Bezpečnostná smernica
na ochranu osobných údajov

v informačných systémoch
prevádzkovateľa:

Vysoká škola múzických umení

Ventúrska 3, 813 01 Bratislava
IČO: 00397431

 Počet strán: 32

Bezpečnostná smernica na ochranu osobných údajov bola spracovaná v zmysle § 19 zákona č. 122/2013 Z. z. v znení zákona č. 84/2014 Z. z. o ochrane osobných údajov (ďalej len „zákon o ochrane osobných údajov“) a v zmysle §4 vyhlášky Úradu na ochranu osobných údajov č. 164/2013 Z. z. o rozsahu a dokumentácii bezpečnostných opatrení.

Bratislava, dňa: 30.4.2015 Schvaľujem: .....

Doc. akad. maliar Milan Rašla

rektor

Predkladateľ:	© Ing. Miroslav Ilavský – MIDITRADE IČO: 46 839 194	Dátum: 13.4.2015	Podpis:
Autor:	Ing. Miroslav Ilavský	Dátum: 13.4.2015	Podpis:
Konzultant prevádzkovateľa:	Ing. Ján Stajník, zodpovedná osoba	Dátum: 20.4.2015	Podpis:

Obsah

1. Vymedzenie pojmov a zoznam použitých skratiek

Adresa – súbor údajov o pobyte fyzickej osoby, do ktorého patria názov ulice, orientačné, príp. súpisné číslo domu, názov obce, prípadne názov časti obce, poštové smerovacie číslo, názov okresu, názov štátu.

Aktívum – čokoľvek, čo má pre spoločnosť hodnotu a je to potrebné chrániť. Medzi hlavné aktíva informačného systému patria hardvér, softvér, údaje, komunikačné prostriedky a ľudské zdroje, využívané na zabezpečovanie informačných služieb.

Analýza rizík – proces identifikovania a ohodnotenia bezpečnostných rizík, ktorý stanovuje ich závažnosť a špecifikuje oblasti vyžadujúce implementáciu opatrení na zníženie úrovne týchto rizík.

Anonymizovaný údaj – osobný údaj upravený do takej podoby, v ktorej ho nemožno priradiť dotknutej osobe, ktorej sa týka.

Autenticita – vlastnosť zaisťujúca, že identita subjektu alebo zdroja je taká, za ktorú je prehlasovaná. Autenticita je aplikovaná na entity ako sú používatelia, procesy, systémy a pod.

Bezpečnostné opatrenie – prax, postup alebo mechanizmus zavedený za účelom zníženia miery rizika.

Blokovanie 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 č. 122/2013 Z. z.

Cezhraničný prenos osobných údajov – prenos osobných údajov mimo územia Slovenskej republiky a na územie Slovenskej republiky.

Dostupnosť – vlastnosť, že je niečo (napríklad údaje alebo služba IS) na požiadanie prístupné a použiteľné oprávnenou entitou.

Dotknutá osoba – každá fyzická osoba, ktorej osobné údaje sú spracovávané.

Dôvernosť – vlastnosť, že informácia nie je dostupná / prístupná neoprávneným jednotlivcom, entitám alebo procesom.

Hrozba – potenciálna príčina nežiaduceho incidentu, ktorý môže mať za následok narušenie bezpečnosti (dôvernosti, integrity alebo dostupnosti) aktív.

Informačný systém 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 zákona č. 122/2013 Z. z. rozumie aj súbor osobných údajov, ktoré sú spracúvané alebo pripravené na spracovanie čiastočne automatizovanými alebo inými ako automatizovanými prostriedkami spracúvania.

Integrita systému – vlastnosť, že systém vykonáva zamýšľanú funkciu nenarušeným spôsobom, bez zámernej alebo náhodnej neoprávnenej manipulácie so systémom.

Integrita údajov – vlastnosť, že údaje neboli zmenené alebo zničené neoprávneným spôsobom.

Likvidácia osobných údajov – zrušenie osobných údajov rozložením, vymazaním alebo fyzickým zničením hmotných nosičov tak, aby sa z nich osobné údaje nedali reprodukovať.

Oprávnená osoba – každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovného pomeru, 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 §21 zákona č. 122/2013 Z. z.

Osobné údaje – 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.

Podmienky 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.

Poskytovanie osobných údajov – odovzdávanie osobných údajov tretej strane, ktorá ich ďalej spracúva.

Prevádzkovateľ – každý, kto sám alebo spoločne s inými, vymedzí účel spracúvania osobných údajov, určí podmienky ich spracúvania a spracúva osobné údaje vo vlastnom mene, v tomto prípade je to SAD Humenné, a. s. (ďalej aj "prevádzkovateľ" alebo "SAD Humenné, a.s.").

Priestor prístupný verejnosti – priestor, do ktorého možno 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.

Príjemca – každý, komu sú osobné údaje poskytnuté alebo sprístupnené, pričom príjemcom môže byť aj tretia strana: prevádzkovateľ, ktorý spracúva osobné údaje na základe §3 ods. 1 písm. g zákona č. 122/2013 Z. z. a úrad, ktorý plní úlohy ustanovené týmto zákonom, sa nepovažuje za príjemcu.

Riziko – potenciálna možnosť, že daná hrozba využije zraniteľnosť aktíva alebo skupiny aktív a spôsobí tak narušenie bezpečnosti aktív.

Spracúvanie osobných údajov – vykonávanie operácií alebo súboru operácií s osobnými údajmi najmä ich získavanie, zhromažďovanie, šírenie, zaznamenávanie, usporadúvanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, uchovávanie, blokovanie, likvidácia, ich cezhraničný prenos, poskytovanie, sprístupňovanie alebo zverejňovanie.

Sprístupňovanie osobných údajov – oznámenie osobných údajov alebo umožnenie prístupu k nim príjemcovi, ktorý ich ďalej nespracúva.

Sprostredkovateľ – každý, kto spracúva osobné údaje v mene prevádzkovateľa v rozsahu a za podmienok dojednaných s prevádzkovateľom v písomnej zmluve podľa §8 zákona č. 122/2013 Z. z. a v súlade s týmto zákonom.

Súhlas dotknutej osoby – akýkoľvek slobodne daný výslovný a zrozumiteľný prejav vôle, ktorým dotknutá osoba na základe poskytnutých informácií vyjadruje súhlas so spracúvaním svojich osobných údajov.

Účel spracúvania osobných údajov – vopred jednoznačne vymedzený alebo ustanovený zámer spracúvania osobných údajov, ktorý sa viaže na určitú činnosť.

Všeobecne použiteľný identifikátor – trvalý identifikačný osobný údaj dotknutej osoby, ktorý zabezpečuje jej jednoznačnosť v informačných systémoch.

Zverejnenie osobných údajov – publikovanie, umiestnenie 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.

Zostatkové riziko – bezpečnostné riziko, ktoré zostane úplne alebo čiastočne nepokryté bezpečnostnými opatreniami z dôvodu, že jeho miera je pre prevádzkovateľa akceptovateľná alebo ju nie je možné eliminovať vhodnými a efektívnymi bezpečnostnými opatreniami.

BOZP	Bezpečnosť a ochrana zdravia pri práci
EPS	Elektrická požiarna signalizácia
IS	Informačný systém
ISO	International Standard Organization - Medzinárodná organizácia pre štandardizáciu
IT	Informačné technológie
IKT	Informačné a komunikačné technológie
LAN	LocalAreaNetwork - Lokálna počítačová sieť
OS	Operačný systém
PC	Personalcomputer - Osobný počítač
PSN	Poplachový systém na hlásenie narušenia
PTV	Priemyselná televízia
STN	Slovenská technická norma
SVK	Systém vstupovej kontroly
TCP/IP	TransmisionControlProtocol/ Internet Protocol - protokoly zabezpečujúce prenos paketov dát medzi počítačmi v sieti
UPS	UninterruptiblePowerSupply - Zdroj neprerušiteľného napájania
WAN	WideAreaNetwork - Miestne rozľahlá počítačová sieť

2. Úvodné ustanovenia

V zmysle zákona o ochrane osobných údajov, za bezpečnosť vo svojich informačných systémoch spracúvaných osobných údajov zodpovedá prevádzkovateľ tým, že ich chráni pred ich poškodením, zničením, stratou, zmenou, neoprávneným prístupom a sprístupnením, poskytnutím alebo zverejnením, ako aj pred akýmikoľvek inými neprípustnými spôsobmi spracúvania. Na tento účel musí prijať primerané technické, organizačné a personálne opatrenia, ktoré zodpovedajú spôsobu spracúvania.

Bezpečnostná smernica na ochranu osobných údajov v informačných systémoch prevádzkovateľa (ďalej tiež „Smernica“) vymedzuje rozsah a spôsob bezpečnostných opatrení, potrebných na eliminovanie a minimalizovanie hrozieb a rizík, pôsobiacich na informačné systémy prevádzkovateľa, v ktorých sú spracúvané osobné údaje, z hľadiska narušenia ich bezpečnosti, spoľahlivosti a funkčnosti.

Smernica bola spracovaná v zmysle § 19 ods. 2 zákona o ochrane osobných údajov a v zmysle §4 vyhlášky Úradu na ochranu osobných údajov č. 164/2013 Z. z. o rozsahu a dokumentácii bezpečnostných opatrení obsahuje:

- popis technických, organizačných a personálnych opatrení a spôsob ich uplatňovania v konkrétnych podmienkach,
- rozsah oprávnení, popis povolených činností jednotlivých oprávnených osôb, spôsob ich identifikácie a autentizácie pri vstupe do informačných systémov prevádzkovateľa („ďalej IS“),
- rozsah zodpovednosti oprávnených osôb a osoby zodpovednej za dohľad nad ochranou osobných údajov,
- spôsob, formu a periodicitu výkonu kontrolných činností, zameraných na dodržiavanie bezpečnostných opatrení,
- postupy pri haváriách, poruchách a iných mimoriadnych situáciách, vrátane preventívnych opatrení na zníženie rizika vzniku mimoriadnych situácií, a možností efektívnej obnovy stavu pred haváriou, poruchou alebo inou mimoriadnou situáciou.

