# Bezpečnostný projekt

v zmysle Zákona č. 18/2018 Z. z. o ochrane osobných údajov v znení neskorších predpisov a NARIADENIE EUROPSKEHO PARLAMENTU A RADY (EÚ) 2016 / 679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov

| **Dokument:** | **VYPRACOVAL** | **SCHVÁLIL** | **Počet výtlačkov: 1** |
|---|---|---|---|
| Meno a priezvisko | **Jozef Homola** | **Jozef Bilčík , Konateľ** | **Číslo výtlačku: 1** |
| Dátum(deň, mesiac, rok) | **21.05.2018** | **24.05.2018** | **Účinnosť od: 25.05.2018** |
| Podpis | | | |

# Obsah

# 1. Dôvody k riešeniu informačnej bezpečnosti

V Slovenskej republike problematiku ochrany osobných údajov upravuje zákon NR SR č. 18/2018 Z. z. o ochrane osobných údajov, účinný od 25.mája 2018, v znení neskorších predpisov. NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

Projekt GDPR obsahuje systémové riešenie ochrany práv dotknutých osôb pred neoprávneným zasahovaním do ich súkromného života, bezpečnosti informačných systémov určených na spracúvanie informácií obsahujúcich osobné údaje dotknutých fyzických osôb, citlivé a chránené údaje.

Cieľom stratégie informačnej bezpečnosti je návrh postupu smerujúceho k zaisteniu bezproblémového fungovania informačných systémov. Na to je potrebné vytvoriť podmienky pre:

- S Ochranu informačných systémov a informácií v nich spracúvaných v priebehu ich celého životného cyklu (prevencia),
- S Rýchlu a efektívnu odpoveď na bezpečnostné incidenty a obnovu narušených systémov (obnova).

Bezpečnosť informačného systému tvorí komplexný systém technických, personálnych a organizačných opatrení. Predstavuje kompromis medzi otvorenosťou dnešných informačných systémov a ich ochranou pred napadnutím prípadne zneužitím citlivých dát.

Bezpečnostný projekt vymedzuje rozsah a spôsob technických, organizačných a personálnych opatrení potrených na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na IS z hľadiska narušenia bezpečnosti, funkčnosti a spoľahlivosti.

Povinnosťou každého prevádzkovateľa IS je ochrana spracúvaných osobných údajov. Zodpovednosť za bezpečnosť prevádzkovaného IS má jeho vlastník (prevádzkovateľ IS).

# 2. Definovanie základných pojmov a právny základ spracovania osobných údajov

Pojmy z oblasti spracovania osobných údajov sú vymedzené v legislatíve SR. Na tomto mieste vymedzíme následne požívanú terminológiu na základe konkrétneho zákonu, právnych predpisov, vykonávajúcich vyhlášok, smerníc, protokolov a dohovorov.

## 2.1. Vymedzenie základných pojmov

Na účely tohto nariadenia:

1. **„Osobné údaje"** sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej len „dotknutá osoba"); identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby.

2. **„Spracúvanie"** je operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami.

3. **„Obmedzenie spracúvania"** je označenie uchovávaných osobných údajov s cieľom obmedziť ich spracúvanie v budúcnosti.

4. **„Profilovanie"** je akákoľvek forma automatizovaného spracúvania osobných údajov, ktoré pozostáva z použitia týchto osobných údajov na vyhodnotenie určitých osobných aspektov týkajúcich sa fyzickej osoby, predovšetkým analýzy alebo predvídania aspektov dotknutej fyzickej osoby súvisiacich s výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom.

5. **„Pseudonymizácia"** je spracúvanie osobných údajov takým spôsobom, aby osobné údaje už nebolo možné priradiť konkrétnej dotknutej osobe bez použitia dodatočných informácií, pokiaľ sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia s cieľom zabezpečiť, aby osobné údaje neboli priradené identifikovanej alebo identifikovateľnej fyzickej osobe.

6. **„Informačný systém"** je akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe.

7. **„Prevádzkovateľ"** je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky

spracúvania osobných údajov; v prípade, že sa účely a prostriedky tohto spracúvania stanovujú v práve únie alebo v práve členského štátu, možno prevádzkovateľa alebo konkrétne kritériá na jeho určenie určiť v práve únie alebo v práve členského štátu.

