Obec Streda nad Bodrogom

podľa § 19 ods. 2 zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a Vyhlášky Úradu na ochranu osobných údajov č. 164/2013 Z. z. o rozsahu a dokumentácii bezpečnostných opatrení vydáva vnútorný predpis

„Bezpečnostný projekt

informačného systému Obce Streda nad Bodrogom.“

Článok 1.
Úvodné ustanovenia

1. Tento predpis sa vzťahuje na každého zamestnanca Obce Streda nad Bodrogom (ďalej len obce), ktorý spracúva osobné údaje, určuje účel a prostriedky spracúvania alebo poskytuje osobné údaje na spracúvanie.
2. Tento predpis sa vzťahuje na osobné údaje systematicky spracúvané úplne alebo čiastočne automatizovanými prostriedkami spracúvania alebo inými ako automatizovanými prostriedkami spracúvania, ktoré sú súčasťou informačného systému alebo sú určené na spracúvanie v informačnom systéme.

Článok 2.
Vymedzenie základných pojmov

1. **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.
2. **Dotknutou osobou** každá fyzická osoba, ktorej sa osobné údaje týkajú.
3. **Prevádzkovateľom** každý, kto sám alebo spoločne s inými vymedzí účel spracúvania osobných údajov, určí podmienky ich spracúvania a spracúva osobné údaje vo vlastnom mene; ak účel, prípadne aj podmienky spracúvania osobných údajov ustanovuje zákon, priamo vykonateľný právne záväzný akt Európskej únie alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, prevádzkovateľom je ten, kto je na plnenie účelu spracúvania za prevádzkovateľa ustanovený alebo kto spĺňa zákonom, priamo vykonateľným právne záväzným aktom Európskej únie alebo medzinárodnou zmluvou, ktorou je Slovenská republika viazaná, ustanovené podmienky.
4. **Oprávnenou osobou** každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovnoprávneho vzťahu, štátnozamestnaneckého pomeru, služobného pomeru, členského vzťahu, na základe poverenia, zvolenia alebo vymenovania, alebo v rámci

výkonu verejnej funkcie, a ktorá spracúva osobné údaje v rozsahu a spôsobom určeným v poučení podľa § 21.
5. **Zodpovednou osobou** je oprávnená osoba, ktorá zabezpečuje dohľad nad ochranou osobných údajov pri spracúvaní osobných údajov u prevádzkovateľa.
6. **Treťou stranou** každý, kto nie je dotknutou osobou, prevádzkovateľom poskytujúcim osobné údaje, jeho zástupcom, sprostredkovateľom alebo oprávnenou osobou.
7. **Príjemcom** každý, komu sú osobné údaje poskytnuté alebo sprístupnené, pričom príjemcom môže byť aj tretia strana.
8. **Spracúvaním osobných údajov**, vykonávanie operácií alebo súboru operácií s osobnými údajmi, najmä ich získavanie, zhromažďovanie, šírenie, zaznamenávanie, usporadúvanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, premiestňovanie, využívanie, uchovávanie, blokovanie, likvidácia, ich cezhraničný prenos, poskytovanie, sprístupňovanie alebo zverejňovanie; niektorými operáciami s osobnými údajmi sa podľa prvej vety rozumie:
a) **poskytovaním osobných údajov**, odovzdávanie osobných údajov tretej strane, ktorá ich ďalej spracúva,
b) **sprístupňovaním osobných údajov** oznámenie osobných údajov alebo umožnenie prístupu k nim príjemcovi, ktorý ich ďalej nespracúva,
c) **zverejňovaním osobných údajov**, publikovanie, uverejnenie alebo vystavenie osobných údajov na verejnosti prostredníctvom masovokomunikačných prostriedkov, verejne prístupných počítačových sietí, verejným vykonaním alebo vystavením diela, verejným vyhlásením, uvedením vo verejnom zozname, v registri alebo v operáte, ich umiestnením na úradnej tabuli alebo na inom verejne prístupnom mieste,
d) **cezhraničným prenosom osobných údajov,** prenos osobných údajov mimo územia Slovenskej republiky a na územie Slovenskej republiky,
e) **likvidáciou osobných údajov,** zrušenie osobných údajov rozložením, vymazaním alebo fyzickým zničením hmotných nosičov tak, aby sa z nich osobné údaje nedali reprodukovať,
f) **blokovaním osobných údajov**, dočasné alebo trvalé pozastavenie spracúvania osobných údajov, počas ktorého možno vykonávať len tie operácie s osobnými údajmi, ktoré sú nevyhnutné na splnenie povinnosti uloženej zákonom 122/2013 Z. z.,
9. **Informačným systémom osobných údajov**, informačný systém, v ktorom sa na vopred vymedzený alebo ustanovený účel systematicky spracúva alebo má spracúvať akýkoľvek usporiadaný súbor osobných údajov prístupných podľa určených kritérií, bez ohľadu na to, či ide o informačný systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe (ďalej len "informačný systém"); informačným systémom sa na účely tohto zákona rozumie aj súbor osobných údajov, ktoré sú spracúvané alebo pripravené na spracúvanie čiastočne automatizovanými alebo inými ako automatizovanými prostriedkami spracúvania.
10. **Účelom spracúvania osobných údajov**, vopred jednoznačne vymedzený alebo ustanovený zámer spracúvania osobných údajov, ktorý sa viaže na určitú činnosť.
11. **Súhlasom dotknutej osoby**, akýkoľvek slobodne daný výslovný a zrozumiteľný prejav vôle, ktorým dotknutá osoba na základe poskytnutých informácií vyjadruje súhlas so spracúvaním svojich osobných údajov.
12. **Podmienkami spracúvania osobných údajov**, prostriedky a spôsob spracúvania osobných údajov, ako aj ďalšie požiadavky, kritériá alebo pokyny súvisiace so spracúvaním osobných údajov alebo vykonanie úkonov, ktoré slúžia na dosiahnutie účelu spracúvania či už pred začatím spracúvania osobných údajov, alebo v priebehu ich spracúvania,
13. **Biometrickým údajom**, osobný údaj fyzickej osoby označujúci jej biologickú alebo fyziologickú vlastnosť alebo charakteristiku, na základe ktorej je jednoznačne a

