BEZPEČNOSTNÝ PROJEKT
PRE SPRACÚVANIE A OCHRANU OSOBNÝCH ÚDAJOV
V ZARIADENÍ

Podľa ustanovení zákona 18/2018 z.z, z 29. novembra 2017 o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, (ďalej len „ZOOÚ“)

Obsahuje technické a organizačné opatrenia, ktoré sa zariadenie zaviazalo dodržiavať, keďže je podľa § 12 ZoOOÚ zodpovedná za dodržiavanie základných zásad spracúvania osobných údajov, za súlad spracúvania osobných údajov so zásadami spracúvania osobných údajov a je povinná tento súlad so zásadami spracúvania osobných údajov na požiadanie úradu preukázať.

Zariadenie: **Centrum sociálnych služieb – Nádej Dolný Lieskov**
Sídlo zariadenia: 018 21 Dolný Lieskov č. 197
IČO: 00 632 414

Dozorný orgán:
Úradu na ochranu osobných údajov Slovenskej republiky
Hraničná 12, 820 07 Bratislava 27
Tel: 02/ 32 31 3214
E-mail: statny.dozor@pdp.gov.sk

Vypracoval: Eleonóra Benediková
Revízia dokumentácie z roku 2018 = v plnom rozsahu
Dňa: 04.04.2012

Schválil: Ing. František Martaus, PhD. – riaditeľ

I. ZÁKLADNÉ USTANOVENIA

ÚČEL A CIEĽ

Účelom tejto dokumentácie je v podmienkach zariadenia CSS Nádej/ďalej len zariadenie/ v súlade so zákonom č. 18/2018 Z.z. O ochrane osobných údajov v informačných systémoch obsahujúcich osobné údaje /ďalej len informačný systém/:

a/ ustanoviť práva a povinnosti FO pri poskytovaní osobných údajov do informačného systému a práva, povinnosti a zodpovednosť oprávnených osôb - zamestnancov zariadenia, ktorí sa zúčastňujú na spracúvaní osobných údajov, resp. prichádzajú do styku s osobnými údajmi,

b/ ustanoviť práva a povinnosti zamestnancov, ktorí prevádzkujú IS používaný v zariadení.

Cieľom tejto dokumentácie je chrániť osoby poskytujúce údaje do informačného systému tak, aby ich osobné údaje boli využité iba na účely, pre ktoré ich osoba poskytla, či už na základe zákona alebo dobrovoľnosti. V konečnom dôsledku tak zabezpečiť ochranu súkromia dotknutých osôb v súvislosti s automatizovaným i manuálnym spracúvaním ich osobných údajov.

Legislatíva:

1. Zákon č. 18/2018 Z. z. o ochrane osobných údajov v z.n.p., (metodiky ÚOOÚ SR, vykonávacie predpisy)
2. Základné ľudské práva a slobody podľa Ústavy SR
3. Ochrana osobnosti – Občiansky zákonník (§ 11 - § 16)
4. Zákonník práce (§ 13 ods. 5) – spracúvanie osobných údajov v pracovnoprávnych vzťahoch a súkromie zamestnanca na pracovisku a v spoločných priestoroch zamestnávateľa
5. Trestný zákon (§ 374) – trestný čin neoprávneného nakladania s osobnými údajmi
6. Zákon č. 215/2004 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v z.n.p.
7.Vyhláška Národného bezpečnostného úradu č.48/2019 Z.z., ktorou sa ustanovujú podrobnosti o administratívnej bezpečnosti utajovaných skutočností
8. Zákon č. 311/2001 Z.z. Zákonník práce v z.n.p.
9. ISO/EC 27001 Informačné technológie. Zabezpečovacie techniky. Pravidlá dobrej praxe manažérstva informačnej bezpečnosti.
10. ISO/EC 27002 Systémy manažérstva informačnej bezpečnosti
11. ISO/EC 27005 Informačné technológie. Bezpečnostné metódy. Riadenie rizík informačnej bezpečnosti

Skratky:

RIAD – riaditeľ
OS – organizačná smernica
AIS – automatizovaný informačný systém
IS – informačný systém
FO – fyzická osoba
PMP – personálny a mzdový pracovník
PC – osobný počítač
TBOZP – bezpečnostný technik
ZO – zodpovedná osoba

Zodpovednosti:

Za vypracovanie a udržovanie tejto dokumentácie zodpovedá ZO.

Za dodržovanie jednotlivých ustanovení tejto dokumentácie sú zodpovední všetci zamestnanci, ktorí využívajú IS zariadenia na evidenciu a spracovanie osobných údajov zamestnancov, alebo iných FO osôb v súlade so zákonom č. 18/2018 Z.z. O ochrane osobných údajov. Za správne uloženie a prístupnosť tohto dokumentu zainteresovaným pracovníkom je zodpovedný RIAD. Zodpovednosť za udržiavanie pracovných kópií v aktuálnom stave je zodpovedný PMP. Oprávnenými osobami v spoločnosti sú: riaditeľ, ekonómka, hlavná sestra, sociálne pracovníčky, správca majetku, bezpečnostný technik, zodpovedná osoba.

1. VYMEDZENIE ZÁKLADNÝCH POJMOV

dotknutou osobou každá FO, ktorej osobné údaje sa spracúvajú,

prevádzkovateľom každý, kto sám alebo spoločne s inými vymedzí účel a prostriedky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene; prevádzkovateľ alebo konkrétne požiadavky na jeho určenie môžu byť ustanovené v osobitnom predpise alebo medzinárodnej zmluve, ktorou je SR viazaná, ak takýto predpis alebo táto zmluva ustanovuje účel a prostriedky spracúvania osobných údajov,

sprostredkovateľom každý, kto spracúva osobné údaje v mene prevádzkovateľa,

spracúvaním osobných údajov spracovateľská operácia alebo súbor spracovateľských operácií s osobnými údajmi alebo so súbormi osobných údajov, najmä získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie, bez ohľadu na to, či sa vykonáva automatizovanými prostriedkami alebo neautomatizovanými prostriedkami,

súhlasom dotknutej osoby akýkoľvek vážny a slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby vo forme vyhlásenia alebo jednoznačného potvrdzujúceho úkonu, ktorým dotknutá osoba vyjadruje súhlas so spracúvaním svojich osobných údajov

informačným systémom akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom základe alebo geografickom základe,

biometrickými údajmi osobné údaje, ktoré sú výsledkom osobitného technického spracúvania osobných údajov týkajúcich sa fyzických charakteristických znakov fyzickej osoby, fyziologických charakteristických znakov fyzickej osoby alebo behaviorálnych charakteristických znakov FO a ktoré umožňujú jedinečnú identifikáciu alebo potvrdzujú jedinečnú identifikáciu tejto FO, ako najmä vyobrazenie tváre alebo daktyloskopické údaje,

obmedzením spracúvania osobných údajov označenie uchovávaných osobných údajov s cieľom obmedziť ich spracúvanie v budúcnosti,

profilovaním akákoľvek forma automatizovaného spracúvania osobných údajov spočívajúceho v použití osobných údajov na vyhodnotenie určitých osobných znakov alebo charakteristík týkajúcich sa FO, najmä na analýzu alebo predvídanie znakov alebo charakteristík dotknutej osoby súvisiacich s jej výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom,

pseudonymizáciou spracúvanie osobných údajov spôsobom, že ich nie je možné priradiť ku konkrétnej dotknutej osobe bez použitia dodatočných informácií, ak sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia na zabezpečenie toho, aby osobné údaje nebolo možné priradiť identifikovanej FO alebo identifikovateľnej FO,

šifrovaním transformácia osobných údajov spôsobom, ktorým opätovné spracúvanie je možné len po zadaní zvoleného parametra, ako je kľúč alebo heslo,

online identifikátorom identifikátor poskytnutý aplikáciou, nástrojom alebo protokolom, najmä IP adresa, cookies, prihlasovacie údaje do online služieb, rádiofrekvenčná identifikácia, ktoré môžu zanechávať stopy, ktoré sa najmä v kombinácii s jedinečnými identifikátormi alebo inými informáciami môžu použiť na vytvorenie profilu dotknutej osoby a na jej identifikáciu,

porušením ochrany osobných údajov porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene alebo k neoprávnenému poskytnutiu prenášaných, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov alebo k neoprávnenému prístupu k nim,

príjemcom každý, komu sa osobné údaje poskytnú bez ohľadu na to, či je treťou stranou; za príjemcu sa nepovažuje orgán verejnej moci, ktorý spracúva osobné údaje na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je SR viazaná, v súlade s pravidlami ochrany osobných údajov vzťahujúcimi sa na daný účel spracúvania osobných údajov,

treťou stranou každý, kto nie je dotknutou osobou, prevádzkovateľ, sprostredkovateľ alebo inou fyzickou osobou, ktorá na základe poverenia prevádzkovateľa alebo sprostredkovateľa spracúva osobné údaje,

informatik je pracovník, majúci kompetenciu riadiť informačné technológie spoločnosti. Je zodpovedný za riadenie, prevádzku a správu IS a počítačovej siete vrátane technického a prevádzkového riešenia bezpečnostných aspektov,

oprávnená osoba je osoba, ktorá spracováva osobné údaje na základe pokynu prevádzkovateľa alebo sprostredkovateľa. Všetky oprávnené osoby musia byť preukázateľne poučené,

aktíva informačného systému sú všetky súčasti IS (servery, pracovné stanice, smerovače, prepínače, rozbočovače, štruktúrovaná kabeláž, modemy, accesspointy, tlačiarne, programové vybavenie, zálohové média ...),

server je počítač, poskytujúci niektoré svoje služby alebo zariadenia ostatným do siete zapojeným počítačom,

pracovná stanica je osobný počítač (PC), prenosný PC (notebook), terminál,

smerovač je sieťové zariadenie pre smerovanie dát z uzla jednej siete so uzla inej siete,

firewall je zariadenie alebo programové vybavenie zamedzujúce nepovoleným infiltráciám vstup do IS,

modem je elektronické zariadenie, ktoré premieňa elektronické impulzy PC na signály, ktoré je možno prenášať telefónnymi linkami, za účelom prepojenia počítačov telefónnymi linkami,

miestna tlačiareň je tlačiareň, ktorá je nakonfigurovaná ako prístupná len s PC, ku ktorému je fyzicky pripojená,

sieťová tlačiareň je nakonfigurovaná ako prístupná zo siete,

štruktúrovaná kabeláž je univerzálny generický systém vyjadrujúci hierarchické prepojenie siete, ktorý poskytuje užívateľom nezávislú prenosovú kapacitu pre dátové, analógové, video a ďalšie signály v rámci budov a areálov,

bezpečnosť IS je súbor opatrení na ochranu IS pred bezpečnostnými udalosťami,

bezpečnostná udalosť je udalosť majúca za následok ohrozenie dôveryhodnosti dát alebo obmedzenie ich dostupnosti v IS,

vyššia moc je náhodná, neočakávaná udalosť, vyvolaná rôznymi prejavmi fyzikálnej alebo sociálnej povahy, ktorá nezávisí od pôsobenia spoločnosti či osoby, napr.: požiar, zatopenie vodou, terorizmus, chrípkové epidémie, komunikačné zlyhania, neidentifikované prírodné vplyvy a pod..,

protiopatrenia sú činnosť, postupy alebo mechanizmus, ktorý minimalizuje riziko redukciou dopadu pri útoku a zlepšuje bezpečnosť IS redukciou hrozby pri výskyte útoku, redukciou slabiny pre útok, redukciou dopadu pri útoku, odhalením útoku alebo obnovou pri útoku,

vírus je malý počítačový program schopný samoreplikácie, ktorý môže poškodiť OS v PC alebo dáta v ňom uložené, alebo ich odosielať, alebo zverejňovať na internete,

spyware je špehovací program, ktorý zhromažďuje informácie o aktivitách používateľa PC na internete (na čo klikáte, aké stránky so prehliadate a pod.),

internet je medzinárodný systém navzájom prepojených počítačových sietí, ktorý umožňuje fungovanie rozličných druhov elektronickej komunikácie,

schválené programové vybavenie je programové vybavenie, ktoré je odsúhlasené štatutárom spoločnosti,

neschválené programové vybavenie je také, ktoré nie je odsúhlasené štatutárom spoločnosti,

princíp najmenších privilégií je princíp, ktorý užívateľovi dovoľuje vykonať iba tie činnosti, na ktoré je oprávnený. Uplatnenie tohto princípu na prístupové práva zabezpečí užívateľovi pridelenie minimálnych prístupových práv na plnenie jeho pracovných povinností.