Smernica je základný dokument pre všetky oprávnené osoby prevádzkovateľa (užívateľov IS) a obsahuje súhrn pravidiel a podmienok používania, ktoré je nevyhnutné rešpektovať pre zabezpečenie bezpečnej prevádzky IS v praxi. Je výsledkom vykonanej bezpečnostnej analýzy v IS prevádzkovateľa, opatrení, prijatých na minimalizáciu a predchádzanie pôsobenia vyhodnotených bezpečnostných rizík, a prijatého bezpečnostného zámeru na splnenie zákonných požiadaviek.

Smernica je súčasťou Bezpečnostného projektu na ochranu osobných údajov Prevádzkovateľa, ktorý podľa §19 ods. 3 Zákona o ochrane osobných údajov obsahuje:

a) názov IS, na ktorý sa vzťahuje,
b) bezpečnostný zámer,
c) analýzu bezpečnosti IS,
d) bezpečnostnú smernicu.

Prílohou Smernice sú vzory, šablóny a formuláre, používané Prevádzkovateľom pri vykonávaní dohľadu nad spracúvaním a ochranou osobných údajov v IS. Zoznam príloh je uvedený v závere Smernice.

3. Podmienky spracúvania osobných údajov

Smernicou stanovené pravidlá sú záväzné pre všetky oprávnené osoby Prevádzkovateľa, vrátane pracovníkov iných organizácií (napr. servisný technik), vykonávajúcich činnosti súvisiace s IS, k čomu ich zaväzuje písomný právny akt.

Nerešpektovanie týchto pravidiel zo strany osôb definovaných v predchádzajúcom odseku bude kvalifikované ako porušenie pracovných (resp. zmluvných) povinností, s následkami podľa platnej legislatívy Slovenskej republiky.

3.1 Prevádzkovateľ

Prevádzkovateľom IS, analyzovaných pre potrebu tejto Smernice, je :

Vysoká škola múzických umení
Ventúrska 3
813 01 Bratislava
IČO: 00397431

Povinnosti Prevádzkovateľa, pri spracúvaní a ochrane osobných údajov, sú uvedené v §6 Zákona o ochrane osobných údajov. Prevádzkovateľ je zodpovedný za bezpečnosť spracúvaných osobných údajov podľa §19 Zákona o ochrane osobných údajov. Takisto je zodpovedný za výkon dohľadu nad ochranou osobných údajov a môže poveriť vykonávaním dohľadu nad ochranou osobných údajov jednu alebo viacero zodpovedných osôb.

3.2 Zodpovedná osoba

Prevádzkovateľ má vymenovanú zodpovednú osobu, poverenú vykonávaním dohľadu nad ochranou osobných údajov podľa §23 Zákona o ochrane osobných údajov. Kontakt na zodpovednú osobu na ochranu osobných údajov je:

Ing. Ján Stajník, stajnik@vsmu.sk

3.3 Sprostredkovatelia a príjemcovia s povinnosťou mlčanlivosti

K osobným údajom, v IS prevádzkovateľa, môžu mať prístup iné právne subjekty (prípadne aj fyzické osoby), v postavení :

1. Sprostredkovateľ - každý, kto spracúva osobné údaje v mene prevádzkovateľa, v rozsahu a za podmienok dojednaných s prevádzkovateľom v písomnej zmluve podľa § 8 a v súlade so zákonom o ochrane osobných údajov,
2. Tretia strana - každý, kto nie je dotknutou osobou, prevádzkovateľom poskytujúcim osobné údaje, jeho zástupcom, sprostredkovateľom alebo oprávnenou osobou,
3. Príjemca - každý, komu sú osobné údaje poskytnuté alebo sprístupnené, pričom príjemcom môže byť aj tretia strana; prevádzkovateľ, ktorý spracúva osobné údaje na základe § 3 ods. 1 písm. g) zákona o ochrane osobných údajov a Úrad na ochranu osobných údajov, sa nepovažujú za príjemcov.

Zoznam spolupracujúcich externých spoločností, s uvedením vykonávanej činnosti pre prevádzkovateľa a vzťahu k spracúvaniu osobných údajov, je uvedený v prílohe č. 7 tejto smernice.

Pre prevádzkovateľa vyplýva povinnosť uzatvoriť so sprostredkovateľmi a prijímateľmi zmluvy, ktoré ich zaviažu mlčanlivosťou o osobných údajoch v IS prevádzkovateľa, pri sprostredkovateľovi navyše musia byť definované deň začiatku spracovávania osobných údajov v mene prevádzkovateľa, účel spracúvania, názov IS, zoznam spracúvaných osobných údajov, okruh dotknutých osôb, podmienky spracúvania, dovolené operácie s osobnými údajmi, vyhlásenie prevádzkovateľa, že postupoval pri výbere sprostredkovateľa v súlade s §8 ods. 2 Zákona o ochrane osobných údajov, dobu na ktorú sa zmluva uzatvára, dátum jej uzavretia a podpisy oboch strán.

3.4 Informačné systémy osobných údajov prevádzkovateľa

Prevádzkovateľ spracúva osobné údaje v nasledovných informačných systémoch osobných údajov:

P.č.	Názov IS OOU	Účel spracúvania OU	Právny základ spracúvania OU
1.	Akademický informačný systém	Evidencia študentov, evidencia pedagógov a garantov študijných programov - účel zabezpečenia vzdelávacieho procesu podľa zákona o vysokých školách a na účely štatistík MŠVVaŠ SR.	Osobitý zákon podľa evidenčného listu
2.	Akreditácie - publikačná a umelecká činnosť	Evidencia životopisov a údajov o vedeckej a publikačnej a umeleckej činnosti pedagógov a garantov študijných programov na účely akreditačného konania.	Osobité zákony podľa evidenčného listu
3.	Archív a registratúra	Archivácia účtovných, mzdových a študijných dokladov v papierovej podobe a v SW na správu registratúry podľa príslušných zákonov.	Osobité zákony podľa evidenčného listu
4.	E-mail	Elektronická komunikácia – prijímanie životopisov, komunikácia študijného oddelenia so študentmi, komunikácia so študentmi ohľadne zahraničných študijných pobytov, pracovná komunikácia medzi zamestnancami školy.	Osobité zákony podľa evidenčného listu
5.	Evidencia pošty	Evidencia došlej a odoslanej pošty – elektronicky pomocou SW Nuntio.	Osobitý zákon podľa evidenčného listu
6.	Integrovaný bezpečnostný systém	Evidencia a ochrana vstupu osôb do priestorov prevádzkovateľa, ochrana a zabezpečenie majetku pred krádežami, vandalizmom, prevencia pred páchaním trestných činov, porušovaním poriadku školy, evidencia prítomnosti zamestnancov na pracovisku.	Osobité zákony podľa evidenčného listu
7.	Interné kontroly zamestnancov	Kontrola požitia alkoholu u zamestnancov na pracovisku, kontrola prítomnosti zamestnanca v mieste bydliska pri PN.	Osobité zákony podľa evidenčného listu
8.	Interné školenia zamestnancov	Evidencia povinných interných školení zamestnancov prevádzkovateľa.	Osobité zákony podľa evidenčného listu
9.	Kamerový systém - rektorát	Ochrana a zabezpečenie majetku pred krádežami, vandalizmom, prevencia pred páchaním trestných činov, porušovaním poriadku školy.	Osobitý zákon podľa evidenčného listu
10.	Kniha návštev	Evidovanie návštev - partneri a potenciálni partneri prevádzkovateľa, hostia a pod. za	Osobité zákony podľa evidenčného listu

		účelom ochrany majetku prevádzkovateľa.	
11.	Knižnica	Evidencia čitateľov v knižnici.	Súhlas dotknutej osoby, osobité zákony podľa evidenčného listu
12.	Mobility študentov a učiteľov	Poskytovanie údajov študentov a učiteľov na zahraničné študijné pobyty v rámci programu ERASMUS+.	Zmluvný vzťah, osobité zákony podľa evidenčného listu
13.	Monitorovanie vozidiel cez GPS	Monitorovanie služobných vozidiel pomocou GPS, za účelom ochrany majetku proti krádeži, porovnanie knihy jázd s cestovnými príkazmi.	Osobitý zákon podľa evidenčného listu
14.	Motivačné (prospechové) štipendiá	Evidencia údajov pre poskytnutie štipendií študentom. Spracúvané v SW AIS.	Osobitý zákon podľa evidenčného listu
15.	Personalistika a mzdy	Plnenie povinností zamestnávateľa súvisiacich s pracovným pomerom, alebo obdobným vzťahom (napr. na základe dohôd o prácach vykonávaných mimo pracovného pomeru) vrátane predzmluvných vzťahov, vedenie mzdového účtovníctva, podklady pre mzdy.	Osobité zákony podľa evidenčného listu
16.	Pracovné úrazy a lekárske prehliadky	Evidencia pracovných a školských úrazov, evidencia povinných lekárskych prehliadok vybraných profesií.	Osobité zákony podľa evidenčného listu
17.	Preukazy študenta a zamestnanca	Evidencia údajov pre personalizáciu preukazov študenta a zamestnanca VŠ.	Súhlas dotknutej osoby, osobité zákony podľa evidenčného listu.
18.	Skartácie	Systémová skartácia papierových dokumentov s OÚ a likvidácia el. údajov podľa registratúrneho plánu.	Osobitý zákon podľa evidenčného listu
19.	Sociálne štipendiá	Evidencia údajov pre poskytnutie štipendií študentom. Spracovanie v SW AIS.	Osobité zákony podľa evidenčného listu
20.	Súdne spory	Vedenie súdnych sporov s FO.	Osobité zákony podľa evidenčného listu
21.	Štipendiá doktorandov	Agenda spojená so štipendiami pre doktorandov v dennej forme štúdia. Spracúvané v SW AIS.	Osobité zákony podľa evidenčného listu
22.	Ubytovacie zariadenie	Evidencia ubytovaných v zariadeniach VŠMU.	Osobité zákony podľa evidenčného listu
23.	Účtovníctvo	Spracovanie účtovných a daňových dokladov.	Osobité zákony podľa evidenčného listu
24.	Verejné obstarávanie	Evidovanie údajov FO – uchádzačov vo verejnom obstarávaní.	Osobitý zákon podľa evidenčného listu
25.	Životopisy	Evidencia životopisov, žiadostí o prácu a motivačných listov záujemcov o prácu za účelom výberového konania.	Súhlas dotknutej osoby, predzmluvný vzťah, osobitý zákon podľa evidenčného listu.