nezameniteľne určiteľná; biometrickým údajom je najmä odtlačok prsta, odtlačok dlane, analýza deoxyribonukleovej kyseliny.
14. **Všeobecne použiteľným identifikátorom**, trvalý identifikačný osobný údaj dotknutej osoby, ktorý zabezpečuje jej jednoznačnosť v informačných systémoch,
15. **Adresou,** súbor údajov o pobyte fyzickej osoby, do ktorého patria názov ulice, orientačné, prípadne súpisné číslo domu, názov obce, prípadne názov časti obce, poštové smerovacie číslo, názov okresu, názov štátu.
16. **Anonymizovaným údajom**, osobný údaj upravený do takej podoby, v ktorej ho nemožno priradiť dotknutej osobe, ktorej sa týka.
17. **Priestorom prístupným verejnosti**, priestor, do ktorého možno voľne vstupovať a v ktorom sa možno voľne zdržiavať bez časového obmedzenia alebo vo vymedzenom čase, pričom iné obmedzenia, ak existujú a sú osobou splnené, nemajú vplyv na vstup a voľný pohyb osoby v tomto priestore, alebo je to priestor, ktorý tak označuje osobitný zákon,

Článok 3.
Informačný systém obce

1. Prevádzkovateľom informačného systému je Obec Streda nad Bodrogom, štatutárny zástupca - starosta obce.

2. Zodpovednou osobou je Mgr. Zuzana Szalontaiová.

3. Informačný systém obce zahŕňa:

a) Vedenie evidencie obyvateľstva, podateľňa
- automatizovaný systém na vedenie evidencie obyvateľstva od spoločnosti Ifosoft,
- ručne vedené záznamy o evidencii obyvateľstva.
- ručne vedené záznamy o došlej a odoslanej pošte

Oprávnená osoba: zamestnanec zodpovedný za vedenie sekretariátu

b) Vedenie personálnej a účtovnej dokumentácie
- automatizovaný systém RIS SAM, automatizovaný systém na vedenie účtovníctva od spol. Ifosoft
- automatizovaný systém na personálnu prácu od spoločnosti Ifosoft
- ručne vedené záznamy o zamestnancoch obce.

Oprávnená osoba: zamestnanci zodpovední za prácu referátu ekonomických činností a personalistiky

c) Vedenie evidencie daňovníkov
- automatizovaný systém spracovania údajov o daniach a daňovníkoch od spoločnosti Ifosoft
- ručne vedené záznamy o daňovníkoch.

Oprávnená osoba: zamestnanci zodpovední za prácu referátu evidencie a výberu daní

d) Vedenie matričných dokladov, výber poplatkov za komunálne odpady

- automatizovaný systém pre matriku WINMATRI 1.1.0 od spoločnosti IVES
- ručne vedené matričné záznamy a údaje o poplatníkoch za komunálne odpady a DSO

Oprávnená osoba: zamestnanec zodpovedný za vedenie matriky a výber poplatkov za komunálne odpady a DSO

e) Vedenie dokumentácie spoločného obecného úradu, dokumentácie CO
- ručne vedená dokumentácia stavebného úradu a CO

Oprávnená osoba: zamestnanec spoločného obecného úradu

f) Vedenie registra čitateľov v obecnej knižnici
- automatizovaný systém
- ručne vedené záznamy o čitateľoch

Oprávnená osoba: vedúca MKS

g) Vedenie dokumentácie obecného zastupiteľstva, žiadosti, sťažnosti a priestupky
- ručne vedená dokumentácia

Oprávnená osoba: prednosta

h) Vedenie zoznamu zamestnancov a žiakov MŠ
- ručne vedená evidencia zamestnancov a žiakov MŠ, ich zákonných zástupcov

Oprávnená osoba: riaditeľ MŠ

4. Vzhľadom k tomu, že sa zamestnanci obce môžu meniť, sú oprávnené osoby uvedené funkciou. Aktuálne obsadenie funkcií jednotlivými osobami je uvedené v prílohe organizačného poriadku obce.

Článok 4.
Bezpečnostný zámer

1. Základné bezpečnostné ciele

a) zabezpečiť ochranu osobných údajov pred odcudzením, stratou, poškodením, neoprávneným prístupom, zmenou,
b) minimalizovať riziká pri prevádzke informačného systému pred napadnutím aktivít,
c) zabezpečiť kontinuitu činnosti v informačnom systéme v prípade jeho narušenia,
d) zabezpečiť ochranu aktivít,
e) zabezpečiť ohodnotenie a ošetrenie možných rizík,
f) stanoviť rovnováhu medzi akceptovateľnými stratami a jednorazovými a ročnými nákladmi,
g) zabezpečiť realizáciu preventívnych opatrení,
h) analyzovať možnosť napadnutia,
i) stanoviť úrovne bezpečnosti.

2. Bezpečnostné opatrenia

a) technické opatrenia

Technické opatrenia realizované prostriedkami fyzickej povahy

- zabezpečenie objektu pomocou mechanických zábranných prostriedkov (napr. uzamykateľné dvere, okná, mreže) a v prípade potreby aj pomocou technických zabezpečovacích prostriedkov (napr. elektrický zabezpečovací systém objektu, elektrická požiarna signalizácia),
- zabezpečenie chráneného priestoru jeho oddelením od ostatných častí objektu (napr. steny, zábrany v podobe prepážok, mreží alebo presklenia),
- umiestnenie informačného systému v chránenom priestore (ochrana informačného systému pred fyzickým prístupom neoprávnených osôb a nepriaznivými vplyvmi okolia,
- bezpečné uloženie fyzických nosičov osobných údajov (napr. uloženie listinných dokumentov v uzamykateľných skriniach alebo trezoroch),
- zamedzenie náhodného odpozerania osobných údajov zo zobrazovacích jednotiek informačného systému (napr. vhodné umiestnenie zobrazovacích jednotiek),
- zariadenie na ničenie fyzických nosičov osobných údajov (napr. zariadenie na skartovanie listín),

Ochrana pred neoprávneným prístupom

- šifrová ochrana obsahu dátových nosičov a šifrová ochrana dát premiestňovaných prostredníctvom počítačových sietí,
- pravidlá prístupu tretích strán k informačnému systému, ak k takému prístupu dochádza,

Riadenie prístupu oprávnených osôb

- identifikácia, autentizácia a autorizácia oprávnených osôb v informačnom systéme,
- zaznamenávanie vstupov jednotlivých oprávnených osôb do informačného systému,

