ktoré slúžia na zaznamenávanie a archivovanie dát. Môžu byt' mechanické, magnetické, optické alebo magnetické.
Záznamová technika zaznamenáva a ukladá informácie transformované elektronickou alebo optickou cestou na dátové nosiče.

Požiadavky na bezpečnostné opatrenia pre technické prostriedky používané k spracovaniu osobných informácii a podporné prostriedky na ochranu určených technických prostriedkov

Aktíva určené pre spracovanie osobných informácii budú v podmienkach obce chránené pred porušením dôvernosti informácie, stratou integrity a zamedzeniu dostupnosti

pred nepovolanými osobami a technickými prostriedkami, ktoré nie sú zaradené do bezpečnostného projektu.
Aktíva predbežne určené: počítače samostatné, počítače zapojené do siete vrátane servov, tlačiarne, modemy, faxy, nahrávacie zariadenia pre audio a video, zálohovacie médiá (pásky, CD disky, diskety a pod.), aplikačné programy, databáza, lokálna sieť, určené pracoviská pre spracovávanie dôverných informácií podľa zákona NR SR č. 122/2013 Z.z. v znení neskorších predpisov.

Zabezpečenie aktív: je tvorené programovými, mechanickými, režimovými a technickými prostriedkami ochrany.

programová metóda (P)
- antivírové programy ,vstupné a prihlasovacie heslá, používanie iba autorizovaných programov, ochrana pomocou kľúča PC, heslo BIOSu, heslo do aplikácie, heslo do siete

mechanická metóda (M)
- vybavenie určených pracovísk mrežami, plnými dverami, zaslepenými kľučkami, trezormi, ohňuvzdornými plechovými skriňami

režimová metóda (R)
- určenie režimu vstupu na pracoviská, zákaz zdržovania sa po pracovnej dobe, určenie zodpovedných zamestnancov za bezpečnosť, určenie podmienok vstupu na pracovisko a spôsob opustenia pracoviska a pod.

technická metóda (T)
- zabezpečenie pracoviska s centrálnou databázou elektronickou požiarnou signalizáciou napojenou na centrálny pult požiarnej ochrany

3. Špecifikácia personálnych opatrení a spôsob ich využitia

Personálne opatrenia -personálna bezpečnosť- je zákonom stanovený postup (§19 a §23 zákona NR SR č. 122/2013 Z.z. v znení neskorších predpisov), ktorý určuje predpoklady k získaniu oprávnenia oboznamovať sa s osobnými údajmi a určuje povinnosti oprávnených osôb.
Personálna bezpečnosť zahŕňa vedenie predpísanej evidencie, na ochranu osobných údajov. Starosta obce Hrušov písomne poverí výkonom dohľadu nad ochranou osobných údajov spracúvaných podľa zákona NR SR č. 122/2013 Z.z. v znení neskorších predpisov zodpovednú osobu alebo viaceré zodpovedné osoby, ktoré dozerajú na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov.
Pri spracovávaní osobných údajov v informačnom systéme sú oprávnené osoby dodržiavať príkaz starostu obce Hrušov o pravidlách používania lokálnej počítačovej siete.

Požiadavky na personálne opatrenia
- Stanoviť kvalifikačné predpoklady
- Personálne zabezpečiť všetky procesy
- Definovať personálnu bezpečnosť
- Zabezpečiť zastupiteľnosť
- Zabezpečiť dodržiavanie bezpečnostných smerníc
- Zabezpečiť školenia k bezpečnosti a novým projektom

Okolie informačného systému a jeho vzťah k možnému narušeniu bezpečnosti

Obec Hrušov prevádzkuje informačný systém v lokálnej počítačovej sieti (LAN) a v personálnych počítačoch nepripojených do LAN. Do siete internet je LAN pripojená pevným pripojením prostredníctvom demilitarizovanej zóny. Užívatelia lokálnej počítačovej siete využívajú pripojenie do internetu na elektronickú poštu a na prístup k www stránkam. Poštový Server je umiestnený v demilitarizovanej zóne a jeho prípadné napadnutie nemá priamy vplyv na prevádzku IS vo väzbe na spracovávanie osobných údajov. WWW Server je umiestnený mimo LAN a demilitarizovanej zóny u poskytovateľa pripojenia do internetu. Riziká spojené s prevádzkou týchto serverov len minimálne ovplyvnia vnútornú sieť. Prostriedky zabezpečenia počítačovej siete a informačného systému slúžia na minimalizáciu rizík.