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

9. **„Príjemca"** je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorému sa osobné údaje poskytujú bez ohľadu na to, či je treťou stranou. Orgány verejnej moci, ktoré môžu prijať osobné údaje v rámci konkrétneho zisťovania v súlade s právom únie alebo právom členského štátu, sa však nepovažujú za príjemcov; spracúvanie uvedených údajov uvedenými orgánmi verejnej moci sa uskutočňuje v súlade s uplatniteľnými pravidlami ochrany údajov v závislosti od účelov spracúvania.

10. **„Tretia strana"** je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt než dotknutá osoba, prevádzkovateľ, sprostredkovateľ a osoby, ktoré sú na základe priameho poverenia prevádzkovateľa alebo sprostredkovateľa poverené spracúvaním osobných údajov.

11. **„Súhlas dotknutej osoby"** je akýkoľvek slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby, ktorým formou vyhlásenia alebo jednoznačného potvrdzujúceho úkonu vyjadruje súhlas so spracúvaním osobných údajov, ktoré sa jej týka.

12. **„Porušenie ochrany osobných údajov"** je porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim.

13. **„Genetické údaje"** sú osobné údaje týkajúce sa zdedených alebo nadobudnutých genetických charakteristických znakov fyzickej osoby, ktoré poskytujú jedinečné informácie o fyziológii alebo zdraví tejto fyzickej osoby a ktoré vyplývajú najmä z analýzy biologickej vzorky danej fyzickej osoby.

14. **„Biometrické údaje"** sú osobné údaje, ktoré sú výsledkom osobitného technického spracúvania, ktoré sa týka fyzických, fyziologických alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby, ako napríklad vyobrazenia tváre alebo daktyloskopické údaje.

15. **„Údaje týkajúce sa zdravia"** sú osobné údaje týkajúce sa fyzického alebo duševného zdravia fyzickej osoby, vrátane údajov o poskytovaní služieb zdravotnej starostlivosti, ktorými sa odhaľujú informácie o jej zdravotnom stave.

16. **„Hlavná prevádzkareň"** je:
    - pokiaľ ide o prevádzkovateľa s prevádzkarňami vo viac než jednom členskom štáte, miesto jeho centrálnej správy v Únii s výnimkou prípadu, keď sa rozhodnutia o účeloch a prostriedkoch spracúvania osobných údajov prijímajú v inej prevádzkarni prevádzkovateľa v Únii a táto iná prevádzka má právomoc presadiť vykonanie takýchto rozhodnutí, pričom v takom prípade sa za hlavnú prevádzkareň považuje

prevádzkareň, ktorá takéto rozhodnutia prijala;

- pokiaľ ide o sprostredkovateľa s prevádzkarňami vo viac než jednom členskom štáte, miesto jeho centrálnej správy v Únii, alebo ak sprostredkovateľ nemá centrálnu správu v Únii, prevádzkareň sprostredkovateľa v Únií, v ktorej sa v kontexte činností prevádzkarne sprostredkovateľa uskutočňujú hlavné spracovateľské činnosti, a to v rozsahu, v akom sa na sprostredkovateľa vzťahujú osobitné povinnosti podľa tohto nariadenia;

17. **„Zástupca"** je fyzická alebo právnická osoba usadená v Únii, ktorú prevádzkovateľ alebo sprostredkovateľ písomne určil podľa článku 27 a ktorá ho zastupuje, pokiaľ ide o jeho povinnosti podľa tohto nariadenia.

18. **„Podnik"** je fyzická alebo právnická osoba vykonávajúca hospodársku činnosť bez ohľadu na jej právnu formu vrátane partnerstiev alebo združení, ktoré pravidelne vykonávajú hospodársku činnosť.

19. **„Skupina podnikov"** je riadiaci podnik a ním riadené podniky.

20. **„Záväzné vnútropodnikové pravidlá"** je politika ochrany osobných údajov, ktorú dodržiava prevádzkovateľ alebo sprostredkovateľ usadený na území členského štátu na účely prenosu alebo súborov prenosov osobných údajov prevádzkovateľovi alebo sprostredkovateľovi v jednej alebo viacerých tretích krajinách v rámci skupiny podnikov alebo podnikov zapojených do spoločnej hospodárskej činnosti

21. **„Dozorný orgán"** je nezávislý orgán verejnej moci zriadený členským štátom podľa článku 51.