Ochrana proti škodlivému kódu

- detekcia prítomnosti škodlivého kódu v prichádzajúcej elektronickej pošte a v iných súboroch prijímaných z verejne prístupnej počítačovej siete alebo z dátových nosičov,
- ochrana pred nevyžiadanou elektronickou poštou,
- používanie legálneho a prevádzkovateľom schváleného softvéru,
- pravidlá sťahovania súborov z verejne prístupnej počítačovej siete,
- **Sieťová bezpečnosť**
- kontrola, obmedzenie alebo zamedzenie prepojenia informačného systému, v ktorom sú spracúvané osobné údaje s verejne prístupnou počítačovou sieťou,
- evidencia všetkých miest prepojenia sietí vrátane verejne prístupnej počítačovej siete,
- ochrana vonkajšieho a vnútorného prostredia prostredníctvom nástroja sieťovej bezpečnosti (napr. firewall),
- pravidlá prístupu do verejne prístupnej počítačovej siete (napr. zamedzenie pripojenia k určitým webovým sídlam),
- ochrana proti iným hrozbám pochádzajúcim z verejne prístupnej počítačovej siete (napr. hackerský útok),

Zálohovanie

- test funkcionality dátového nosiča zálohy,
- vytváranie záloh s vopred zvolenou periodicitou,
- test obnovy informačného systému zo zálohy,
- bezpečné ukladanie záloh,

Likvidácia osobných údajov a dátových nosičov

- bezpečné vymazanie osobných údajov z dátových nosičov,
- zariadenie na likvidáciu dátových nosičov osobných údajov,

Aktualizácia operačného systému a programového aplikačného vybavenia

b) personálne opatrenia

- poučenie oprávnených osôb pred uskutočnením prvej spracovateľskej operácie s osobnými údajmi,
- poučenie o právach a povinnostiach vyplývajúcich zo zákona a zodpovednosti za ich porušenie,
- vymedzenie osobných údajov, ku ktorým má mať konkrétna oprávnená osoba prístup na účel plnenia jej povinností alebo úloh,
- určenie postupov, ktoré je oprávnená osoba povinná uplatňovať pri spracúvaní osobných údajov,
- vymedzenie zakázaných postupov alebo operácií s osobnými údajmi,
- vymedzenie zodpovednosti za porušenie zákona,
- poučenie oprávnených osôb o postupoch spojených s automatizovanými prostriedkami spracúvania a súvisiacich právach a povinnostiach (v priestoroch prevádzkovateľa a mimo týchto priestorov),
- písomné poverenie zodpovednej osoby podľa § 23 zákona,
- vzdelávanie oprávnených osôb (napr. právna oblasť, oblasť informačných technológií),
- postup pri ukončení pracovného alebo obdobného pomeru oprávnenej osoby (napr. odovzdanie pridelených aktív, zrušenie prístupových práv, poučenie o následkoch porušenia zákonnej alebo zmluvnej povinnosti mlčanlivosti)

c) organizačné opatrenia

Vedenie zoznamu aktív a jeho aktualizácia,

Riadenie prístupu oprávnených osôb k osobným údajom

- kontrola vstupu do objektu a chránených priestorov prevádzkovateľa (napr. prostredníctvom technických a personálnych opatrení),
- správa kľúčov (individuálne prideľovanie kľúčov, bezpečné uloženie rezervných kľúčov),
- prideľovanie prístupových práv a úrovní prístupu (rolí) oprávnených osôb,
- správa hesiel,
- vzájomné zastupovanie oprávnených osôb (napr. v prípade nehody, dočasnej pracovnej neschopnosti, ukončenia pracovného alebo obdobného pomeru),

Organizácia spracúvania osobných údajov

- pravidlá spracúvania osobných údajov v chránenom priestore,
- nepretržitá prítomnosť oprávnenej osoby v chránenom priestore, ak sa v ňom nachádzajú aj iné ako oprávnené osoby,
- režim údržby a upratovania chránených priestorov,

- pravidlá spracúvania osobných údajov mimo chráneného priestoru, ak sa také spracúvanie predpokladá,
- pravidlá manipulácie s fyzickými nosičmi osobných údajov (napr. listiny, fotografie) mimo chránených priestorov a vymedzenie zodpovednosti,
- pravidlá používania automatizovaných prostriedkov spracúvania (napr. notebooky) mimo chránených priestorov a vymedzenie zodpovednosti,
- pravidlá používania prenosných dátových nosičov mimo chránených priestorov a vymedzenie zodpovednosti,

Likvidácia osobných údajov

- určenie postupov likvidácie osobných údajov s vymedzením súvisiacej zodpovednosti jednotlivých oprávnených osôb (bezpečné vymazanie osobných údajov z dátových nosičov, likvidácia dátových nosičov a fyzických nosičov osobných údajov),

Bezpečnostné incidenty

- postup pri ohlasovaní bezpečnostných incidentov a zistených zraniteľných miest informačného systému na účel včasného prijatia preventívnych alebo nápravných opatrení,
- evidencia bezpečnostných incidentov a použitých riešení,
- postup pri riešení jednotlivých typov bezpečnostných incidentov,
- identifikácia, evidencia a odstraňovanie následkov bezpečnostných incidentov,
- postupy pri haváriách, poruchách a iných mimoriadnych situáciách (napr. oznamovanie bezpečnostných incidentov),
- postup pri poruche, údržbe alebo oprave automatizovaných prostriedkov spracúvania (napr. ochrana osobných údajov na pevnom disku opravovaného počítača),

Kontrolná činnosť

- kontrolná činnosť prevádzkovateľa zameraná na dodržiavanie prijatých bezpečnostných opatrení s určením spôsobu, formy a periodicity jej realizácie (napr. pravidelné kontroly prístupov k informačnému systému),
- informovanie oprávnených osôb o kontrolnom mechanizme, 3) ak je u prevádzkovateľa zavedený (rozsah kontroly a spôsoby jej uskutočňovania)

3. Okolie informačného systému a jeho vzťah k možnému narušeniu bezpečnosti

Obec Streda nad Bodrogom prevádzkuje informačný systém v lokálnej počítačovej sieti (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 webovým 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 (Slovak telekom). 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 obecného úradu Obce Streda nad Bodrogom.
V objektoch sa nenachádzajú iné spoločnosti mimo organizačných zložiek Obce Streda nad Bodrogom.
Nie je možné vylúčiť priame napadnutie pracoviska mimo pracovných hodín.