Prevádzkovateľ je povinný evidovať v základnej dokumentácii na ochranu osobných údajov všetky informačné systémy, ktoré nespadajú pod povinnosť osobitnej registrácie.

3.5 Právny základ spracúvania osobných údajov v IS

Prevádzkovateľ môže spracovávať osobné údaje v IS iba so súhlasom dotknutej osoby alebo pokiaľ mu to dovoľuje osobitý zákon. Právny základ spracúvania osobných údajov v jednotlivých IS je uvedený v evidenčných listoch informačných systémov, ktoré prevádzkovateľ na vyžiadanie poskytne na nahliadnutie.

Prevádzkovateľ musí dodržiavať minimálne opatrenia a to najmä:

- Pred začatím spracúvania osobných údajov jednoznačne a konkrétne vymedziť účel spracúvania osobných údajov. Účel spracúvania musí byť jasný a nesmie byť v rozpore s Ústavou Slovenskej republiky, ústavnými zákonmi, zákonmi a medzinárodnými zmluvami, ktorými je Slovenská republika viazaná.
- Prevádzkovateľ vypracuje ku každému IS dokumentáciu predpísanú zákonom, v evidenčnom liste IS, pri registrácii alebo osobitej registrácii IS uvedie názov IS, účel spracúvania, rozsah osobných údajov, právny základ spracúvania, dotknuté osoby, ktorých údaje sú v IS spracúvané a či dochádza k poskytovaniu, zverejňovaniu alebo sprístupňovaniu osobných údajov.
- Prevádzkovateľ a ním poverení sprostredkovatelia a oprávnené osoby sú povinné zachovať mlčanlivosť o osobných údajoch, ktoré im boli poskytnuté, alebo k nim majú prístup. (Povinnosť mlčanlivosti zaniká, ak je to potrebné na plnenie úloh orgánov činných v trestnom konaní, správnom a priestupkovom konaní a právnych veciach. V takomto prípade povinnosť mlčanlivosti zaniká len vo vzťahu k uvedeným orgánom).
- Povinnosť mlčanlivosti trvá aj po zániku funkcie oprávnenej osoby, aj po skončení jej pracovného pomeru/ zmluvného vzťahu.

3.6 Likvidácia osobných údajov

Likvidácia produktov informačného systému – likvidácia osobných údajov je samostatná operácia spracúvania osobných údajov, pri ktorej dôjde k zničeniu osobných údajov tak, že nie sú čitateľné a obnoviteľné. Nakoľko je zálohu dátového záznamu možné uchovávať iba lehote definovanej zákonom, je potrebné, aby sa po tomto čase záznam zlikvidoval.

- Všetky písomné, obrazové, zvukové a iné záznamy, ktoré obsahujú osobné údaje (zoznamy, výpisy, pamäťové média a pod.), musia byť po vylúčení z ďalšieho spracúvania (ak nakladanie s nimi nepredpisuje iný zákon, napr. zákon č. 395/2002 Z. z. o archívoch a registratúrach) fyzicky zlikvidované skartovaním, rozložením, alebo spálením v zmysle § 17 zákona o ochrane osobných údajov
- Prepisovateľné pamäťové média (CDRW, DVDRW média, USB kľúče, pamäťové karty a pod.) sa musia likvidovať vymazaním, alebo naformátovaním tak, aby sa z nich osobné údaje nedali reprodukovať. Neprepisovateľné pamäťové médiá (CD a DVD médiá a pod.) sa musia fyzicky likvidovať, napr. zlomením.

4. Zameranie bezpečnostných opatrení

Účelom prijatia bezpečnostných opatrení je vytvorenie funkčného, efektívneho a z hľadiska finančnej náročnosti optimálneho systému ochrany osobných údajov, a to najmä:

- **Neoprávneným osobám znemožniť akýkoľvek nedovolený prístup k dátovému záznamu** manipuláciou s technickými zariadeniami a manipuláciou s nosičmi osobných údajov.
- **Oprávneným osobám prevádzkovateľa zabezpečiť prístup k IS** v rozsahu potrebnom na plnenie ich povinností alebo úloh, obsiahnutých v poučení oprávnenej osoby, ak to automatizované prostriedky spracúvania umožňujú. Prevádzkovateľ na

účel spätnej identifikácie osoby, miesta a času spracúvania osobných údajov v IS, zabezpečí zaznamenanie každého vstupu oprávnenej osoby do IS.
- **Zabezpečiť odolnosť IS** proti škodlivým kódom (napr. počítačový vírus) a nežiadúcej modifikácii systému, ako aj zabezpečiť pravidelné mazanie dátového záznamu, v lehote stanovenej príslušným zákonom, resp. po uplynutí doby potrebnej na splnenie účelu spracúvania osobných údajov v IS prevádzkovateľa.

5. Úrovne riešenia bezpečnosti

Cieľom riešenia bezpečnosti je vytvoriť maximálnu ochranu IS pred jeho možným narušením, s minimálnymi nákladmi. Bezpečnosť IS je nutné riešiť tak, aby riziká, ktorým je IS vystavený, boli pomocou vhodných opatrení znížené na maximálnu možnú úroveň. Takéto riešenie potom zabezpečí elimináciu prevažnej časti rizík, v kombinácii s vhodnými preventívnymi opatreniami, ešte pred ich vznikom.

Bezpečnosť je riešená na úrovniach:
- **Technická –** chráni prostredie, v ktorom sa IS prevádzkuje.
- **Organizačná –** pomocou organizačných opatrení sa dosiahne výrazné zvýšenie bezpečnosti, s citlivými informáciami sa zoznamuje iba osoba, ktorá ich potrebuje k výkonu svojej činnosti (oprávnená osoba).
- **Personálna –** presné definovanie pravidiel, povinností a oprávnení pre osoby, ktoré prichádzajú do styku s IS.

5.1 Technické opatrenia

Ide o implementáciu technických prostriedkov a technológií na ochranu IS.

5.1.1 Popis technických opatrení

Technické opatrenia tvoria neoddeliteľnú časť pri bezpečnostných opatreniach slúžiacich na ochranu informácií pred zneužitím. Delia sa na mechanické opatrenia a elektronické opatrenia.

Mechanické opatrenia: Zabezpečenie samostatného objektu pomocou mechanických zábranných prostriedkov (napr. uzamykateľné dvere, gule na dverách, mreže na dverách a oknách), mechanické oddelenie chráneného priestoru od ostatných častí objektu (napr. stenou, zábranou v podobe deliacich stien, mreží alebo presklenia). Takto vymedzený priestor spĺňa určitú ochranu IS pred fyzickým prístupom neoprávnených osôb a nepriaznivými vplyvmi okolia. Nutné je zamedziť náhodnému odpozeraniu osobných údajov zo zobrazovacích zariadení IS, preto je potrebné klásť dôraz na vhodné umiestnenie zobrazovacích jednotiek.

Elektronické opatrenia: elektrické zabezpečovacie prostriedky – alarmy a pod.

5.1.2 Ochrana pred neoprávneným prístupom – šifrovanie

- na ochranu citlivých informácií pred neoprávneným prístupom používať šifrovacie technológie,
- používať vysoko bezpečné systémy zálohovania dátového záznamu,
- každú inštaláciu a nastavovanie prístupov prevádza správca IS,
- kontrolu technických zariadení vykonáva systémový správca, priebežne a podľa potreby, minimálne každých šesť mesiacov,
- profylaktika na technických zariadeniach by sa mala robiť minimálne každé tri mesiace.

5.1.3 Riadenie prístupu oprávnených osôb

Veľmi dôležitá je identifikácia, autentizácia a autorizácia oprávnených osôb v IS, aby sme vedeli čo najrýchlejšie analyzovať narušenie bezpečnosti a odstrániť toto bezpečnostné riziko a opätovnú možnosť bezpečnostnej udalosti. Pre vstup do IS je potrebné, aby každá oprávnená osoba mala svoje vlastné identifikačné prístupové údaje. Z tohto dôvodu je potrebné:

- každý užívateľ musí mať pre prístup do IS vlastné heslo, ktoré musí uchovávať v tajnosti,
- pri výbere a používaní hesiel by používatelia mali dodržiavať vhodné bezpečnostné praktiky,
- pokiaľ by mal čo i len podozrenie z toho, že jeho heslo preniklo na verejnosť, alebo sa k nemu dostala neoprávnená osoba, musí ho okamžite zmeniť, prípadne ak takúto možnosť nemá, musí o to požiadať systémového správcu,
- pre každého nového užívateľa je potrebné zadať heslo, pokiaľ by v čase zadávania hesla nebol fyzicky prítomný, môže systémový správca (alebo osoba poverená) zadať hocijaké heslo a povedať užívateľovi, aby si ho pri prvom používaní zmenil,
- vhodný môže byť zvláštny súhlas s prístupovými právami od nadriadeného používateľa,
- nepoužívať heslo, ktoré je napr. dátum narodenia, často používaná fráza, niečo, čo sa nachádza na stole, alebo niečo, čo sa spája s užívateľom,
- odporúčame tvoriť heslo reťazcom náhodných znakov vrátane malých a veľkých písmen a číslic, znak tabulátor sa nesmie používať,
- heslo by sa malo pravidelne meniť,
- zaznamenávanie vstupov jednotlivých oprávnených osôb do IS,
- užívateľ sa nesmie žiadnymi prostriedkami pokúšať získať prístupové práva alebo privilegovaný stav, ktorý mu nebol pridelený správcom IS,
- pokiaľ užívateľ v dôsledku chyby programových alebo technických prostriedkov získa privilegovaný stav, ktorý mu nebol udelený, alebo prístupové práva, ktoré mu neboli pridelené, je povinný túto skutočnosť bezprostredne oznámiť správcovi IS a osobe zodpovednej za dohľad nad ochranou osobných údajov,
- minimálne na zálohovacie zariadenie IS by sa mal použiť záložný zdroj napájania – lokálne a centrálne záložné systémy bez prerušenia napájania UPS s výdržou aspoň 15 min. a alarmom,
- kontrolu technických zariadení vykonáva systémový správca priebežne a podľa potreby,
- profylaktika na technických zariadeniach by sa mala robiť minimálne každé tri mesiace.