22. **„Dotknutý dozorný orgán"** je dozorný orgán, ktorého sa spracúvanie osobných údajov týka, pretože:
    - prevádzkovateľ alebo sprostredkovateľ je usadený na území členského štátu tohto dozorného orgánu;
    - dotknuté osoby s pobytom v členskom štáte tohto dozorného orgánu sú podstatne ovplyvnené alebo budú pravdepodobne podstatne ovplyvnené spracúvaním; alebo
    - sťažnosť sa podala na tento dozorný orgán;

23. **„Cezhraničné spracúvanie"** je buď:
    - spracúvanie osobných údajov, ktoré sa uskutočňuje v Únii v kontexte činností prevádzkarní prevádzkovateľa alebo sprostredkovateľa vo viac ako jednom členskom štáte, pričom prevádzkovateľ alebo sprostredkovateľ sú usadení vo viac ako jednom členskom štáte; alebo
    - spracúvanie osobných údajov, ktoré sa uskutočňuje v Únii kontexte činností jedinej prevádzkarne prevádzkovateľa alebo sprostredkovateľa v Únii, ale ktoré podstatne ovplyvňuje alebo pravdepodobne podstatne ovplyvní dotknuté osoby vo viac ako jednom členskom štáte;

24. **„Relevantná a odôvodnená námietka"** je námietka voči návrhu rozhodnutia, či došlo k porušeniu tohto nariadenia, alebo či je plánované opatrenie vo vzťahu k prevádzkovateľovi alebo sprostredkovateľovi v súlade s týmto nariadením, ktoré musí jasne preukázať závažnosť rizík, ktoré predstavuje návrh rozhodnutia, pokiaľ ide o základné práva a slobody dotknutých osôb a prípadne voľný pohyb osobných údajov v

rámci Únie.

25. **„Služba informačnej spoločnosti"** je služba vymedzená v článku 1 bode 1 písm. b) smernice Európskeho parlamentu a Rady (EÚ) 2015/1535 jl).

26. **„Medzinárodná organizácia"** je organizácia a jej podriadené subjekty, ktoré sa riadia medzinárodným právom verejným, alebo akýkoľvek iný subjekt, ktorý bol zriadený dohodou medzi dvoma alebo viacerými krajinami alebo na základe takejto dohody.

27. **Dôvernosť** je súhrn opatrení k ochrane aktív pred nepovolaným prístupom

28. **Integrita** je charakteristika systému z hľadiska presnosti a komplexnosti zabezpečenia informácií a zabezpečenia programového vybavenia.

29. **Dostupnosť** je charakteristika systému z hľadiska oprávneného prístupu k utajovaným informáciám.

30. **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.

31. **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.

32. **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, zvukový záznam, časť operačnej pamäte, externé nosiče informácií.

33. **Hrozby** - sú vplyvy okolia, iných osôb, zariadení a prostriedkov, ktoré úmyselne alebo neúmyselne vplývajú na aktíva prevádzkovateľa tak, že ich prevádzkovateľ nemôže využívať alebo inak ohrozujú oprávnené záujmy prevádzkovateľa.

## 2.2. Právny základ spracúvania osobných údajov

Bezpečnostný projekt ochrany osobných údajov je spracovaný v súlade s:

1. Ochrana osobných údajov sa rieši v súlade so zákonom NR SR č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

2. Zoznam preberaných právne záväzných aktov Európskej únie a OECD:
   - Všeobecné nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracovaní osobných údajov a o voľnom pohybe týchto údajov a o zrušení smernice 95/46/ES, tzv. General Data Protection Regulation alebo „Obecné nariadenie na ochranu osobných údajov" - (ďalej len „GDPR").

- Smernica Európskeho parlamentu a Rady (EÚ) 2016/943 z 8. júna 2016 o ochrane nesprístupneného know - how a obchodných informácií (obchodného tajomstva).
- Európsky dohovor o počítačovej kriminalite c. 185 z roku 2001 (transponovaný v Trestnom zákonníku SR).

# 3. Rozsah projektu

Bezpečnostný projekt obsahuje všetky skutočnosti, ktoré sú spracovateľovi známe v čase jeho vypracovania a ktoré ovplyvňujú bezpečnosť IS. Svojím rozsahom je zameraný na zabezpečenie nevyhnutnej bezpečnosti IS proti možnému útoku zo strany interných a externých osôb a to na jeho:

- Dôvernosť - ochrana pred neoprávneným prístupom nepovolaných osôb,
- Integritu - ochrana proti poškodeniu, zmene, vymazaniu a zničeniu,
- Dostupnosť - ochrana proti výpadkom napájania a iným havarijným stavom.

