ActiveNet,s.r.o.
Škultétyho 1, 831 03 Bratislava

B E Z P E Č N O S T N Ý P R O J E K T
I N F O R M A Č N Ý C H S Y S T É M O V
podľa zákona č. 122/2013 Z. z. o ochrane osobných údajov

Vypracoval: Ladislav Šipeky, PhD.
Posledná aktualizácia:02.09.2022
Podpis:

Schválil: Mgr. Ivan Škultéty
Dátum: 03.09.2022
Podpis:

1 ÚČEL A DÔVOD ZOSTAVENIA BEZPEČNOSTNÉHO PROJEKTU

Účelom Bezpečnostného projektu je zabezpečiť ochranu osobných údajov v podmienkach spoločnosti ActiveNet, s.r.o. so sídlom na ulici Škultétyho 1, 831 03 Bratislava.

V súlade so zákonom č. 122/2013 Z.z. o ochrane osobných údajov v znení neskorších predpisov tento bezpečnostný projekt definuje minimálne technické, technologické, organizačné a personálne opatrenia na zabezpečenie bezpečnosti osobných údajov pred ich prípadným odcudzením, stratou, poškodením, neoprávneným prístupom, zmenou a rozširovaním.

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

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

K zabezpečeniu bezpečnostného projektu je potrebné prijať opatrenia k stanoveniu pravidiel vstupu do objektu, príchodového a odchodového režimu na pracovisko, stanovenia spôsobu udeľovania a rušenia prístupov do informačných systémov, rozsahu údajov potrebných pre jednotlivé kategórie a o ochrane údajov v informačných systémoch. K tomuto účelu sú spracované smernice, ktoré sú súčasťou tohto bezpečnostného projektu a bezpečnostné opatrenia na ochranu osobných údajov.

2 ZÁMER BEZPEČNOSTNÉHO PROJEKTU

Zámerom bezpečnostného projektu je stanovenie citlivých a rizikových faktorov v rámci IS, kde by mohlo dôjsť k úniku informácií z IS. Takýmito rizikovými oblasťami sú:

- zabránenie získavania osobných údajov nad rozsah, ako to vyžaduje účel, na ktorý sú získavané,
- zabezpečenie fyzickej a automatizovanej ochrany kritických miest a rizikových oblastí informačného systému, ktorými sú:
    - získavanie osobných údajov
    - manipulácia s nimi a ich spracovávanie,
    - prenos dát z IS, ich kopírovanie a používanie osobných údajov v rámci výkonu činnosti spoločnosti,
    - úschova a likvidácia osobných údajov po skončení účelu, na ktoré boli získané.

3 DEFINÍCIA POJMOV

- **systém ochrany osobných údajov** - je súhrn prostriedkov, metód, činností opatrení a zariadení, ktoré vo svojom komplexe pôsobia k zamedzeniu úniku osobných údajov alebo ich vyzradeniu, zneužitiu pred nepovolanými osobami,
- **aktíva** - sú hmotné a nehmotné objekty, ktoré sú súčasťou chráneného systému, pričom ich narušením dochádza k strate dôvernosti, dostupnosti a integrity, alebo až k strate predmetu ochrany,
- **bezpečnostná politika** - je súhrn zákonov, predpisov, nariadení a pravidiel, podľa ktorých sa chráni, distribuuje a riadi prístup k informáciám. Bezpečnostná politika stanovuje spôsob a vykonáva opatrenia pre ochranu skutočností. Pre vzťah medzi subjektom a objektom predstavuje súhrn pravidiel, predpisov a nariadení, podľa ktorých určuje vzájomné pôsobenie. Súčasťou bezpečnostnej politiky je i personálna bezpečnosť,
- **osobný údaj** - osobnými údajmi sú údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, pričom takou osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu a ich význam treba chrániť pred zneužitím, poškodením, zničením, stratou alebo odcudzením,
- **objekt** - je pasívna časť", ktorá prijíma, spracúva, prenáša, ukladá informáciu. Prístup k objektu znamená oboznamovanie sa s informáciami, ktoré obsahuje. Objekt môže byť sektor na disku, záznam na magnetofónovej páske, časť operačnej pamäti, externé nosiče informácií,
- **subjekt** - je aktívna časť. Môže ňou byt' osoba, proces ,zariadenie, ktoré zabezpečuje tok informácií medzi objektmi a spôsobuje zmenu stavu systému,
- **zdroj** -je čas, informácie, objekty alebo procesy, ktoré sú použité alebo spotrebované pri spracovaní informácii,
- **dôveryhodný výpočtový systém** - je systém, ktorého organizačné, technické a programové vybavenie a bezpečnostné opatrenia sú na takej úrovni, že dovoľuje bezpečne pracovať s informáciami,
- **chránený systém** -je tvorený jednotlivými objektmi, pre ktoré je definovaný určitý stupeň ochrany,
- **elektronická zabezpečovacia signalizácia** - je systém elektronických prostriedkov určených k fyzickej ochrane a technickej ochrane určených priestorov a aktív pred nepovolaným vniknutím, narušením, požiarom a iným vplyvom, ktoré môžu spôsobiť poruchu systému,
- **elektronická požiarna signalizácia** - je systém elektronických prostriedkov určených k ochrane priestorov a aktív pred požiarom,
- **zadávateľ úlohy** - je orgán alebo organizácia, ktorá podľa platných predpisov požaduje

spracovanie informácii, obsahujúce osobné údaje, pomocou technických prostriedkov,

- **užívateľ** - je orgán alebo organizácia, ktorá využíva informácie z výsledkov spracovania pre vlastnú odbornú činnosť a riadenie. Táto organizácia zodpovedá za vydanie a dodržiavanie smerníc, režimových opatrení, pre ochranu osobných údajov subjektmi. Užívateľom je osoba ktorá je v priamej interakcii s technickými prostriedkami,
- **riešiteľ** - je subjekt, ktorý spracúva projektovú úlohu. Spracovateľom môže byt' právnická alebo fyzická osoba, ktorá na zmluvnom základe vypracúva bezpečnostnú, programovú, projektovú a prevádzkovú dokumentáciu k ochrane osobných údajov,
- **bezpečnostný pracovník** - je subjekt určený vedúcim organizácie k obhospodarovaniu prevádzkových systémov určených pre ochranu a spracúvanie osobných informácii. Vykonáva kontroly v oblasti dodržiavania zásad manipulácie, ukladania, spracovania, prenášania a archivovania osobných informácii,
- **kontrolný záznam (audit)** - je súbor údajov, ktoré poskytujú prehľad o činnosti a aktivitách subjektu na technických prostriedkoch,
- **dôvernosť** -je súhrn opatrení k ochrane aktíva pred nepovolaným prístupom,
- **integrita** - je charakteristika systému z hľadiska presnosti a komplexnosti zabezpečenia informácii a zabezpečenia programového vybavenia,
- **dostupnosť** - je charakteristika systému z hľadiska oprávneného prístupu k utajovaným informáciám.