5.1.4 Ochrana proti škodlivému kódu

Na ochranu IS, hlavne pred jeho napadnutím neautorizovanými osobami, odporúčame inštalovať na pracovné stanice, z ktorých je možné v prípade otvoreného systému pripojiť sa do IS, také programy, ktoré eliminujú možnosť napadnutia stanice a spĺňajú tieto bezpečnostné ochrany:

- **antivírová ochrana –** centralizované systémy ochrany pred vírusovými napadnutiami,
- **firewall –** kombinácia softvérových a hardvérových nástrojov na zabezpečenie LAN pred útokmi z internetu,
- **personal firewall –** softvérové nástroje na zabezpečenie pracovných staníc s vymedzením prístupových práv,
- **sniffer technológia –** detailné sledovanie a vyhodnocovanie dátovej komunikácie,
- **IDS a IPS –** detekcia a ochrana LAN a WAN pred vnútornými a vonkajšími narušeniami bezpečnosti,
- **antispamová ochrana –** ochrana proti nevyžiadaným spam-om, ktoré sa voľne šíria internetom,
- **antispamová ochrana –** ochrana pred nevyžiadanou elektronickou poštou,
- **backdoor ochrana –** backdoor – program, ktorý umožňuje tretím osobám vstup do počítača a jeho použitie na rôzne ciele (napr. internetové útoky, rozposielanie nevyžiadanej pošty – spam). Infikovaným počítačom sa zvykne hovoriť aj zombie,
- **ochrana proti trójskym koňom –** trójsky kôň je program, ktorý sa vydáva za užitočný, ale v skutočnosti má vlastnosti backdoor programu,
- **ochrana proti keyloggerom –** keylogger je program, ktorým sa infikuje počítač a slúži na odchytávanie a zaznamenávanie stlačených kláves, ktoré posiela tretím stranám,
- **pokiaľ je požadovaný prístup z internetu do lokálnej siete –** je nutné, aby bolo toto pripojenie a aj samotný prenos údajov, zabezpečený pomocou kryptovania. Pripojenie cez RD (Remote desktop) funkciu priamo vo Windows OS sa používať nesmie.
  Odporúča sa používať VPN (VirtualPrivateNetwork). V prípade prenosu pomocou SSH (SecureShell) sa neodporúča používať pre autorizáciu vstupov meno a heslo, ale privátne a verejné kľúče v minimálnej dĺžke 512 bite, optimálne 1024 bite.

Antivírový program musí byť nainštalovaný na každej pracovnej stanici, ktorá je z technického hľadiska pripojená do IS. Vyhlásenie o tom, či je z technického hľadiska pracovná stanica pripojená do IS, vydá systémový správca.

5.1.5 Sieťová bezpečnosť

Oblasť sieťovej bezpečnosti sa skladá hlavne z predpisov a zásad, ktoré pripravuje správca siete a sú určené na prevenciu a monitorovanie pred neoprávneným prístupom, zneužitím, narušením dostupných sieťových zdrojov. Pri práci v sieti je potrebné dodržiavať tieto zásady:

- prístup do siete je potrebné zabezpečiť minimálne pomocou mena a hesla,
- v prípade spracúvania obzvlášť citlivých údajov, sa odporúča zabezpečiť vstup pomocou bezpečnostného kľúča alebo čipovej karty,
- je potrebné presne definovať, ktoré služby v sieti sú pre jednotlivých užívateľov povolené a ktoré zakázané,

- zabrániť neoprávnenému prístupu pri kontrole potenciálne škodlivého obsahu, ako sú počítačové vírusy alebo trójske kone, ktoré sú prenášané cez sieť,
- prenos údajov po LAN sieti je potrebnézakryptovať, nepoužívať nekryptované služby ako je napr. telnet, ftp, http,...
- tam, kde je to možné, používať na komunikáciu VPN systém,
- je potrebné mať zdokumentované všetky miesta prepojenia sietí vrátane verejne prístupovej počítačovej siete,
- zabezpečiť ochranu vonkajšieho a vnútorného prostredia prostredníctvom bezpečnostných opatrení a to hlavne správne nastavenia politiky firewallu, nedefinovať, alebo blokovať vstupné porty a zamedziť prístup k určitým rizikovým web stránkam a tým eliminovať bezpečnostné riziká – hackerský útok.

5.1.6 Základná prevencia pred napadnutím (infiltráciou):

- je nutné pravidelne aktualizovať operačný systém, na počítačoch z ktorých je možné pripájať sa do IS, za účelom zaplátania a odstránenia rizikových miest, vždy, keď sú k dispozícii dostupné bezpečnostné balíčky,
- zakázať užívateľom na pracovných staniciach, z ktorých je možné pripájať sa do IS, používať privilegované administrátorské práva, ktoré majú slúžiť výhradne na zmenu systémových nastavení, prípadne inštaláciu nových programov,
- nainštalovať v rámci možností čo najviac programov z odseku 5.1.4, minimálne však antivírový program,
- antivírový program pravidelne aktualizovať, vždy keď sú k dispozícii nové antivírové reťazce,
- pravidelne (minimálne 1x mesačne) celý počítač prekontrolovať týmto antivírovým programom,
- pred využitím pamäťového média v počítači (CD, DVD, diskety, USB flash disky,...) tento dátový nosič skontrolovať antivírovým programom,
- neotvárať podozrivú nevyžiadanú e-mailovú prílohu,
- nenavštevovať dubiózne stránky (môžu obsahovať spyware),
- nesťahovať a neinštalovať žiadny softvér, ktorý nebol vopred schválený systémovým správcom, a to ani z povolených stránok.

5.2 Organizačné opatrenia

Ide o interné nariadenia prevádzkovateľa na zabezpečenie bezpečnosti osobných údajov.

5.2.1 Pravidlá v rámci organizačnej štruktúry

- spracúvať a zhromažďovať osobné údaje smú len organizačné zložky a pracoviská na to určené,

5.2.2 Rozdelenie kompetencií

- v prípade mimoriadnej situácie, kedy dôjde k narušeniu bezpečnosti činnosť koordinuje a riadi krízový štáb,
- pri narušení počítačovej bezpečnosti, bezpečnosti v oblasti IS a LAN koordinuje činnosť poverený informatik,
- pri narušení globálnej bezpečnosti koordinuje činnosť zamestnanec poverený agendou CO,
- pri narušení informačnej bezpečnosti v oblasti dokumentov, telefónnych liniek a mobilných sieti koordinuje činnosť prevádzkovateľ alebo zástupca prevádzkovateľa.

5.2.3 Určenie pracovných a bezpečnostných postupov

- spracúvať a zhromažďovať audio/video záznamy údaje smú len zamestnanci na to určení. Spracúvanie údajov musí byť v súlade so zákonom o ochrane osobných údajov. Zamestnanci sa musia riadiť všetkými prijatými opatreniami a nariadeniami vydanými prevádzkovateľom.

5.2.4 Ďalšie organizačné opatrenia

- po pracovnej dobe je zakázané zdržiavať sa na pracovisku,
- mimo pracovnej doby sa pracovníci môžu zdržiavať na pracovisku len so súhlasom prevádzkovateľa alebo zástupcu prevádzkovateľa,
- krízový štáb vypracuje havarijný plán na zabezpečenie kontinuity činnosti v prípade narušenia bezpečnosti,

- pre krízový štáb musí byť zrejmé:
    - personálne obsadenie,
    - hierarchia podriadenosti a zodpovednosti,
    - spôsob komunikácie,
    - rozdelenie úloh,
    - krízový štáb má právomoci vydávať rozhodnutia.

- všetky nároky dotknutých osôb v zmysle tretej hlavy zákona o ochrane osobných údajov zabezpečuje zodpovedná osoba prevádzkovateľa,
- osoby mimo okruh oprávnených osôb prizvané na technickú pomoc budú preukazne poučené osobou zodpovednou za osobné údaje o zákaze oboznamovať sa s obsahom informácií a v prípade podvedomého oboznámenia o povinnosti mlčanlivosti,
- v organizačnom poriadku určiť režim vstupu na pracoviská, zákaz zdržovať sa na pracovisku po pracovnej dobe bez vedomia nadriadeného, určiť zodpovedných zamestnancov za bezpečnosť, určiť podmienky vstupu na pracovisko a spôsob opustenia pracoviska,
- heslá a administratívne prístupy musia byť zdokumentované a uložené v zapečatenej obálke v trezore, pokyn na jej otvorenie môže vydať len štatutár alebo zodpovedná osoba prevádzkovateľa – otvorenie musí byť zdokumentované,
- architektúra LAN musí byť zdokumentovaná a uložená v trezore (uzamykateľnej skrini) v zapečatenej obálke.

5.2.5 Sťažnosti

- Prijímanie sťažností: Sťažnosti sa podávajú v zmysle Zákona č. 9/2010 Z. z. o sťažnostiach v znení neskorších predpisov. Zodpovedný pracovník prijímajúci sťažnosť okamžite vyrozumie zodpovednú osobu a štatutára prevádzkovateľa.
- Vybavovanie sťažností: Sťažnosti sa vybavujú v zmysle citovaného zákona.

5.2.6 Nakladanie s nosičmi údajov

- akékoľvek materiálne nosiče údajov musia byť zabezpečené pred prístupom neoprávnených osôb. Miestom uloženia nosičov živých údajov môžu byť trezorové prípadne uzamykateľné skrine,
- chránené údaje v elektronickej forme sa ukladajú na databázový server a na prenosné nosiče (CD a DVD média) a tie sú uložené v trezorových skriniach, resp. v archíve. Údaje, ktoré sú uložené na HD PC sa chránia nasledovne:

  - počítače musia byť chránené antivírovým programom s pravidelnou aktualizáciou databáz vírusov,
  - konkrétne programy musia byť zaheslované, pre vstup do programov používa každý užívateľ vlastné heslo,
- oprávnené osoby spracúvajú údaje na mieste a spôsobom znemožňujúcim odcudzenie údajov,
- oprávnené osoby zabezpečia, aby nosiče údajov pri prenášaní medzi miestom uloženia a miestom spracúvania nemohli byť sprístupnené neoprávneným osobám.

5.2.7 Interné smernice prevádzkovateľa

Interné smernice prevádzkovateľa, záväzné pre všetky oprávnené osoby, sú prístupné na sekretariáte rektorátu. Evidenčné listy informačných systémov na ochranu osobných údajov sú prístupné k nahliadnutiu u zodpovednej osoby prevádzkovateľa.