4. Vymedzenie hraníc určujúcich množinu zostatkových rizík

Hranicu zostatkových rizík stanovuje súbor všetkých opatrení, pomocou ktorých je zabezpečený normálny chod informačného systému (IS) a sú splnené všetky podmienky na dodržiavanie zásad ochrany IS. Množina zostatkových rizík je ohraničená nepredvídateľnými udalosťami, alebo činnosťami, ktoré sa nedajú ovplyvniť. Pravdepodobnosť možnosti nastania škody je malá. Zostatkové riziká môžu mať za následok čiastočné narušenie IS alebo úplné narušenie aktivít so znefunkčnením IS.

Definovanie množiny zostatkových rizík

Vplyv na znefunkčnenie systému	**Riziká na aktíva**	**Hrozba na aktíva**
Čiastočné	Napadnutie hrubou silou	• Vyradenie bezpečnostného systému • Prelomenie technických zábran vstupov: mreží, bezpečnostných dverí • Krádež dokumentov • Krádež technických prostriedkov IS • 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

Článok 5.
Analýza bezpečnosti informačného systému

1. Rozsah spracúvaných údajov – vstup údajov

a) Vedenie evidencie obyvateľstva
- dokumentácia a rozsah osobných údajov sú spracúvané v zmysle ustanovení zák. č. 496/2008 Z. z. o hlásení pobytu občanov Slovenskej republiky a registri obyvateľov Slovenskej republiky.

b) Podateľňa a výpravňa písomností
- dokumentácia vedená a spracúvaná v súlade s Registratúrnym plánom obce

c) Vedenie personálnej dokumentácie
- dokumentácia a osobné údaje zamestnancov a uchádzačov o zamestnanie sú spracúvané v rozsahu potrieb vyplývajúcich zo Zákonníka práce, tlačív na hlásenia pre Sociálnu poisťovňu, zdravotné poisťovne, daňový úrad.

d) vedenie účtovnej dokumentácie
- dokumentácia a osobné údaje sú spracúvané v rozsahu potrieb na vydanie licencie na hracie automaty, na vydanie, zmenu, zrušenie osvedčenia o SHR, na spracovanie kúpnych, nájomných zmlúv.

e) Vedenie evidencie daňovníkov
- dokumentácia a osobné údaje sú spracúvané v rozsahu potrebnom na spoľahlivú identifikáciu daňovníkov.

f) Vedenie dokumentácie pre sociálnu prácu
- dokumentácia a osobné údaje sú spracúvané v súlade s ustanoveniami zák. č. 448/2008 Z. z. o sociálnych službách

g) Vedenie matričných dokladov
- dokumentácia a osobné údaje sú spracúvané v súlade s ustanoveniami zák. č. 420/2006 Z. z. o matrikách

h) Vedenie evidencie poplatníkov za komunálne odpady
- dokumentácia a osobné údaje sú spracúvané v rozsahu potrebnom na spoľahlivú identifikáciu poplatníkov.

i) Vedenie dokumentácie spoločného obecného úradu
- dokumentácia a osobné údaje sú spracúvané v súlade s ustanoveniami zák. č. 50/1976 Zb. stavebný zákon

j) Vedenie registra čitateľov v obecnej knižnici
- dokumentácia a osobné údaje sú spracúvané v rozsahu potrebnom na spoľahlivú identifikáciu klientov obecnej knižnice, v prípade detí údaje ich zákonných zástupcov

k) Vedenie dokumentácie obecného zastupiteľstva, žiadosti, sťažnosti a priestupky
- dokumentácia a osobné údaje sú spracúvané v súlade s ustanoveniami zák. č. 369/1990 Z. z. o obecnom zriadení, zák. č. 9/2010 Z. z. o sťažnostiach a zák. č. 372/1990 Zb. o priestupkoch

l) Vedenie zoznamu zamestnancov a žiakov MŠ
- dokumentácia a osobné údaje sú spracúvané v súlade s ustanoveniami zák. č. 596/2003 Z. z. o štátnej správe v školstve a školskej samospráve

2. Analýza spracovania a uchovávania údajov

V rámci obecného úradu, obecnej knižnice a materskej školy sa nachádzajú dva typy spracovania a uchovávania osobných údajov:
- **manuálne – neautomatizovane** (technológia spracovania) na papierových nosičoch – jedná sa predovšetkým o staršie údaje, ako aj o pracoviská dosial nevybavené výpočtovou

technikou, archivácia na papierových nosičoch. Na papierových nosičoch sa aj naďalej uchovávajú niektoré – predovšetkým vstupné – osobné údaje (žiadosti, zmluvy, dotazníky...)
- **automatizovaná** (technológia spracovania) na PC v rámci LAN ako aj WAN (spojenie s bankou, zdravotnou poisťovňou, sociálnou poisťovňou a pod.)

Popis miestností:
Všetky IS, v ktorých sa spracúvajú osobné údaje, sú umiestnené v uzamykateľných miestnostiach, okná miestností na prízemí sú chránené kovovými mrežami.

Popis budovy:
1. Obecný úrad sa nachádza v budove barokového kaštieľa, ktorý v 80. rokoch 20. storočia prešiel rozsiahlou rekonštrukciou. Kaštieľ je poschodová budova s pôdorysom v tvare L, v mieste styku dvoch krídel orientovanom do dvora stojí trojpodlažná stará veža. Vstup do budovy je cez hlavné vchodové dvere na západnej strane budovy, vstup je možný aj bočným vchodom na východnej strane budovy. Od hlavného vchodu majú kľúč všetci zamestnanci obecného úradu.
Kancelárske priestory sa nachádzajú na prízemí a na prvom podlaží. V budove po ukončení pracovnej doby nie je nepretržitá služba. Budova je chránená elektronickým zabezpečovacím zariadením. Prízemie je od podlažia oddelené uzamykateľnými mrežami. Okná na prízemí sú zabezpečené mrežami.
2. Obecná knižnica sa nachádza v budove Miestneho kultúrneho strediska v samostatnej, uzamykateľnej miestnosti. Okrem obecnej knižnice sa v budove nachádza aj Základná umelecká škola. Budova je po pracovnej dobe uzamykaná a chránená elektronickým zabezpečovacím zariadením.
3. Materská škola (MŠ) je umiestnená v účelovej dvojpodlažnej budove, vstup do budovy je zo zadnej časti oproti vstupnej bránke. MŠ je v prevádzke v pracovných dňoch od 7,00 hod. do 16,30 hod. Budovu otvárajú upratovačky o 6,30 hod. a zatvárajú o 17,00hod. V budove je bez sprievodu zamestnanca MŠ zakázaný akýkoľvek pohyb cudzej osoby.
Vchod do MŠ je zaistený bezpečnostným zámkom, kľúč od budovy vlastní riaditeľka a upratovačka.