Osobné údaje sú spracovávané na pracoviskách obce Hrušov so stálou službou ochrany. V objektoch sa nenachádzajú aj iné spoločnosti mimo organizačných zložiek obce Hrušov. Nie je možné vylúčiť priame napadnutie pracoviska mimo pracovných hodín.

Vymedzenie hraníc určujúcich množinu zvyškových rizík

Hranicu zvyškových rizík stanovuje súbor všetkých opatrení pomocou ktorých je zabezpečený normálny chod informačného systému a sú splnené všetky podmienky na dodržanie zásad ochrany IS. Množina zvyškových rizík je ohraničená nepredvídateľnými udalosťami alebo činnosťami, ktoré sa nedajú ovplyvniť. Pravdepodobnosť možnosti nastatia škody je malá. Zvyškové riziká môžu mať za následok čiastočne narušenie IS, alebo úplné narušenie aktív s znefunkčnením informačného systému.

Definovanie množiny zvyškových rizík.

Vplyv na znefunkčnenie systému	Riziká na aktíva	Hrozba na aktíva
Čiastočné	Napadnutie hrubou silou	• Vyradenie bezpečnostného systému • Prelomenie technických zábran vstupov : dverí • Krádež dokumentov • Krádež technických prostriedkov informačného systému • Znefunkčnenie technických prostriedkov
Čiastočné	Narušenie aktív následkom porúch technologických zariadení	• Porucha na vodovodnom, kanalizačnom a vykurovacom potrubí
Úplné	Živelná pohroma	• Povodeň • Zasiahnutie bleskom - požiar • Zemetrasenie
Úplné	Teroristický útok	• Výbuch • Zamorenie • Požiar
Úplné	Porucha na technologickom zariadení	• Výbuch plynu • Zamorenie priestoru • Požiar

Analýza bezpečnosti informačného systému

Analýza bezpečnosti informačného systému je podrobný rozbor stavu bezpečnosti informačného systému.

Analýza rizík

Príloha č. 2

Bezpečnostné štandardy, metódy a prostriedky ochrany osobných údajov

Súčasťou analýzy bezpečnosti informačného systému je posúdenie zhody navrhnutých bezpečnostných opatrení s použitými bezpečnostnými štandardmi, metódami a prostriedkami. Pri riešení ochrany osobných údajov sa vychádza z obecnej schémy bezpečnostnej architektúry informačných technológií.

<table>
<tr><td colspan="9">Bezpečnostná architektúra</td></tr>
<tr><td colspan="7">Bezpečnosť dokumentácie, plány obnovy (havarijne plány)</td><td rowspan="2">Monitorovanie</td><td rowspan="2">Podpora</td><td rowspan="4">Riadenie bezpečnosti</td></tr>
<tr><td colspan="7">Implementované bezpečnostné opatrenia</td></tr>
<tr><td>Personálna bezpečnosť</td><td>Fyzická bezpečnosť</td><td>Organizačná bezpečnosť</td><td>Bezpečnosť systémových technológií</td><td>Bezpečnosť komunikačných technológií</td><td>Bezpečnosť aplikácií</td><td>Bezpečnosť počítačová</td><td>Implementácia</td><td rowspan="2">Návrh riešenia</td></tr>
<tr><td colspan="8">Bezpečnostná politika, analýza rizík, bezpečnostný projekt</td></tr>
<tr><td colspan="9">Legislatíva, metodiky, normy, štandardy</td></tr>
</table>

Ochrana osobných údajov sa rieši v súlade so zákonom NR SR č. 122/2013 Z.z. o ochrane osobných údajov v znení neskorších predpisov. Ďalej vychádza z nasledujúcich zákonov:

- Zákon NR SR č. 215/2002 Z.z. o elektronickom podpise v znení neskorších predpisov
- Zákon NR SR č. 261/1995 Z.z. o štátnom informačnom systéme
- Zákon NR SR č. 211/2000 Z.z. o slobodnom prístupe k informáciám v znení neskorších predpisov

Pri riešení ochrany osobných údajov sa odporúča vychádzať z uznávaných metodík, štandardov a noriem:

- STN ISO/IEC TR 13335 Informačné technológie – Smernice pre riadenie bezpečnosti IT
  - časť 1: Koncepcie a modely bezpečnosti IT
  - časť 2: Riadenie a plánovanie bezpečnosti IT
  - časť 3: Techniky pre manažment bezpečnosti IT
  - časť 4: Výber bezpečnostných opatrení
- STN ISO/IEC 15408 Informačné technológie, bezpečnostné techniky, kritéria na hodnotenie bezpečnosti IT
  - časť 1: Úvod a všeobecný model
  - časť 2: Bezpečnostné funkčné požiadavky
  - časť 3: Požiadavky na záruky bezpečnosti
- STN ISO/IEC 17799 Informačné technológie – kódex praxe manažérstva informačnej bezpečnosti
- Pre metodiku sa dajú použiť aj :
  - Zákon NR SR č. 241/2001 Z.z. o ochrane utajovaných skutočností v znení neskorších predpisov
  - Vyhláška NBÚ č. 455/2001 Z.z. o administratívnej bezpečnosti
  - Vyhláška NBÚ č. 2/2002 Z.z. o personálnej bezpečnosti
  - Vyhláška NBÚ č. 28/2002 Z.z. o priemyselnej bezpečnosti
  - Vyhláška NBÚ č. 88/2002 Z.z. o fyzickej a objektovej bezpečnosti
  - Vyhláška NBÚ č. 90/2002 Z.z. o bezpečnosti technických prostriedkov
  - Vyhláška NBÚ č. 537/2002 Z.z. o formáte a spôsobe vyhotovenia zaručeného elektronického podpisu, spôsobe zverejňovania verejného kľúča úradu, postupe pri overovaní a podmienkach overovania zaručeného elektronického podpisu, formáte časovej pečiatky a spôsobe jej vyhotovenia, požiadavkách na zdroj časových údajov a požiadavkách na vedenie dokumentácie časových pečiatok (o vyhotovení a overovaní elektronického podpisu a časovej pečiatky)
  - Vyhláška NBÚ č. 542/2002 Z.z. o spôsobe a postupe používania elektronického podpisu v obchodnom a administratívnom styku

Zabezpečenie aktív pred hrozbami

Hrozby	Úroveň bezpečnosti	Opatrenia
1. Prírodné udalosti		
a. Búrka, blesk	Globálna	Technické
b. Potopa	Zvyškové riziko	Zabezpečené polohou
c. Námraza	Globálna	Technické
d. Zemetrasenie	Zvyškové riziko	Havarijný plán
2. Technologické havárie		
a. Požiar	Globálna	Technické
b. Únik nebezpečných látok	Zvyškové riziko	Havarijný plán
c. Únik nebezpečných látok mimo objekt	Zvyškové riziko	Havarijný plán
d. Výbuch	Zvyškové riziko	Havarijný plán

3. Sociálne a. Štrajk, nespokojnosť zamestnancov b. Politické zámery	 Globálna Globálna	 Organizačné, personálne Organizačné
4. Organizačné a. Nepokryté pracovné postupy b. Kompetenčné	 Globálna Globálna	 Organizačné Personálne, organizačné
5. Výpadky a. Technologické b. Infraštruktúry c. Komunikačné linky d. Servre e. Služby	 Globálna Globálna, informačná Informačná Počítačová Globálna, informačná, počítačová	 Technické Organizačné Technické Technické Organizačné, personálne
6. Infiltrácia a. Ľudské – vnútorné b. Ľudské – vonkajšie c. Počítačová	 Globálna Počítačová, informačná	 Personálne, organizačné Technické, organizačné
7. Chyby a. HW b. SW c. Užívateľov d. Správcov	 Počítačová, informačná Počítačová Globálna Globálna	 Technické Technické Personálne, organizačné Personálne

Bezpečnostné smernice

Bezpečnostné smernice upresňujú a aplikujú závery vyplývajúce z bezpečnostného projektu na konkrétne podmienky prevádzkovaného informačného systému.

Pre zabezpečenie výkonu stanovených úloh a opatrení obsiahnutých v bezpečnostnom projekte pre určené pracoviská obce vydáva starosta obce tieto bezpečnostné smernice.

Popis technických opatrení

Technické opatrenia predstavujú všetky určené technické prostriedky (aktíva), určené pre spracúvanie, manipuláciu, archiváciu a skartáciu dôverných skutočností a všetky prostriedky a metódy ochrany určených technických prostriedkov.