2. MAPOVANIE OSOBNÝCH ÚDAJOV

Naše zariadenie definuje, aké osobné údaje spracúva, aby bolo schopné zanalyzovať spracúvanie osobných údajov a zabezpečiť ochranu všetkých spracuvávaných osobných údajov.

a) Osobné údaje prijímateľov sociálnej služby

meno, priezvisko, titul, ulica a číslo, PSČ, mesto, dátum narodenia, rodné číslo, telefónny kontakt, majetkové pomery, údaje o zdravotnom stave, kontakt na rodinného príslušníka (spracovateľské operácie: Agenda sociálna, Agenda zdravotná, Kniha návštev, Správa registratúry, Stravovanie, Účtovné doklady, Sťažnosti, Občania – poradovník, Sprístupnenie informácií, Sťažnosti).

b) Osobné údaje zamestnancov:

meno, priezvisko, titul, trvalý pobyt - ulica a číslo, PSČ, mesto, dátum narodenia, rodné číslo, číslo bankového účtu (IBAN), názov zdravotnej poisťovne, doplnkovej dôchodkovej sporiteľne, číslo OP, email, telefónny kontakt, najvyššie ukončené vzdelanie, základná mzda, osobné ohodnotenie (spracovateľské operácie: PAM, BOZP, Evidencia dochádzky, Oznamovanie protispoločenskej

činnosti, Správa registratúry, Sťažnosti, Súdne spory, Účtovné doklady, Žiadosti o prijatie do zamestnania).

c) Osobné údaje rodinných príslušníkov zamestnancov:

mená, priezviská, adresa, rodné čísla rodinných príslušníkov (spracovateľské operácie: PAM, Účtovné doklady, Správa registratúry).

d) Osobné údaje žiadateľov o zamestnanie:

meno, priezvisko, titul, vzdelanie, prax, email, telefónny kontakt (spracovateľské operácie: Správa registratúry).

3. VŠEOBECNÉ POVINNOSTI PREVÁDZKOVATEĽA (§ 31 ZOOÚ)

Naše zariadenie ako prevádzkovateľ dodržuje nasledovné všeobecné povinnosti:

a) S ohľadom na povahu, rozsah a účel spracúvania osobných údajov a na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva FO sa zaväzujeme prijať vhodné technické a organizačné opatrenia na zabezpečenie a preukázanie toho, že spracúvanie osobných údajov sa vykonáva v súlade so ZOOÚ.
b) Uvedené opatrenia budeme podľa potreby aktualizovať.
c) Budeme pravidelne preverovať trvanie účelu spracúvania osobných údajov a po jeho splnení bez zbytočného odkladu zabezpečiť výmaz osobných údajov
d) Naše zariadenie bude zachovávať mlčanlivosť o osobných údajoch, ktoré spracúva. Povinnosť mlčanlivosti trvá aj po ukončení spracúvania osobných údajov.

4. ŠPECIFICKY NAVRHNUTÁ A ŠTANDARDNÁ OCHRANA OSOBNÝCH ÚDAJOV (§ 32 ZOOÚ)

Naše zariadenie sa zaväzuje pred spracúvaním osobných údajov zaviesť a počas spracúvania osobných údajov mať zavedenú špecificky navrhnutú ochranu osobných údajov, ktorá spočíva v prijatí primeraných technických a organizačných opatrení, napríklad aj vo forme pseudonymizácie, na účinné zavedenie primeraných záruk ochrany osobných údajov a dodržiavanie základných zásad podľa § 6 až 12, ZOOÚ.

Naše zariadenie sa zaväzuje pri špecificky navrhnutej ochrane osobných údajov zohľadniť najnovšie poznatky ochrany osobných údajov, náklady na vykonanie opatrení, povahu, rozsah, kontext a účel spracúvania osobných údajov a riziká spracúvania osobných údajov s rôznou pravdepodobnosťou a závažnosťou, ktoré spracúvanie osobných údajov predstavuje pre práva dotknutej osoby.

Naše zariadenie sa zaväzuje zaviesť štandardnú ochranu osobných údajov, ktorá spočíva v prijatí primeraných technických a organizačných opatrení na zabezpečenie spracúvania osobných údajov len na konkrétny účel, minimalizácie množstva získaných osobných údajov a rozsahu ich spracúvania, doby uchovávania a dostupnosti osobných údajov. Naše zariadenie zabezpečí, aby osobné údaje neboli bez zásahu FO štandardne prístupné neobmedzenému počtu FO.

5. PRÁVA DOTKNUTEJ OSOBY

Povinnosti prevádzkovateľa pri uplatňovaní práv dotknutej osoby sú upravené § 29 ZOOÚ. Obmedzenia práv dotknutej osoby, podľa § 30 ZOOÚ.

Práva dotknutej osoby sú upravené § 19 - § 28 ZOOÚ a naše zariadenie sa zaväzuje ich dodržiavať.

Ide napríklad o nasledovné práva:

a) Dotknutá osoba má právo získať od prevádzkovateľa potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú.
b) Dotknutá osoba má právo byť informovaná o primeraných zárukách týkajúcich sa prenosu podľa § 48 ods. 2 až 4, ak sa osobné údaje prenášajú do tretej krajiny alebo medzinárodnej organizácii.
c) Prevádzkovateľ je povinný poskytnúť dotknutej osobe jej osobné údaje, ktoré spracúva.
d) Dotknutá osoba má právo na to, aby prevádzkovateľ bez zbytočného odkladu opravil nesprávne osobné údaje, ktoré sa jej týkajú. So zreteľom na účel spracúvania osobných údajov má dotknutá osoba právo na doplnenie neúplných osobných údajov.
e) Dotknutá osoba má právo na to, aby prevádzkovateľ bez zbytočného odkladu vymazal osobné údaje, ktoré sa jej týkajú.
f) Dotknutá osoba má právo na to, aby prevádzkovateľ obmedzil spracúvanie osobných údajov
g) Dotknutá osoba má právo získať osobné údaje, ktoré sa jej týkajú a ktoré poskytla prevádzkovateľovi
h) Dotknutá osoba má právo namietať spracúvanie osobných údajov
i) Dotknutá osoba má právo na to, aby sa na ňu nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní osobných údajov vrátane profilovania a ktoré má právne účinky, ktoré sa jej týkajú alebo ju obdobne významne ovplyvňujú.

6. SPROSTREDKOVATEĽ (§ 34 ZOOÚ)

Sprostredkovateľ je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa.

Naše zariadenie ako prevádzkovateľ využíva sprostredkovateľov, ktorí v jej mene spracuvávajú osobné údaje.

Pre naše zariadenie spracovávajú údaje nasledovní sprostredkovatelia:

- Autorizovaný bezpečnostný technik a technik OPP
- Školiteľ CO – z Obecného úradu, alebo VÚC
- Technik IT (na objednávku)
- Zodpovedná osoba v zmysle Zákona č. 18/2018 Z.z. O ochrane osobných údajov v z.n.p.

Naše zariadenie využíva len sprostredkovateľov poskytujúcich dostatočné záruky na to, že sa prijmú primerané technické a organizačné opatrenia tak, aby spracúvanie spĺňalo požiadavky ZoOOÚ a aby sa zabezpečila ochrana práv dotknutej osoby.

Spracúvanie sprostredkovateľom pre naše zariadenie sa riadi „zmluvou o spracúvaní osobných údajov“, ktorej vzor je prílohou tohto dokumentu. Zaväzuje sprostredkovateľa voči prevádzkovateľovi a stanovuje sa ňou predmet a doba spracúvania, povaha a účel spracúvania, typ osobných údajov a kategórie dotknutých osôb a povinnosti a práva prevádzkovateľa a sprostredkovateľa.

Naše zariadenie podpíše dodatky k zmluvám so spomenutými sprostredkovateľmi, aby zmluvy spĺňali všetky náležitosti ZOOÚ.

7. ZÁSADY SPRACÚVANIA OSOBNÝCH ÚDAJOV V NAŠOM ZARIADENÍ

7.1. Zásada zákonnosti (§ 6 a § 13 ZOOÚ)

Naše zariadenie sa zaviazalo spracúvať údaje len zákonným spôsobom tak, aby nedošlo k porušeniu základných práv dotknutej osoby.

Spracúvanie osobných údajov naším zariadením je zákonné a to zabezpečením, že sa vykonáva na základe aspoň jedného z týchto právnych základov:

a) dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov aspoň na jeden konkrétny účel,
b) spracúvanie osobných údajov je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo na vykonanie opatrenia pred uzatvorením zmluvy na základe žiadosti dotknutej osoby,
c) spracúvanie osobných údajov je nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná,
d) spracúvanie osobných údajov je nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby alebo inej fyzickej osoby,
e) spracúvanie osobných údajov je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi alebo
f) spracúvanie osobných údajov je nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany okrem prípadov, keď nad týmito záujmami prevažujú záujmy alebo práva dotknutej osoby vyžadujúce si ochranu osobných údajov, najmä ak je dotknutou osobou dieťa; tento právny základ sa nevzťahuje na spracúvanie osobných údajov orgánmi verejnej moci pri plnení ich úloh.

Právny základ pre jednotlivé kategórie osobných údajov sú nasledovné:

Získavanie osobných údajov

Ten, kto získava osobné údaje, je povinný na požiadanie dotknutej osoby preukázať svoju totožnosť a vopred oznámiť dotknutej osobe alebo inej fyzickej osobe, od ktorej osobné údaje požaduje

- účel získavania osobných údajov,
- zákon, ktorý ustanovuje povinnosť poskytovať požadované údaje a následky odmietnutia poskytnúť osobné údaje,
- predpokladaný okruh užívateľov.