4 ROZSAH BEZPEČNOSTNÝCH OPATRENÍ

1. Bezpečnostné opatrenia v oblasti fyzickej ochrany osobných údajov v informačnom systéme v manuálnej (písomnej) podobe,
2. bezpečnostné opatrenia v oblasti fyzickej a automatizovanej ochrany osobných údajov v informačnom systéme v automatizovanej, t. j. elektronickej podobe, zabezpečenie PC, bezpečnosť HW a SW,
3. organizačné a personálne opatrenia na ochranu osobných údajov,
4. rozsah tohto bezpečnostného projektu je zameraný na zabezpečenie nevyhnutnej bezpečnosti informačného systému proti možnému útoku zo strany interných a externých osôb, a to na jeho:
   - **dôvernosť** (ochrana pred neoprávneným prístupom nepovolaných osôb – hackerov, vlamačov, počítačových vírusov, neoprávneného rozmnožovania a pod.),
   - **integritu** (ochrana proti poškodeniu, zmene, vymazaniu a zničeniu) a
   - **dostupnosť** (ochrana proti výpadkom napájania a iným havarijným stavom).

5 INFORMAČNÉ SYSTÉMY

Prevádzkovateľ používa na svoju činnosť:

a) Automatizovaný informačný systém (ďalej: ”AIS”) - prostriedky výpočtovej techniky obsahujúce údaje uložené na pamäťových nosičoch.

b) Dokumentárny informačný systém (ďalej: ”DIS”) - manuálne alebo výpočtovou technikou vytvorené písomnosti a listiny používané na spracúvanie osobných údajov.

5.1. Rozdelenie informačných systémov

- **IS ÚČTOVNÉ DOKLADY (spracovanie účtovných dokladov)** súbor všetkých písomných a elektronických informácii týkajúcich sa spracovania účtovných dokladov v zákonom stanovenom rozsahu
    - údajov, zákonníkom práce, občianskym zákonníkom a i.
- **IS MZDY A PERSONALISTIKA (personálna a mzdová agenda)** súbor všetkých písomných a elektronických informácii týkajúcich sa údajov o zamestnancoch, ktorý obsahuje:
    - vedenie personálnej a mzdovej agendy zamestnancov prevádzkovateľa pre účely pracovnoprávne, mzdové a pre účely zdravotného a sociálneho poistenia, starobného dôchodkového sporenia a dane z príjmov zo závislej činnosti fyzických osôb zamestnancov prevádzkovateľa v pracovnom pomere a pre osoby pracujúce pre prevádzkovateľa na základ dohôd o prácach vykonávaných mimo pracovného pomeru v zmysle Zákonníka práce.

5.2. Zoznam osobných údajov spracúvaných v informačných systémoch

V IS ÚČTOVNÉ DOKLADY osobné údaje bez osobitných kategórií:

- meno, priezvisko a titul, číslo občianskeho preukazu, alebo pasu, IČO, ak sa jedná o fyzickú osobu - podnikateľa, číslo účtu, kontakty /telefón, e-mail, skype a pod.../, kontaktné adresy, DIČ a IČ DPH ak sa jedná o právnickú osobu.

V IS MZDY A PERSONALISTIKA aj osobitné kategórie osobných údajov a to hlavne z dôvodu evidencie rodných čísel.

- U zamestnancov (aj bývalých) sa spracovávajú údaje:
    - meno, priezvisko a titul, národnosť, štátna príslušnosť, dátum a miesto narodenia, rodné číslo, kontakty /telefón, e-mail, skype a pod.../, kontaktné adresy, výpisy z registra trestov, informácie

o poistení a čísla bankových účtov, informácie o odborárskej príslušnosti, informácie o vykonanej práci a mzde, vybrané informácie o zdravotnom stave – register úrazov, potvrdenie o zdravotnej spôsobilosti na prácu, oznámenia o lek. ošetreniach a o PN, osobný dotazník

- rodinných príslušníkoch zamestnancov sa spracovávajú údaje:
  - meno, priezvisko a titul, národnosť, dátum a miesto narodenia, kontakty /telefón, eMail, skype a pod.../, kontaktné adresy, rodné číslo*, informácie o príjme (pre potreby soc. dávok)
- uchádzačoch o zamestnanie sa spracovávajú údaje:
  - meno, priezvisko a titul, národnosť, dátum a miesto narodenia, kontakty /telefón, eMail, skype a pod.../, životopis /CV/, kontaktné adresy

5.3. Účel spracúvania osobných údajov

Tieto údaje prevádzkovateľ spracováva v aplikačnom softvéri a v dokumentoch za účelom:

- vedenia účtovníctva
- vedenia personálnej a mzdovej agendy zamestnancov
- archivovania dokumentácie v elektronickej podobe
- bezpečnosť a ochrana majetku prevádzkovateľa
- vypracovania štatistík a rôznych reportov slúžiacich pre manažment a externých používateľov informácií (banky, Daňové úrady, obchodných partnerov, atď.)

Pre informačný systém personálna a mzdová agenda (IS MZDY A PERSONALISTIKA) Vedenie personálnej a mzdovej agendy zamestnancov prevádzkovateľa pre účely pracovnoprávne, mzdové a pre účely zdravotného a sociálneho poistenia, starobného dôchodkového sporenia a doplnkového dôchodkového sporenia (len ak spoločnosť má aj doplnkové dôchodkové zabezpečenie zamestnancov) a dane z príjmov zo závislej činnosti fyzických osôb zamestnancov prevádzkovateľa v pracovnom pomere a pre osoby pracujúce pre prevádzkovateľa na základe dohôd o prácach vykonávaných mimo pracovného pomeru v zmysle Zákonníka práce a evidencia zmlúv o výkone funkcie členov orgánov spoločnosti a vedenie agendy pre potreby ich odmeňovania za ich výkon funkcie člena orgánu spoločnosti podľa zmluvy o výkone funkcie.

