Inštitút teológie, misie a soc. práce, n. o.;
IČO: 45737614

Bezpečnostná smernica
na ochranu osobných údajov

Bezpečnostná smernica vypracovaná na základe Zákona č. 122/2013 Z. z. o ochrane osobných údajov v znení neskorších predpisov.

Vypracoval a schválil: Mgr. Daniela Masariková
Smernica sa vzťahuje na právnu formu a fyzické objekty:
Inštitút teológie, misie a soc. práce, n. o.; IČO: 45737614
Sídlo neziskovej organizácie: Tajov 216, 976 34 Tajov
Registrovaná prevádzka neziskovej organizácie: A. Bernoláka 18, 034 01 Ružomberok
Dátum: 24. 3. 2014

A. Úvodné ustanovenia

Účel a dôvod vydania

V v zmysle zákona NR SR č. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov bezpečnostná smernica Inštitútu teológie, misie a soc. práce, n. o. definuje minimálne technické, technologické, organizačné a personálne opatrenia na zabezpečenie bezpečnosti osobných údajov pred ich prípadným odcudzením, stratou, poškodením, neoprávneným prístupom, zmenou a rozširovaním.

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

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

Súvisiace predpisy

- Zákon NR SR č. 428/2002 Z.z. o ochrane osobných údajov v znení neskorších predpisov
- Zákon NR SR č. 215/2002 Z.z. o elektronickom podpise
- Zákon NR SR č. 261/1995 Z.z. o štátnom informačnom systéme
- Zákon NR SR č. 211/2000 Z.z. o slobodnom prístupe k informáciám
- Zákon NRSR č. 122/2013 Z.z. o ochrane osobných údajov
- Vyhláška Úradu na ochranu osobných údajov SR č. 164/2013

Bezpečnostný zámer

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

- Globálna
- Informačná
- Počítačová

Základné bezpečnostné ciele

Obsahujú formuláciu základných bezpečnostných cieľov.

1. Popis bezpečnostných opatrení a spôsob ich uplatňovania v konkrétnych podmienkach.
2. Rozsah oprávnení, popis povolených činností a spôsob identifikácie a autetizácie jednotlivých oprávnených osôb
3. Rozsah zodpovednosti oprávnených osôb.
4. Spôsob, formu a periodicitu výkonu kontrolných činností zameraných na dodržiavanie bezpečnostných opatrení,
5. Postupy pri haváriách, poruchách a iných mimoriadnych situáciách

6. Preventívne opatrenia na zníženie rizika vzniku mimoriadnych situácií
7. Možnosti efektívnej obnovy stavu pred haváriou, poruchou alebo inou mimoriadnou sit.

B. Popis bezpečnostných opatrení

Úrovne bezpečnosti

1. Globálna bezpečnosť

Patria sem všetky opatrenia slúžiace k zabezpečeniu všeobecnej bezpečnosti, pôsobiace na všetky druhy aktív. (objekty, dlhodobý hmotný a nehmotný majetok, zamestnanci, financie..)

Špecifikácia globálnych opatrení.

- Protipožiarne smernice, hlásiče
- Organizačné opatrenia
- Personálne opatrenia

2. Informačná a komunikačná bezpečnosť

Zahrňuje bezpečnostné opatrenia týkajúce sa informačného systému ako celku. K aktívam patria sieť LAN, dokumenty, komunikačné linky, mobilné telekomunikačné zariadenia.

3. Počítačová bezpečnosť.

Zahrňuje aktíva ako sú počítače, pamäťové médiá, operačné systémy, aplikácie, databázy.

Bezpečnostné opatrenia

Formulujú minimálne požadované bezpečnostné opatrenia. Bezpečnostná politika Bratskej jednoty baptistov je súhrn:

- organizačných
- technických
- personálnych

opatrení, ktoré zabezpečujú ochranu dôverných skutočností v jeho pôsobnosti .

1. Špecifikácia organizačných opatrení a spôsob ich využitia

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

Požiadavky na organizačné opatrenia.

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

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

Základnú normu tvoria zakladacia listina a štatút no. Riaditeľ neziskovej organizácie, ktorý je zodpovedný za vedenie neziskovej organizácie, zabezpečí kontinuitu činností v prípade narušenia informačného systému, mimoriadnej udalosti, živelnej pohromy a inej nepredvídanej situácie.