Bezpečnostný projekt obsahuje:

- Bezpečnostný zámer - opisuje súčasný stav informačného systému, špecifikuje jeho nedostatky a poukazuje na tie oblasti, ktoré je potrebné akútne riešiť,
- Analýzu bezpečnosti informačného systému - podrobný rozbor stavu bezpečnosti z hľadiska možného útoku na dôvernosť, integritu a dostupnosť osobných údajov pri ich spracúvaní,
- Opatrenia na riešenie bezpečnostných rizík a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu s týmto nariadením - základný dokument pre všetkých zamestnancov, ktorí sú užívateľmi informačného systému. Obsahuje súhrn základných pravidiel, ktoré je potrebné rešpektovať pre zachovanie bezpečného chodu informačného systému v praxi.

# 4. Základne údaje o prevádzkovateľovi

## 4.1. Prevádzkovateľ

| *Prevádzkovateľ* | ***Bilčík, spol. s r. o.*** |
|---|---|
| *Sídlo* | Šenkvická cesta 12C, 902 01 Pezinok |
| *Obchodný register* | Výpis z Obchodného registra Okresného súdu Bratislava, Oddiel: Sro, Vložka číslo: 38123/T |
| *IČO* | 35 962 321 |
| *IČ DPH* | SK 2022080038 |
| *Osobné údaje* | Meno a priezvisko, titul, rodné číslo, trvalé bydlisko, prechodné bydlisko, číslo občianskeho alebo iného preukazu, dátum a miesto narodenia, rodinný stav, štátna príslušnosť, údaje o vzdelaní a predchádzajúcich zamestnaniach, údaje o zmene pracovnej schopnosti, údaje o vedených súdnych konaniach, údaje o rodinných príslušníkoch |
| *Používatelia osobných údajov* | Zamestnanci prevádzkovateľa zabezpečujúci spracovanie |

| | |
|---|---|
| | personálnej, mzdovej a účtovnej agendy |
| *Manipulácia s osobnými údajmi* | Zber, spracovanie, archivovanie alebo likvidácia |
| *Charakter prace s osobnými údajmi* | Spracovane osobne údaje v informačnom systéme Databáza klientov nie sú poskytovane, sprístupňované ani zverejňované<br>Spracovane údaje v IS Mzdy a Personalistika sú poskytovane sociálna poisťovňa, zdravotné poisťovne, orgány finančnej správy a iné orgány verejnej správy |
| *Cezhraničný prenos* | Neuskutočňuje a tým ani poskytovanie osobných údajov do zahraničia |
| *Spôsob spracovaná osobných údajov* | Automatizovaným a neautomatizovaným spôsobom, písomná dokumentácia |
| *Profilovanie* | Nie |
| *Biometrické údaje* | Nie |
| *Kamerové systémy* | Áno |

### 4.1.1. Predmet činnosti

Prevádzkovateľ je právnickou osobou, vystupuje v právnych vzťahoch vo svojom mene a nesie zodpovednosť vyplývajúcu z týchto vzťahov. Za porušenie svojich záväzkov zodpovedá do výšky základného imania, a to 9959 €.

Predmetom činnosti prevádzkovateľa je:

- kúpa tovaru za účelom jeho predaja iným prevádzkovateľom živnosti (veľkoobchod) alebo za účelom jeho predaja konečnému spotrebiteľovi (maloobchod)
- sprostredkovateľská činnosť v oblasti obchodu a služieb v rozsahu voľnej živnosti
- reklamná a propagačná činnosť.
- opravy cestných motorových vozidiel
- opravy karosérií
- pneuservis
- umývanie cestných motorových vozidiel
- predaj motorových vozidiel a motocyklov
- vykupovanie ojazdených motorových vozidiel a motocyklov
- prenájom motorových vozidiel a motocyklov
- odťahová služba motorových vozidiel
- cestná nákladná doprava vykonávaná automobilmi do 3,5 tony celkovej hmotnosti vrátane prípojného vozidla
- skladovanie
- administratívne služby
- prenájom nehnuteľností spojený s poskytovaním iných než základných služieb spojených s prenájmom

### 4.1.2. Účel spracovania osobných údajov

Prevádzkovateľ spracúva len také osobné údaje, ktoré svojím rozsahom a obsahom zodpovedajú účelu spracúvania vyplývajúceho z definovaného predmetu činnosti prevádzkovateľa, sú časovo a vecne aktuálne vo vzťahu k účelu spracúvania a sú nevyhnutné na jeho dosiahnutie.