Oprávnenie na získavanie osobných údajov vydáva riaditeľka zariadenia. Pokiaľ zamestnanec získava osobné údaje za podmienok ustanovených osobitnými zákonmi / napr. hore uvedené zákony / a jeho pracovné zaradenie si vyžaduje konanie podľa týchto zákonov, nevyžaduje sa písomná forma tohto oprávnenia.

a) Osobné údaje prijímateľov sociálnej služby

Právny základ – písmeno a) spracúvanie osobných údajov je nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je SR viazaná.

b) Osobné údaje zamestnancov:

Právny základ – písmeno b) dotknutá osoba dáva automaticky súhlas so spracúvaním svojich osobných údajov za účelom spracovania miezd,

Právny základ – písmeno b) spracúvanie osobných údajov je nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je SR viazaná.

c) Osobné údaje rodinných príslušníkov zamestnancov:

Právny základ – písmeno c) spracúvanie osobných údajov je nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná. Predovšetkým podľa zákona č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov

d) Osobné údaje žiadateľov o zamestnanie:

Právny základ – písmeno d) dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov za účelom evidencie uchádzačov o zamestnanie.

Spracúvanie osobných údajov

Spracúvanie osobných údajov vykonáva iba zamestnanec v rámci plnenia povinností vyplývajúcich mu z pracovného zaradenia / z pracovnej náplne / a iba pre služobné účely. Uvedené sa vzťahuje aj na likvidáciu osobných údajov, ktorú bezodkladne zabezpečí zamestnanec po splnení účelu spracovania, pokiaľ osobitný zákon neustanovuje inak.

Zamestnanec, ktorý vykonáva spracúvanie osobných údajov, je oprávnený toto vykonávať za podmienok a v rozsahu určených písomnou zmluvou alebo v poverení konateľom spoločnosti.

Spracúvanie osobných údajov zamestnancov sa vykonáva na mzdovom softvéri „Asseco Wéčko“, zálohovanie údajov vykonáva PMP 1 x mesačne v elektronickom archíve PC na externý, uloženie – sídlo zariadenia. Ekonomika sa spracováva v ekonomickom softvéri. PC, na ktorom sa spracovávajú osobné údaje je chránený antivírusovým systémom, pravidelne sa vykonáva upratovanie súborov pomocou systémových nástrojov. Sociálna agenda sa spracováva v IS „CYGNUS“ aj kartotékovej forme, kuchyňa využíva IS „CYGNUS“.

7.2. Zásada obmedzenia účelu (§ 7 ZOOÚ)

Naše zariadenie získava osobné údaje len na konkrétne určený, výslovne uvedený a oprávnený účel a nebude ich ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmto účelom. Naše zariadenie informuje dotknutú osobu o účele spracúvania osobných údajov pred ich spracúvaním.

7.3. Zásada minimalizácie osobných údajov (§ 8 ZOOÚ)

Naše zariadenie spracováva osobné údaje tak, aby toto spracúvanie primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú.

S cieľom zabezpečiť minimalizáciu osobných údajov sa naše zariadenie rozhodlo zanalyzovať, či sú spracuvávané údaje primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú.

Analyzujú sa nasledovné kategórie, konkrétne druhy osobných údajov sú uvedené v časti „mapovanie osobných údajov“.

a) Osobné údaje zamestnancov:

Všetky spracuvávané údaje sú nevyhnutné. Sú spracovávané na účely evidencie zamestnancov, výplaty miezd, alebo komunikáciu so zamestnancami.

b) Osobné údaje rodinných príslušníkov zamestnancov:

Všetky spracuvávané údaje sú nevyhnutné. Sú spracovávané na účely uplatnenia nezdaniteľnej časti základu dane na daňovníka a daňového bonusu podľa § 36 ods. 6 zákona č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov, alebo na účely vykonania ročného zúčtovania dane.

7.4. Zásada správnosti (§ 9 ZOOÚ)

Naše zariadenie spracováva osobné údaje tak, aby boli správne a podľa potreby aktualizované; a prijme primerané a účinné opatrenia na zabezpečenie toho, aby sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bez zbytočného odkladu vymazali alebo opravili.

Na zabezpečenie zásady správnosti má naše zariadenie v písomnom súhlase so spracovaním osobných údajov nasledovnú formuláciu:

„Dotknutá osoba je povinná poskytnúť pravdivé a aktuálne osobné údaje. V prípade zmeny osobných údajov je dotknutá osoba povinná zmenu bezodkladne oznámiť prevádzkovateľovi.“

7.5. Zásada minimalizácie uchovávania (§ 10 ZOOÚ)

Osobné údaje naše zariadenie uchováva vo forme, ktorá umožňuje identifikáciu dotknutej osoby najneskôr dovtedy, kým je to potrebné na účel, na ktorý sa osobné údaje spracúvajú.

7.6. Zásada integrity a dôvernosti (§ 11 ZOOÚ)

Osobné údaje sú v našom zariadení spracúvané spôsobom, ktorý zaručuje primeranú bezpečnosť osobných údajov vrátane ochrany pred neoprávneným spracúvaním osobných údajov, nezákonným spracúvaním osobných údajov, náhodnou stratou osobných údajov, výmazom osobných údajov alebo poškodením osobných údajov.

7.6.1. Osobné údaje uložené v elektronických dokumentoch

Naše zariadenie používa antivírus a firewall od spoločnosti ESET.

Zálohovanie sa vykonáva 1x mesačne, zálohujeme elektronické dokumenty na externý disk. Spoločnosť má počítačovú sieť, zálohy sa vytvárajú na serveri na VÚC.

Počítač s osobnými údajmi je chránený heslom, ktoré vie len oprávnená osoba.

7.6.2. Osobné údaje uložené vo fyzických dokumentoch

Fyzické dokumenty sú uložené v obaloch a v uzamknutej skrini v kancelárii ekonómky, čím je zabezpečená ochrana pred poškodením.

Šanóny s fyzickými dokumentmi ekonomickými sú uložené v uzamknutej skrinke v kancelárii ekonómky.

7.7. Zásada zodpovednosti (§ 12 ZOOÚ)

Každý zamestnanec, ktorý spracúva osobné údaje, zodpovedá za bezpečnosť osobných údajov tým, že ich chráni pred odcudzením, stratou, poškodením, zničením, sprístupnením neoprávneným osobám,

zmenou alebo rozširovaním / zverejňovaním/. Zamestnanec, ktorý príde pri výkone svojho povolania do styku s osobnými údajmi, zodpovedá za bezpečnosť osobných údajov najmä tým, že ich chráni pred rozširovaním, neoprávneným prístupom, stratou a odcudzením.

Za týmto účelom sa stanovujú nasledovné opatrenia:

Technické

a/ PC, na ktorom sa spracúvajú osobné údaje, jeho užívateľ zabezpečil heslom pre spustenie počítača a heslom pre spustenie programu,

b/ každý zamestnanec, ktorý spracúva osobné údaje na PC, je povinný riadiť sa pokynmi RIAD.

c/ osobné údaje, ktoré sa nachádzajú v kartotékovom systéme /spracúvané písomnou formou/ musia byť uskladňované a uzamykané v uzamykateľných boxoch, skriniach alebo kontajneroch. V osobnej zložke zamestnanca sa nachádza: kópie dokladu totožnosti, o vzdelaní, osobný dotazník, pracovná zmluva, prihlášky a odhlášky do poisťovní. Všetko je uložené v kancelárii vedúcej sestry. Účtovné doklady sa archivujú u externej účtovníčky – uzamknuté. Sociálna a zdravotná agenda sa nachádza v ošetrovni, v uzamknutej kovovej registračke.

d/ miesto, kde je umiestnený PC, na ktorom sa spracúvajú osobné údaje, ako aj miesto, kde sa nachádzajú osobné údaje spracúvané v kartotékovom systéme musia byť mimo dosah neoprávnených osôb – v sídle zariadenia,

e/ pri likvidácii osobných údajov z PC zabezpečí PMP ich likvidáciu z hlavného disku PC. Likvidáciu údajov z nosičov , alebo externého disku – USB kľúča slúžiaceho na zálohovanie, resp. na prenos zabezpečí PMP. Okrem vymazania dát z nosičov musí dôjsť k ich fyzickému zničeniu (rozlámaním, rozdrvením).

f/ likvidácia osobných údajov vedených písomne sa vykoná skartáciou, za prítomnosti zamestnanca, ktorý tieto osobné údaje spracúva a likviduje.

Organizačné:

a/ v prípade výskytu technických závad súvisiacich s opatreniami uvedenými v bode 7.7 sa tieto nahlásia RIAD,

b/ zákaz poskytovať osobné údaje v telefonickom styku o všetkých dotknutých osobách,

c/ premiestňovanie PC, na ktorom sa spracúvajú osobné údaje sa môže vykonávať len so súhlasom riaditeľky,

d/ v prípade odovzdania PC do servisu z dôvodu opravy, RIAD pripraví k podpisu odovzdávací protokol.

Povinnosť mlčanlivosti

Každý zamestnanec, ktorý spracúva, resp. prichádza do styku s osobnými údajmi:

- je povinný zachovať mlčanlivosť o osobných údajoch. Táto povinnosť trvá aj po zmene pracovného zaradenia, aj po ukončení pracovného pomeru v zariadení. Povinnosť mlčanlivosti neplatí, ak osobné údaje je zamestnanec poskytnúť v zmysle osobitných zákonov, napr. pre potreby orgánov činných v trestnom konaní,

- nesmie využiť osobné údaje pre vlastnú potrebu,

- bez súhlasu podniku ich nesmie nikomu sprístupňovať.

Povinnosť mlčanlivosti neplatí vo vzťahu k orgánu štátneho dozoru nad ochranou osobných údajov v informačných systémoch, ktorému je zamestnanec povinný pri plnení jeho úloh poskytnúť ním všetky požadované údaje a poskytnúť mu potrebnú súčinnosť.

8. PODMIENKY POSKYTNUTIA SÚHLASU SO SPRACÚVANÍM OSOBNÝCH ÚDAJOV

Zariadenie zabezpečí splnenie nasledovných podmienok pri vyjadrení súhlasu dotknutou osobou

a) súhlas so spracúvaním osobných údajov musí byť vyjadrený slobodne, konkrétne, informovane a jednoznačným prejavom vôle.
b) žiadosť o vyjadrenie súhlasu musí byť predložená tak, aby bola jasne odlíšiteľná od týchto iných skutočností, v zrozumiteľnej a ľahko dostupnej forme a formulovaná jasne a jednoducho.

Naše zariadenie zrevidovalo písomné súhlasy so spracovaním osobných údajov, aby spĺňali požiadavky ZOOÚ, predovšetkým § 14 a § 19. Písomné súhlasy, ktoré spoločnosť využíva sú prílohou tohto dokumentu.

9. SPRACÚVANIE OSOBITNÝCH KATEGÓRIÍ OSOBNÝCH ÚDAJOV

Naše zariadenie nespracúva osobitné kategórie osobných údajov. Osobitnými kategóriami osobných údajov sú údaje, ktoré odhaľujú rasový pôvod alebo etnický pôvod, politické názory, náboženskú vieru, filozofické presvedčenie, členstvo v odborových organizáciách, genetické údaje, biometrické údaje, údaje týkajúce sa zdravia alebo údaje týkajúce sa sexuálneho života alebo sexuálnej orientácie FO.