2. Špecifikácia technických opatrení a spôsob ich využitia

Technické opatrenia predstavujú všetky určené technické prostriedky (aktíva), určené pre spracúvanie, manipuláciu, archiváciu a skartáciu dôverných skutočností a všetky prostriedky a metódy ochrany určených technických prostriedkov. Používanie technických prostriedkov pre spracúvanie osobných informácii je povolené iba osobám oprávneným oboznamovať sa s osobnými informáciami.
Technické prostriedky, sú využívané zásadne zamestnancami alebo dobrovoľníkmi, ktorí majú tieto prostriedky pridelené. Osoba zodpovedná za informačnú techniku je riaditeľka neziskovej organizácie.

Technickými prostriedkami na účely zákona NR SR č. 428/2002 Z. z. sú :

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

a) Písaný text vyhotovený na mechanickom alebo elektrickom písacom stroji je originál. Kópie sa vytvárajú na rozmnožovacom stroji.
b) Tlačiarne sú periférne zariadenia výpočtovej techniky, na priame vytváranie tlačených dokumentov.

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

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

Aktíva určené pre spracovanie osobných informácii budú chránené pred porušením dôvernosti informácie, stratou integrity a zamedzeniu dostupnosti pred nepovolanými osobami a technickými prostriedkami, ktoré nie sú zaradené do bezpečnostného projektu.

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

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

programová metóda (P)

- antivírové programy (avast Free edition), vstupné a prihlasovacie heslá (je nimi chránený vstup do užívateľskej aj administratívnej časti IS), používanie iba autorizovaných programov , heslo BIOSu, heslo do aplikácie, heslo do siete

mechanická metóda (M)

- vybavenie budovy plnými dverami, ukladanie médií v ohňuvzdornej uzamykateľnej plechovej skrini

režimová metóda (R)

- určenie zodpovedných zamestnancov za bezpečnosť

- samotný informačný systém je umiestnený na serveri sprostredkovateľa (viď. zmluva), ktorý vykonáva ochranu zálohovaním, obnovou, vývojom a údržbou softvéru.

3. Špecifikácia personálnych opatrení a spôsob ich využitia

Personálne opatrenia -personálna bezpečnosť- je zákonom stanovený postup (§17 a §18 zákona NR SR č. 428/2002 Z.z.), ktorý určuje predpoklady k získaniu oprávnenia oboznamovať sa s osobnými údajmi a určuje povinnosti oprávnených osôb. Personálna bezpečnosť zahŕňa vedenie predpísanej evidencie na ochranu osobných údajov. Štatutárny zástupca písomne poverí výkonom dohľadu nad ochranou osobných údajov spracúvaných podľa zákona NR SR č. 428/2002 Z.z. zodpovednú osobu, ktorá dozerá na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov.

Požiadavky na personálne opatrenia

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

C. Bezpečnostné smernice

Bezpečnostné smernice upresňujú a aplikujú uvedené zákonné normy a vyhlášku na konkrétne podmienky prevádzkovaného informačného systému.

Pre zabezpečenie výkonu stanovených úloh a opatrení obsiahnutých v bezpečnostnom projekte vydáva riaditeľka neziskovej organizácie tieto bezpečnostné smernice.

Popis technických opatrení

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

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

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

programová metóda (P)

- antivírová ochrana
  - na každom počítači musí byť inštalovaná antivírová ochrana
  - denne musí byť zabezpečená kontrola aktualizácie antivírových knižníc
- vstupné a prihlasovacie heslá
  - každý užívateľ systému musí mať pridelené heslo, ktorým sa autentifikuje a toto heslo uchováva v tajnosti
  - vhodne zvolená doba životnosti a dĺžka hesla spolu s vynucovaním dostačujúcej zložitosti hesla dostatočne zabraňujú úspešným útokom zameraným na uhádnutie hesla
  - je zakázané vstupovať do systému pod cudzím užívateľským menom a heslom
  - tie isté opatrenia platia aj pre prístup k aplikáciám
- používanie programov
  - smú byť používané iba autorizované programy
  - aktualizácia programov, inštalácia bezpečnostných opráv (záplat)
  - inštaláciu softvéru (SW) smie vykonávať len osoba na to poverená
- ochrana PC pred nepovolaným prístupom
  - heslo BIOSu
- záloha systému
  - týždenne sa musia vytvárať kópie databáz
  - aplikačný softvér musí byť zálohovaný po každej aktulizacií

mechanická metóda (M)