Popis PC, na ktorých sa osobné údaje spracúvajú automatizovane

Na automatické spracovanie údajov sa využívajú PC. PC sú v sieti (LAN, a cez server WAN) a v rámci siete k PC majú prístup len oprávnené osoby.

PC jednotlivých pracovníkov sú pripojene k NET-u Slovak telecom.

LAN je pripojená na WAN, prechod je chránený firewallom cez server, jednotlivé PC v sieti sú chránené antivírovými programami.

Do systému sa vstupuje cez užívateľské meno a heslo, jednotlivým užívateľom sa dajú nastaviť oprávnenia. Jednotlivé programy, ako aj súbory, v ktorých sú uložené osobné údaje sú chránené heslom.

3. Bezpečnostné štandardy, metódy a prostriedky ochrany osobných údajov

Súčasťou analýzy bezpečnosti IS je posúdenie zhody navrhnutých bezpečnostných opatrení s použitými bezpečnostnými, metódami a prostriedkami. Pri riešení ochrany osobných údajov sa vychádza z obecnej schémy bezpečnostnej architektúry informačných technológií.
Ochrana osobných údajov sa rieši v súlade so zák. č. 122/2013 Z. z. o ochrane osobných údajov.

4. Kvalitatívna analýza rizík, zoznam hrozieb, úroveň bezpečnosti a návrh opatrení

Zoznam hrozieb	*Úroveň bezpečnosti*	*Opatrenie*
Riziká od oprávnených osôb		
Zber nadbytočných údajov	Globálna	Zberať len údaje v zmysle platnej legislatívy, alebo vnútorného predpisu, v ktorom je starostlivo posúdený a zvážený rozsah zberu údajov
Chybné spracovanie údajov	Globálna	Spätnou kontrolou overovať správnosť spracovania
Strata nosičov údajov	Globálna	Nosiče údajov vždy odkladať na určené miesto
Nedostatočná likvidácia údajov	Globálna, počítačová	Spätná kontrola dodržiavania bezpečnostného zámeru
Mimovoľné vyzradenie údajov	Globálna	Pravidelne preškoľovať zamestnancov a upozorňovať ich na možné nedostatky
Neoprávnené poskytnutie, zverejnenie, alebo sprístupnenie údajov	Globálna	Pravidelne preškoľovať zamestnancov a upozorňovať ich na možné postihy
Zneužitie údajov	Globálna	Upozorňovať zamestnancov na možné postihy a nebezpečnosť ich konania
Psychologické problémy - predovšetkým vydieranie správcu siete, alebo oprávnených osôb	Globálna	Dôsledne preverovať spoľahlivosť a dôveryhodnosť zamestnancov
Sociálne riziká		
Štrajk, nespokojnosť zamestnancov	Globálna	Organizačné, personálne
Politické zámery	Globálna	Organizačné
Infiltrácia		
Ľudské – vnútorné	Globálna	Personálne, organizačné
Ľudské – vonkajšie		
Počítačová	Počítačová, informačná	Technické, organizačné
Organizačné riziká		
Bezpečnostný projekt nedocenil riziká	Globálna	Prehodnotiť bezpečnostný projekt
Bezpečnostné smernice nezohľadnili riziká	Globálna	Doplniť smernice tak, aby sa nedostatky odstránili
Bezpečnostné smernice sú ťažko aplikovateľné,	Globálna	Prepracovať bezpečnostné smernice

alebo príliš komplikované		
Bezpečnostné smernice sú oprávnenými osobami podceňované	Globálna	Výchovou vplývať na oprávnené osoby, v prípade pretrvávania, resp. vážnejšieho porušenia postih v zmysle ZP
Bezpečnostné smernice nevybalansovali požiadavky rôznych zákonov, alebo záujmov	Globálna	Zosúladiť s právnym stavom
Nepokryté pracovné postupy	Globálna	Organizačné – doplniť
Kompetenčné	Globálna	Organizačné, personálne – doplniť, upresniť pracovné náplne, organizačnú schému
Technologické havárie		
Požiar	Globálna	Technické – požiarno – poplachové smernice, evakuačný plán
Únik nebezpečných látok	Zvyškové riziko	Havarijný plán – vypracovaný a nacvičený
Únik nebezpečných látok mimo objekt	Zvyškové riziko	Havarijný plán – vypracovaný a nacvičený
Výbuch	Zvyškové riziko	Havarijný plán – vypracovaný a nacvičený
Výpadky		
Technologické	Globálna	Technické
Infraštruktúry	Globálna, informačná	Organizačné
Komunikačné linky	Informačná	Technické
Servre	Počítačová	Technické
Služby	Globálna, informačná, počítačová	Organizačné, personálne
Technické riziká		
Poškodia sa, alebo zničia údaje na nosiči elektronických údajov	Počítačová	Pravidelné zálohovanie údajov
Nedostatočná likvidácia údajov s možnosťou obnovy neoprávnenou osobou	Globálna, počítačová	Vytvoriť technické podmienky pre likvidáciu a poučiť oprávnené osoby o správnom a bezpečnom postupe
Prírodné udalosti		
Búrka, blesk	Globálna	Technické – zabezpečiť funkčné bleskozvody na objektoch, pravidelné revízie
Potopa	Zvyškové riziko	Zabezpečené polohou školy