10. OZNÁMENIE PORUŠENIA OCHRANY OSOBNÝCH ÚDAJOV DOZORNÉMU ORGÁNU

V prípade porušenia ochrany osobných údajov naša spoločnosť bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín po tom, čo sa o tejto skutočnosti dozvedela, oznámi porušenie ochrany osobných údajov dozornému orgánu.

Ak oznámenie nebolo dozornému orgánu predložené do 72 hodín, pripojí sa k nemu zdôvodnenie omeškania.

Oznámenie o porušení ochrany osobných údajov bude obsahovať aspoň:

a) opis povahy porušenia ochrany osobných údajov vrátane, podľa možnosti, kategórií a približného počtu dotknutých osôb, ktorých sa porušenie týka a kategórií a približného počtu dotknutých záznamov o osobných údajoch;

b) kontaktné údaje zodpovednej osoby v našom zariadení, kde možno získať viac informácií o porušení ochrany osobných údajov;

c) opis pravdepodobných následkov porušenia ochrany osobných údajov;

d) opis opatrení prijatých alebo navrhovaných prevádzkovateľom s cieľom napraviť porušenie ochrany osobných údajov vrátane, podľa potreby, opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov.

Naše zariadenie zdokumentuje každý prípad porušenia ochrany osobných údajov vrátane skutočností spojených s porušením ochrany osobných údajov, jeho následky a prijaté opatrenia na nápravu.

V prípade porušenia ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, naša spoločnosť bez zbytočného odkladu oznámi porušenie ochrany osobných údajov dotknutej osobe.

11. URČENIE ZODPOVEDNEJ OSOBY

Prevádzkovateľ je povinný určiť zodpovednú osobu, ak

a) spracúvanie osobných údajov vykonáva orgán verejnej moci alebo verejnoprávna inštitúcia okrem súdov pri výkone ich súdnej právomoci,

b) hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa sú spracovateľské operácie, ktoré si vzhľadom na svoju povahu, rozsah alebo účel vyžadujú pravidelné a systematické monitorovanie dotknutej osoby vo veľkom rozsahu alebo

c) hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa je spracúvanie osobitných kategórií osobných údajov podľa § 16 ZOOÚ vo veľkom rozsahu alebo spracúvanie osobných údajov týkajúcich sa uznania viny za spáchanie trestného činu alebo priestupku podľa § 17 ZOOÚ vo veľkom rozsahu.

Naše zariadenie určuje zodpovednú osobu na základe zmluvy.

12. PRENOS OSOBNÝCH ÚDAJOV DO TRETEJ KRAJINY ALEBO MEDZINÁRODNEJ ORGANIZÁCIE

Prenos osobných údajov, ktoré sa spracúvajú alebo sú určené na spracúvanie po prenose do tretej krajiny alebo medzinárodnej organizácie, sa môže uskutočniť len vtedy, ak prevádzkovateľ a sprostredkovateľ dodržiavajú podmienky vrátane podmienok následného prenosu osobných údajov z predmetnej tretej krajiny alebo od predmetnej medzinárodnej organizácie do inej tretej krajiny alebo inej medzinárodnej organizácie.

Úrad na ochranu osobných údajov uverejňuje na svojej webstránke zoznam tretích krajín, území a určených sektorov v danej tretej krajine a medzinárodných organizácií, v prípade ktorých Európska komisia rozhodla, že v nich je zaručená primeraná úroveň ochrany alebo už prestala byť primeraná úroveň ochrany zaručená.

Zoznam je dostupný na stránke https://dataprotection.gov.sk/uoou/sk/content/prenos-do-krajin-zarucujucich-primeranu-uroven-ochrany

Naše zariadenie bude tento zoznam pravidelne sledovať a v prípade, že by prenášala osobné údaje do krajín mimo zoznam úradu na ochranu osobných údajov, bude postupovať podľa § 47 - § 51 ZOOÚ.

13. PROSTREDIE

Umiestnenie informačného systému je v jednej budove, v sídle zariadenia, ktoré sa uzatvára na hlavnom aj vedľajšom vchode zámkom bezpečnostnej triedy minimálne 2. Kancelárie sa nachádzajú na druhom nadzemnom podlaží, všetky dvere sa uzamykajú, ak administratívny pracovník opustí kanceláriu. Po ukončení pracovnej doby si kľúč od kancelárie riaditeľka, mzdová účtovníčka, prevádzkarka, ekonómka a vrchná sestra zároveň berie so sebou.

Manipulácia s náhradnými kľúčmi je popísaná v samostatnej „Inštrukcii o používaní náhradných kľúčov“. Všetci zamestnanci recepcie a vedúci zamestnanci sú o používaní náhradných kľúčov poučení, o poučení je vytvorený záznam.

Po pracovnej dobe administratívnych pracovníkov sú vedľajšie vchody do budovy uzamknuté. Hlavný vchod je počas dňa otvorený, uzamyká sa v čase od 20:00 do 06:00 hod. Na recepcii je stála služba. V budove je stála služba zdravotného personálu. Kancelárie sú po pracovnej dobe kódované, všetky oprávnené osoby majú rovnaký kód.

Kľúče od sídla zariadenia majú k dispozícii oprávnení zamestnanci.

Upratovačské práce sa vykonávajú len v pracovnej dobe a za podmienok, ktoré vylučujú možnosť styku s osobnými údajmi.

Poučenie nového zamestnanca pri nástupe do pracovného pomeru o pracovných povinnostiach, platných smerniciach a postupoch, o vykonávaní záznamov vykonáva priamy nadriadený.

Poučenie pracovníkov o bezpečnostných pokynoch platných v zariadení vykonáva pri nástupe do pracovného pomeru a v rámci opakovaných školení bezpečnostný technik na základe zmluvy. Poučenie je zdokumentované v zázname zo školenia.

Zariadenie využíva kamerový systém verejnosti neprístupný za účelom ochrany majetku a osôb, v prípade nežiaducich udalostí na identifikáciu ich príčiny a dôsledkov.

II. BEZPEČNOSTNÝ ZÁMER

Správny chod vnútorných procesov zariadenia si vyžaduje bezporuchovú a bezpečnú prevádzku IS. Najdôležitejšou úlohou je zabezpečenie dostupnosti a správnosti informácií v IS a ich bezpečnosť pred poškodením alebo zneužitím. Na tento účel zariadenie prijalo súbor opatrení vo forme bezpečnostných smerníc.

Vzhľadom na neustále prispôsobovanie sa IS požiadavkám zariadenia a užívateľov, sme stanovili hlavné zásady dlhodobého zabezpečovania ochrany IS. Tieto musia permanentne sledovať zmeny legislatívy dotýkajúcej sa informačných technológií a smerovaniu vývoja technického a programového vybavenia.

Veľký dôraz kladieme na vzdelávanie pracovníkov prichádzajúcich do styku s IS. Ich oboznámenie s legislatívou, týkajúcou sa ochrany osobných údajov, je len jedným z krokov na zabezpečenie IS. Zariadenie nikdy nepokryje ani najjednoduchšie riešiteľné riziká, ak k IS budú mať prístup osoby, ktoré nemajú prehľad o možných negatívnych vplyvoch na bezpečnosť údajov v IS, ako aj na IS samotný.

Nevyhnutnou súčasťou bezpečnostných opatrení je prispôsobenie organizačnej štruktúry potrebám ochrany údajov v IS. Vykonávaním funkcie :informatik“ poverí zariadenie osobu alebo inú externú spoločnosť odborne spôsobilú vykonávať túto funkciu. Pridelenie osobnej zodpovednosti za konkrétne činnosti s IS a stanovenie štruktúry kontrolných mechanizmov je kľúčom k úspešnosti väčšiny ostatných opatrení.

Okolie IS obsahuje množstvo faktorov, ktoré môžu mať negatívny vplyv na jeho chod. Porušenie dostupnosti alebo dôveryhodnosti údajov v IS v sebe prináša vysoké nároky na riešenie vzniknutej bezpečnostnej udalosti a tým aj zaťažuje financie zariadenia. Prevencia je teda nevyhnutným nástrojom na zníženie nákladovosti prevádzky IS.

Opatrenia musia okrem prevencie riešiť aj protiopatrenia v prípade stavu ohrozenia IS, ako aj havarijných udalostí. Podrobné plány postupu pri závažných udalostiach umožňujú skrátenie trvania nedostupiteľnosti IS a podstatne znižujú mieru ohrozenia samotných informácií.

Napriek úsiliu prevádzkovateľa IS je zrejmé, že časť rizík zostane nepokrytá. Vhodne zvolená stratégia bezpečnosti IS môže vplyv týchto rizík na IS minimalizovať.

Riadenie bezpečnosti

Na dosiahnutie ochrany IS pred jeho ohrozením zabezpečujeme technické, organizačné a personálne opatrenia. Tieto opatrenia je prevádzkovateľ povinný zabezpečiť v takej miere, aby sa zabránilo neoprávnenému prístupu k informáciám, narušeniu ich dôveryhodnosti a dostupnosti.

Prevádzkovateľ - zariadenie zabezpečí najmä:

- oboznámenie všetkých pracovníkov o právach a povinnostiach vyplývajúcich z prijatia bezpečnostných smerníc,
- vyhlásenie o mlčanlivosti všetkými osobami oprávnenými spracovávať osobné údaje,
- fyzický prístup k prostriedkom IS iba oprávneným osobám,
- elimináciu škodlivých vstupov z okolia IS do IS,
- odovzdávanie produktov IS, ktoré obsahujú osobitné osobné údaje externým organizáciám na ďalšie spracovanie tak, aby nemohlo dôjsť k úniku informácií,
- likvidovanie produktov IS spôsobom zamedzujúcim úniku informácií.

Za účelom zabezpečenia ochrany osobných údajov v IS boli prijaté **bezpečnostné opatrenia** vo forme poučenia dotknutých osôb, bezpečnostných smerníc a iných dokumentov.

III. ANALÝZA BEZPEČNOTI INFORMAČNÉHO SYSTÉMU

Popis informačného systému

Zariadenie na spracovanie údajov využíva AIS. AIS obsahuje osobné údaje zamestnancov prevádzkovateľa a osobné údaje poberateľov sociálnej starostlivosti. Prevádzkovateľ vedie o zamestnancoch a o poberateľoch sociálnej starostlivosti písomnú aj elektronickú evidenciu. Písomná evidencia je uchovávaná v uzamknutých skriniach. Ochrana vstupu do elektronickej evidencie je riešená priradením práv užívateľom. Oprávnené osoby sa prihlasujú do AIS pomocou užívateľského mena a hesla.

Hodnota informácií

V AIS prevádzkovateľa sú spracovávané osobné údaje, ktoré nepatria do kategórie „utajované skutočnosti“ podľa Zákona o ochrane utajovaných skutočností. AIS obsahuje rodné číslo, údaje

o zdravotnej spôsobilosti, údaje o rodinných príslušníkov. Presný zoznam spracovávaných údajov je uvedený v „Záznamoch o spracovateľských operáciách“.