Účel spracúvania osobných údajov, popis jednotlivých záznamov:

- Personálna a mzdová agenda zamestnancov
- Účtovné doklady
- Došlá a odoslaná pošta
- Kamerový systém
- Agenda BOZP a OPP
- Správa registratúry

Osobné údaje sú v jednotlivých IS spracúvané:

- Neautomatizovanou technológiou spracúvania na nosičoch a to žiadostiach, kartotékach, zoznamoch, záznamoch alebo sústave obsahujúcej spisy a spisové obaly, potvrdeniach, posudkoch, hodnoteniach apod.
- Automatizovanou technológiou spracúvania na PC zapojených do lokálnej počítačovej siete - LAN, s pripojením na verejne prístupnú počítačovú sieť Internet.

## 4.2. Základne údaje jednotlivých záznamov o spracovateľských činnostiach

### 4.2.1. Personálna a mzdová agenda zamestnancov

**Právny základ spracúvania osobných údajov v predmetnom zazname:**

- Spracúvanie osobných údajov je povolené zákonom č. 431/2002 Z. z. o účtovníctve, zákonom č. 311/2001 Z. z. Zákonník práce a zákonom č. 18/2018 Z. z. o ochrane osobných údajov v znení neskorších predpisov.

**Účel spracúvania osobných údajov v predmetnom zazname:**

- Záznam zabezpečuje spracovanie osobnej, pracovno-právnej agendy zamestnancov, potrebných štatistických výkazov, miezd, vykonávanie zrážok zo mzdy voči štátu a iným subjektom podľa príslušných zákonov.

**Zoznam spracúvaných osobných údajov v predmetnom zazname:**

- Rozsah spracúvaných osobných údajov predstavuje titul, meno, priezvisko, rodné číslo, podpis, číslo OP, adresa, e-mailová adresa, zdravotná spôsobilosť, telefónne číslo apod.

**Okruh dotknutých osôb v predmetnom zazname:**

- Dotknutými osobami v tomto zazname sú uchádzači o zamestnanie, zamestnanci, bývalí zamestnanci a osoby zamestnané na dohodu.

**Okruh tretích strán - spracovateľské operácie s osobnými údajmi v predmetnom zazname:**

- Osobné údaje z tohto záznamu sa poskytujú Ústrediu práce, sociálnych vecí a rodiny, Sociálnej poisťovni, Zdravotným poisťovniam, Daňovému úradu, Doplnkovým dôchodkovým sporiteľniam, Dôchodcovským správcovským spoločnostiam, Orgánom štátnej správy a verejnej moci na výkon kontroly a dozoru, Orgánom činnom v trestnom konaní a Exekútorom, Iným príjemcom sa osobné údaje nesprístupňujú ani sa nezverejňujú. Cezhraničný prenos osobných údajov sa neuskutočňuje.
- Prevádzkovateľ využíva na spracovanie miezd sprostredkovateľa, z ktorým ma podpísanú sprostredkovateľskú zmluvu podľa nariadenia Európskeho parlamentu a rady (EU) 2016/679- konkrétny článok/články 28/ 2,3 Nariadenia EP a R (EÚ) o ochrane fyzických osôb pri spracovaní osobných údajov a o voľnom pohybe takýchto údajov.

### 4.2.2. Účtovne doklady

**Právny základ spracúvania osobných údajov v predmetnom zazname:**

- Spracúvanie osobných údajov je povolené zákonom č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov, zákonom č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov, zákonom č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov, zákonom č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov, zákonom č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov, zákonom č. 152/1994 Z. z. o sociálnom fonde v znení neskorších predpisov a zákonom č. 18/2018 Z. z. o ochrane osobných údajov v znení neskorších predpisov.

**Účel spracúvania osobných údajov v predmetnom zazname:**

- Osobné údaje sú v tomto zazname spracúvané za účelom spravovania a spracovania všetkých typov účtovných dokladov používaných pri vedení účtovníctva spoločnosti.