Námraza	Globálna	Technické – včasné a účinné odstraňovanie
Zemetrasenie	Zvyškové riziko	Vypracovaný a nacvičený havarijný plán
Riziká z okolia informačného systému		
Neoprávnené osoby prekonajú zábrany prístupu k údajom	Globálna	Prehodnotiť systém ochrany a zvýšiť stupeň ochrany, udržiavať ochranu na požadovanej úrovni
Neoprávnené osoby prekonajú ochranu prístupu k elektronickým údajom v sieti	Globálna, počítačová, informačná a komunikačná	Pravidelne aktualizovať OS, databázy antivírových programov, sledovať sieť, neustále zvyšovať bezpečnosť siete. **Nepovoliť zásahy do nastavenie PC, siete, ako aj serveru iným osobám ako správcovi siete.**
Nabúranie siete VUC NET	Globálna, informačná, počítačová	Technické, **nepovoliť zásahy do nastavenie PC, siete, ako aj serveru iným osobám ako správcovi siete**
Riziká od poskytovateľov osobných údajov		
Poskytnutie nepravdivých osobných údajov	Globálna	Upozorniť poskytovateľov osobných údajov, že za nepravdivosť zodpovedá poskytovateľ
Chyby		
HW	Počítačová, informačná	Technické
SW	Počítačová	Technické
Užívateľské	Globálna	Personálne, organizačné
Správcov- úmyselné, neúmyselné	Globálna	Personálne, organizačné

Článok 6.
Závery vyplývajúce z bezpečnostného zámeru a analýzy bezpečnosti IS

1. Popis bezpečnostných opatrení a spôsob ich uplatňovania

a) Spôsob získavania osobných údajov

- Osobné údaje môžu získavať len oprávnené osoby.
- Osobné údaje oprávnené osoby môžu získavať len v rozsahu stanovenom zákonom.
- Postup pri získavaní osobných údajov:
- *Osobné údaje nevyžiadané* – napr. poštou (žiadosť o zamestnanie) v prípade, že nedôjde k podpisu pracovnej zmluvy je tieto preukazne potrebné vrátiť žiadateľovi. Pokiaľ sa budú z nejakých dôvodov uchovávať (napr. možnosť zamestnania v blízkej budúcnosti), je potrebný súhlas dotknutej osoby.

- *Ostatné osobné údaje* oprávnená osoba, ktorá získava osobné údaje v mene prevádzkovateľa preukáže na požiadanie tomu, od koho osobné údaje dotknutej osoby požaduje, svoju totožnosť a bez vyzvania mu vopred oznámi:
    - názov a sídlo, alebo trvalý pobyt prevádzkovateľa,
    - účel spracúvania osobných údajov vymedzený prevádzkovateľom, alebo ustanovený osobitným zákonom; je vylúčené získavať osobné údaje pod zámienkou iného účelu, alebo inej činnosti,
    - dobrovoľnosť alebo povinnosť poskytovať požadované osobné údaje,
    - zákon, ktorý ustanovuje povinnosť poskytovať požadované osobné údaje,
    - okruh užívateľov, ktorým budú osobné údaje sprístupnené.

Za nepravdivosť osobných údajov zodpovedá ten, kto ich do informačného systému poskytol.
Zamestnanec je povinný aktualizovať osobné údaje, ktoré poskytol zamestnávateľovi.
Spracovať osobné údaje môžu len oprávnené osoby.
Ak sa spracúvajú osobné údaje už zverejnené, je potrebné ich náležite označiť – predovšetkým ich spôsob získania (preukazne).

b) Personálne opatrenia

Používanie technických prostriedkov pre spracovanie informácií je povolené iba osobám oprávneným oboznamovať sa s osobnými informáciami.
Technické prostriedky, sú využívane zásadne zamestnancami, ktorí majú tieto prostriedky pridelené.
Každá 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, mimo situácií vymedzených zákonom.
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.
Technické prostriedky, sú využívané zásadne zamestnancami, ktorí majú tieto prostriedky pridelené. Zamestnanci, ktorí majú pridelené technické prostriedky, sú zodpovední za ich správny chod a musia dodržiavať všetky zásady práce s nimi. Za informačný systém (počítačový) zodpovedá pracovník poverený správou PC a LAN siete. Pretože túto činnosť obec zabezpečuje dodávateľsky je povinná uzavrieť mandátnu zmluvu s presne formovanými cieľmi a opatreniami zabezpečujúcimi naplnenie bezpečnostného projektu.

Požiadavky na personálne opatrenia:

- **Kvalifikačné predpoklady:**
  Spracovávať osobné údaje v informačnom systéme môžu len osoby:
    - znalé práce na PC,
    - vyškolené pre prácu s aplikačným programom,
    - ostatné oprávnené osoby smú spracovávať osobné údaje len dokumentačne.
- **Personálne zabezpečenie procesov:**
    - proces prevádzky IS zabezpečuje poverený informatik (administrátor),
    - proces zadávania údajov zabezpečujú oprávnené osoby,

- proces archivácie zabezpečuje poverený zamestnanec v spolupráci s príslušným oddelením.

- **Personálna bezpečnosť:**
  - zamestnanci musia byť poučení,
  - každý zamestnanec je povinný zachovávať mlčanlivosť.
- **Zabezpečenie zastupiteľnosti:**
  Najdôležitejšie procesy pri ochrane osobných údajov v IS musia byť zabezpečené zastupiteľnosťou.
- **Zabezpečenie dodržiavania bezpečnostných smerníc:**
  - zamestnanci musia byť preukazne oboznámení s bezpečnostnými smernicami,
  - pri prijímaní zamestnanca do zamestnania musí byť zamestnanec riadne poučený.

c) Organizačné opatrenia

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,
  - starosta ustanovuje krízový štáb na čele so starostom alebo ním povereným zamestnancom.

- 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,
  - zamestnanci sa musia riadiť všetkými prijatými opatreniami a nariadeniami vydanými starostom,
  - po pracovnej dobe je zakázané zdržiavať sa na pracovisku,
  - na pracovisku sa pracovníci môžu zdržiavať len so súhlasom starostu alebo prednostu OcÚ,
  - pre krízový štáb musí byť zrejmé:
    - personálne obsadenie,
    - hierarchia v tíme, podriadenosť a zodpovednosť,
    - spôsob komunikácie,
    - rozdelenie úloh medzi členmi tímu,
    - krízový štáb má právomoc vydávať rozhodnutia.

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 starosta obce.

Nakladanie s nosičmi údajov:

Akékoľvek materiálne nosiče údajov musia byť zabezpečené pred prístupom neoprávnených osôb.
Nosiče živých údajov sú uložené:

- v kovových uzamykateľných skriniach,
- v iných uzamykateľných skriniach.

Spisy a údaje, ktoré podliehajú archivácii sú uložené v zabezpečenom archíve – samostatná miestnosť, uzamykateľná.
Údaje s prešlou dobou archivácie sa musia bezodkladne zlikvidovať tak, aby neboli čitateľné.