Vymedzenie okolia informačného systému

Okolie AIS pre účely bezpečnostného projektu tvoria osoby prichádzajúce do styku s technickým zariadením prevádzkovateľa súvisiacim s AIS alebo s priestormi, kde sú uložené súčasti AIS. Z technického hľadiska je okolím AIS verejne prístupná počítačová sieť alebo počítačová sieť mimo výhradného vlastníctva prevádzkovateľa.

Všeobecná analýza rizík

1	**Bezpečnostná politika**	
	Riziko 1:	Neaktuálnosť bezpečnostnej politiky
	Popis rizika:	Neaktualizovanie bezpečnostnej politiky má za následok zanedbanie prevencie a zanedbanie aktualizácie postupov protiopatrení pri vzniku bezpečnostnej udalosti.
2	**Organizácia bezpečnosti**	
	Riziko 1:	Organizačná štruktúra
	Popis rizika:	Neprispôsobenie organizačnej štruktúry potrebe ochrany osobných údajov znemožňuje efektívne využívanie bezpečnostného potenciálu prevádzkovateľa IS a narušuje časovú a priestorovú následnosť priebehu kontrol a tým ich kvalitu.
	Riziko 2:	Riadenie prístupu k informačnému systému
	Popis rizika:	Nejednoznačne definovaný postup pri prideľovaní hesiel a nadstavovaní zdieľania prostriedkov IS môže mať za následok prístup k prostriedkom IS neoprávneným osobám.
	Riziko 3:	Prideľovanie užívateľských práv
	Popis rizika:	Užívatelia môžu náhodnou manipuláciou v moduloch, ktoré nevyužívajú pri svojej práci svojou neznalosťou spôsobiť stratu alebo poškodenie spracovávaných údajov.
	Riziko 4:	Stanovenie postupov protiopatrení
	Popis rizika:	Pri vzniku bezpečnostnej udalosti nepresné stanovenie postupov protiopatrení zvyšuje pravdepodobnosť straty dôveryhodnosti a dostupnosti spracovávaných informácií.
3	**Klasifikácia a riadenie aktív**	
	Riziko 1:	Klasifikácia aktív
	Popis rizika:	Nevhodná klasifikácia aktív so sebou zvyčajne prináša nevhodné priestorové rozmiestnenie a tým ich nedostatočnú ochranu.
	Riziko 2:	Vlastníctvo aktív
	Popis rizika:	Nevyjasnené vlastníctvo aktív má za následok nemožnosť stanovenia zodpovednosti konkrétnych osôb za vznik bezpečnostnej udalosti a oneskorenie výkonu protiopatrení pri ich vzniku.
4	**Fyzická bezpečnosť**	
	Riziko 1:	Bezpečnosť miestností s aktívami IS
	Popis rizika:	Nevhodné zabezpečenie miestností, kde sa aktíva nachádzajú, má za následok zvýšenie rizika odcudzenia, poškodenia IS a informácií v ňom spracovávaných alebo neoprávneného prístupu tretích osôb.
	Riziko 2:	Poškodenie technických prostriedkov
	Popis rizika:	Nezabezpečenie technických prostriedkov pred poškodením slnečným žiarením, striekajúcou vodou pri poruche vykurovacích telies, prachom, atď.

		má za následok možnosť straty dostupnosti informácií.
	Riziko 3:	Poškodenie záloh informačného systému
	Popis rizika:	Nevhodné uloženie záloh IS má za následok zvýšenie rizika ich poškodenia faktormi prostredia (slnko, prach ...), a tým aj nákladnosti a časovej náročnosti výkonu protiopatrení.
5	**Personálna bezpečnosť**	
	Riziko 1:	Vzdelávací proces
	Popis rizika:	Zanedbanie vzdelávania všetkých osôb pracujúcich s IS zvyšuje pravdepodobnosť vzniku bezpečnostnej udalosti z dôvodu neznalosti pracovných a bezpečnostných postupov
	Riziko 2:	Disciplinárne postihy
	Popis rizika:	Nevyvodzovanie osobnej zodpovednosti za vznik bezpečnostných udalostí má za následok vyššiu pravdepodobnosť opätovného zlyhania ľudského faktoru.
6	**Údržba aktív a informačného systému**	
	Riziko 1:	Údržba a profylaxia technických prostriedkov
	Popis rizika:	Zanedbanie údržby a profylaxie má za následok zníženie spoľahlivosti technického vybavenia IS, dôsledkom čoho je vyšia pravdepodobnosť porúch dostupnosti informácií a zníženia ich dôveryhodnosti.
	Riziko 2:	Zálohovanie
	Popis rizika:	Plánovanie zálohovania IS je dôležitou súčasťou protiopatrení. Zanedbanie zálohovania výrazne zvyšuje dobu nedostupnosti IS a znižuje dôveryhodnosť informácií po bezpečnostnej udalosti.
7	**Nepokryté riziká** Napriek dodržiavaniu vypracovaných bezpečnostných smerníc existuje nasledovná množina zvyškových rizík:	
	Riziko 1:	Živelné katastrofy
	Popis rizika:	Možnosť straty alebo poškodenia údajov v IS alebo zničenie celého IS
	Riziko 2:	Prekonanie bezpečnostných opatrení úmyselnou činnosťou tretích osôb
	Popis rizika:	Prekonanie fyzických a programových bezpečnostných opatrení zámernou činnosťou tretích osôb a následné poškodenie IS alebo strata dôvernosti osobných údajov.
	Riziko 3:	Bombový alebo teroristický útok
	Popis rizika:	Prekonanie fyzických a programových bezpečnostných opatrení zámernou činnosťou tretích osôb a následné poškodenie IS alebo jeho plné zničenie.

Kvalitatívna analýza rizík

Jedným z najdôležitejších cieľov tejto dokumentácie je trvalo udržiavať vysokú úroveň ochrany spracovávaných osobných údajov pred odcudzením, stretou, poškodením, neoprávneným prístupom, zmenou alebo šírením. Pokiaľ by totiž došlo k niektorému z uvedených dopadov, znamenalo by to porušenie povinnosti zakotvených v ustanoveniach zákona č. 18/2018 Z.z. o ochrane osobných údajov a spoločnosti by hrozili sankcie. Ochrana osobných údajov má v zariadení vysokú prioritu.

V nasledujúcej tabuľke je znázornený zoznam hrozieb pôsobiacich na jednotlivé aktíva informačného systému spôsobilých narušiť jeho bezpečnosť alebo funkčnosť, a ktoré môžu ohroziť dôvernosť, integritu a dostupnosť spracúvaných osobných údajov. Zoznam hrozieb vyplýva zo zistených zraniteľností prostredia a infraštruktúry, hardwaru, softwaru, komunikácie, dokumentácie a personálu. Miera jednotlivých rizík je ohodnotená stupnicou: nízka – stredná – vysoká.

Por. č.	Zraniteľnosť	Hrozby vyplývajúce zo zraniteľnosti	Miera rizika
1.	Nedostatočná fyzická ochrana budovy, dverí a okien	Zemetrasenie	nízka
		Blesk	stredná
		Požiar	stredná
		Povodeň	nízka
		Odcudzenie	nízka
		Bombový útok	nízka
		Úmyselná škoda	nízka
2.	Riadenie fyzického prístupu k budove a miestnostiam	Odcudzenie	nízka
		Bombový útok	nízka
		Úmyselná škoda	nízka
3.	Dodávka elektrickej energie	Kolísanie elektrického prúdu	stredná
		Zastavenie dodávky elektrického prúdu	stredná
4.	Nedostatočná fyzická ochrana IS v písomnej podobe	Odcudzenie	nízka
		Poškodenie	nízka
		Neoprávnený prístup	nízka
5.	Riadenie prístupu k IS v elektronickej podobe	Neoprávnený prístup	stredná
		Poškodenie	nízka
		Strata dát	stredná
		Odcudzenie dát	nízka
		Zmena dát	nízka
		Šírenie dát	stredná
6.	Riadenie obehu výmenných médií	Odcudzenie	nízka
		Škodlivý programový kód	nízka
7.	Nedostatočná kontrola pamäťových médií	Strata dát	nízka
		Poškodenie	nízka
		Chyba údržby	stredná
8.	Nedostatočný manažment hesiel	Predstieranie identity používateľa	nízka
		Chyby používateľov	stredná
9.	Nechránená pamäť	Odcudzenie	nízka
10.	Nekontrolované kopírovanie	Odcudzenie	stredná
11.	Absencia personálu	Nedostatok zamestnancov	nízka
12.	Nedostatočné bezpečnostné školenia	Chyba pri spracovávaní osobných údajov	stredná
13.	Absencia kontroly bezpečnostnej zhody	Porušovanie právnych predpisov	stredná
		Porušovanie interných predpisov	stredná
14.	Nedostatočná správa a riadenie incidentov	Strata dát	stredná
		Poškodenie dát	stredná

Zostatkové riziká

a) Riziko neoprávneného vniknutia do kancelárií počas pracovnej doby.
Okolnosť, že kancelárie sa počas neprítomnosti na pracovisku uzamykajú, existujúce opatrenia a prijatie navrhnutých ochranných opatrení znižuje toto riziko na minimum.

Riziko je akceptovateľné.

b) Riziko zneužitia osobných údajov zo strany zamestnancov
Vzhľadom k prijatým ochranným opatreniam, poučeniu oprávnených osôb v zmysle ustanovení Zákona č. 18/2018 Z.z. O ochrane osobných údajov a neustálemu zvyšovaniu povedomia zamestnancov o bezpečnosti je toto riziko veľmi nízke.

Riziko je akceptovateľné.

c) Riziko šírenia osobných údajov vyhotovovaním neoprávnených kópií
Riziko je vzhľadom k okolnostiam popísaným v dokumentácii akceptovateľné.

d) Riziko škodlivého počítačového kódu
Na PC, na ktorých sa spracovávajú osobné údaje, je inštalovaný antivírový skenovací softvér. PC sú pripojené na internet. Prijaté ochranné opatrenia znižujú riziko nainfikovania PC s osobnými údajmi škodlivým počítačovým kódom na minimum.

Riziko je akceptovateľné.

CSS Nádej Dolný Lieskov, 018 21 Dolný Lieskov č. 197

BEZPEČNOSTNÉ SMERNICE

I. Základné ustanovenia

Účel smerníc:

Bezpečnostné smernice predpisujú súbor opatrení slúžiacich na zvýšenie bezpečnostnej úrovne IS. Vychádzajúc z analýzy bezpečnosti IS a riadia sa vypracovaným bezpečnostným zámerom.

Záväznosť smernice:

Bezpečnostné smernice sú povinní dodržiavať všetci zamestnanci zariadenia (prevádzkovateľ) CSS Nádej Dolný Lieskov, 018 21 Dolný Lieskov č. 197, vrátane pracovníkov iných organizácií vykonávajúcich činnosti súvisiace s IS, k čomu ich zaviaže písomný právny akt.