5.3 Personálne opatrenia

Personálne opatrenia – personálna bezpečnosť – je zákonom stanovený postup (§ 21 a§ 22 zákona č. 122/2013 Z. z.), ktorý určuje predpoklady na získanie oprávnenia oboznamovať sa s osobnými údajmi a určuje povinnosti oprávnených osôb. Personálna bezpečnosť zahŕňa vedenie predpísanej evidencie na ochranu osobných údajov. Prevádzkovateľ sa môže rozhodnúť, že písomne poverí výkonom dohľadu nad ochranou osobných údajov zodpovednú osobu alebo viaceré zodpovedné osoby podľa § 23 Zákona o ochrane osobných údajov, ktoré dozerajú na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov.

5.3.1 Požiadavky na personálne opatrenia

- **Povedomie o bezpečnosti –** program dosiahnutia povedomia bezpečnosti musí byť implementovaný na všetkých úrovniach organizácie, od vrcholového manažmentu až po používateľov.
- **Pridelenie zodpovednosti v oblasti bezpečnosti informácií –** musí byť jednoznačne definovaná zodpovednosť za ochranu jednotlivých aktív a za vykonávanie určitých bezpečnostných postupov.
- **Zodpovednosť za aktíva –** pre všetky dôležité aktíva musia byť určení vlastníci a musí byť stanovená ich zodpovednosť za dodržiavanie primeraných bezpečnostných opatrení. Zodpovednosť za realizáciu jednotlivých bezpečnostných opatrení môže byť delegovaná, ale vlastná zodpovednosť za ne musí ostať vlastníkovi aktív. O týchto aktívach si prevádzkovateľ vedie písomný zoznam, ktorý je pri akejkoľvek zmene aktualizovaný.
- **Dodržiavanie mlčanlivosti –** 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, okrem situácií vymedzených zákonom. Povinnosť mlčanlivosti trvá aj po ukončení ich spracúvania. Povinnosť mlčanlivosti platí aj pre iné fyzické osoby, ktoré v rámci svojej činnosti (napr. údržba a servis technických prostriedkov) prídu so styku s osobnými údajmi. Povinnosť mlčanlivosti nemajú, ak je to podľa osobitného zákona nevyhnutné na plnenie úloh orgánov činných v trestnom

konaní. Povinnosť mlčanlivosti trvá aj po zániku funkcie oprávnenej osoby alebo po skončení jej pracovného pomeru alebo obdobného pracovného vzťahu.

- **Kvalifikačné predpoklady –** spracúvať osobné údaje v IS majú len oprávnené osoby znalé práce na počítači, vyškolené pre prácu s aplikačným programom a IS.
- **Personálne oddelenie, resp. zamestnanec zodpovedný za personálne záležitosti** vedie evidenciu osôb prichádzajúcich do styku s IS. Každú takúto osobu pracovník poučí a vyhotoví o tom záznam.
- **Poučenie oprávnených osôb –** pred uskutočnením prvej spracovateľskej operácie s IS, zodpovedná osoba, alebo iná poverená osoba za prevádzkovateľa alebo sprostredkovateľa poučí oprávnenú osobu v zmysle § 21 zákona o ochrane osobných údajov o právach a povinnostiach ustanovených týmto zákonom a o zodpovednosti za ich porušenie. Oprávnená osoba poučenie **potvrdí svojim podpisom,** o poučení prevádzkovateľ alebo sprostredkovateľ vedie **preukázateľný záznam.** Prevádzkovateľ je povinný **opätovne** poučiť oprávnenú osobu, ak došlo k podstatnej zmene jej pracovného, služobného alebo funkčného zaradenia, a tým sa významne zmenil obsah náplne jej pracovných činností, alebo sa podstatne zmenili podmienky spracúvanie osobných údajov v rámci jej pracovného, služobného alebo funkčného zaradenia.
- **Postupy oprávnených osôb** spojené s automatizovanými prostriedkami spracúvania a súvisiacich právach a povinnostiach (v priestoroch prevádzkovateľa a mimo týchto priestorov) – používanie technických prostriedkov pre spracúvanie osobných informácií je povolené iba osobám oprávneným oboznamovať sa s osobnými informáciami. 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.
- **Zodpovednosť za informačný systém –** za IS zodpovedá vedúci referátu informatiky, alebo informatik, alebo pracovník poverený správou IS. V prípade, že túto činnosť prevádzkovateľ zabezpečuje dodávateľsky, je nutné uzavrieť mandátnu zmluvu s presne formovanými cieľmi a opatreniami zabezpečujúcimi naplnenie bezpečnostného projektu. To isté platí aj vtedy, ak sa uvedená činnosť organizuje pracovným vzťahom na dohodu.
- **Vymedzenie zodpovednosti za porušenie zákona –** osoby oprávnené pracovať s IS sú zodpovedné za uchovávanie, ochranu a manipuláciu dátových záznamov. Sú zodpovedné za preukázateľnosť súhlasu na spracúvanie údajov v IS, a to tak, že možno o ňom podať dôkaz (§ 11 zákona o ochrane osobných údajov). Sú zodpovedné za poriadok na pracovisku a odloženie všetkých písomností obsahujúcich osobné údaje a iných dokumentov, ktoré by mohli viesť k slobodnému prístupu k osobným údajom, do uzamykateľných odkladacích skriniek, resp. skríň. Sú zodpovedné za dodržiavanie zásad práce v IS podľa príkazu prevádzkovateľa.
- **Osoby oprávnené, ktoré prevádzkujú informačný systém –** sú zodpovedné za riadny chod IS, zodpovedajú za aplikačné programové vybavenie, sú zodpovedné za antivírovú ochranu LAN na pridelených počítačoch z ktorých je možné pristupovať do IS, spoluzodpovedajú s užívateľmi pracovných staníc za antivírovú ochranu a zodpovedajú za modernizáciu hmotných a nehmotných aktív.
- **Oboznámenie oprávnených osôb s bezpečnostnými smernicami –** každá oprávnená osoba musí byť preukázateľne oboznámená s obsahom bezpečnostných smerníc v rozsahu potrebnom na plnenie ich povinností a úloh, uvedená povinnosť prevádzkovateľa sa vzťahuje aj na každú zmenu bezpečnostnej smernice.

- **Vzdelávanie oprávnených osôb –** prevádzkovateľ zabezpečí školenia k bezpečnosti napr. v právnej oblasti (pri zmenách zákonov), v oblasti informačných technológií.
- **Postup pri ukončení pracovného alebo obdobného pomeru oprávnenej osoby –** po skončení pracovného pomeru alebo obdobného pomeru je oprávnená osoba povinná odovzdať všetky pridelené aktíva. Oprávnenej osobe budú zrušené prístupové práva do IS (meno, heslo). Oprávnená osoba bude preukázateľne poučená o následkoch porušenia zákonnej alebo zmluvnej mlčanlivosti.

Zabezpečenie zastupiteľnosti:
- najdôležitejšie procesy pri ochrane IS musia byť zabezpečené zastupiteľnosťou
    - správca systému,
    - správca aplikácie,
    - správca LAN,
    - užívateľ aplikácie alebo agendy.

5.3.2 Rozsah oprávnení a povinností zodpovednej osoby

V zmysle § 23 zákona o ochrane osobných údajov za výkon dohľadu nad ochranou osobných údajov spracúvaných podľa tohto zákona zodpovedá prevádzkovateľ. Prevádzkovateľ môže poveriť vykonávaním dohľadu nad ochranou osobných údajov zodpovednú osobu. Pokiaľ nemá poverenú zodpovednú osobu, za výkon nižšie uvedených činností zodpovedá priamo konateľ prevádzkovateľa.

Zodpovedná osoba zabezpečuje:
- potrebnú súčinnosť s Úradom na ochranu osobných údajov Slovenskej republiky (ďalej len Úrad) pri plnení úloh patriacich do jeho pôsobnosti, na požiadanie je zodpovedná osoba povinná Úradu kedykoľvek predložiť svoje písomné poverenie a písomné oznámenia vystavené pre prevádzkovateľa.
- posúdenie pred začatím spracúvania osobných údajov v IS, či ich spracúvaním nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb,
- pri akomkoľvek podozrení z porušenia práv dotknutých osôb, alebo iného porušenia zákona o ochrane osobných údajov vykonanie práva zastaviť aktivitu, zabezpečiť nosiče údajov a povinnosti okamžite upozorniť prevádzkovateľa na vzniknutú situáciu, ak prevádzkovateľ po upozornení bezodkladne nevykoná nápravu, vzniká zodpovednej osobe povinnosť oznámi túto skutočnosť Úradu,
- sledovanie potrieb spracúvania osobných údajov a postupujúc pritom v zmysle § 27 ods. 2.,
- povoľovanie spracúvania údajov v rozsahu svojej pôsobnosti tak, aby nedošlo k porušeniu zákona,
- dohľad nad plnením základných povinností prevádzkovateľa podľa § 6,
- poučenie oprávnených osôb podľa § 21,
- vybavovanie žiadostí dotknutých osôb podľa § 28 až 30,
- prijatie bezpečnostných opatrení podľa § 19 ods. 1 až 3, dohliadanie na ich aplikáciu v praxi a zabezpečovanie ich aktualizácie podľa § 19 ods. 4,
- dohľad pri výbere sprostredkovateľa, prípravu písomnej zmluvy so sprostredkovateľom a počas trvania zmluvného vzťahu preverovanie dodržiavania dohodnutých podmienok podľa § 8,

- prihlásenie IS na osobitnú registráciu, ich odhlásenie alebo nahlasovanie zmien alebo zabezpečovanie vedenia evidencie IS podľa § 34 až 44.

Zodpovedná osoba vypracováva:
- postupy pri bezpečnostných udalostiach,
- analýzu bezpečnostných udalostí,
- postupy riadenia prístupu do IS.