Pre informačný systém účtovná a daňová agenda (ID ÚČTOVNÉ DOKLADY) Vedenie vecnej a správnej účtovnej a daňovej evidencie v súlade s platnými účtovnými a daňovými zákonmi, vedenie evidencie klientov.

5.4. Vymedzenie okolia informačného systému a jeho vzťah k možnému narušeniu bezpečnosti

Okolie AIS a DIS tvoria:

a) V prvom rade pracovníci zariadenia, ktorí môžu narušiť bezpečnosť IS či už z nedbanlivosti, alebo cielene. Tieto osoby musia byť poučené a musia si byť vedomé disciplinárneho a právneho postihu v prípade porušovania predpisov.

b) Servisní pracovníci zabezpečujúci údržbu a opravu techniky AIS a zariadení na úschovu dokumentov.

c) Osoby, ktoré zabezpečujú servis iných zariadení (servisní technici, zástupcovia a díleri firiem, obslužný personál budov). Tieto osoby sa nesmú zdržiavať v blízkosti IS v neprítomnosti oprávnených osôb.

d) Nepovolané osoby, ktoré môžu preniknúť k IS prostredníctvom vlámania sa do priestorov prevádzkovateľa.

e) Nepovolané osoby, ktoré sa môžu nedbalosťou obslužného personálu dostať do blízkosti IS.

f) V prípade prenosu údajov do domáceho počítača tvorí okolie IS aj rodiny pracovníkov, ktorí si údaje prenášajú.

g) Sprostredkovateľ, ktorý pre prevádzkovateľa spracúva niektoré agendy (napr. spracovanie mzdovej a personálnej agendy, spracovanie účtovnej agendy).

6 STUPEŇ BEZPEČNOSTI OSOBNÝCH ÚDAJOV PODĽA BEZPEČNOSTNÝCH ŠTANDARDOV

6.1. Základné bezpečnostné ciele a minimálne bezpečnostné opatrenia

Pri stanovení základných bezpečnostných cieľov a štandardov ochrany sme postupovali v prvom rade s prihliadnutím na v praxi overené riešenia, štandardy o ochrane informačných systémov.

Bezpečnostné ciele prevádzkovateľa sú:

a) zamedziť vstupu nepovolaných osôb do súkromných priestorov prevádzkovateľa,

b) minimalizovať riziká vzniku a šírenia požiaru, alebo zničenia údajov vplyvom živelnej pohromy,

c) ochrániť osobné údaje pred manipuláciou neoprávnenými osobami,

d) vytvoriť systém spracovania osobných údajov, ktorý zamedzí neprehľadnému a nekontrolovanému používaniu údajov, strate, odcudzeniu alebo zničeniu počas práce v DIS a AIS,

e) zabezpečiť ochranu osobných údajov pred neoprávneným šírením alebo zneužitím na iný účel, ako boli spracované.

6.2. Špecifikácia technických, organizačných a personálnych opatrení na zabezpečenie ochrany osobných údajov v informačnom systéme a spôsob ich využitia

Fyzická a objektová bezpečnosť

- Realizovať účinnú a nákladovo primeranú kombináciu uzamykania, ochrany a monitoringu vstupných dverí, priestorov a okien prevádzkovateľa.
- Monitorovací systém prístupu osôb do objektu je zabezpečený službou na vrátnici.
- Kancelárie v objekte, kde sa nachádzajú miesta uloženia komponentov IS v manuálnej a automatizovanej podobe sú zabezpečené mechanickými zábranami (zámky na dverách, uzamykateľná skriňa).
- Objekt, v ktorom sa nachádzajú komponenty IS, je z hľadiska požiarnej bezpečnosti vybavený zodpovedajúcimi hasiacimi prístrojmi, je spracovaný požiarny plán v zmysle zákona o ochrane pred požiarmi a spĺňa požiadavky týmto zákonom stanovené.

Bezpečnosť automatizovaného informačného systému (AIS), technických prostriedkov

- Používanie identifikátorov (hesiel, kariet) používateľa na prístup oprávnených osôb do AIS.
- Označovanie počítačových výstupov a nosičov osobných údajov.
- Použitie nepretržitých zdrojov napájania počítačov na zvýšenie stability systémov, ako aj na zníženie rizika poškodenia programov a počítačov pri kolísaní a výpadku elektrickej siete.
- Použitie antivírových programov na elimináciu poškodenia vplyvom počítačových vírusov.
- Použitie ochranných programov alebo zariadení, ktoré definujú prístupové práva k jednotlivým zdrojom počítačového systému, na zabránenie úniku a narušenia informácií z počítača.
- Zabezpečiť, aby aj pri krátkodobom opustení pracoviska bol AIS riadne ukončený a aby pre ďalšie pokračovanie práce bolo potrebné zadať prístupové heslo.
- Zabezpečiť, aby nepovolané osoby nemohli nazerať na osobné údaje zobrazované na obrazovke počítača.
- Použitie ochranných programov alebo zariadení proti prieniku nepovolaných osôb z iných sietí tzv. FireWall, ktorý napr. ochraňuje počítačový systém počas pripojenia do internetu proti cieleným a náhodným prístupom z prostredia internetu.
- Uzamknutie databázového servera v osobitnej skrini, alebo v samostatnej na to určenej miestnosti zvýši bezpečnosť IS proti odcudzeniu.

Personálna bezpečnosť

- Stanoviť zodpovednosť, povinnosti a práva prevádzkovateľa a zamestnancov vo vzťahu k AIS,

DIS a práci s osobnými údajmi.

- Zabezpečiť zachovávanie mlčanlivosti zamestnancov o spracovávaných osobných údajoch a skutočnostiach.
- Zabezpečiť poučenie pracovníkov o vybraných skutočnostiach vyplývajúcich z bezpečnostného projektu.
- Zabezpečiť informovanosť pracovníkov o práci s dokumentmi obsahujúcimi osobné údaje.
- Zaviesť pracovné postupy na ochranu dokumentov proti rizikám pri personálnych zmenách.
- Zabezpečiť stálu informovanosť pracovníkov o postupoch v prípade požiaru a dostupnosti protipožiarnych zariadení.

Administratívna bezpečnosť

- Stanoviť a uviesť do praxe pravidlá obehu dokladov obsahujúcich osobné údaje tak, aby sa minimalizovali možnosti straty, odcudzenia a šírenia informácií.
- Vybaviť prevádzkovateľa kancelárskymi pomôckami, používanie ktorých zvýši bezpečnosť manipulácie s písomnosťami.
- Organizačne zabezpečiť spracovanie dokumentov tak, aby za bežných okolností bol znemožnený prístup cudzích osôb k dokumentácii.
- Vytvoriť systém kontrolných postupov a mechanizmov, ktoré budú signalizovať narušenie ochrany písomností obsahujúcich osobné údaje.