**Zoznam spracúvaných osobných údajov v predmetnom zazname:**

- Rozsah spracúvaných osobných údajov v tomto zazname predstavuje IČO, DIČ, IČ-DPH, názov firmy/fyzickej osoby, typ právnej formy, číslo registra, meno, priezvisko, titul, typ osoby, adresa trvalého pobytu, adresa prechodného pobytu, telefónne číslo, e-mailová adresa, dátum narodenia, druh a číslo dokladu totožnosti, podpis, číslo bankového účtu apod.

**Okruh dotknutých osôb v predmetnom zazname:**

- Dotknutými osobami v tomto zazname sú zamestnanci prevádzkovateľa, zamestnanci dodávateľov tovaru a služieb, majitelia a zamestnanci zmluvných partnerov, ktorým vznikla povinnosť uhradiť platbu za tovar alebo poskytnuté služby.

**Okruh tretích strán - spracovateľské operácie s osobnými údajmi v predmetnom zazname:**

- Osobné údaje z tohto záznamu sa poskytujú Sociálnej poisťovni, Zdravotným poisťovniam a Daňovému úradu. Iným príjemcom sa osobné údaje nesprístupňujú ani sa nezverejňujú. Cezhraničný prenos osobných údajov sa neuskutočňuje.
- Prevádzkovateľ využíva na spracovanie účtovníctva sprostredkovateľa, z ktorým ma podpísanú sprostredkovateľskú zmluvu podľa nariadenia Európskeho parlamentu a rady (EU) 2016/679- konkrétny článok/články 28/ 2,3 Nariadenia EP a R (EÚ) o ochrane fyzických osôb pri spracovaní osobných údajov a o voľnom pohybe takýchto údajov.

### 4.2.3. Sprava registratúry

**Právny základ spracúvania osobných údajov v predmetnom zazname:**

- Spracúvanie osobných údajov je povolené zákonom č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov.

**Účel spracúvania osobných údajov v predmetnom zazname:**

- Súčasťou vnútorného záznamu je aj systém informácií registratúrneho charakteru, ktoré vznikajú v procese komunikácie medzi dvomi subjektmi. Tento druh informácií môže byť zaznamenávaný písmom, obrazom, zvukom alebo iným spôsobom. Riadna správa registratúrnych záznamov si vyžaduje vypracovanie a dodržiavanie systému ich úplnej a presnej evidencie, systému ukladania, účelnej a bezpečnej ochrany, ako aj plánovitého vyraďovania. Tieto úlohy zabezpečuje systém správy registratúry ako neoddeliteľná a nenahraditeľná súčasť činnosti prevádzkovateľa IS ako celku.

**Zoznam spracúvaných osobných údajov v predmetnom zazname:**

- V tomto zazname sú spracúvané osobné údaje zo všetkých informačných systémov, ktoré prevádzkovateľ využíva.

**Okruh dotknutých osôb v predmetnom zazname:**

- V tomto zazname sú spracúvané osobné údaje dotknutých osôb zo všetkých informačných systémov, ktoré prevádzkovateľ využíva.

**Okruh tretích strán - spracovateľské operácie s osobnými údajmi v predmetnom zazname:**

- Osobné údaje z tohto zazname sa neposkytujú, nesprístupňujú ani nezverejňujú tretím stranám. Cezhraničný prenos osobných údajov sa neuskutočňuje.

### 4.2.4. Došlá a odoslaná pošta

**Právny základ spracúvania osobných údajov v predmetnom zazname:**

- Spracúvanie osobných údajov je povolené zákonom č. 324/2011 Z. z. o poštových službách a o zmene a doplnení niektorých zákonov.

**Účel spracúvania osobných údajov v predmetnom zazname:**

- Účel spracúvania osobných údajov tvorí spracovanie a vybavenie prijatej a odoslanej pošty.

**Zoznam spracúvaných osobných údajov v predmetnom zazname:**

- V tomto zazname sú spracúvané osobné údaje fyzických a právnických osôb v rozsahu titul, meno, priezvisko, podpis, adresa, dátum prijatia, odoslania, obsah, značka, predmet apod.

**Okruh dotknutých osôb v predmetnom zazname:**

- Dotknutými osobami sú v tomto zazname fyzické a právnické osoby - odosielatelia a prijímatelia poštovej a emailovej korešpondencie.

**Okruh tretích strán - spracovateľské operácie s osobnými údajmi v predmetnom zazname:**

- Osobné údaje z tohto záznamu sa neposkytujú, nesprístupňujú ani nezverejňujú tretím stranám. Cezhraničný prenos osobných údajov sa neuskutočňuje.