Aktíva predbežne určené: počítače samostatné, počítače zapojené do siete vrátane servrov, tlačiarne, modemy, faxy, nahrávacie zariadenia pre audio a video, zálohovacie médiá (pásky, CD disky, diskety a pod.), aplikačné programy, databáza, lokálna sieť, určené pracoviská pre spracovávanie dôverných informácií podľa zákona NR SR č. 428/2002 Z.z. v znení neskorších predpisov.

Zabezpečenie aktív: je tvorené programovými, mechanickými, režimovými a technickými prostriedkami ochrany.

programová metóda (P)

- antivírová ochrana
  - na každom užívateľskom počítači a centrálnom počítači musí byť inštalovaná antivírová ochrana
  - denne musí byť zabezpečená kontrola aktualizácie antivírových knižníc
- vstupné a prihlasovacie heslá
  - každý užívateľ LAN musí mať pridelené heslo ktorým sa autentifikuje a toto heslo uchováva v tajnosti
  - vhodne zvolená doba životnosti a dĺžka hesla spolu s vynucovaním dostačujúcej zložitosti hesla dostatočne zabraňujú úspešným útokom zameraným na uhádnutie hesla
  - účinnejšie opatrenia na autentizáciu užívateľov tvoria biometrické metódy, prípadne identifikácia prostredníctvom čipových kariet a pod.
  - je zakázané vstupovať do LAN pod cudzím užívateľským menom a heslom
  - tie isté opatrenia platia aj pre prístup k aplikáciám
- používanie programov
  - smú byť používané iba autorizované programy
  - kontrola integrity získaného softvérového balíka pred jeho inštaláciou
  - aktualizácia programov zabezpečujúce činnosť demilitarizovanej zóny (firewallov, smerovačov, prekladačov adries)
  - inštaláciu softvéru (SW) smie vykonávať len osoba na to poverená
  - je zakázaná inštalácia SW z prostredia internetu
- ochrana PC pred nepovolaným prístupom

    - heslo BIOSu
- záloha systému
    - aplikačný softvér musí byť zálohovaný stále po aktulizacii

mechanická metóda (M)

- vybavenie určených pracovísk plnými dverami, trezormi, ohňuvzdornými plechovými skriňami

režimová metóda (R)

- určenie režimu vstupu na pracoviská, zákaz zdržovania sa po pracovnej dobe, určenie zodpovedných zamestnancov za bezpečnosť, určenie podmienok vstupu na pracovisko a spôsob opustenia pracoviska a pod.
- záložné kópie operačného systému servrov, personálnych staníc, aplikačných programov a databáz je nutné uskladňovať mimo centrálnej budovy magistrátu (napr. trezor banky v oblasti vytipovanej ako najmenej postihnuteľnú živelnými pohromami)
- všetky dôležité administrátorské prístupy a heslá musia byť zdokumentované a uložené v zapečatenej obálke v trezore starostu obce
- architektúra LAN musí byť zdokumentovaná a uložená v trezore u starostu obce
-

technická metóda (T)

- zabezpečenie LAN pomocou technických zariadení pred nepovoleným prístupom z prostredia internetu
    - vytvorenie demilitarizovanej zóny
- zabezpečenie záložných zdrojov
    - pri dôležitých samostatných PC a sieťových PC
    - pri aktívnych prvkoch LAN

Popis organizačných opatrení

Organizačné opatrenie:

- V rámci organizačnej štruktúry
    - Spracovávať, zhromažďovať a rušiť osobné údaje smú len organizačné zložky a pracoviská na to určené. Spracovávanie údajov musí byť v súlade so zákonom NR SR č. 122/2013 Z.z. o ochrane osobných údajov v znení neskorších predpisov
    - Starosta ustanovuje krízový štáb na čele so starostom, alebo ním povereným zamestnancom
- Rozdelenie kompetencií
    - V prípade mimoriadnej situácie, kedy dôjde k narušeniu bezpečnosti činnosti koordinuje a riadi krízový štáb všetky činnosti.
    - Pri narušení počítačovej bezpečnosti koordinuje činnosti poverený informatik.
    - Pri narušení globálnej bezpečnosti koordinuje činnosti poverený agendou CO.
    - Pri narušení informačnej bezpečnosti v oblasti IS a LAN koordinuje činnosti poverený informatik.
    - Pri narušení informačnej bezpečnosti v oblasti dokumentov, telefónnych a mobilných sietí koordinuje činnosti vedúci starosta obce.
- Určenie pracovných a bezpečnostných postupov
    - Spracovávať, zhromažďovať a rušiť osobné údaje smú len zamestnanci na to určení. Spracovávanie údajov musí byť v súlade so zákonom NR SR č. 122/2013 Z.z. o ochrane osobných údajov v znení neskorších predpisov. Zamestnanci sa musia riadiť všetkými prijatými opatreniami a nariadeniami vydanými starostom.
- Organizačné opatrenia
    - Po pracovnej dobe je zakázané zdržiavať sa na pracovisku.
    - Na pracovisku sa pracovníci môžu zdržiavať len so súhlasom starostu.
    - Krízový štáb vypracuje havarijne plány na zabezpečenie kontinuity činností v prípade narušenia bezpečnosti.
    - Pre krízový štáb musí byť zrejmé:
        - Personálne obsadenie
        - Hierarchia tímov, podriadenosť a zodpovednosť
        - Spôsob komunikácie
        - Prerozdelenie úloh medzi členmi tímov
        - Krízový štáb má právomoci vydávať rozhodnutia

Popis personálnych opatrení

Používanie technických prostriedkov pre spracúvanie osobných informácii je povolené iba osobám oprávneným oboznamovať sa s osobnými informáciami.
Technické prostriedky, sú využívané zásadne zamestnancami, ktorí majú tieto prostriedky pridelené.
Oprávnené osoby preukázateľne poučia právnické osoby a fyzické osoby, ktoré majú alebo môžu mať prístup k ich informačnému systému, o právach a povinnostiach ustanovených zákonom NR SR č. 122/2013 Z.z. v znení neskorších predpisov a o zodpovednosti za ich porušenie.
Každá oprávnená osoba je povinná zachovávať mlčanlivosť o osobných údajoch, ktoré spracúvajú. Povinnosť mlčanlivosti trvá aj po ukončení spracovania. Povinnosť mlčanlivosti nemajú, ak je to podľa osobitného zákona nevyhnutné na plnenie úloh orgánov činných v trestnom konaní.
Oprávnená osoba je povinná zachovávať mlčanlivosť o osobných údajoch, s ktorými príde do styku; tie nesmie využiť ani pre osobnú potrebu a bez súhlasu prevádzkovateľa ich nesmie zverejniť a nikomu poskytnúť ani sprístupniť.
Povinnosť mlčanlivosti platí aj pre iné fyzické osoby, ktoré v rámci svojej činnosti (napr. údržba a servis technických prostriedkov) prídu do styku s osobnými údajmi.
Povinnosť mlčanlivosti trvá aj po zániku funkcie oprávnenej osoby alebo po skončení jej pracovného pomeru alebo obdobného pracovného vzťahu.
Personálny referát vedie evidenciu osôb prichádzajúcich do styku s osobnými údajmi. Každú takúto osobu pracovník personálneho referátu poučí a vyhotoví o tom záznam.
Technické prostriedky, sú využívané zásadne zamestnancami, ktorí majú tieto prostriedky pridelené. Zamestnanci, ktorý majú pridelené technické prostriedky, sú zodpovedný za ich správny chod a musia dodržiavať všetky zásady práce s nimi. Za informačný systém (počítačový) zodpovedá vedúci referátu informatiky.

P**ožiadavky na personálne opatrenia**

- kvalifikačné predpoklady
    - Spracovávať osobné údaje v informačnom systéme majú len osoby:
        - znalé práce na počítači
        - vyškolené pre prácu s aplikačným programom
        - ostatné oprávnené osoby smú spracovávať osobné údaje len dokumentačne
- Personálne zabezpečenie procesov
    - proces prevádzky IS, proces zadávania údajov a proces archivácie zabezpečuje oprávnená pracovníčka obecného úradu.
- Personálna bezpečnosť
    - zamestnanci musia byť poučení
    - každý zamestnanec je povinný zachovávať mlčanlivosť
- Zabezpečenie zastupiteľnosťi
    - najdôležitejšie procesy pri ochrane informačného systému musia byť zabezpečené zastupiteľnosťou
        - užívateľ aplikácie, alebo agendy

- Zabezpečenie dodržiavania bezpečnostných smerníc
    - zamestnanci musia byť poučení s bezpečnostnými smernicami