Chránené údaje v elektronickej forme sa ukladajú na databázový server a na prenosné nosiče (FD, CD a USB kľúč), ktoré sú uložené v kovových skriniach.

Údaje uložené na HD PC sa chránia nasledovne:

- PC sú chránené antivírovým programom s pravidelnou aktualizáciou databáz vírusov,
- konkrétne programy sú zaheslované, pre vstup do programov používa každý užívateľ vlastné heslo.

d) Technické opatrenia

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 serverov, tlačiarne, modemy, faxy, nahrávacie zariadenia pre audio a video, zálohovacie médiá (pásky, CD disky, diskety, USB kľúče a pod.), aplikačné programy, databáza, lokálna sieť,

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 antivírového programu.
- Vstupné a prihlasovacie heslá:
  - každý užívateľ LAN musí mať pridelené heslo, ktorým sa autentifikuje a toto heslo uchováva v tajnosti,
  - hesla k počítaču sú uložené v zapečatenej obálke u prednostu OcÚ, ich komisonálne otvorenie môže byť len so súhlasom starostu alebo prednostu OcÚ. O otvorení obálky sa vyhotoví zápis, v ktorom sa uvedie, kto, kedy a za

akým účelom vydal nariadenie na otvorenie obálky s heslom, mená členov komisie doba práce na PC. Po použití je potrebné zmeniť prístupové heslo.
  - vhodne zvolená doba životnosti a dĺžka hesla spolu s vynucovaním dostačujúcej zložitosti hesla dostatočne zabraňujú úspešným útokom zameraným na uhádnutie hesla,
  - je zakázané vstupovať do LAN pod cudzím užívateľským menom a heslom,
  - tie isté opatrenia platia aj pre prístup k aplikáciám.
- Používanie programov:
  - na pracovisku OcÚ, obecnej knižnice a MŠ smú byť používané iba autorizované programy,
  - kontrola integrity získaného softvérového balíka pred jeho inštaláciou,
  - aktualizácia programov zabezpečujúca 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:
  - pomocou kľúča PC,
  - heslo BIOSu.
- Záloha systému:
  - denne sa musia vytvárať kópie databáz,
  - aplikačný softvér musí byť zálohovaný stále po aktualizácii.

Zakazuje sa (mimo poverených osôb) :

- meniť a nastavovať konfiguráciu PC,
- vyraďovať ochranné prvky z činnosti,
- inštalovať programy,
- umožniť prístup na PC neoprávneným osobám,
- ukladať dáta s osobnými údajmi mimo miest na to určených.

2. Rozsah oprávnení, popis povolených činností

Vymedzenie okruhu a rozsah oprávnení (príloha č. 1):

Osoby oprávnené spracúvať osobné údaje (vymedzenie okruhu a rozsah)

- starosta obce - všetky,
- prednosta OcÚ – všetky,
- zástupca starostu – podľa rozsahu poverenia,
- ostatní zamestnanci – údaje v rozsahu svojej pracovnej náplne.

Osobné údaje oprávnené osoby v rámci úradu použijú len na zákonom vymedzené účely. Osobné údaje mimo úradu môže poskytovať len starosta, resp. v jeho neprítomnosti prednosta OcÚ alebo zástupca starostu. Oprávnená osoba len na priamy pokyn starostu, resp. prednostu OcÚ alebo ak jej to ukladá zákon.

Oprávnené osoby sú povinné osobné údaje chrániť pred zneužitím treťou osobou. Pokiaľ bezprostredne nepracujú s osobnými údajmi tieto držať v kovovej skrini, resp. v zabezpečenej skrini.

Rozsah zodpovednosti zodpovednej a oprávnených osôb

Za výkon dohľadu nad ochranou osobných údajov spracúvaných podľa zákona zodpovedá prevádzkovateľ. Prevádzkovateľ, ktorý spracúva osobné údaje prostredníctvom oprávnených osôb, môže výkonom dohľadu písomne poveriť zodpovednú osobu.

Zodpovedná osoba:

- zodpovednou osobou pre dohľad nad ochranou osobných údajov v zmysle § 23 zákona je poverený pracovník úradu,
- zodpovedná osoba dozerá na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov,
- zodpovedná osoba má postavenie oprávnenej osoby prevádzkovateľa s právom prístupu do informačných systémov prevádzkovateľa v rozsahu potrebnom na plnenie úloh podľa § 27 zákona,
- zodpovedná osoba pri akomkoľvek podozrení z porušenia práv dotknutých osôb, alebo iného porušenia zákona, má právo zastaviť aktivitu, zabezpečiť nosiče údajov a povinnosť okamžite upozorniť starostu obce na vzniknutú situáciu,
- kontroluje zásady spracovávania osobných údajov a vyhotovujú o tom písomný záznam.

Oprávnené osoby:

- sú zodpovedné za komplexné, pravdivé, aktuálne údaje a vkladanie týchto údajov do IS,
- sú zodpovedné za uchovávanie, ochranu a manipuláciu s nimi v prípade , že tieto údaje sú v textovej forme,
- sú zodpovedné za preukázateľnosť súhlasu na spracovanie osobného údaju a to tak, že možno o ňom podať dôkaz,
- sú zodpovedné za poriadok na pracovisku a odloženie všetkých písomností obsahujúcich osobné údaje a iných dokumentov, ktoré by mohli viesť k vyzradeniu osobných údajov do uzamykateľných skríň na to určených,
- sú zodpovedné za dodržiavanie zásad práce v LAN, WAN a PC podľa príkazu starostu obce o pravidlách používania počítačovej siete,
- sú povinné včas informovať zodpovednú osobu o pripravovanom začatí spracovávania osobných údajov a o všetkých skutočnostiach, ktoré by mohli viesť k zneužitiu týchto údajov.

Oprávnené osoby, ktoré prevádzkujú informačný systém:

- sú zodpovedné za riadny chod IS,
- zodpovedajú za archiváciu údajov aplikačného softvéru,
- sú zodpovedné za antivírovú ochranu PC,
- zodpovedajú za modernizáciu hmotných a nehmotných aktív.