### 4.2.5. Agenda BOZP a OPP

**Právny základ spracúvania osobných údajov v predmetnom zazname:**

- Spracúvanie osobných údajov je povolené zákonom č.124/2006 Z. z. o ochrane zdravia pri práci v znení neskorších predpisov a zákonom č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov.

**Účel spracúvania osobných údajov v predmetnom zazname:**

- Osobné údaje sú v tomto zazname spracúvané za účelom plnenia povinností zamestnávateľa súvisiacich s pracovným pomerom alebo obdobným vzťahom (napr. na základe dohôd o prácach vykonávaných mimo pracovného pomeru) vrátane predzmluvných vzťahov v záujme ochrany zdravia pri práci.

**Zoznam spracúvaných osobných údajov v predmetnom zazname:**

- Rozsah spracúvaných osobných údajov v tomto zazname predstavuje meno, priezvisko, rodné priezvisko, titul, osobné číslo, dátum a miesto narodenia, podpis, rodinný stav, trvalé bydlisko, prechodné bydlisko, údaje ozdrav. Poisťovni, pracovné zaradenie, pracovisko, veľkostné čísla pre pridelenie OOPP, fotografia, údaje o zaradení v systéme BOZP, PO, počet a druh pridelených OOPP.

**Okruh dotknutých osôb v predmetnom zazname:**

- Dotknutými osobami sú v tomto zazname zamestnanci prevádzkovateľa.

**Okruh tretích strán - spracovateľské operácie s osobnými údajmi v predmetnom zazname:**

- Osobné údaje z tohto zazname sa poskytujú orgánom štátnej správy a verejnej moci na výkon kontroly a dozoru (inšpektorát práce) a Zdravotným poisťovniam. Iným príjemcom sa osobné údaje nesprístupňujú ani sa nezverejňujú. Cezhraničný prenos osobných údajov sa neuskutočňuje.
- Prevádzkovateľ využíva na spracovanie BOZP sprostredkovateľa, z ktorým ma podpísanú sprostredkovateľskú zmluvu podľa nariadenia Európskeho parlamentu a rady (EU) 2016/679- konkrétny článok/články 28/ 2,3 Nariadenia EP a R (EÚ) o ochrane fyzických osôb pri spracovaní osobných údajov a o voľnom pohybe takýchto údajov.

### 4.2.6. Kamerový systém

**Právny základ spracúvania osobných údajov v predmetnom zazname:**

- V zmysle Článku 6 ods.l pism.f všeobecného Nariadenia EP a R (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov.

**Účel spracúvania osobných údajov v predmetnom IS:**

- Informačný systém je určený na nepretržité monitorovanie priestorov, ochrana majetku a osôb pred krádežami, vandalizmom, prevencia pred páchaním trestných činov, bezpečnosť a odhaľovania kriminality

**Zoznam spracúvaných osobných údajov v predmetnom zazname:**

- Rozsah spracúvaných osobných údajov predstavuje obrazový záznam fyzickej osoby.

**Okruh dotknutých osôb v predmetnom zazname:**

- Dotknutými osobami sú v tomto zazname fyzické osoby vstupujúce do monitorovaného priestoru, (fyzické osoby, dodávatelia a odberatelia tovaru a služieb, zamestnanci, zamestnanci klientov, dodávatelia a odberatelia klientov).

**Okruh tretích strán - spracovateľské operácie s osobnými údajmi v predmetnom zazname:**

- Osobné údaje z tohto zaznáme sa poskytujú orgánom činným v trestnom konaní v prípade spáchania trestného činu. Iným príjemcom sa osobné údaje nesprístupňujú ani sa nezverejňujú. Cezhraničný prenos osobných údajov sa neuskutočňuje.