- pri príjmani zamestnanca do zamestnania musí byť riadne poučený

- Zabezpečenie školenia k bezpečnosti, k novým projektom a k novým skutočnostiam vyplývajúcich z vedeckého a technického pokroku
  - zabezpečiť prehlbovanie odborných znalostí

Rozsah oprávnení

Rozsah oprávnení a popis povolených činností jednotlivých oprávnených osôb, spôsob ich identifikácie a autentizácie pri prístupe k informačnému systému.
Každý zamestnanec, ktorý pristupuje k osobným údajom, je uvedený v zozname osôb oprávnených s oboznamovaním sa s osobnými údajmi, na referáte PAM.
Poverený zamestnanec vedie evidenciu zamestnancov, ktorí vstupujú do IS.
Evidencia obsahuje :

Vzor: Príloha č. 1

Rozsah zodpovednosti oprávnených osôb

Rozsah zodpovednosti oprávnených osôb a osoby zodpovednej za dohľad nad ochranou osobných údajov (§ 23).

1. Osoby oprávnené spracovávať osobné údaje
   a. sú zodpovedné za komplexné, pravdivé, aktuálne údaje a vkladanie týchto údajov do IS
   b. sú zodpovedné za uchovávanie, ochranu a manipuláciu s nimi v prípade, že tieto údaje sú v textovej forme
   c. sú zodpovedné za preukázateľnosť súhlasu na spracovanie osobného údaju, a to tak, že možno o ňom podať dôkaz (§7 zákona NR SR č.122/2013 Z.z v znení neskorších predpisov)
   d. sú zodpovedné za poriadok na pracovisku a odloženie všetkých písomností obsahujúce osobné údaje a iných dokumentov, ktoré by mohli viesť k slobodnému prístupu k osobným údajom, do uzamykateľných odkladacích políc
   e. sú zodpovedné za dodržiavanie zásad práce v LAN a PC podľa príkazu starostu obce o pravidlách používania lokálnej počítačovej siete
   f. sú povinné včas informovať osobu zodpovednú za dohľad nad ochranou osobných údajov o pripravovanom začatí spracovania osobných údajov a o všetkých skutočnostiach, ktoré by mohli viesť k zneužitiu týchto údajov

2. Osoby oprávnené, ktoré prevádzkujú informačný systém
   a. sú zodpovedné za riadny chod IS
   b. zodpovedajú za archiváciu údajovej základne a aplikačného programového vybavenia
   c. sú zodpovedné za antivírovú ochranu LAN
   d. spoluzodpovedajú s užívateľmi pracovných staníc za antivírovú ochranu
   e. zodpovedajú za modernizáciu hmotných a nehmotných aktív

3. Osoby zodpovedné za dohľad nad ochranou osobných údajov (§ 23)

a. zodpovedajú za dozeranie na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov
b. posúdia pred začatím spracúvania osobných údajov v informačnom systéme, či ich spracúvaním nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb. Zistenie narušenia práv a slobôd dotknutých osôb pred začatím spracúvania alebo porušenia zákonných ustanovení v priebehu spracúvania osobných údajov zodpovedná osoba bezodkladne písomne oznámi prevádzkovateľovi; ak prevádzkovateľ po upozornení bezodkladne nevykoná nápravu, oznámi to zodpovedná osoba úradu na ochranu osobných údajov
c. kontrolujú zásady spracovávania osobných údajov a vyhotovujú o tom písomný záznam

Kontrolné činnosti zamerané na dodržiavanie bezpečnosti informačného systému

Spôsob, forma a periodicita výkonu kontrolných činností.

Pred začatím spracúvania osobných údajov v informačnom systéme, osoby zodpovedné za dohľad nad ochranou osobných údajov preveria, či ich spracúvaním nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb. Zistenie narušenia práv a slobôd dotknutých osôb pred začatím spracúvania alebo porušenia zákonných ustanovení v priebehu spracúvania osobných údajov zodpovedná osoba bezodkladne písomne oznámi starostovi; ak príslušný vedúci pracovník po upozornení bezodkladne nevykoná nápravu, oznámi to zodpovedná osoba úradu na ochranu osobných údajov.
Kontrolujú sa zásady spracovávania osobných údajov a vyhotovujú o tom písomný záznam.
Pred započatím kontroly je o kontrole upovedomený príslušný vedúci pracovník zodpovedný za danú agendu.
Zásady spracovávania osobných údajov sa kontrolujú minimálne raz za rok.
Kontrola prevádzky automatizovaného IS sa prevádza nepretržite a to technickými a programovými prostriedkami. V pracovnej dobe sa prevádza denne povereným správcom siete.
Kontrola zabezpečenia miestností pred nedovoleným prístupom v pracovnej dobe ale i v mimopracovnom čase je vykonávaná námatkovo vedúcimi pracovníkmi.