6.3. Vymedzenie hraníc určujúcich množinu zvyškových rizík

Po uplatnení zásad a opatrení uvedených v bezpečnostných smerniciach zostanú nekryté nasledovné riziká:

a) odcudzenie alebo zničenie osobných údajov pri násilnom preniknutí cudzích osôb do priestorov prevádzkovateľa,

b) strata alebo odcudzenie údajov pri prenose alebo preprave,

c) úmyselné šírenie (rozmnožovanie, požičiavanie) osobných údajov oprávnenými osobami,

d) zničenie, alebo poškodenie písomností a počítačov vplyvom poruchy sieťových rozvodov

e) zničenie objektu prevádzkovateľa a v ňom uložených AIS a DIS požiarom, záplavou alebo inou živelnou pohromou.

7 ANALÝZA BEZPEČNOSTI INFORMAČNÉHO SYSTÉMU

7.1. Hodnotenie stavu bezpečnosti priestorov prevádzkovateľa

FYZICKÉ A ORGANIZAČNÉ PARAMETRE SPOLOČNOSTI ActiveNet, s.r.o. (ďalej len

prevádzkovateľ)

ActiveNet, s.r.o. je spoločnosť, ktorej hlavným zameraním je poskytovanie služieb v oblasti informačných technológií. Prevádzkovateľ vykonáva svoju podnikateľskú činnosť v prenajatých priestoroch budovy Dom Techniky spoločnosti Trnavské Mýto, a.s., na ulici Škultétyho 1, 831 03 Bratislava. Priestory sú vo vlastníctve spoločnosti Trnavské Mýto, a.s. Priestory kancelárie (2 miestnosti) sú umiestnené na 2. nadzemnom podlaží. Priestory serverovne (1 miestnosť) sú umiestnené v suteréne.

Prevádzkovateľ vykonáva svoju podnikateľskú činnosť v prenajatých priestoroch budovy JMF Dom odborov na adrese Trnavské Mýto 1, 831 04 Bratislava- Nové Mesto. Priestory sú vo vlastníctve Jednotného majetkového fondu zväzov odborových organizácií v Slovenskej republike. Priestory serverovne (1 miestnosť) sú umiestnené v suteréne.

Vchod do oboch budov a následný vstup do priestorov spoločnosti ActiveNet, s.r.o. je realizovaný cez recepciu s použitím výťahov resp. schodiska. Priestory sú zabezpečené bezpečnostnými dverami. Zároveň je celý vonkajší priestor monitorovaný kamerovým systémov prenajímateľa.

Z pohľadu fyzickej odolnosti priestorov sa jedná o štandardne zabezpečený priestor.

Štruktúra pracovníkov zariadenia je nasledovná:

Konateľ spoločnosti:	1
Administratívny pracovníci:	2
Programátor	2
Počet oprávnených osôb, ktoré pracujú s AIS a osobnými údajmi	4

AUTOMATIZOVANÝ INFORMAČNÝ SYSTÉM

Spoločnosť neuskutočňuje cezhraničný prenos osobných údajov.

Zoznam využívaných automatizovaných IS /AIS/			
Názov IS	**Ochrana heslom áno/nie**	**Počet znakov hesla**	**Zmena hesla**
IS MZDY A PERSONALISTIKA	Áno	>7	polročne
IS ÚČTOVNÉ DOKLADY	Áno	>7	polročne

Údaje do poisťovní sa odovzdávajú pomocou internetu cez portály poisťovní, alebo sú zasielané poštovou zásielkou. Prevádzkovateľ používa na svojich počítačoch operačné systémy WIN 7, WIN 10.

Vstup do operačného systému je chránený heslom, ktoré obsahuje minimálne 7 znakov. Počet počítačov s osobnými údajmi v spoločnosti: 10.

Prevádzkovateľ má vytvorenú počítačovú sieť zloženú z 10 počítačov. Ako server je vyčlenený samostatný počítač. Server je umiestnený v samostatnej uzamknutej miestnosti a od siete internetu je oddelený routerom.

Pripojenie na internet je zrealizované pomocou optickej siete prostredníctvom spoločnosti ACS. V priestoroch prevádzkovateľa je používaná vlastná WiFi sieť zabezpečená heslom. Prístup do siete cez WiFi je s použitím protokolu WPA, WPA2 alebo novším. Prístupnosť priečinkov zdieľaných cez sieť je možná len pre presne definovaných používateľov. Obsluha informačného systému využíva pre prácu z iného miesta vzdialenú správu. Na všetkých počítačoch je nainštalovaný permanentne aktívny, licencovaný antivírusový program ESET SMART SECURITY, ktorého súčasťou je aj aktívna brána FIREWALL.

Zálohovanie servera prebieha denne.

DOKUMENTÁRNE SPRACOVANÝ INFORMAČNÝ SYSTÉM

Zoznam neautomatizovaných IS	**Umiestnenie IS**	**Poznámka**
IS Účtovné doklady	Skriňa na dokumenty, kancelária	
IS Mzdy a personalistika	Skriňa na dokumenty	

Na likvidáciu záznamov používa prevádzkovateľ skartovací stroj, čo je štandardná metóda likvidácie dokumentov. Na úschovu dokumentov je prevádzkovateľ vybavený uzamykateľnou skriňou, v uzamykateľných miestnostiach.

ZHRNUTIE - OPATRENIA A ZÁSADY

Celkový počet oprávnených osôb na prácu s osobnými údajmi je 4**.** Spoločnosť nemá 20 a viac oprávnených osôb, ktoré pracujú s osobnými údajmi. Z toho vyplýva, že zodpovednou osobou je štatutár zariadenia /konateľ/ a nevzniká povinnosť poverenia, oznámenia a vyškolenia zodpovednej osoby na úrade. Zároveň podľa informácií na stránke úradu ani nemôže poveriť zodpovednú osobu dohľadom. Spoločnosť spracúva osobné údaje podľa osobitných zákonov. Z toho vyplýva, že nemá ani povinnosť registrovať svoje informačné systémy. Spoločnosť má povinnosť, nakoľko má svoj IS pripojený k internetu, vytvoriť bezpečnostný projekt a viesť evidenciu svojich informačných systémov. Ďalšou významnou povinnosťou je písomné poučenie oprávnených osôb

Pre pamäťové nosiče so záznamom z kamerového systému platia rovnaké pravidlá ako pre všetky pamäťové nosiče AIS, ktoré obsahujú osobitné kategórie osobných údajov s tým rozdielom, že ak vyhotovený záznam nie je využitý na účely trestného konania alebo konania o priestupkoch, je ten, kto záznam vyhotovil, povinný ho zlikvidovať najneskôr v lehote 15 dní odo dňa nasledujúceho po dni, v

ktorom bol záznam vyhotovený, ak osobitný zákon neustanovuje inak.