Príprava oprávnených osôb

Starosta obce poučí oprávnené osoby o ich právach a povinnostiach v zmysle zákona

a tohto bezpečnostného projektu, poučenie opakuje spravidla jedenkrát ročne.
Všetky oprávnené osoby sú poučené o povinnosti mlčanlivosti a sú si vedomé, že zneužitie chránených údajov je dôvodom na rozviazanie pracovného pomeru.
O poučení oprávnených osôb sa vyhotoví Záznam o poučení oprávnenej osoby(ďalej len záznam). Záznam je uložený u zodpovednej osoby.

3. Kontrola na dodržiavanie bezpečnostných opatrení

Kontrolu dodržiavania bezpečnostných opatrení vykonáva:

- starosta obce,
- prednosta OcÚ,
- zodpovedná osoba.

Tieto osoby môžu kontrolovať spôsob spracovania, poskytovania, sprístupňovania, archivácie a likvidácie údajov.

Riešenie zistených nedostatkov

Pri zistení porušenia zákona sa okamžite pozastaví zber údajov, údaje sa zablokujú a hľadajú sa postupy, ako dostať situáciu do súladu so zákonom.
Pri zistení nedostatku spracuje zodpovedná osoba zápis o zistenom nedostatku, jeho odstránení a navrhovanom riešení do bezpečnostných smerníc.
Zápis sa musí vykonať vždy pri zistení systémového nedostatku a pri porušení práv dotknutých osôb. Pri porušení povinností oprávnených osôb sa postupuje v zmysle ZP.

Zakazuje sa:

a) Spracúvať osobné údaje:

- ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženskú vieru alebo svetonázor, členstvo v politických stranách alebo politických hnutiach, členstvo v odborových organizáciách (ak k takému spracovaniu nedala dotknutá osoba súhlas) a údaje týkajúce sa zdravia,
- pri spracúvaní osobných údajov možno využiť na účely určenia fyzickej osoby všeobecne použiteľný identifikátor ustanovený osobitným zákonom len vtedy, ak jeho použitie je nevyhnutné na dosiahnutie daného účelu spracúvania. Spracúvať iný identifikátor, ktorý v sebe skrýva charakteristiky dotknutej osoby, alebo zverejňovať všeobecne použiteľný identifikátor,
- o porušení ustanovení predpisov trestného práva, priestupkového práva alebo občianskeho práva, ako aj o výkone právoplatných rozsudkov alebo rozhodnutí môže vykonávať len ten, komu to umožňuje osobitný zákon,
- spracúvanie biometrických údajov možno vykonávať len za podmienok ustanovených v osobitnom zákone,
- o psychickej identite fyzickej osoby alebo o jej psychickej pracovnej spôsobilosti môže vykonávať len psychológ alebo ten, komu to umožňuje osobitný zákon,
- poskytovanie osobných údajov tretím osobám mimo zákonom stanovených prípadov.

b) Zakazuje sa zhromažďovanie a rozmnožovanie zhromaždených osobných údajov mimo zákonom stanovených prípadov.
c) Zhromažďovať, zapisovať, evidovať osobné údaje mimo k tomu určených a zabezpečených médií.
d) Poskytovať osobné údaje telefonicky, internetom (výnimka je zabezpečené spojenie).
e) Poskytovať osobné údaje bez overenia oprávnenosti osoby.
f) Zhromažďovať iné osobné údaje ako je stanovené zákonom.
g) Odnášať nosiče s osobnými údajmi z pracoviska bez súhlasu starostu.

Kontrolné činnosti zamerané na dodržiavanie bezpečnosti IS

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 spracúvania osobných údajov a vyhotovuje sa o tom písomný záznam.
Pred začatím kontroly je o kontrole upovedomený príslušný vedúci pracovník zodpovedný za danú agendu.
Zásady spracúvania osobných údajov sa kontrolujú minimálne raz za rok.
Kontrola prevádzky automatizovaného IS sa vykonáva nepretržite a to technickými a programovými prostriedkami. V pracovnej dobe sa vykonáva 1x týždenne povereným správcom siete.
Kontrola zabezpečenia miestností pred nedovoleným prístupom v pracovnej dobe ale i v mimopracovnom čase je vykonávaná námatkovo vedúcimi pracovníkmi.

4. 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.

a) Pri poruche počítačovej databázy (softvéru, výpadku dodávky el. energie...) sú oprávnené osoby spolu so zodpovednou osobou povinné zabezpečiť ochranu osobných údajov v informačných systémoch a utajovaných skutočností pred ich znehodnotením, zničením, neoprávneným prístupom a inými formami ohrozenia alebo zničenia nasledujúcimi úkonmi a opatreniami:

- použitie záložných zdrojov a zálohovanie údajov.

b) Pri ostatných haváriách a mimoriadnych situáciách (požiar, povodeň) sú oprávnené osoby spolu so zodpovednou osobou povinné zabezpečiť ochranu osobných údajov v informačných systémoch a utajovaných skutočností pred ich znehodnotením, zničením, neoprávneným prístupom a inými formami ohrozenia alebo zničenia prostredníctvom nasledujúcich opatrení:

- v prípade ohrozenia fyzická ochrana údajov prenosom do iných bezpečných priestorov.

Zároveň sú tieto osoby povinné dodržiavať všetky právne predpisy vzťahujúce sa k protipožiarnej ochrane a bezpečnosti a ochrane zdravia pri práci.
Preventívne opatrenia na zníženie vzniku mimoriadnych situácií a možností efektívnej obnovy stavu pred haváriou v podmienkach obce Streda nad Bodrogom:

- pravidelná kontrola hasiacich prístrojov,
- zálohovanie údajov,
- , kontrola technického zabezpečenia budov obecného úradu, materskej školy, miestneho kultúrneho strediska.

Článok 7.
Záverečné ustanovenia

1. S vyššie uvedenými pravidlami na zaistenie bezpečnosti a ochrany osobných údajov informačných systémoch prevádzkovateľa, ktorým je Obec Streda nad Bodrogom boli oboznámené:
   - oprávnené osoby (zamestnanci OcÚ),
   - osoby, ktoré môžu prísť do styku s osobnými údajmi,
   - osoba zodpovedná za servis PC.
2. Znenie bezpečnostného projektu je uložené u zodpovednej osoby. Sprístupňovanie jeho obsahu nepovolaným osobám nie je možné, nakoľko dokument má charakter dôverného dokumentu.
3. Tento bezpečnostný projekt nadobudol účinnosť dňom 1.5.2014

V Strede nad Bodrogom dňa 25.4.2014

OBEC STREDA NAD BODROGOM 2

Ing. František Gecse
starosta obce