Zodpovedná osoba zodpovedá za:
- aktualizáciu bezpečnostnej politiky,
- údržbu bezpečnostných smerníc a autorizáciu ich zmien príslušnými riadiacimi pracovníkmi a následnú aktualizáciu súvisiacej dokumentácie,
- riadenie školení pracovníkov – zodpovedá osoba, alebo iná poverená osoba vykoná poučenie pracovníkov o ich oprávneniach, právach a povinnostiach, o prístupoch do zamestnania v pracovnom čase a mimo pracovného času a o spôsobe narábania s údajmi, ktoré obsahujú osobné údaje, poučené musia byť aj osoby, ktoré nenarábajú s údajmi osobného charakteru, ak sú zamestnancami prevádzkovateľa, alebo ak majú voľný prístup do priestorov prevádzkovateľa (napr. upratovačka, údržbár a pod.),
- poučenie osôb, ktoré nenarábajú priamo s údajmi osobného charakteru, ak sú zamestnancami prevádzkovateľa, alebo majú voľný prístup do priestorov prevádzkovateľa, kde sa nachádza IS (napr. upratovačka, údržbár a pod.),
- zamedzenie vstupu nepovolaným osobám do IS.

Zodpovedná osoba kontroluje:
- dodržiavanie zákonných ustanovení pri spracúvaní dátového záznamu z IS a vyhotovuje o tom záznam,
- dodržiavanie a plnenie bezpečnostných smerníc,
- pravidelnosť a dodržiavanie termínov údržby a profylaktiky IS,
- pravidelnosť a dodržiavanie termínov likvidácie a dátového záznamu,
- správne nakladanie so záznamom z IS,
- správne umiestnenie kľúčových prvkov.

5.3.3 Rozsah povinností oprávnených osôb
- oboznámiť sa s bezpečnostnými smernicami IS,
- oboznámiť sa s činnosťou, obsluhou a používaním IS,
- zodpovedať 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,
- zodpovedať za dodržiavanie zásad práce v IS, LAN, WAN podľa poučenia o pravidlách používania počítačovej siete,
- včas informovať zodpovednú osobu o pripravovanom začatí spracúvania osobných údajov a o všetkých skutočnostiach, ktoré by mohli viesť k zneužitiu týchto údajov,
- potvrdiť podpisom dodržiavanie bezpečnostných smerníc IS,
- dodržiavať bezpečnostné smernice IS,
- rešpektovať a riadiť sa pokynmi zodpovednej osoby,
- používať IS len na účely určené bezpečnostnými smernicami,
- použiť záznam osobných údajov z IS ako dôkaz v priestupkovom, správnom alebo trestnom konaní, poznačiť do registratúrneho záznamu konkrétnu udalosť,
- pri archivácii záznamu ako dôkazu na externom médiu archiváciu záznamu poznačiť v predpísanej forme do protokolu,

- v prípade, že konkrétny archivovaný záznam je potrebné uložiť na viac ako jedno záznamové médium, dôvod takéhoto postupu a počet externých záznamových médií poznačiť do protokolu archivovaných záznamov,
- s archivovanými záznamami nakladať tak, aby nemohlo dôjsť k ich zneužitiu, strate, poškodeniu alebo zámene,
- dodržiavať zákaz využitia dátového záznamu na iný účel ako je stanovený bezpečnostnými smernicami, zákaz jeho poskytnutia, zverejnenia a/alebo sprístupnenia ďalšej osobe,
- zachovávať mlčanlivosť o osobných údajoch získaných pomocou IS. (Povinnosť mlčanlivosti zaniká, ak je to potrebné na plnenie úloh orgánov činných v trestnom konaní, správnom a priestupkovom konaní a právnych veciach. V takomto prípade povinnosť mlčanlivosti zaniká len vo vzťahu k uvedeným orgánom.).
- dodržiavať povinnosť mlčanlivosti aj po zániku funkcie, alebo po skončení pracovného pomeru oprávnenej osoby,
- dodržiavať všetky ďalšie ustanovenia zákona č. 122/2013 Z. z. v znení zákona č. 84/2014 Z. z. o ochrane osobných údajov a vyhlášok Úradu na ochranu osob. údajov.

5.3.4 Rozsah povinností správcu systému

Správca systému zodpovedá za:
- prevádzku systému, jeho technický rozvoj, dátovú bezpečnosť a dodržiavanie pravidiel pripojenia do siete,
- pravidelnosť a dodržiavanie termínov údržby a profylaktiky systému.

Správca systému zabezpečuje:
- inštaláciu a reinštaláciu operačných systémov,
- inštaláciu schváleného programového vybavenia,
- aktualizácie programového vybavenia pracovných staníc,
- vykonanie analýzy bezpečnostných incidentov z log súborov firewallu, routerov, antivírového programu a pod.,
- súborovú integritu OS a obnovu údajov zo záloh pri bezpečnostnej udalosti,
- potvrdenie dodržiavania bezpečnostných smerníc IS podpisom,
- dodržiavanie bezpečnostných smerníc IS,
- rešpektovanie a riadenie sa pokynmi zodpovednej osoby,
- používanie IS len na účely stanovené bezpečnostnými smernicami,
- použitie záznamu osobných údajov z IS ako dôkazu v priestupkovom, správnom alebo trestnom konaní, vrátanie poznačenia konkrétnej udalosti do registratúrneho záznamu,
- v prípade archivácie obrazového záznamu, ako dôkazového materiálu pre potreby orgánov činných vo vyšetrovaní, vykonanie písomného protokolu o takejto archivácii a jeho založenie do dokumentácie ochrany osobných údajov,
- v prípade, že konkrétny archivovaný záznam je potrebné uložiť na viac ako jedno záznamové médium, poznačenie dôvodu takéhoto postupu a počtu externých záznamových médií do písomného protokolu,
- nakladanie s archivovanými záznamami tak, aby nemohlo dôjsť k ich zneužitiu, strate, poškodeniu alebo zámene,
- skartovanie externého nosiča záznamu spolu s dokumentom v prípade, že archivovaný záznam už pre ďalšie konanie nie je potrebný a uplynula registratúrnym poriadkom stanovená doba skartácie dokumentu, s ktorým archivovaný záznam súvisí,

- dodržiavanie zákazu využitia dátového záznamu na iný účel ako je stanovený bezpečnostnými smernicami, zákazu jeho poskytnutia, zverejnenia a/alebo sprístupnenia ďalšej osobe,
- zachovanie mlčanlivosti o osobných údajoch získaných pomocou IS. (Povinnosť mlčanlivosti zaniká, ak je to potrebné na plnenie úloh orgánov činných v trestnom konaní, správnom a priestupkovom konaní a právnych veciach. V takomto prípade povinnosť mlčanlivosti zaniká len vo vzťahu k uvedeným orgánom.),
- povinnosť mlčanlivosti trvá aj po zániku funkcie, alebo po skončení pracovného pomeru,
- dodržiavanie všetkých ďalších ustanovení zákona o ochrane osobných údajov.

5.4 Fyzická a objektová bezpečnosť

Implementácia prostriedkov a systémov opatrení na ochranu bezpečnostných aktív pred nepovolanými osobami a pred neoprávnenou manipuláciou v budovách a objektoch.

5.4.1 Formy fyzickej a objektovej bezpečnosti:

- **Mechanické zabezpečovacie systémy –** mechanické zábrany a bariéry proti neoprávnenému vstupu do objektov a priestorov, kde sa nachádza IS. Sú to všetky druhy mechanických zabezpečovacích mechanizmov, uzamykateľné kovové skrine, uzamykacie systémy, dvere, bezpečnostné fólie, okná a zasklenia.

- **Technické zabezpečovacie systémy:**
    - elektromechanické zámkové zariadenia a systémy na kontrolu vstupov do objektov, chránených priestorov a systémy slúžiace na elektronické preukazovanie oprávnenosti a totožnosti osôb,
    - zariadenia poplachových systémov slúžiace na zisťovanie a vyhodnocovanie neoprávneného vstupu do objektu alebo chráneného priestoru,
    - zariadenia na fyzické ničenie nosičov informácií,
    - zariadenia na nepretržité vedenie kontrolného záznamu o činnosti prostriedku pre elektronický podpis a systémov evidencie poskytovaných certifikačných služieb s možnosťou sledovania a spätného preskúmania záznamu, ako aj určenia zodpovednosti za vykonané činnosti,
    - iné technické prostriedky slúžiace na zabezpečenie objektu, chráneného priestoru, prevádzky produktu elektronický podpis, systémov evidencie poskytovaných certifikačných služieb a médií so záložnými a archívnymi kópiami údajov.

5.4.2 Minimálne požadované bezpečnostné opatrenia:

- **Bezpečnosť prostredia**
    - umiestniť IS v takom priestore, aby IS alebo aspoň jeho najdôležitejšie komponenty boli chránené pred nepriaznivými prírodnými vplyvmi a vplyvmi prostredia, možnými dôsledkami havárií technickej infraštruktúry a fyzickým prístupom nepovolaných osôb,
    - zabezpečiť, aby sa v okolí zabezpečeného priestoru nevyskytovali zariadenia, ktorými sú najmä kanalizácia a vodovod, alebo materiály, ktorými sú najmä horľaviny, ktoré by mohli ohroziť IS umiestnený v tomto zabezpečenom priestore.

- **Ochrana pred prístupom nepovolaných osôb –** IS chrániť pred prístupom nepovolaných osôb. Ochranu pred prístupom nepovolaných osôb do areálu prevádzkovateľa riešiť minimálne mechanickými zabezpečovacími systémami prípadne aj strážnou službou. Nadštandardnú ochranu je možné riešiť formou technických zabezpečovacích systémov, napr. elektronickým zabezpečovacím zariadením a pod.
    - vybaviť určené pracoviská mrežami, plnými dverami, trezormi, ohňovzdornými plechovými skriňami,
    - priestory určené pre spracúvanie osobných údajov zamykať mimo pracovnej doby i pri dočasnej pracovnej neprítomnosti oprávnenej alebo oprávnených osôb,
    - neautomatizované prostriedky IS umiestniť v čase prítomnosti oprávnenej osoby alebo oprávnených osôb na pracovisku mimo dosahu neoprávnených osôb,
    - v čase ich neprítomnosti na pracovisku uzamknúť tieto prostriedky v skrini, alebo inak zabezpečiť pred neoprávneným prístupom,
    - zabezpečiť nepretržitú prítomnosť oprávnenej osoby v chránenom priestore, ak sa v ňom nachádzajú aj iné, ako oprávnené osoby (napr. upratovačka),
    - uzamykať trezorové skrine, resp. skrine s nosičmi údajov,
    - miestnosti so skriňami uzamykať bezpečnostným zámkom a osoby, ktorým boli vydané kľúče evidovať.