Berieme na vedomie, že podľa § 15 článok (7) Priestor prístupný verejnosti možno monitorovať len na účely ochrany verejného poriadku a bezpečnosti, odhaľovania kriminality, narušenia bezpečnosti štátu, ochrany majetku alebo zdravia, a to len vtedy, ak je priestor zreteľne označený ako monitorovaný; monitorovaný priestor je prevádzkovateľ povinný zreteľne označiť bez ohľadu na to, či sa snímaný obraz alebo zvuk zaznamenáva na nosič informácií. Označenie monitorovaného priestoru sa nevyžaduje, ak tak ustanovuje osobitný zákon. Vyhotovený záznam možno využiť len na účely trestného konania alebo konania o priestupkoch, ak osobitný zákon neustanovuje inak.

Prevádzkovateľ **berie na vedomie**, že v prípade zvýšenia počtu oprávnených osôb na 20 a viac podľa §23 odsek 2 zákona 122/2013 Z.z.: je povinný najneskôr v lehote 60 dní od začatia ich spracúvania výkonom dohľadu písomne poveriť zodpovednú osobu alebo viaceré zodpovedné osoby, ktoré dozerajú na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov. V súvislosti s poverením zodpovednej osoby vzniká povinnosť ohlásenia tejto osoby na úrade a následne povinnosť vyškoliť túto osobu na úrade na ochranu osobných údajov.

Berieme na vedomie, že listové zásielky, ktoré obsahujú osobné údaje by sa mali posielať doporučenou zásielkou.

Berieme na vedomie, že vyšší štandard bezpečnosti informácií na pevných diskoch PC zabezpečujú OS na báze technológie NT-Windows NT, 2000 a WIN7,8, ktoré zabezpečia pri zadaní hesla ochranu proti neoprávnenému vstupu do PC.

Žiaľ ani tento spôsob nie je bezpečný proti premontovaniu pevného disku do iného PC.

Z týchto skutočností vyplýva, že najvyšší stupeň bezpečnosti IS možno zabezpečiť, len ak sa k IS a jeho komponentom nedostanú nepovolané osoby. Z tohto pohľadu sa javí fyzická, objektová a personálna bezpečnosť IS ako prioritná.

Berieme na vedomie, že zle konfigurované a používané sieťové pripojenie do Internetu je veľmi často extrémne zraniteľným miestom.

Berieme na vedomie, že použitie UPS k PC znižuje riziko poškodenia databáz na pevnom disku počítača, ako aj riziko poškodenia pevného disku vplyvom kolísania napätia. Pri nepredvídanom výpadku napájania môže nastať neukončený zápis na pevný disk. Pri tomto môže dôjsť od jednoduchého porušenia integrity až po vážne poškodenie databázového súboru aplikácie. Vzhľadom na význam

databázových informácií v IS je UPS považované pri permanentnej práci za štandardný nástroj bezpečnosti osobných údajov a počítača a naša spoločnosť tento nástroj využíva.

Berieme na vedomie, že inštalácia antivírusového programu a pravidelné (denné) udržiavanie jeho aktualizácie pomáha chrániť počítač pred vírusmi. Antivírusové programy vyhľadávajú škodlivé kódy, ktoré sa snažia napadnúť operačný systém alebo nainštalované programy.

Overené riešenia:

Za roky existencie máme overené dve riešenia.

- *Platené riešenie* - ESET Smart Security

Slovenská spoločnosť ESET produkuje špičkové riešenie na najvyššej svetovej úrovni pod názvom ESET Smart Security. V cenovo dostupnom programe získate softvérové riešenie renomovanej spoločnosti, ktoré obsahuje antivírus a antispyware + personálny FireWall + antispamová ochrana

- *Riešenie zadarmo* - Microsoft Security Essentials.

Firma Microsoft sprístupňuje na svojich stránkach pre majiteľov operačného systému Windows zadarmo celkom slušný ochranný antivírusový program. Tento v kombinácii so zapnutou a dobre nastavenou bránou FireWall systému Windows poskytuje štandardnú ochranu menej exponovaných systémov. Pri dodržiavaní zásad je Váš počítač primerane chránený.

Program môžete stiahnuť zo stránky: **http://windows.microsoft.com/sk-sk/windows/security-essentialsdownload**

Užitočné Informácie: **http://windows.microsoft.com/sk-sk/windows/how-protect-computer-fromviruses#how-protect-computer-from-viruses=windows-7**

Berieme na vedomie, že bežné zmazanie a rýchle formátovanie nezabezpečí dokonalé vymazanie pamäťového nosiča, a hoci sa javí ako prázdne, jeho obsah je veľmi ľahko obnoviteľný

7.2. Kvalitatívna analýza rizík

ZOZNAM RIZÍK V OBJEKTOVEJ BEZPEČNOSTI

a) Strata alebo odcudzenie kľúčov od objektov prevádzkovateľa

- rozsah rizika: 3
- (na hodnotenie rozsahu rizika bola použitá stupnica: 1-ojedinelé, 2-malé, 3-významné, 4-veľké)
- alternatívne opatrenia:
  - uzamykanie vstupných dverí dvoma kľúčmi, s ktorými disponujú dve rôzne osoby,

- zabezpečenie servisnej služby na operatívnu výmenu uzamykania.

b) Neuzamknutie vstupných dverí do priestorov s informačným systémom

- rozsah rizika: 3
- alternatívne opatrenia:
  - otváranie dverí kľučkou iba z vnútornej strany miestnosti.

c) Prekonanie mechanických zábranných prostriedkov

- rozsah rizika: 1
- alternatívne opatrenia:
  - vyšší stupeň ochrany poplachovým systémom a bezpečnostnými úschovnými objektmi,
  - zálohovanie údajov AIS.