- vstup do budovy je zabezpečený uzamykateľnými dverami, kancelárie sú vybavené plnými dverami, v prevádzkových priestoroch sa nachádza plechová uzamykateľná skrinka ktorá je ohňuvzdorná a slúži na uchovávanie nosičov dát.

režimová metóda (R)

- určenie režimu vstupu na pracoviská, určenie zodpovedných zamestnancov za bezpečnosť, určenie podmienok vstupu na pracovisko a spôsob opustenia pracoviska a pod.

- záložné kópie operačného systému, aplikačných programov a databáz je nutné uskladňovať mimo prevádzkovej budove, napríklad v sídle.
- dôležité administrátorské prístupy a heslá musia byť zdokumentované a uložené v zapečatenej obálke v uzamykateľnej skrinke
- architektúra LAN musí byť zdokumentovaná a uložená v uzamykateľnej skrinke

technická metóda (T)

- zabezpečenie pracoviska bezpečnostným signalizačným systémom
- zabezpečenie LAN pomocou technických zariadení pred nepovoleným prístupom z prostredia internetu
    - firewall na routeri

Popis organizačných opatrení

Organizačné opatrenie:

- V rámci organizačnej štruktúry
    - Spracovávať, zhromažďovať a rušiť osobné údaje smie len oprávnený pracovník. Spracovávanie údajov musí byť v súlade so zákonom NR SR č. 428/2002 Z.z. o ochrane osobných údajov.
- Rozdelenie kompetencií
    - V prípade mimoriadnej situácie, kedy dôjde k narušeniu bezpečnosti činnosti koordinuje a riadi všetky činnosti riaditeľka neziskovej organizácie.
    - Pri narušení počítačovej bezpečnosti koordinuje činnosti riaditeľka neziskovej organizácie (NO) so sprostredkovateľom IS a ostatnými oprávnenými osobami.
    - Pri narušení globálnej bezpečnosti koordinuje činnosti riaditeľka NO
    - Pri narušení informačnej bezpečnosti v oblasti IS a LAN koordinuje činnosti riaditeľka NO v spolupráci s osobou zodpovednou za IT
    - Pri narušení informačnej bezpečnosti v oblasti dokumentov, telefónnych a mobilných sietí koordinuje činnosti riaditeľka NO.
- Určenie pracovných a bezpečnostných postupov
    - Spracovávať, zhromažďovať a rušiť osobné údaje smú len zamestnanci na to určení. Spracovávanie údajov musí byť v súlade so zákonom NR SR č. 428/2002 Z.z. o ochrane osobných údajov. Zamestnanci sa musia riadiť všetkými prijatými opatreniami a nariadeniami vydanými riaditeľkou NO.

    .

Popis personálnych opatrení

Používanie technických prostriedkov pre spracúvanie osobných informácii je povolené iba osobám oprávneným oboznamovať sa s osobnými informáciami. Technické prostriedky, sú využívané zásadne zamestnancami, ktorí majú tieto prostriedky pridelené.

Oprávnené osoby preukázateľne poučia právnické osoby a fyzické osoby, ktoré majú alebo môžu mať prístup k ich informačnému systému, o právach a povinnostiach ustanovených zákonom NR SR č. 428/2002 Z.z. a o zodpovednosti za ich porušenie. Každá oprávnená

osoba je povinná zachovávať mlčanlivosť o osobných údajoch, ktoré spracúvajú. Povinnosť mlčanlivosti trvá aj po ukončení spracovania. Povinnosť mlčanlivosti nemajú, ak je to podľa osobitného zákona nevyhnutné na plnenie úloh orgánov činných v trestnom konaní. Oprávnená osoba je povinná zachovávať mlčanlivosť o osobných údajoch, s ktorými príde do styku; tie nesmie využiť ani pre osobnú potrebu a bez súhlasu prevádzkovateľa ich nesmie zverejniť a nikomu poskytnúť ani sprístupniť.