Postupy pri haváriách, poruchách a iných mimoriadnych situáciách

Postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení na zníženie vzniku mimoriadnych situácií a možností efektívnej obnovy stavu pred haváriou.

Popis havárie	**Návrh preventívnych opatrení**	**Postupy na zabezpečenie stavu obnovy**

1. Havárie IS spôsobené technickou chybou niektorého komponentu počítača	○ zabezpečiť záložné zdroje s automatickým shutdownom ○ zabezpečiť dostatok finančných prostriedkov na obnovu IS ○ eliminovať možnosti vzniku porúch inštalovaním antistatickej podlahy a klimatizácie v priestoroch kde sú umiestnené servre	• Aktualizovať DB na servri z poslednej zálohy na záložných médiách
2. Porucha servra spôsobená vírusom, neautorizo-vaným programom,	• Zabezpečiť antivírovú ochranu • Inštalovať len autorizované programy oprávnenými pracovníkmi referátu informatiky • Preverovanie cudzích nosičov (FD, CD ROM...) • Neotvárať nevyžiadané e-mailové prílohy • Nespúšťať programy z prostredia internetu • Nesťahovať neautorizované programy z prostredia internetu • Sledovať aktuálne dianie na LAN a v sieti internet	1. odpojiť každého užívateľa 2. spustiť antivírový program s aktuálnou db známych vírusov 3. detekovať spôsob narušenia 4. odstrániť príčinu poruchy 5. opraviť narušenú funkčnosť 6. opätovne skontrolovať systém antivírovým programom 7. prekontrolovať všetky počítače fyzicky pripojené aj nepripojené do LAN 8. nájsť zdroj infiltrácie a zabezpečiť jeho eliminovanie 9. znovu spustenie systému a pripojenie užívateľov
3. Porucha napájania, strata dodávky elektrickej energie	Každý server a aktívny prvok siete má mať záložný zdroj elektrickej energie. V prípade dlhodobej poruchy zabezpečiť generátor elektrickej energie. Elektrickú sieť na ktorú sa pripájajú servre zabezpečiť stabilizátorom sieťového napätia. Vybraní pracovníci by mali byť vybavení hlásičmi stavu IS prostredníctvom telekomunikačnej techniky aby mohli zabezpečiť protiopatrenia.	V čase výpadku sa musia automaticky aktivovať záložné zdroje a po stanovenom čase sa musí previesť automatický shutdown servrov. Po nábehu elektrickej energie je potrebné spustiť servre a prekontrolovať ich funkčnosť.
4. Porucha prostriedkov demilitarizo-vanej zóny	• Monitorovať činnosť zariadení. • Monitorovať funkčnosť všetkých zariadení • Zabezpečiť prístup len pre pracovníkov s oprávnením	V prípade narušenia • Odpojiť LAN od prostriedkov demilitarizovanej zóny • Vyhľadať príčinu nefunkčnosti • Odstrániť príčinu výmenou častí, inštalovaním