ZOZNAM RIZÍK V DOKUMENTÁRNOM INFORMAČNOM SYSTÉME

d) Šírenie informácií personálom prevádzkovateľa

- rozsah rizika: 3
- alternatívne opatrenia:
  - záväzok mlčanlivosti a poučenie oprávnených osôb,
  - komisionálna práca s údajmi (prítomnosť najmenej 2 osôb).

e) Šírenie informácií nezlikvidovanými nepotrebnými písomnosťami

- rozsah rizika: 2
- alternatívne opatrenia:
  - vyhradenie priestorov na zber nepotrebných písomností, zničenie alebo znehodnotenie dokumentov (spálenie, rozomletie, skartácia) pod dohľadom zodpovednej osoby,
  - vybavenie prevádzkovateľa skartovacím zariadením.

AUTOMATIZOVANÝ INFORMAČNÝ SYSTÉM

Riziká prieniku osobných údajov k nepovolaným osobám

a) Prienik nepovolaných osôb k počítačovému systému, a to aj v prípade, že nepovolaná osoba má krátkodobý zrakový kontakt s obrazovkou počítača

- rozsah rizika: 2
- alternatívne opatrenia:

- zamedzenie prístupu nepovolaným osobám,
- umiestnenie obrazovky mimo zorného poľa,
- prerušenie práce s osobnými údajmi v prítomnosti nepovolaných osôb.

b) Odcudzenie počítačového systému

- rozsah rizika: 3
- alternatívne opatrenia:
  - zabezpečenie objektovej bezpečnosti,
  - uzamknutie databázového serveru v osobitnej skrini, alebo na to určenej miestnosti.

c) Strata, alebo odcudzenie dátových nosičov pri prenose domov alebo na iné pracovisko. Treba vziať na vedomie, že tieto nosiče sú nechráneným zdrojom osobných údajov.

- rozsah rizika: 3
- alternatívne opatrenia:
  - bezpečné uloženie pamäťových nosičov,
  - používanie doporučených zásielok.

d) Sprístupnenie pevného disku alebo údajových štruktúr z vonkajšieho prostredia neoprávnenými osobami z lokálnej počítačovej siete

- rozsah rizika: 2
- alternatívne opatrenia:
  - definovanie prístupových práv a hesiel do aplikácií,
  - definovanie prístupových práv a hesiel do sieťových adresárov.

e) Sprístupnenie pevného disku alebo údajových štruktúr z vonkajšieho prostredia osobami, ktoré sú pripojené na internet

- rozsah rizika: 2
- alternatívne opatrenia:
  - konfigurácia prehliadača na vyšší bezpečnostný stupeň,
  - použitie antivírových programov,
  - použitie ochranných programov alebo zariadení (FireWall).

Riziká straty osobných údajov a narušenia integrity

a) Narušenie objektovej bezpečnosti prienikom nepovolaných osôb do priestorov s informačným systémom

- rozsah rizika: 3
- alternatívne opatrenia:
  - zvýšenie objektovej bezpečnosti,
  - záloha na prenosnom médiu uložená mimo priestoru s IS.

b) Zničenie počítača alebo jeho kľúčových komponentov vplyvom živelnej katastrofy, požiaru alebo zatopenia

- rozsah rizika: 2
- alternatívne opatrenia:
  - záloha na prenosnom médiu uložená mimo priestoru s IS.

c) Odcudzenie počítačového systému

- rozsah rizika: 3
- alternatívne opatrenia:
  - zvýšenie objektovej bezpečnosti,
  - záloha na prenosnom médiu uložená mimo priestoru s IS.

d) Poškodenie pevného disku počítača mechanickou závadou

- rozsah rizika: 1
- alternatívne opatrenia:
  - pravidelná kontrola disku skenovaním,
  - záloha na prenosnom médiu uložená mimo priestoru s IS.

e) Poškodenie pevného disku alebo údajových štruktúr vplyvom výpadku elektrického napájania

- rozsah rizika: 2
- alternatívne opatrenia:
  - používať nepretržité zdroje napájania (UPS), alebo stabilizátory napájania.

f) Poškodenie pevného disku alebo údajových štruktúr vplyvom počítačových vírusov

- rozsah rizika: 3
- alternatívne opatrenia:
  - použitie antivírových programov,

- opatrná manipulácia s podozrivými médiami.

g) Poškodenie pevného disku alebo údajových štruktúr z vonkajšieho prostredia neoprávneným prístupom iných používateľov lokálnej počítačovej siete

- rozsah rizika: 2
- alternatívne opatrenia:
  - definovanie prístupových práv a hesiel do aplikácií,
  - definovanie prístupových práv a hesiel do sieťových adresárov.

h) Poškodenie pevného disku alebo údajových štruktúr z vonkajšieho prostredia neoprávneným prístupom iných používateľov internetu

- rozsah rizika: 2
- alternatívne opatrenia:
  - konfigurácia prehliadača na vyšší bezpečnostný stupeň,
  - použitie ochranných antivírusových programov a firewallu.

7.3. Použitie bezpečnostných štandardov

ŠTANDARDNÉ POŽIADAVKY

Objekt je zabezpečený kombináciou opatrení fyzickej a objektovej bezpečnosti. Bezpečnostné štandardy pre prevádzkovateľa sú:

a) Vstup do objektu a pohyb osôb v objekte v pracovnom a mimopracovnom čase určuje prevádzkovateľ, alebo vlastník budovy.

b) Určenie spôsobu a formy výkonu fyzickej ochrany objektu je v právomoci prevádzkovateľa.

c) Objekt minimálne ľahkej stavebnej konštrukcie z pórobetónu, drevotriesky a podobne.

d) Okná, zabezpečené mrežou alebo bezpečnostnou fóliou, ak sú voľne prístupné z okolitého terénu, alebo ak sú ľahko prístupné z iných stavebných prvkov (strecha, bleskozvod). Montáž mreže, alebo fólie je na zvážení prevádzkovateľa, aby posúdil nebezpečenstvo preniknutia do objektu vzhľadom na okolie a faktory, ktoré môžu znížiť riziko.

e) Dvere drevené, drevotrieskové alebo z podobných materiálov, jeden dózický zámok.

f) Dodržanie zásady, že pri snahe o násilné vniknutie do priestorov s IS by mal potenciálny narušiteľ prekonať dve prekážky.