- **Protipožiarna ochrana –** IS chrániť pred poškodením požiarom minimálne ručnými hasiacimi prístrojmi, ktorých funkčnosť musí byť pravidelne kontrolovaná. Nadštandardnú ochranu je možné riešiť inštalovaním:
    - zariadení elektronickej požiarnej signalizácie,
    - EPS – centrálna detekcia vzniku požiaru v chránených priestoroch a okamžitá signalizácia,
    - systémov automatického hasenia – systémy detekcie požiaru v technologických miestnostiach a technologických zariadeniach a následným spustením prívodu hasiaceho média.

- **Dôležité technické časti automatizovaného informačného systému** (servery, zálohovacie zariadenia, aktívne prvky siete) – umiestniť v samostatnej miestnosti, do ktorej majú prístup iba poverení pracovníci. Okná a dvere musia byť zabezpečené proti neoprávnenému vniknutiu.

- zabezpečiť ochranu pred výpadkom zdroja elektrickej energie pre tie časti IS, ktoré vyžadujú nepretržitú prevádzku a zabezpečiť, aby takýto výpadok nenastal.

- **Režim zaobchádzania s kľúčmi –**minimálne jedna kópia kľúčov od miestnosti musí byť bezpečne uložená v úschovnom zariadení (napr. trezor, kovová skriňa a pod.).
  - prístup do miestnosti s IS môžu mať len oprávnené osoby,
  - osoby, ktorým boli vydané kľúče sú evidované a prevádzkovateľ si o nich vedie zoznam.

- **Evidencia prístupov do IS –**pri vstupe do priestorov, kde sa nachádza IS, viesť knihu evidencie návštev. Potrebné údaje získať nahliadnutím do osobných dokladov. Evidovať nasledujúce údaje:
  - meno, priezvisko, titul,
  - číslo občianskeho preukazu, služobného preukazu alebo číslo pasu,
  - účel vstupu do IS,
  - čas príchodu a odchodu.

- **Bezpečnosť pamäťových médií –**v prípade, že je potrebné vykonať zálohu dátového záznamu na vymeniteľné pamäťové médiá, toto je možné iba v súlade so zákonom o ochrane osobných údajov, každé médium označiť a evidovať.

- **Sprístupňovanie dátového záznamu**

  - dátový záznam sa nesmie poskytovať tretím osobám, nevzťahuje sa naň ustanovenie zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
  - Vo veciach podozrení alebo konaní o priestupkoch a trestných činoch sa osobné údaje poskytujú len príslušníkovi Policajného zboru a to iba v čase jeho výkonu služby, ktorý vykonáva objasňovanie, vyšetrovanie, preverovanie, alebo operatívne šetrenie vo veci, ktorej sa takýto záznam týka.
  - Osobné údaje získané z IS, u ktorých je dôvodný predpoklad, že budú použité ako dôkazy v priestupkovom, správnom, prípadne trestnom konaní, sa v digitalizovanej podobe archivujú na externom médiu – nosiči.
  - Externý nosič musí byť označený príslušnou registratúrnou, resp. spisovou značkou udalosti alebo konania, v rámci ktorého bol dôkaz produkovaný, menom, priezviskom a funkciou oprávnenej osoby, ktorá archiváciu vykonala, menom, priezviskom a funkciou osoby, ktorá konanie vedie. Vykonanie archivácie osobného údaja na externom nosiči musí byť zapísané v protokole.
  - Archivovaných záznamov IS v nasledovnom rozsahu:
    - registratúrna značka konania, právna kvalifikácia skutku
    - dátum a čas archivácie
    - oprávnená osoba, ktorá archiváciu vykonala
    - dátum, doba trvania a časového rozsahu archivovaného záznamu

- **Bezpečná likvidácia nosičov osobných údajov** v súlade so zásadami uvedenými v kapitole č. 3.6.

6. Bezpečnostné incidenty

Postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení na zníženie vzniku mimoriadnych situácií a možností efektívnej obnovy stavu pred haváriou. Štandardom pre periodické hodnotenie zraniteľnosti je pravidelné hodnotenie slabých miest a ohrození IS prevádzkovateľa s periodicitou najmenej raz ročne.

6.1 Narušenie personálnej bezpečnosti

- strata, vyzradenie, alebo krádež hesiel pre vstup do IS – môže dôjsť k narušeniu integrity, alebo zneužitiu dátového záznamu z IS
    - zmeniť všetky prihlasovacie heslá do IS a to aj administrátorské
    - vykonať poučenie osôb o ochrane a utajení hesiel pre vstup do IS
    - vykonať disciplinárne opatrenie, ak sa jednoznačne zistí, že išlo o poskytnutie autorizácie pre vstup, neoprávnenej osobe osobou oprávnenou
- oprávnený vstup neoprávnenej osoby – môže dôjsť k narušeniu integrity alebo zneužitiu osobných údajov
    - zmeniť všetky prihlasovacie heslá do IS a to aj administrátorské
    - vykonať poučenie osôb o ochrane a utajení hesiel pre vstup do IS
    - vykonať disciplinárne opatrenie, ak sa jednoznačne zistí, že išlo o poskytnutie autorizácie pre vstup, neoprávnenej osobe osobou oprávnenou

6.2 Narušenie fyzickej bezpečnosti

- Narušenie dverí, okien
    - preventívne opatrenia:
        - pravidelne sledovať funkčnosť
    - postup pre zabezpečenie stavu obnovy:
        - neodkladne zabezpečiť opravu,
        - hľadať príčinu a odstrániť.
- Narušenie monitorovaného objektu
    - preventívne opatrenia:
        - pravidelne sledovať funkčnosť,
    - postup pre zabezpečenie stavu obnovy:
        - hľadať a eliminovať príčinu narušenia.
- Krádež záznamového zariadenia/počítača – môže dôjsť k zneužitiu osobných údajov
    - zabezpečiť miesto, kde je uložený počítač proti opätovnému odcudzeniu – napr. inštalovaním doplnkových mechanických zábran,
    - zakúpiť nový počítač s vyššími bezpečnostnými prvkami, inštalovať systém a obnoviť dáta zo záloh,
    - zabezpečiť ukladanie archivovaných údajov v kryptovanom tvare.

- Krádež, alebo strata kľúčov – môže dôjsť k neoprávnenému vstupu do miestností s aktívami IS a odcudzeniu osobných údajov, prípadne počítačov s osobnými údajmi
    - okamžite vymeniť zámky, prípadne doplniť bezpečnostné ochrany IS – napr. inštalovaním doplnkových mechanických zábran.

- Strata záložných médií – môže dôjsť k zneužitiu osobných údajov
    - zabezpečiť zálohu údajov v kryptovanom tvare s prístupom cez heslo.
- Krádež záložných médií – môže dôjsť k zneužitiu osobných údajov
    - zabezpečiť miesto, kde sú uložené média, proti opätovnému odcudzeniu – napr. inštalovaním doplnkových mechanických zábran,
    - zabezpečiť zálohu údajov v kryptovanom tvare s prístupom cez heslo.

6.3 Narušenie technicko-softvérovej bezpečnosti

- Havárie IS spôsobené technickou chybou niektorého komponentu centrálneho počítača – serveru
    - preventívne opatrenia:
        - zabezpečiť záložné zdroje s automatickým vypnutím,
        - monitorovať činnosť severov, kontrolovať chybové hlásenia,
        - zabezpečiť dostatok finančných prostriedkov na obnovu IS, podľa možnosti obmieňať sever každé tri roky,
        - zachovávať pravidlo – novší server sa stáva hlavným a starší záložným
    - postup na zabezpečenie stavu obnovy:
        - pri zálohovacom zariadení presmerovať prevádzku na záložné zálohovacie zariadenie/PC,
        - obnoviť nastavenie zo zálohy,
        - presmerovať aplikácie a užívateľov na záložný server,
        - odstrániť poruchu na hlavnom serveri,
        - po odstránení poruchy presmerovať prevádzku na hlavný server.
- Vírusová infiltrácia – môže dôjsť k narušeniu integrity alebo straty a zneužitiu dát s osobnými údajmi
    - preventívne opatrenia:
        - zabezpečiť antivírovú ochranu,
        - inštalovať len autorizované programy oprávnenými zamestnancami,
        - preverovať cudzie nosiče (FD, CD, ROM, USB...),
        - nepripájať nepreverené PC bez vedomia admin do LAN,
        - nepoužívané pasívne rozvody odpojiť od aktívnych prvkov LAN,
        - neotvárať nevyžiadané e-mailové prílohy,
        - sledovať aktuálne dianie na LAN a v sieti internet,
    - postup na zabezpečenie stavu obnovy:
        - odpojiť každého užívateľa,
        - okamžite skontrolovať aktualizácie antivírového programu, prípadne inštalovať aktualizácie, alebo zakúpiť kvalitnejší (z hľadiska bezpečnosti) antivírový program,
        - skontrolovať všetky počítače zapojené do spoločnej LAN siete aktualizovaným antivírovým programom,
        - detekovať spôsob narušenia,
        - odstrániť príčiny,
        - opraviť narušenú funkčnosť,
        - opätovne skontrolovať systém antivírovým programom,
        - prekontrolovať všetky PC,
        - nájsť zdroj infiltrácie a zabezpečiť jeho eliminovanie,
        - znovu spustiť systém a pripojiť užívateľov,
        - inštalovať doplnkové programy uvedené v bode 4.2.4, ktoré eliminujú možnosť napadnutia počítača.