II. Bezpečnostné opatrenia

Organizačno – právne opatrenia

Zodpovedná osoba

Zabezpečuje:

- potrebnú súčinnosť s Úradom na ochranu osobných údajov SR /ďalej len Úrad) pri plnení úloh patriacich do jeho pôsobnosti, na požiadanie Úradu predložiť svoje písomné poverenie, písomné oznámenia vystavené pre prevádzkovateľa, preukázať rozsah získaných vedomostí odborným školením,
- dohľad nad plnením základných povinností prevádzkovateľa,
- poučenie oprávnených osôb,
- príprava sprostredkovateľskej zmluvy alebo poverenia pre sprostredkovateľa,

vypracováva:

- postupy pri bezpečnostných udalostiach,
- analýzu bezpečnostných udalostí,
- postupy riadenia prístupu do IS,

zodpovedá za:

- aktualizáciu bezpečnostnej politiky,
- aktualizáciu súvisiacej dokumentácie,
- riadenie školení pracovníkov,

kontroluje:

- plnenie plánu údržby a profylaxie systému,
- plnenie plánu zálohovania,
- dodržiavanie bezpečnostných smerníc,
- dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov,

Informatik

Zodpovedá za:

- vykonávanie údržby a profylaxie technických prostriedkov,

vykonáva:

- inštaláciu a reinštaláciu operačného systému,
- inštaláciu schváleného programového vybavenia,
- úplné zálohovanie pracovných staníc,
- aktualizácie programového vybavenia pracovných staníc.

Vlastník aktíva informačného systému

Zodpovedá za:
- priebežné zálohovanie pracovnej stanice,
- označovanie a archiváciu záloh,
- správne umiestnenie aktív.

Oprávnená osoba

Je povinná:
- získavať osobné údaje výlučne na stanovený účel. Je neprípustné získavať osobné údaje pod zámienkou iného účelu alebo inej činnosti.
- Spracovávať len správne, úplné a podľa potreby aktualizované osobné údaje vo vzťahu účelu spracovania. Nesprávne a neúplné osobné údaje je prevádzkovateľ povinný blokovať a bez zbytočného odkladu opraviť alebo doplniť. Osobné údaje, ktoré nemožno opraviť alebo doplniť tak, aby boli správne a úplné, prevádzkovateľ zreteľne označí a zlikviduje ihneď, ako to okolnosti dovolia.

Oprávnená osoba je povinná preukázať svoju totožnosť na požiadanie tomu, od koho osobné údaje dotknutej osoby požaduje a bez vyzvania mu vopred oznámiť:
- názov a sídlo alebo trvalý pobyt prevádzkovateľa. Ak v jeho mene koná sprostredkovateľ, aj jeho názov a sídlo alebo trvalý pobyt.
- Účel spracovania osobných údajov vymedzený prevádzkovateľom alebo ustanovený osobitným zákonom.
- Dobrovoľnosť alebo povinnosť poskytovať požadované osobné údaje,
- okruh užívateľov, ktorým budú osobné údaje poskytnuté, ak dotknutej osobe povinnosť poskytnúť osobné údaje vyplýva z osobitného zákona, prevádzkovateľ oznámi dotknutej osobe zákon, ktorý jej túto povinnosť ukladá a upovedomí ju o následkoch odmietnutia poskytnúť osobné údaje,
- právnické osoby, fyzické osoby, prípadne subjekty v cudzine, ktorým budú osobné údaje poskytnuté,
- okruh príjemcov, ak sa predpokladá alebo je zrejmé, že im budú osobné údaje sprístupnené,
- formu zverejnenia, ak majú byť osobné údaje zverejnené,
- poučenie o existencii práv dotknutej osoby.

Organizačno – právne opatrenia

Určenie kľúčových prvkov informačného systému

Na základe analýzy IS boli ako kľúčové prvky vyhotovené:
- servery,
- smerovače, prepínače,
- pracovné stanice,
- tlačiarne,
- archívne skrine so zálohami IS a písomnej dokumentácie,
- archívne skrine s inštalačnými médiami.

Umiestnenie kľúčových prvkov IS

Pracovné stanice a servery musia byť umiestnené v samostatnej miestnosti. Okná a dvere musia byť zabezpečené proti neoprávnenému vniknutiu. Všetky kľúčové prvky musia byť v miestnosti zabezpečené tak, aby v prípade požiaru alebo poruchy vykurovacieho telesa nemohli byť poškodené ohňom alebo striekajúcou vodou.
Pri spracovávaní osobných údajov je nevyhnutné zabezpečiť, aby obrazovky monitorov nesprístupňovali osobné údaje dotknutých osôb iným fyzickým osobám. Zabezpečenie je možné vykonať vhodným usporiadaním pracoviska (umiestnenie a natočenie monitora). Ak má nepoučená osoba obrazovku monitora v dohľade, treba zabezpečiť, aby na nej neboli zobrazené osobné údaje inej osoby.
Prístup do miestnosti s kľúčovými prvkami môžu mať len oprávnené osoby. Jeden kľúč musí byť uložený v zapečatenej obálke v skrinke (napr. v prípade požiaru).

Umiestnenie záloh IS

Nosiče záloh (CD média, diskety, ZIP médiá, USB kľúče, externé pevné disky...) nesmú byť archivované v miestnosti s inými kľúčovými prvkami IS, aby v prípade bezpečnostnej udalosti (požiaru, krádeže ...) neprišlo k ich poškodeniu súčasne s údajmi v IS. Najvhodnejšie je umiestniť archívne skrine v inej budove prevádzkovateľa. Miestnosť so zálohami musí byť zabezpečená podobne ako miestnosť s kľúčovými prvkami IS.

Prístup k neautomatizovaným prostriedkom

Neautomatizované prostriedky IS musia byť v čase prítomnosti oprávnenej osoby na pracovisku umiestnené mimo dosahu tretích osôb. V čase ich neprítomnosti na pracovisku musia byť tieto prostriedky uzamknuté v skrini alebo inak zabezpečené pred neoprávneným prístupom.

Likvidácia produktov IS

Všetky papierové záznamy a nosiče elektronických informácií obsahujúce osobné údaje (zoznamy, výpisy, CD média a pod.) musia byť po vylúčení z ďalšieho spracovávania (ak nakladanie s nimi nepredpisuje iný zákon, napr. Zákon č. 395/2002 Z.z. o archívoch a registratúrach v z.n.p.) fyzicky zlikvidované skartovaním, ale spálením. Tieto výstupy nesmú byť odovzdávané do zberného dvora. Prepisovateľné nosiče informácií sa likvidujú vymazaním, alebo naformátovaním, neprepisovateľné nosiče informácií je potrebné fyzicky zlikvidovať (skartovaním, zlomením ...). Ak sú predmetom spracovania úradné doklady obsahujúce osobné údaje, tieto musia byť vrátené dotknutej osobe, ak o to požiada.

Poskytovanie údajov z IS

Nosiče a výpisy požadované inými právnickými osobami na ďalšie spracovanie môžu byť odovzdávané nasledovným spôsobom:

- osobne, odovzdaním priamo pracovníkovi povereným zberom dát,
- poštovou zásielkou typu „doporučený cenný list“ v tomto prípade podľa „Poštového poriadku“ pošta preberá zodpovednosť za doručenie nepoškodenej zásielky adresátovi,
- bežnou poštovou, alebo emailovou zásielkou za predpokladu, že si obe strany dohodnú také zabezpečenie, ktoré znemožní ich zneužitie inou osobou. Tento spôsob nie je možné použiť pri zasielaní tlačových výstupov obsahujúcich osobitné kategórie osobných údajov.

Programovo - technické opatrenia

Prideľovanie a zmena hesiel

Prístup do IS musí byť chránený menom a heslom pre každú oprávnenú osobu. Oprávnené osoby sú povinné udržiavať heslá v tajnosti.

Novej oprávnenej osobe prideľuje prihlasovacie meno a prvé heslo osoba zodpovedná za ich správu na základe písomného pokynu riaditeľky zariadenia. Prihlasovacie údaje odovzdá oprávnenej osobe v zapečatenej obálke spôsobom zamedzujúcim prezradenie hesla (najlepšie osobne). Nový užívateľ si ihneď po prvom prihlásení do IS zmení heslo podľa uvedených zásad.
V prípade podozrenia o prezradení hesla oprávnená osoba ihneď zmení prístupové heslá do IS a vykoná záznam bezpečnostnej udalosti do prevádzkovej knihy IS.
Heslá správcu IS (heslá do biosu, konfiguračných nadstavení inštalovaného programového vybavenia ...) musia byť uložené pre prípad mimoriadnej udalosti v samostatnej uzamknutej skrinke, najlepšie v miestnosti so zálohami. Pri otvorení skrinky alebo poškodení pečate musia byť všetky heslá zmenené.

Zásady tvorby hesiel

Ako heslo sa neodporúča použiť z dôvodu ľahkého odhalenia slová súvisiace s oprávnenou osobou (meno, dátum narodenia seba alebo blízkych osôb), slová uvedené v slovníku, alebo jediné písmeno abecedy. Vhodné je použiť kombináciu veľkých a malých písmen v kombinácii s číslicami o minimálnej dĺžke 5 znakov. Heslo sa musí pravidelne, aspoň raz štvrťročne meniť.

Zálohovanie pracovných staníc

Zálohovanie IS sa vykonáva podľa plánu zálohovania. Plán zálohovania vypracuje informatik. Plán obsahuje časové a priestorové vymedzenie vykonávania pravidelného zálohovania. Zálohovanie podľa rozsahu sa rozdeľuje na úplné a čiastkové. Vlastník pracovnej stanice vykonáva čiastkové zálohovanie vždy pred mesačnou uzávierkou a po nej. Úplné zálohovanie IS vykonáva informatik podľa plánu zálohovania a vždy pred zmenou a po zmene konfigurácie pracovnej stanice.
Každý, kto vyhotoví zálohu IS, je povinný vykonať záznam o zálohovaní do knihy záloh pracovnej stanice. Do záznamu uvedie minimálne dátum zálohovania, účel zálohovania, rozsah zálohovaných údajov, druh zálohovacieho média, počet médií a ich číselné označenie. Podobne zapíše aj prípadné kópie záloh, pričom zaznačí, z ktorých médií boli tieto kópie vyhotovené.

Inštalácia programového vybavenia

Inštaláciu programového vybavenia môže vykonávať len informatik. Na pracovné stanice sa môže inštalovať len autorizované programové vybavenie. Z dôvodu zachovania bezpečnosti je zakázané inštalovať a používať neznáme programové vybavenie, kde hrozí riziko nevedomého zavedenia „spyware“ funkčnosti. Táto funkčnosť odosiela dáta z pripojeného PC bez vedomia užívateľa. V prípade, že užívateľ potrebuje na iné účely použiť neznámy program, je nutné nainštalovať súčasne s ním aj niektorý z programov, ktorý takúto funkčnosť dokáže odhaliť.

Údržba aktív IS

Pasívne a aktívne prvky IS musia byť udržiavané podľa pokynov výrobcu. Výpočtová technika musí byť minimálne 1 x za polrok vyčistená od prachu. Kontrola povrchu pevného disku a defragmentácia musí byť vykonaná minimálne 1 x štvrťročne.