Napríklad:

- prekonať uzamknuté dvere budovy a následne dvere do priestorov s informačným systémom,
- preniknúť do objektu cez stráženú vrátnicu a potom prekonávať dvere priestorov s informačným

systémom,

- prekonať dva zámky na dverách.

g) Uzamykateľné, nerozoberateľné skrine na úschovu písomností a pamäťových nosičov obsahujúcich osobné údaje. Úschovné objekty nemusia byť uzamykateľné v prípade stálej fyzickej ochrany priestorov strážnou službou, alebo ak vstupné dvere do miestnosti sú uzamykané bezpečnostným zámkom s bezpečnostným kovaním.

h) Prideľovanie, používanie, úschovu a evidenciu kľúčov do zámkov a uzamykateľných zariadení stanovuje vlastník (prevádzkovateľ) v prevádzkovom poriadku.

Nadštandardná objektová a fyzická bezpečnosť

a) Použitie bezpečnostného kovania a bezpečnostnej vložky.

b)Použitie bezpečnostných dverí s viacbodovým uzamykaním so zárubňou zaliatou betónovou zmesou.

c) Použitie uzamykateľnej mreže na dverách.

d) EPS (elektrické požiarne hlásiče)

e) Monitorovací systém (priemyselná TV, video, infrasnímače)

f) Poplašné zariadenie s pohybovými senzormi a sirénou umiestnenou vo vonkajšom priestore.

g) EZS (Elektrické zabezpečovacie zariadenie), centrálne prepojenie prípadne prepojenie na políciu.

7.4. Štandardné požiadavky na bezpečnosť DIS

Štandardy personálnej bezpečnosti

a) Pre personál sú vypracované písomné poverenia na prácu s osobnými údajmi.

b) Súčasťou výberu zamestnancov je posúdenie bezúhonnosti a spoľahlivosť pri dodržiavaní bezpečnostných pravidiel.

c) Personál prichádzajúci do kontaktu s osobnými údajmi bol poučený o povinnosti mlčanlivosti.

d) Všetci zamestnanci majú uloženú informačnú povinnosť a dodržiavanie stanoveného postupu pri zistení neoprávnenej manipulácie alebo nájdení písomnosti s osobnými údajmi, s ktorou nie sú oprávnení pracovať.

Nadštandardná personálna bezpečnosť

a) Pri získavaní osobných údajov a práci s týmito písomnosťami prevádzkovateľ uplatňuje zásadu komisionálnosti (prítomnosť najmenej dvoch osôb).

b) Prevádzkovateľ používa štandardizovaný postup školenia personálu v oblasti ochrany údajov (manuál). Každý zamestnanec písomne potvrdzuje, že preštudoval manuál a že súhlasí a podriaďuje sa všetkým požiadavkám uvedeným v manuáli.

c) Osoba zodpovedná za ochranu osobných údajov (prevádzkovateľ, alebo poverená osoba) vykonáva pravidelné kontroly stavu týchto písomností a evidencií.

ŠTANDARDY ADMINISTRTÍVNEJ BEZPEČNOSTI

Nové záznamy, aktualizácia a používanie záznamov

a) Zisťovanie a evidovanie osobných údajov vykonávajú výlučne osoby, ktorým túto kompetenciu ukladajú pracovné povinnosti. Pracovné povinnosti stanovujú presne, ktoré osobné údaje má pracovník právo zisťovať a evidovať. Stanovujú tiež spôsob a povinnosti poverenej osoby pri získavaní osobných údajov. (Bezpečnostná smernica č.1 bod 6)

b) Záznamy a zmeny v písomnostiach s osobnými údajmi majú právo vykonávať iba oprávnené osoby s písomným potvrdením poučenia a rozsahu poverení.

c) Jednotlivé písomnosti v zázname sú upevnené k obalu tak, aby sa zabránilo ich vypadávaniu pri bežnej práci so záznamom.

Úschova písomností

a) Písomnosti obsahujúce osobné údaje sa ukladajú do uzamykateľných skríň (kartoték), kontajnerov, zásuviek kancelárskeho stola alebo do iných uzamykateľných zariadení. Požiadavka na uzamykateľnosť zariadení na úschovu písomností nie je záväzná v prípade stálej fyzickej ochrany priestorov strážnou službou, alebo uzamknutím vstupných dverí zámkom s bezpečnostnou vložkou a bezpečnostným kovaním.

Prenášanie písomností obsahujúcich osobné údaje

a) Písomnosti je možné prenášať výhradne v zalepenej obálke alebo uzavretom obale, s otvorom prelepeným lepiacou páskou.

b) Písomnosti prenášajú dotknuté osoby alebo na to určená oprávnená osoba.

c) V prípade, že prevádzkovateľ dostane zásielku v poškodenom obale, preverí dôvod poškodenia u doručujúcej osoby a odsúhlasí obsah zásielky s odosielateľom.

d) Odovzdanie písomnosti na prenos musí byť zaznamenané v príslušnej evidencii.

Preprava písomností

a) Písomnosti obsahujúce osobné údaje sa prepravujú doporučenou poštovou zásielkou, alebo kuriérom.

b) O písomnostiach odovzdaných na prepravu sa vedie evidencia.

Kopírovanie a rozmnožovanie písomností

a) Rozmnožovaním sa rozumie opakovaná tlač dokumentov z automatizovaného systému, vyhotovovanie fotokópií, odpisov a výpisov písomností.

b) Rozmnožovať písomnosti môže len oprávnená osoba.

Vypožičiavanie

a) Písomnosti s osobnými údajmi je možné zapožičať iba so súhlasom oprávnenej osoby.

b) Záznamy a originály písomností obsahujúcich osobné údaje je možné zapožičať alebo sprístupniť len osobám a inštitúciám presne špecifikovaných v evidenčnom liste DIS.

c) Vypožičanie písomností obsahujúcich osobné údaje odovzdávajúca oprávnená osoba zapíše do evidencie vypožičiavania a poskytnutia výpisu dokumentov.

Evidencie písomností

a) Prevádzkovateľ eviduje písomnosti obsahujúce osobné údaje v nižšie uvedených evidenciách, ktoré môžu byť v listinnej alebo počítačovej forme:

_ evidencia zamestnancov a ich rodinných príslušníkov na vedenie mzdovej a personálnej agendy

_ evidencia vypožičiavania a poskytnutia výpisu dokumentov

_ evidencia písomností zaslaných poštou

_ evidencia pridelených kľúčov /ak prijme smernicu č. 6/

Archivácia písomností

a) Písomnosti, ktoré nie sú bežne využívané na činnosť prevádzkovateľa sa uschovávajú oddelene, za podmienok štandardnej fyzickej bezpečnosti.

Skartácia písomností (likvidácia)

a) Písomnosti sa likvidujú skartovacím zariadením, alebo spálením pod komisionálnym dohľadom osôb zodpovedných za spracovanie údajov zaznamenaných na médiách.