Povinnosť mlčanlivosti platí aj pre iné fyzické osoby, ktoré v rámci svojej činnosti (napr. údržba a servis technických prostriedkov) prídu do styku s osobnými údajmi. Povinnosť mlčanlivosti trvá aj po zániku funkcie oprávnenej osoby alebo po skončení jej pracovného pomeru alebo obdobného pracovného vzťahu.

Riaditeľka NO vedie evidenciu osôb prichádzajúcich do styku s osobnými údajmi. Každú takúto osobu poučí a vyhotoví o tom záznam.

Technické prostriedky, sú využívané zásadne zamestnancami, ktorí majú tieto prostriedky pridelené. Zamestnanci, ktorý majú pridelené technické prostriedky, sú zodpovední za ich správny chod a musia dodržiavať všetky zásady práce s nimi. Za informačný systém (počítačový) zodpovedá poverená osoba.

Požiadavky na personálne opatrenia

- kvalifikačné predpoklady
  - Spracovávať osobné údaje v informačnom systéme majú len osoby:
    - znalé práce na počítači
    - vyškolené pre prácu s aplikačným programom
    - ostatné oprávnené osoby smú spracovávať osobné údaje len dokumentačne
- Personálne zabezpečenie procesov
  - proces prevádzky IS zabezpečuje poverená osoba zodpovedná za IT
  - proces zadávania údajov zabezpečuje riaditeľka NO
  - proces archivácie zabezpečuje taktiež riaditeľka NO
- Personálna bezpečnosť
  - zamestnanci musia byť poučení
  - každý zamestnanec je povinný zachovávať mlčanlivosť

- Zabezpečenie dodržiavania bezpečnostných smerníc
  - zamestnanci musia byť oboznámení s bezpečnostnými smernicami
  - nový zamestnanec musí byť pri prijímaní do zamestnania riadne poučený

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

Rozsah oprávnení

Rozsah oprávnení a popis povolených činností jednotlivých oprávnených osôb, spôsob ich identifikácie a autentizácie pri prístupe k informačnému systému.
Každý zamestnanec, ktorý pristupuje k osobným údajom, je uvedený v zozname osôb oprávnených s oboznamovaním sa s osobnými údajmi,.
.

D. Rozsah zodpovednosti oprávnených osôb

Rozsah zodpovednosti oprávnených osôb a osoby zodpovednej za dohľad nad ochranou osobných údajov (§ 19).

1. Osoby oprávnené spracovávať osobné údaje
    a. sú zodpovedné za komplexné, pravdivé, aktuálne údaje a vkladanie týchto údajov do IS
    b. sú zodpovedné za uchovávanie, ochranu a manipuláciu s nimi v prípade, že tieto údaje sú v textovej forme
    c. sú zodpovedné za preukázateľnosť súhlasu na spracovanie osobného údaju, a to tak, že možno o ňom podať dôkaz (§7 zákona NR SR č. 428/2002 Z.z.)
    d. sú zodpovedné za poriadok na pracovisku a odložnie všetkých písomností obsahujúce osobné údaje a iných dokumentov, ktoré by mohli viesť k slobodnému prístupu k osobným údajom, do uzamykateľných odkladacích skriniek, resp. skríň

    e. sú povinné včas informovať osobu zodpovednú za dohľad nad ochranou osobných údajov o pripravovanom začatí spracovania osobných údajov a o všetkých skutočnostiach, ktoré by mohli viesť k zneužitiu týchto údajov

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

3. Osoby zodpovedné za dohľad nad ochranou osobných údajov (§ 19)
    a. zodpovedajú za dozeranie na dodržiavanie zákonných ustanovení pri spracovávaní osobných údajov
    b. posúdia pred začatím spracúvania osobných údajov v informačnom systéme, či ich spracovávaním nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb. Zistenie narušenia práv a slobôd dotknutých osôb pred začatím spracovávania alebo porušenia zákonných ustanovení v priebehu spracovávania osobných údajov zodpovedná osoba bezodkladne písomne oznámi riaditeľke NO, ak prevádzkovateľ po upozornení bezodkladne nevykoná nápravu, oznámi to zodpovedná osoba úradu na ochranu osobných údajov
    c. kontrolujú zásady spracovávania osobných údajov a vyhotovujú o tom písomný záznam

E. Kontrolné činnosti zamerané na dodržiavanie bezpečnosti informačného systému

Spôsob, forma a periodicita výkonu kontrolných činností.