- Neautorizovaný vstup z internetu – môže dôjsť k narušeniu integrity, odcudzeniu alebo strate a zneužitiu dát s osobnými údajmi
    - preventívne opatrenia:
        - nespúšťať programy z prostredia internetu nepodpísané certifikačnou autoritou,
        - nesťahovať neautorizované programy z prostredia internetu,
    - postup na zabezpečenie stavu obnovy.
        - skontrolovať log súborov firewallu, routerov, antivírového programu a pod. a vyhodnotiť ich,
        - zabezpečiť súborovú integritu OS a obnovu poškodených alebo infiltrovaných údajov zo záloh,
        - zvýšiť bezpečnosť firewallov,
        - nastaviť kryptované prenosy v LAN sieti,
        - pokiaľ existuje prístup z internetu do lokálnej siete, je nutné, aby bol vytvorený iba kryptovaným prenosom minimálne cez protokol SSH a nepoužívalo sa pre autorizáciu a vstupov meno a heslo, ale privátne a verejné kľúče v minimálnej dĺžke 512 bite, optimálne 1024 bite,
        - inštalovať doplnkové programy uvedené v bode 4.2.4, ktoré eliminujú možnosť napadnutia počítača z internetu.
- Technické narušenie, alebo zlyhanie bezpečnosti zariadenia v IS
    - pamäť počítača – môže dôjsť k narušeniu integrity alebo strate dát (v prípade vykazovania podozrivého správanie je nutná výmena),
    - procesor - môže dôjsť k narušeniu integrity alebo strate dát (nutná výmena),
    - CD/DVD RW - môže dôjsť k narušeniu integrity zálohovaných dát alebo strate dát (v prípade, že sa zistí na záložnom CD/DVD médiu sú nečitateľné alebo inak znehodnotené informácie nutná výmena zálohovacieho zariadenia),
    - hard disk – tvorí najdôležitejšiu časť počítača a preto mu je potrebné venovať náležitú ochranu. Môže dôjsť k narušeniu integrity alebo strate dát (v prípade, že sa zistí, že na disku sú nečitateľné alebo inak znehodnotené údaje je nutná kontrola antivírusovým programom, prípadne výmena za nový a skopírovanie dát, ktoré neboli znehodnotené, alebo použiť dáta zo záloh),
    - wifi zariadenie – môže dôjsť k úniku informácií a neautorizovanému vstupu do systému (nutná rekonfigurácia hesiel a v prípade nefunkčnosti celková výmena a konfigurácia).
- Porucha napájania, strata dodávky elektrickej energie
    - preventívne opatrenia:
        - dôležité aktívne prvky siete je nutné chrániť záložnými zdrojmi elektrickej energie so stabilizátorom sieťového napätia,
    - postup na zabezpečenie stavu obnovy:
        - v čase výpadku sa musí záložný zdroj automaticky aktivovať,
        - pri dlhodobejšom výpadku sa server musí automaticky vypnúť (shutdown),
        - po nábehu el. energie je nutné server spustiť a skontrolovať.
- Porucha prostriedkov demilitarizovanej zóny
    - preventívne opatrenia:
        - monitorovať činnosť zariadení,

        - monitorovať funkčnosť všetkých zariadení,
        - zabezpečiť prístup len pre pracovníkov s oprávnením,
        - periodicky meniť administrátorské a užívateľské prístupy s heslami,
        - zabezpečiť antivírovú ochranu všetkých PC, ako aj e-mailového prístupu,
        - zabezpečiť programovú aktuálnosť,
        - zabezpečiť technickú aktuálnosť,
        - kontrolovať súbory zaznamenávajúce činnosť systému,
        - kontrolovať súbory,
    - v prípade narušenia:
        - odpojiť LAN od prostriedkov demilitarizovanej zóny
        - vyhľadať príčinu nefunkčnosti,
        - odstrániť príčinu výmenou častí, inštalovaním aktualizácií, výmenou celku,
        - preveriť prostriedky firewallu, prekladu adries (DNS) a proxy,
        - po otestovaní funkčnosti pripojiť LAN.
- Porucha aktívnych prvkov IS/siete
    - preventívne opatrenia:
        - monitorovať činnosť,
        - zabezpečiť dostatočnú kapacitu,
        - pripájať ich prostredníctvom záložného zdroja,
        - zabezpečiť dostatočnú ochranu pred nepovolaným prístupom.
    - postup na zabezpečenie stavu obnovy:
        - vymeniť nefunkčnú časť.
- Porucha pasívnej časti siete
    - preventívne opatrenia:
        - premerať a kontrolovať kabeláž, zásuvky a konektory,
- postup na zabezpečenie stavu obnovy:
    - opraviť, prípadne vymeniť chybnú časť.
- Havária databáz
    - preventívne opatrenia:
        - sledovať konfiguračné súbory,
        - monitorovať hlásenia programov a včas na ne reagovať,
        - denne kontrolovať chybové hlásenia aplikácie a databázy,
    - postup na zabezpečenie stavu obnovy:
        - po odstránení nedostatkov a kontrole spätne inštalovať databázu zo zálohy.
- Havária aplikácie
    - preventívne opatrenia:
        - sledovať hlásenia aplikácie a zaznamenávať postrehy užívateľov,
        - sledovať konfiguračné súbory,
        - monitorovať hlásenia a včas na ne reagovať,
        - denne kontrolovať chybové hlásenia aplikácie,
    - postup na zabezpečenie stavu obnovy:
        - preinštalovať aplikáciu,
        - nainštalovať novšiu verziu aplikácie,
        - konzultovať chyby s dodávateľom.
- Porucha pracovných staníc
    - preventívne opatrenia:

- používať len autorizované programy,
- inštalovať antivírové programy,
- inštalovať nové programy smie len poverený zamestnanec,
- nezasahovať do konfiguračných súborov,
- chybové hlásenia hlásiť správcovi systému,
- zálohovať dáta na určené média,
- za zálohy, prevádzku a bezpečnosť zodpovedá zamestnanec.

- postup pre zabezpečenie stavu obnovy:
  - technická chyba – zabezpečiť opravu nefunkčnej časti,
  - softvérová chyba – identifikovať príčinu, obnoviť súbory zo zálohy, preinštalovať OS, aktualizovať antivírovú ochranu.

6.4 Mimoriadne udalosti spôsobené vplyvom zvyškových rizík

- preventívne opatrenia:
  - zabezpečiť niekoľkonásobné záložné kópie,
  - zhotovenie havarijných plánov na zabezpečenie kontinuity činnosti,
  - kontrolovať, či sú splnené protipožiarne opatrenia,
  - kontrolovať osoby pri vstupe do budovy,
  - vo vybraných priestoroch inštalovať EZS, bezpečnostné mreže, dvere,
  - zabezpečiť autentizáciu osôb pri vstupe do chránených priestorov,
- v prípade vyradenia IS z činnosti:
  - zvolať krízový štáb,
  - koordinovať činnosť podľa havarijných smerníc,
  - aktivovať záložné pracovisko,
  - skontrolovať úplnosť systému na záložnom pracovisku,
  - spustiť záložnú prevádzku,
  - odstrániť škody na pôvodnom pracovisku,
  - po obnovení funkčnosti vrátiť činnosti na pôvodné pracovisko,
- v prípade napadnutia len časti IS:
  - presunúť aktíva do vyhovujúcich priestorov,
  - inštalovať záložné databázy a pripojenia ak sú nutné,
  - spustiť prevádzku,
  - po odstránení dôsledkov vrátiť činnosť do stavu pred udalosťou.

7. Kontrolná činnosť

Kontrolné činnosti sú zamerané na dodržiavanie bezpečnosti IS. Štandardom pre periodické hodnotenie zraniteľnosti je pravidelné hodnotenie slabých miest a ohrození IS prevádzkovateľa identifikovaných podľa bezpečnostnej politiky prevádzkovateľa s periodicitou najmenej raz ročne. Kontroly spravidla vykonáva zodpovedná osoba prevádzkovateľa, pokiaľ nie je vymenovaná, konateľ prevádzkovateľa s vyhotovením písomných záznamov o zistených skutočnostiach, nedostatkoch a opatreniach prijatých na ich odstránenie.

Prevádzkovateľ a sprostredkovateľ IS sú povinní umožniť kontrolu Úradu na ochranu osobných údajov v zmysle ustanovení § 56 ods. e) zákona č. 122/2013 Z. z., vstupom do IS do úrovne správcu systému, v rozsahu potrebnom na vykonanie kontroly.

Štandardom pre kontrolný mechanizmus riadenia informačnej bezpečnosti je:
- dodržiavanie bezpečnostnej politiky prevádzkovateľa a zabezpečenie a vykonávanie vnútornej kontroly alebo auditu informačnej bezpečnosti,
- zabezpečenie archivácie, ochrany a vyhodnocovania auditných správ,
- spôsob, forma a periodicita výkonu kontrolných činností.

7.1 Kontrola dodržiavania bezpečnostných smerníc

- pred začatím používania IS, 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 prevádzkovateľovi, ak príslušný vedúci pracovník po upozornení bezodkladne nevykoná nápravu, oznámi to zodpovedná osoba úradu na ochranu osobných údajov,
- pri zistení porušenia zákona o ochrane osobných údajov sa okamžite pozastaví zálohovanie dátového záznamu 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,
- zodpovedná osoba musí vždy vykonať zápis pri zistení systémového nedostatku a pri porušení práv dotknutých osôb,
- pri porušení povinností oprávnených osôb sa postupuje v zmysle ZP,
- kontrolu dodržiavania bezpečnostných smerníc vykonáva zodpovedná osoba a to pravidelne, minimálne raz ročne,
- 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,
- o každej kontrole zodpovedná osoba musí vypracovať zápis do knihy kontrol bezpečnosti IS a musí obsahovať minimálne:
    - dátum a čas kontroly,
    - rozsah kontroly,
    - zistené nedostatky pri kontrole,
    - návrh protiopatrení,
    - zoznam osôb zodpovedných za vykonanie protiopatrení,
    - termín kontroly splnenia protiopatrení,

- záznam z kontroly zodpovedná osoba predloží prevádzkovateľovi IS,
- pri bezpečnostnej udalosti musí zodpovedná osoba vykonať mimoriadnu kontrolu a vypracovať zápis do knihy kontrol bezpečnosti IS,
- kontrola prevádzky automatizovaného IS sa prevádza nepretržite a to technickými a programovými prostriedkami. V pracovnej dobe sa prevádza denne povereným správcom siete,
- kontrola zabezpečenia miestností pred nedovoleným prístupom v pracovnej dobe ale i v mimopracovnom čase, je vykonávaná náhodne vedúcimi pracovníkmi zodpovednými za danú agendu.

8. Záznamy o revíziách

Č.	Popis zmeny / poznámky	Záznam: Meno Priezvisko	Dátum	Podpis
A0	Vytvorenie, úpravy a schválenie dokumentu	Vypracoval: Ing. Miroslav Ilavský	13.4.2015	
		Preveril: Ing. Ján Stajník	20.4.2015	
		Schválil: Doc. Milan Rašla	30.4.2015	
A1	Popis zmeny	Vypracoval:		
		Preveril:		
		Schválil:		
A2	...	Vypracoval:		
		Preveril:		
		Schválil:		
B3	Nové vydanie	Vypracoval:		
		Preveril:		
		Schválil:		