Evidencia bezpečnostných udalostí - incidentov

Vlastník pracovnej stanice v prevádzkovej knihe (môže to byť aj tabuľka v PC) eviduje všetky bezpečnostné udalosti týkajúce sa zvereného technického prostriedku. Záznamy vykonáva po bezpečnostnej udalosti, pričom v poznámke uvedie okolnosti, za ktorých k bezpečnostnej udalosti došlo. Každú bezpečnostnú udalosť je povinný nahlásiť informatikovi, riaditeľke, zodpovednej osobe.

Ochrana IS pred infiltráciami z internetu

Každý PC, ktorý je pripojený na internet musí byť chránený jedným z nasledovných spôsobov:

- operačným systémom Windows XP (Windows 10) aj s inštalovanou a aktivovanou súčasťou „Personal (osobný) firewall“,

- využívaním služieb poskytovateľa pripojenia k internetu, ktorý používa zabezpečenie technológiou firewall, nainštalovaním niektorého z komerčných firewallov na PC s konektivitou na internet.

PC pripojené k sieti Internet musia mať nainštalovaný a pravidelne aktualizovaný antivírusový program. Kontrola infiltrácií počítačového vírusu musí byť vykonávaná minimálne týždenne. Rezidentný štít musí byť trvale zapnutý, na PC so slabou konfiguráciou minimálne počas pripojenia na internet.

Kontroly

Periodické kontroly dodržiavania bezpečnostných smerníc vykonáva zodpovedná osoba 1 x štvrťročne. Pri kontrole sa zameriava najmä na plnenie opatrení dôležitých pre zabezpečenie písomných a elektronických aktív pred poškodením alebo zneužitím.
O vykonanej periodickej kontrole vypracuje záznam, ktorý obsahuje minimálne tieto údaje:

- dátum a čas vykonania kontroly,
- rozsah kontroly,
- zoznam odhalených nedostatkov pri spracovávaní osobných údajov,
- návrh opatrení na riešenie zistených nedostatkov,
- odporúčania zmien pracovných postupov,
- termín opakovanej kontroly zameranej na zistené nedostatky.

Záznam z vykonanej kontroly bezodkladne predloží prevádzkovateľovi IS.
Mimoriadne kontroly zodpovedné osoba vykonáva vždy po bezpečnostnej udalosti alebo vtedy, ak má podozrenie z porušovania zákona o ochrane osobných údajov alebo bezpečnostných smerníc. Po kontrole vypracuje záznam, ktorý obsahuje náležitosti ako záznam z periodickej kontroly. V zázname je nutné uviesť dôvod vykonania mimoriadnej kontroly.

Postup pri bezpečnostných udalostiach – incidentoch

Ak oprávnená osoba alebo osoba, ktorá môže prísť do styku s osobnými údajmi zistí, alebo má podozrenie, že došlo, alebo hrozí porušenie bezpečnostných smerníc (zavírený PC, neuzamknutá kartotéka ...), je povinná bezodkladne upozorniť prevádzkovateľa a zodpovednú osobu. Prevádzkovateľ bezodkladne rozhodne o ďalšom postupe.

Špecifikácia bezpečnostných udalostí a návrh protiopatrení

Bezpečnostná udalosť:	Neautorizované prihlásenie do IS
Popis bezpečnostnej udalosti:	Po prekonaní fyzických prekážok, môže dôjsť k neautorizovanému vstupu do IS.
Minimálne opatrenie:	Zmena zneužitého prihlasovacieho mena a hesla na vstup do IS. Kontrola logovacích súborov databáz a vizuálna kontrola správnosti údajov.
Odporúčané opatrenie:	Zmena všetkých prihlasovacích mien a hesiel na vstup do IS vrátane hesiel správcu IS. Obnovenie databáz IS zo záloh.

Bezpečnostná udalosť:	Neautorizovaný prienik z internetu
Popis bezpečnostnej udalosti:	Možnosť zneužitia alebo odcudzenia databáz počas pripojenia PC k internetu.
Minimálne opatrenie:	Kontrola logovacích súborov databáz a vizuálna kontrola správnosti údajov. Zmena nadstavenia firewallu.
Odporúčané opatrenie:	Obnovenie databáz IS zo záloh. Analýza pravdepodobných infiltrácií do systému a následné prispôsobenie bezpečnostných opatrení a protiopatrení.

Bezpečnostná udalosť:	Krádež počítača
Popis bezpečnostnej udalosti:	Po prekonaní fyzických prekážok môže nepovolaná osoba odcudziť pracovné stanice. Krádežou dôjde k strate a je pravdepodobné, že aj následnému zneužitiu údajov.
Minimálne opatrenie:	Nahlásenie udalosti polícii a následná kontrola fyzického zabezpečenia miestností, v ktorých sa informačný systém nachádza, výmena poškodených prvkov zabezpečenia. Kontrola nadstavení šifrovania dát pracovných staníc. Inštalácia IS na záložný PC a obnova dát IS a záloh.
Odporúčané opatrenie:	Nahlásenie udalosti polícii a následná kontrola fyzického zabezpečenia miestností, v ktorých sa informačný systém nachádza. Výmena poškodených prvkov zabezpečenia za prvky s vyššou odolnosťou. Prehodnotenie ochrany IS a zmena ich klasifikácie. Inštalácia pohybových a otrasových senzorov v miestnostiach s kľúčovými prvkami IS. Kontrola nadstavení šifrovania dát IS zo záloh.

Bezpečnostná udalosť:	Krádež alebo strata záznamových médií
Popis bezpečnostnej udalosti:	Po prekonaní fyzických prekážok môže nepovolaná osoba poškodiť zálohové médiá. Krádežou dôjde k strate a je pravdepodobné, že aj následnému zneužitiu údajov.
Opatrenie:	Obdobne ako v predchádzajúcom popise.

Bezpečnostná udalosť:	Strata údajov spôsobená chybou IS
Popis bezpečnostnej udalosti:	Strata alebo poškodenie informácií v IS poruchou programového vybavenia.
Opatrenie:	Reinštalácia PC a obnovenie databáz zo zálohy. Zozbieranie informácií potrebných na simuláciu postupu, pri ktorom došlo k chybe IS a informovanie jeho poskytovateľa.

Bezpečnostná udalosť:	Zavírenie systému
Popis bezpečnostnej udalosti:	Strata dostupnosti alebo dôveryhodnosti údajov činnosťou vírusov v IS.
Minimálne opatrenie:	Odvírenie PC, kontrola nadstavenia antivírového programu a jeho aktuálnosti. Vizuálna kontrola stanu databáz.
Odporúčané opatrenie:	Odvírenie PC, reinštalácia IS a obnova databáz zo záloh. Prípadná zmena antivírového programu.

Ostatné bezpečnostné udalosti programového vybavenia

Chyba operačného systému PC	• chybné súbory – narušenie dostupnosti IS • nedokonalosť systému, diery v systéme – narušenie dostupnosti a dôvernosti IS
Chyba konfiguračných súborov OS	• narušenie dostupnosti IS
Chyba konfiguračných súborov aplikácií	• poškodenie konfiguračného súboru – strata, narušenie dostupnosti
Opatrenia:	
Operačný systém PC	• kontrola integrity a zálohovania systémových súborov, vedenie kontrolných záznamov 1 x mesačne • zabezpečenie pravidelnej aktualizácie OS
Konfiguračné súbory OS	• zákaz používania neautorizovaného programového vybavenia, vytvorenie zálohy, kontrola integrity
Konfiguračné súbory aplikácie	• zákaz používania neautorizovaného programového vybavenia, zabezpečenie náhrady

Ostatné bezpečnostné udalosti technického vybavenia

Operačná pamäť	• pamäť nepracuje štandardne – strata, narušenie dostupnosti • pri zaznamenávaní údajov došlo i chybe – strata, narušenie dostupnosti a integrity
Pevný disk	• zničenie časti magnetickej vrstvy – strata, narušenie dostupnosti • poškodenie krokového motora – strata, narušenie integrity • poškodenie snímacej hlavy – strata, narušenie dostupnosti • poškodenie riadiacej jednotky – strata, narušenie dostupnosti • logické poškodenie – strata, narušenie integrity
Pružné disky	• zanesenie vírusu – strata, narušenie dôvernosti a dostupnosti • pri čítaní dochádza k chybe – narušenie integrity • použitie cudzích diskiet – strata, narušenie dostupnosti • poškodenie, narušenie dostupnosti
CD ROM	• použitie neautorizovaného programového vybavenia – strata, narušenie dostupnosti • zanesenie vírusu použitím CD diskov – strata, narušenie dostupnosti • poškodenie, zničenie mechaniky – strata, narušenie integrity a dostupnosti • zničenie – narušenie dostupnosti
Matičná doska	• zhorenie, elektronické poškodenie – strata, narušenie dostupnosti a dôvernosti
	• funkčná chyba procesora – strata, narušenie dostupnosti
Grafická karta	• zhorenie, poškodenie – strata, narušenie dostupnosti
Vnútorný zdroj	• poškodenie, zničenie – strata, narušenie dostupnosti
Monitor	• prečítanie údajov cudzou osobou – narušenie dôvernosti • prečítanie údajov na diaľku zo susedných objektov – narušenie dôvernosti • elektromagnetické vyžarovanie – narušenie dôvernosti • mechanické, elektrické poškodenie – strata, narušenie dôvernosti
Opatrenia	
Operačná pamäť	• zabezpečenie testovania činnosti pamäte, v prípade jej nespôsobilosti zabezpečiť náhradu, vytváranie zálohy údajov • vykonať kontrolu správnosti zaznamenaných údajov
Pevný disk	• zabezpečenie náhrady pevného disku, obnova dát zo zálohy
Pružné disky	• pred spustením súboru vykonať kontrolu antivírovým programom • kontrola aktuálnej diskety, kontrola súborov po stiahnutí na pevný disk • používať iba pridelené, preverené diskety, vykonávať kontrolu • vyradiť chybné diskety, zabezpečiť náhradu, skartácia diskiet
CD ROM	• zákaz používania neautorizovaného programového vybavenia • používanie antivírusového programu • zabezpečenie náhradného CD ROM • vykonať kontrolu funkčnosti, vyčistiť mechaniku
Matičná doska	• zabezpečenie náhrady
Grafická karta	• zabezpečenie náhrady
Vnútorný zdroj	• zabezpečenie náhrady
monitor	• zabezpečiť vypnutie monitora pri návšteve cudzích osôb • zabezpečiť umiestnenie monitora v miestnosti nie oproti oknu • zabezpečiť ochranu PC, alebo pracoviska • zabezpečiť náhradu

CSS Nádej Dolný Lieskov, 018 21 Dolný Lieskov č. 197

Príloha č. 1

Smernica o Zásadách práce s počítačom v IS pre používateľov

Čl. I.

Základné pojmy

(1) IS – Informačný systém predstavuje technické HW (hardwarové) a SW (softwarové) vybavenie.
(2) Používateľ – pre účel tejto smernice sa jedná o používateľov počítačovej techniky na užívateľskej úrovni.
(3) Užívateľská úroveň – používateľ na tejto úrovni pracuje v systéme len do takej miery, aká mu je preddefinovaná administrátorom a správcom IS. Nemá možnosť samovoľne meniť nastavenia systému.