Pred začatím spracovávania osobných údajov v informačnom systéme, osoba zodpovedná za dohľad nad ochranou osobných údajov preverí, či ich spracovávaním nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb. Zistenie narušenia práv a slobôd dotknutých osôb pred začatím spracovávania alebo porušenia zákonných ustanovení v priebehu spracovávania osobných údajov zodpovedná osoba bezodkladne písomne oznámi riaditeľke NO.. Ak príslušný vedúci pracovník po upozornení bezodkladne nevykoná nápravu, oznámi to zodpovedná osoba úradu na ochranu osobných údajov.

Kontrolujú sa zásady spracovávania osobných údajov a vyhotovujú o tom písomný záznam.

Zásady spracovávania osobných údajov sa kontrolujú minimálne raz za rok.

Kontrola prevádzky automatizovaného IS sa vykonáva mesačne a to technickými a programovými prostriedkami. .

F. Postupy pri haváriách, poruchách a iných mimoriadnych situáciách

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

Popis havárie	**Návrh preventívnych opatrení**	**Postupy na zabezpečenie stavu obnovy**
1. Havárie IS spôsobené technickou chybou niektorého komponentu centrálneho počítača -	○ zabezpečiť dostatok finančných prostriedkov na obnovu IS	
2. Porucha aktívnych prvkov siete	• Monitorovať činnosť, používať menežovateľné aktívne prvky. • Zabezpečiť dostatočnú kapacitu. • Zabezpečiť dostatočnú ochranu pred nepovolaným prístupom.	Vymeniť chybnú časť
3 Porucha v pasívnej časti siete	• Premeranie kabeláže, zásuviek a konektorov	Opraviť, prípadne vymeniť chybnú časť.
4 Havária aplikácie	• Sledovať hlásenia aplikácie a zaznamenávať postrehy užívateľov • Monitorovať hlásenia a včas na ne reagovať • Denne kontrolovať chybové hlásenia aplikácie a databázy	Nainštalovať novšiu verziu aplikácie. Konzultovať chyby s dodávateľom.

5. Porucha pracovných staníc	• Používať len autentizované programy • Inštalovať antivírové programy • Inštalovať nové programy smie len poverený pracovník • Užívatelia nesmú zasahovať do konfiguračných súborov • Chybové hlásenia sú povinný hlásiť • Zálohovať dáta na externé preverené médiá. • Za zálohy, prevádzku a bezpečnosť zodpovedá poverená osoba	Technická chyba: Zabezpečiť opravu vadnej časti. Softvérová chyba: Identifikovať príčinu Obnoviť súbory zo zálohy, alebo preinštalovať operačný systém. Aktualizovať antivírovú ochranu.
6 Narušenie dverí, okien	• Pravidelne sledovať funkčnosť	Neodkladne zabezpečiť opravu.

G. Záverečné ustanovenia

1. Bezpečnostná smernica predkladá spôsoby riešenia pre všetky úrovne zabezpečenia spolu s popisom bezpečnostných opatrení.
2. Bezpečnostnú smernicu je z týchto dôvodov potrebné považovať za dôverný dokument, ktorého obsah je nevyhnutné chrániť pred neoprávneným prístupom rovnako ako najcitlivejšie osobné údaje spracúvané v IS.
3. Sprístupnenie tohto obsahu neoprávneným osobám a nepovolaným osobám môže mať za následok eliminovanie bezpečnostných mechanizmov informačného systému a ohrozenie jeho dôvernosti. Z uvedených dôvodov Inštitút teológie, misie a soc. práce, n. o. stanovuje, že s obsahom tohto bezpečnostného projektu sa môže okrem spracovateľa oboznámiť len oprávnená osoba.
4. V prípade vyžiadania si osobných údajov zo strany kontrolnej komisie je potrebné písomné potvrdenie kontrolnej komisie o prevzatí a vrátení osobných údajov. Kontrolná komisia musí byť poučená v zmysle zákona č. 428/2002 Z .z. o povinnosti mlčanlivosti a zodpovednosti za to, aby jej poskytnuté osobné údaje nemohli byť známe inej nepovolanej osobe alebo takouto osobou zneužité, so stanovením zodpovednosti za následky úniku osobných údajov, ktoré im boli poskytnuté.

Mgr. Daniela Masariková
20. 3. 2014