Zistenie neoprávnenej manipulácie s písomnosťou

a) Osoba zodpovedná za ochranu osobných údajov vykonáva najmenej jedenkrát za rok kontrolu stavu písomností v rozsahu stanovenom bezpečnostnou smernicou.

b) Oprávnená osoba poverená spravovaním písomností je povinná vykonať najmenej raz za polrok fyzickú inventarizáciu vypožičaných, prenášaných alebo prepravovaných písomností podľa vedenej evidencie.

Nadštandardná administratívna bezpečnosť

a) Na prácu s písomnosťami sú vyhradené miesta, mimo dosahu nepovolaných osôb.

b) Písomnosti sú uschovávané v samostatnej miestnosti (spisovni) určenej výhradne na tento účel.

c) Práca s osobnými údajmi sa riadi komplexným pracovným poriadkom, ktorý stanovuje pravidlá na používanie, odkladanie, úschovu, archiváciu a skartáciu písomností.

7.5. Štandardné požiadavky na bezpečnosť AIS

a) Použitie operačných systémov na báze WINDOWS a LINUX pričom za systémy s vyšším stupňom bezpečnosti možno považovať: WIN NT, WIN 2000, WIN XP, WIN VISTA, WIN 7, WIN 8 a LINUX.

b) Použitie antivírového, antispywareového, antispamového programu a aktivácia a správne nastavenie brány FireWall.

c) Použitie bežných databázových systémov (napr. DBASE, CLIPPER, FOX, PARADOX, ACCES), pričom za systémy s vyšším stupňom bezpečnosti možno považovať relačné databázy renomovaných firiem ORACLE, MICROSOFT, INFORMIX, SYBASE, PROGRESS a pod.

d) Štandardnou ochranou počítačového systému je prístup do počítačového programu zadaním prístupového hesla. Heslo by malo obsahovať minimálne šesť znakov a malo by obsahovať čísla aj písmená (malé aj veľké) alebo iné znaky (*,_,& a pod.). Pri nebezpečenstve prezradenia hesla, by sa malo toto v pravidelných intervaloch meniť.

e) V prípade počítačovej siete treba pomocou používateľských mien, hesiel a prístupových práv konfigurovať systém tak, aby prístup k osobným údajom mali iba oprávnené osoby.

f) Na zamedzenie straty, alebo integrity databázových údajov v počítačových systémoch je nevyhnutné každodenné zálohovanie údajov na prenosné médiá. Tieto médiá nie je dovolené v žiadnom prípade neuzamknuté nechávať v priestoroch s IS. V prípade použitia externých pamäťových nosičov je vhodné používať minimálne tri nezávislé súbory médií. Tieto je treba v intervale 1 mesiaca formátovať a kontrolovať (tzv. zálohovanie s cirkuláciou média). Treba dodržiavať zásadu, že na danom nosiči je permanentne udržiavaných niekoľko kompletných záloh. Musí platiť zásada, že v prípade zničenia, alebo neopraviteľnej poruchy pevného disku sú tieto databázy plne obnoviteľné.

g) V súvislosti s dlhodobým skladovaním databázových údajov je potrebné minimálne 1x za rok zálohovať všetky databázy počítačového informačného systému a zálohy uložiť na zapisovateľný veľkokapacitný nosič (napr. CD R, CD RW, DVD R, DVD RW, externý HDD a pod.).

Nadštandardná HW a SW bezpečnosť

a) Vyšším štandardom ochrany je zadefinovanie hesla do počítača cez systém BIOS.

b) Automatické zálohovanie na inú lokalitu /cloudové úložisko, iný PC v rámci siete, alebo inej siete/
c) Veľmi účinnou ochranou počítačového systému je umiestnenie databázového servera v uzamykateľnej skrini, alebo samostatnej na to určenej miestnosti.
d) V systémoch s vyšším stupňom bezpečnosti sa presadzujú systémy identifikácie užívateľov pomocou biometrických údajov, čipových kariet a dotykovými senzormi. Pri zápise na pevný disk sa uplatňuje elektronický podpis a šifrovanie údajov. Vzhľadom na cenovú úroveň týchto systémov voči ekonomickej sile bežných prevádzkovateľov je použitie týchto zariadení veľmi obmedzené.

8 BEZPEČNOSTNÉ SMERNICE, POUČENIA, ZMLUVY A FORMULÁRE

Na zabezpečenie bezpečnosti a ochrany informačných systémov a osobných údajov prevádzkovateľ vydal tieto bezpečnostné smernice:

1. Smernica o prideľovaní, modifikácii a rušení užívateľských prístupov do informačných systémov osobných údajov v spoločnosti (príloha č. 1).
2. Smernica o ochrane informácií v podmienkach spoločnosti (príloha č. 2).
3. Smernica o získavaní osobných údajov, okruhu osôb oprávnených k získavaniu a likvidácii osobných údajov, o stanovení rozsahu osobných údajov potrebných k zabezpečeniu účelu, na ktorý sú získavané v rámci jednotlivých informačných systémov, o pravidlách spracúvania osobných údajov a o nakladaní s osobnými údajmi po skončení účelu, na ktorý boli získavané (príloha č. 3).

Tieto bezpečnostné smernice sú súčasťou tohto bezpečnostného projektu.

Na zabezpečenie bezpečnosti a ochrany informačných systémov a osobných údajov prevádzkovateľ vydal tieto poučenia:

1. Poučenie o povinnosti mlčanlivosti fyzickej osoby (právnickej osoby), ktorá má alebo môže mať prístup k informačnému systému prevádzkovateľa. (príloha č. 4)

Na zabezpečenie bezpečnosti a ochrany informačných systémov a osobných údajov prevádzkovateľ vydal tento vzor evidenčného listu informačného systému :

1 Evidenčný list – IS MZDY A PERSONALISTIKA (príloha č. 5)
2 Evidenčný list – IS ÚČTOVNÉ DOKLADY (príloha č. 6)

ActiveNet,s.r.o.
Škultétyho 1, 831 03 Bratislava

Na zabezpečenie bezpečnosti a ochrany informačných systémov a osobných údajov prevádzkovateľ vydal tento vzor formulára:

1 Zmluva o zabezpečení ochrany osobných údajov spracúvaných sprostredkovateľom uzatvorená v zmysle ustanovenia § 8 ods. 1 zákona č. 122/2013 Z.z. o ochrane osobných údajov (príloha č. 7)