Čl. II

Technické zabezpečenie práce s IS

(1) Na základe existencie elektronického systému IS, musí mať každý používateľ fyzický prístup k počítačovej technike.
(2) Každý používateľ musí mať možnosť prístupu k tlačiarni a inej technike, ktorá je nutná na prácu v IS.
(3) HW a SW vybavenie má na starosti technik IT..

Čl. III

Práca s počítačom a vstup do programu IS

(1) Používateľ sa prihlási do jemu určenému programu z balíka IS kam má prístupové práva na základe svojho hesla.
(2) Po dokončení práce sa zo systému odhlási.

Čl. IV

Plnenie systému dátami a výstupy

(1) Do celého IS je potrebné zadávať dáta s použitím diakritiky a zachovaním veľkých a malých písmen.
(2) Do polí, kde je možnosť výberu (výberové menu) je potrebné vybrať z preddefinovaných možností. Do polí, kde nie je možnosť výberu, je potrebné vpísať konkrétny text.
(3) Tlač výstupov je daná automaticky alebo ručne podľa prístupových práv používateľa IS. Formát výstupov je podľa zadania A4, alebo A5.

Čl. V.

Bezpečnosť práce

(1) Zákaz prezradiť heslo druhej osobe.
(2) Zákaz prihlásiť sa svojím heslom a dovoliť pod svojím prístupom pracovať v systéme inej osobe.
(3) Bezpečnosť prihlásenia je vyriešená time-outom.
(4) Ak používateľ IS má akýkoľvek problém s technickým prevedením napĺňania údajov, kontaktuje vedúceho THÚ telefonicky, e-mailom, alebo osobne.

CSS Nádej Dolný Lieskov, 018 21 Dolný Lieskov č. 197

Príloha č. 2

Smernica o zásadách práce počítačom v IS pre administrátora.

Čl. I.

Základné pojmy

Administrátor – súčasne správca systému - pracovník s počítačovou technikou na najvyššej možnej úrovni. Má prístup k všetkým existujúcim dátam, nastaveniam, aké sú v IS možné. Má právo a povinnosť riešiť nastavenia, prístupové práva, heslá a zálohovanie dát, ako aj komplexnú správu celého systému. V zariadení CSS Nádej Dolný Lieskov, má pozíciu administrátora technik IT.

(1) IS – Informačný systém predstavuje technické HW (hardwarové) a SW (softwarové) vybavenie.

Čl. II.

Práca s počítačom v IS

(1) Administrátor sa do systému hlási heslom. Prístupové práva ma maximálne.
(2) Heslá do jednotlivých modulov systému sú rozdielne.
(3) Administrátor, ktorý je zároveň správcom systému upgraduje systém, sleduje zmeny legislatívy a následne ich uplatňuje, spravuje všetky moduly komplexného systému. Nastavuje a prideľuje prístupové práva, heslá, mení ich podľa potreby. Rieši certifikácie programov. Verifikuje dáta. Stará sa o profylaxiu, zálohovanie dát. Zabezpečuje chod systému po stránke HW (kontrola techniky, výber vhodnej techniky k danému software), ako aj po stránke SW (platnosť, dodržiavanie licencie, zapracovanie noviniek, apod.)

Čl. III.

Bezpečnosť práce

(1) Administrátor má právo a povinnosť v prípade akejkoľvek poruchy, alebo z iného opodstatneného dôvodu odstaviť celý IS, na dobu potrebnú na vyriešenie danej problematiky.

Čl. IV.

Pridelenie právomoci administrátora pre programy

(1) Administrátor v zariadení má prístup na všetky programy podliehajúce jeho správe.
(2) Administrátor má právo (ak je to personálne možné) určiť svojho zástupcu, alebo zástupcov s rovnakými právomocami.
(3) Prevádzkovateľ spravuje programy týkajúce sa dát s osobnými údajmi.

CSS Nádej Dolný Lieskov, 018 21 Dolný Lieskov č. 197

Príloha č. 3

Smernica na postup pre tvorbu záloh a obnovu údajov

Čl. I.

Základné pojmy

(1) Záloha údajov – vytvorenie kópie aktuálnych dát na definované pamäťové médium s kompresiou alebo bez.
(2) Pamäťové médium – externý pevný disk, DVD média, páskové média, USB disk
(3) Obnova údajov - vrátenie vytvorenej kópie dát na pôvodné miesto na požiadanie alebo pri havarijných stavoch.
(4) Administrátor – súčasne správca systému - pracovník s počítačovou technikou na najvyššej možnej úrovni. Má prístup k všetkým existujúcim dátam, nastaveniam, aké sú v IS možné. Má právo a povinnosť riešiť nastavenia, prístupové práva, heslá a zálohovanie dát, ako aj komplexnú správu celého systému. V zariadení má pozíciu administrátora technik IT.

Čl. II

Postup práce

(1) Postup pri zálohovaní údajov :
    - Stanoviť politiku zálohovania
    - Zabezpečiť personálnu oblasť – zodpovedného pracovníka za zálohovanie
    - Vybrať vhodné pamäťové médium s dostatočnou pamäťovou kapacitou
    - Naplánovanie automatickej činnosti zálohovania
    - Naplánovanie pravidelnej kontroly automatického zálohovania
    - Vykonanie nastavenia automatického zálohovania dát
    - Určiť zdroje dát k zálohovaniu
    - Určiť periodicitu zálohovania
(2) Postup pri obnove dát :
    - Definovanie cieľových údajov k obnoveniu
    - Presun údajov na pôvodné miesto – pri odstávke systému
    - Kontrola obnovených údajov používateľom

Čl. III

Bezpečnosť

(1) Zálohované údaje na cieľových pamäťových nosičoch sú umiestnené na inom mieste ako zdrojové údaje, ktorých záloha sa vykonáva.
(2) Prístup k zálohovým pamäťovým nosičom má len administrátor systému (prípadne jeho zástupca/ci).

Čl. IV.

Personálne zabezpečenie

(1) Zálohovanie systému je plne v réžii administrátora, ak je obnova v rámci jeho dostupných technických a programových možností.

CSS Bystričan, Zákvašov 1935/453, 017 07 Považská Bystrica

Príloha č. 4

Smernica na postup pri likvidácii nepotrebných dokumentov v elektronickej podobe a nosičov údajov.

Čl. I

Základné pojmy

(1) Nosič údajov – akékoľvek pamäťové médium.
(2) Nepotrebný dokument v elektronickej podobe – akýkoľvek dokument v systéme, ktorý nie je potrebné ďalej v systéme uchovávať.

Administrátor – súčasne správca systému - pracovník s počítačovou technikou na najvyššej možnej úrovni. Má prístup k všetkým existujúcim dátam, nastaveniam, aké sú v IS možné. Má právo a povinnosť riešiť nastavenia, prístupové práva, heslá a zálohovanie dát, ako aj komplexnú správu celého systému. V zariadení má pozíciu administrátora technik IT.

Čl. II

Postupy likvidácie

(1)Postup likvidácie nosičov údajov :

- Pred fyzickou likvidáciou nosičov údajov zabezpečiť totálne vymazanie nosiča, bez možnosti obnovy údajov.
- Fyzická likvidácia v zmysle ochrany životného prostredia (certifikovaná firma na tento účel)

(3) Postup likvidácie nepotrebných elektronických dokumentov :

- Vymazanie dokumentu bez možnosti obnovy.

Čl. III

Personálne zabezpečenie

(1) Pracovníka na likvidáciu určuje administrátor systému, prípadne to rieši sám.
(2) Ak majú používatelia v rámci svojej právomoci správu dokumentov, je likvidácia na ich zodpovednosti. Prípadne môžu požiadať o likvidáciu dokumentov administrátora.

CSS Nádej Dolný Lieskov, 018 21 Dolný Lieskov č. 197

Príloha č. 5

Smernica o pláne obnovy IS po havárii.

Čl. I

Základné pojmy

(1) Havária systému – neplánovaná celoplošná nefunkčnosť všetkých modulov informačného systému.
(2) Administrátor – súčasne správca systému - pracovník s počítačovou technikou na najvyššej možnej úrovni. Má prístup k všetkým existujúcim dátam, nastaveniam, aké sú v IS možné. Má právo a povinnosť riešiť nastavenia, prístupové práva, heslá a zálohovanie dát, ako aj komplexnú správu celého systému. V zariadení. má pozíciu administrátora technik IT.
(3) IS – Informačný systém predstavuje technické HW (hardwarové) a SW (softwarové) vybavenie.
(4) Používateľ – pre účel tejto smernice sa jedná o používateľov počítačovej techniky na užívateľskej úrovni.

Čl. II

Plán obnovy

(1)Postup obnovy IS po havárii :

- Po znovu nabehnutí systému zabezpečiť aby sa používatelia nemohli prihlásiť do systému
- Analýza dátových škôd spôsobených haváriou systému
- Výber najaktuálnejších údajov zachovaných pred haváriou pomocou zálohy
- Koordinácia obnovy údajov s dodávateľom IS
- Vrátenie údajov do IS
- Kontrola vrátených údajov a funkčnosti IS
- Sprístupnenie prihlásenia sa používateľom do IS

Čl. III

Personálne zabezpečenie

(1) Obnova systému je plne v réžii administrátora, ak je obnova v rámci jeho dostupných technických a programových možností.
(2) Obnova systému je v koordinácii administrátora s dodávateľom systému.

Obnova systému je plne v réžii dodávateľa systému (ak sa jedná o technické prevedenie, ktoré nepodlieha právomoci administrátora, alebo je havária spôsobená priamo dodávateľom).

CSS Bystričan, Zákvašov 1935/453, 017 07 Považská Bystrica

Príloha č. 6

Zoznam sprostredkovateľov

Oprávnená osoba, ktorá pracuje s osobnými údajmi v programoch, ktoré prevádzkuje sprostredkovateľ, je povinná viesť zoznam sprostredkovateľov, pre IS vedie zoznam sprostredkovateľov informatik prevádzkovateľa.

ZOZNAM SPROSTREDKOVATEĽOV

Por. č.	Obchodné meno	Sídlo	IČO	Zmluva č.
1				
2				
3				
4				
5				

*** len v elektronickej podobe**

Meno a priezvisko

CSS Nádej Dolný Lieskov, 018 21 Dolný Lieskov č. 197

Príloha č. 7

Protokol o vykonaní kontroly:

Kontrolu nad dodržiavaním ochrany osobných údajov vykonáva zodpovedná osoba raz ročne, v prípade potreby viackrát podľa nižšie uvedeného tlačiva.

Protokol o vykonaní kontroly – ochrana osobných údajov

1. Číslo 1/ rok

Kontrola vykonaná dňa:

Na pracovisku, prevádzke, úseku, oddelení :

Kontrolu vykonal:

Ku kontrole prizvaný:

1. Cieľ kontroly :

2. Zistené nedostatky :

3. Uložené opatrenia k náprave:

4. Osoba určená na odstránenie nedostatkov a termín ich odstránenia:
   Meno a priezvisko, dátum

V ....., dňa ..... Kontroloval: .....

Meno a priezvisko

S Protokolom bol/a oboznámený/á za kontrolovaný úsek: .....

Meno a priezvisko

Dátum odstránenia nedostatkov: deň/mesiac/rok

Nedostatky odstránil/ Podpis : .....

Meno a priezvisko