	• Periodicky meniť administrátorské prístupy s heslami • Zabezpečiť antivírovú ochranu mail servra • Zabezpečiť programovú aktuálnosť • Zabezpečiť technickú aktuálnosť • Kontrolovať súbory zaznamenavájuce činnosť • Kontrolovať súbory • Vybaviť obsluhu hlásičmi stavu IS prostredníctvom telekomunikačnej techniky aby mohli včas zabezpečiť protiopatrenia.	aktualizácií, výmenou celku • Preveriť prostriedky firewallu, prekladu adries a proxy • Po otestovaní funkčnosti pripojiť LAN
5. Porucha aktívnych prvkov siete	• Monitorovať činnosť, používať menežovateľné aktívne prvky. • Zabezpečiť dostatočnú kapacitu. • Pripájať ich prostredníctvom záložného zdroja. • Zabezpečiť dostatočnú ochranu pred nepovolaným prístupom.	Vymeniť vadnú časť
6. Porucha v pasívnej časti siete	• Premeranie kabeláže, zásuviek a konektorov	Opraviť, prípadne vymeniť vadnú časť.
7. Havária databáz	• Sledovať konfiguračné súbory. • Monitorovať hlásenia a včas na ne reagovať • Denne kontrolovať chybové hlásenia aplikácie a databázy	Zo zálohy inštalovať databázu na záložný server. (viď bod 1) Po odstránení príčin výpadku a kontrole databáz, vrátiť databázu na hlavný server.
8. Havária aplikácie	• Sledovať hlásenia aplikácie a zaznamenávať postrehy užívateľov • Sledovať konfiguračné súbory. • Monitorovať hlásenia a včas na ne reagovať • Denne kontrolovať chybové hlásenia aplikácie a databázy	Nainštalovať novšiu verziu aplikácie. Konzultovať chyby s dodávateľom.
9. Porucha mail	• Sledovať konfiguračné súbory.	Vymeniť vadnú časť. Aktualizovať softvér

servra	• Monitorovať hlásenia a včas na ne reagovať • Denne kontrolovať chybové hlásenia • Nainštalovať antivírovú ochranu • Zálohovať systém – obraz disku	V prípade výmeny disku previesť inštaláciu zo zálohy.
10. Narušenie dverí, okien	• Pravidelne sledovať funkčnosť	Neodkladne zabezpečiť opravu.
11 Mimoriadne udalosti spôsobené vplyvom zvyškových rizík	• vybudovať kompletný záložný systém mimo priestorov budovy v bezpečnej vzdialenosti • zabezpečiť niekoľkonásobné záložné kópie • vytvorenie chráneného komunikačného dátového kanálu na záložné pracovisko • zhotovenie havarijných plánov na zabezpečenie kontinuity činností • kontrolovať či sú splnené protipožiarne opatrenia • kontrolovať osoby pri vstupe do budovy • vo vytipovaných priestoroch inštalovať EZS, bezpečnostné mreže, dvere • zabezpečiť autentizáciu osôb pri vstupe do chránených priestorov vybraní pracovníci by mali byť vybavení hlásičmi stavu IS prostredníctvom telekomunikačnej techniky aby mohli zabezpečiť protiopatrenia.	V prípade vyradenia IS z činnosti: 1. Zvolať krízový štáb 2. Koordinovať činnosti podľa havarijných smerníc 3. Aktivovať záložné pracovisko zo záloh 4. Skontrolovať úplnosť systému 5. Spustenie prevádzky 6. Odstránenie škôd na pôvodnom pracovisku 7. Po obnovení funkčnosti vrátenie činností V prípade napadnutia len časti IS: 1. Presunúť aktíva do vyhovujúcich priestorov 2. Inštalovať záložný server a pripojenia 3. Obnoviť IS zo zálohy 4. Spustiť prevádzku 5. Po odstránení dôsledkov vrátiť činnosti do stavu pred udalosťou

PRÍLOHA č.1

EVIDENCIA ZAMESTNANCOV VSTUPUJÚCICH DO IS

P.č.	Meno s priezvisko	Účel vstupu do Informačného systému	Poznámka
1.	Katarína Zsebiková, Ing.	Oprávnená osoba	

Príloha č.2

ANALÝZA RIZÍK

l.**Neoprávnená modifikácia osobných údajov**

Dopad hrozby na aktíva systému: narušenie integrity, dostupnosti, dôvemosti.

Potencionálne slabiny: zmeny programov, vrátane zavedeni a škodlivých programov (roznych červov, logických bomb, trójskych koni, zadných vrátok atd'.), zmeny súborov s citlivými údajmi.

Súčasný stav zabezpečenia:
- je nainštalovaná antivírová ochrana
- nie je pripojenie do počítačovej siete
- nie je potreba prenášať údaje z prenosných médií do PC a naopak

2.Neoprávnený lokálny prístup k osobným údajom v pracovnej stanici

Dopad hrozby na aktíva systému: narušenie integrity, dôvernosti.

Potencionálne slabiny: neoprávnená osoba može získať neautorizovaný pristup k údajom vplyvom nepoužívania hardvérových alebo softvérových autentizačných prostriedkov, krátkodobé opustenie počítača, čítanie údajov z obrazovky monitora neoprávnenou osobou