## 5. Zodpovednosť za bezpečnosť osobných údajov

| | |
|---|---|
| *Za bezpečnosť osobných údajov zodpovedá prevádzkovateľ a sprostredkovateľ:* | Prevádzkovateľ a sprostredkovateľ prijmú so zreteľom na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb, primerané technické a organizačné opatrenia s cieľom zaistiť úroveň bezpečnosti primeranú tomuto riziku, pričom uvedené opatrenia prípadne zahŕňajú aj:<br>▪ pseudonymizáciu a šifrovanie osobných údajov;<br>▪ schopnosť zabezpečiť trvalú dôvernosť, integritu, dostupnosť a odolnosť systémov spracúvania a služieb;<br>▪ schopnosť včas obnoviť dostupnosť osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu;<br>▪ proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania; |
| *Prevádzkovateľ:* | Spracúvať osobné údaje vo vlastnom mene môže len prevádzkovateľ. Prevádzkovateľ spracúva osobné údaje v súlade Článok/Články 6 / 40,41,50 všeobecného Nariadenia EP a R (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov |
| *Bezpečnosť osobných údajov prevádzkovateľ zdokumentuje:* | V súlade všeobecným nariadením Európskeho parlamentu údajov prevádzkovateľ a rady (EU) 2016/679- konkrétny Článok/Články 35/ 75- zdokumentuje: 78,83,84 Nariadenia EP a R (EÚ) o ochrane fyzických osôb pri spracovaní osobných údajov a o voľnom pohybe takýchto údajov. Zmysle zákona č.18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. |
| *Zodpovednosť za ochranu osobných údajov:* | Zodpovedá konateľ spoločnosti konateľ spoločnosti |

# 6. Bezpečnostné ciele

Cieľom bezpečnostného projektu je chrániť základné práva a slobody fyzických osôb pri spracovaní ich osobných údajov v súlade sústavou Slovenskej republiky a Zákonom č. 18/2018 Z. z. o ochrane osobných údajov a NARIADENIA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov. Bezpečnostný projekt stanovuje zásady spracovania osobných údajov, zodpovednosť za bezpečnosť ich spracovania, upravuje bezpečnosť osobných údajov na jednotlivých pracoviskách, upravuje ochranu práv všetkých dotknutých osôb.

Bezpečnostný projekt je interným predpisom prevádzkovateľa Bilčík, spol. s r. o. na úseku ochrany osobných údajov a jeho obsahová náplň je totožná s ustanoveniami NARIADENIA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov a zákona č. 18/2018 Z. z. o ochrane osobných údajov.

Bezpečnostný projekt je záväzný pre všetkých zamestnancov spoločnosti, ktorí sú s ňou v pracovnom alebo obdobnom vzťahu. Bezpečnostný projekt je potrebné považovať za dôverný dokument, ktorého obsah je nutné chrániť pred neoprávneným prístupom rovnako ako citlivé osobné údaje spracúvané v informačnom systéme. Sprístupnenie jeho obsahu nepovolaným osobám môže mať za následok eliminovanie bezpečnostných mechanizmov informačného systému a ohrozenie jeho dôvernosti a stability. Z tohto dôvodu spoločnosť vymedzuje úzky okruh osôb, ktoré sú oprávnené oboznamovať sa s ním.

## 6.1. Formulácia základných bezpečnostných cieľov

Základnými bezpečnostnými cieľmi prevádzkovateľa sú tieto skutočnosti:

- Chrániť základné práva a slobody fyzických osôb pri spracovaní ich osobných údajov;
- Zabezpečiť dodržiavanie zákona a súvisiacich legislatívnych noriem,
- Zabezpečiť ochranu prevádzkovateľa a jej klientov pred diskreditáciou a únikom osobných údajov,
- Zachovať prevádzkové schopnosti a prevádzkovú spoľahlivosť prevádzkovateľa a tak zabezpečiť jej poslanie na trhu.

Vyžaduje sa, aby osobné údaje dotknuté zákonom, boli chránené najmä pred:

- Odcudzením,
- Stratou,
- Poškodením (zničením),
- Neoprávneným prístupom,
- Rozširovaním

a to takými opatreniami, aby sa z hľadiska bezpečnosti zabránilo nežiaducim dôsledkom (v súvislosti s údajmi):

- Strate predmetných údajov
- Zachovala sa dôvernosť, integrita, dostupnosť pre oprávnené osoby a hodnovernosť

údajov

# 7. Minimálne požadované bezpečnostné opatrenia

U prevádzkovateľa musia byť vykonané technické, organizačné a personálne opatrenia tak, aby boli zachované minimálne tieto bezpečnostné opatrenia:

- Udržiavanie pracovnej pozície (autority), ktorá je poverená zodpovednosťou a riadením procesu ochrany osobných údajov,
- Udržiavanie organizačných - riadiacich aktov na usmernenie ochrany osobných údajov,
- Pravidelné vyčleňovanie primeraného objemu finančných prostriedkov na realizáciu a zlepšovanie opatrení na ochranu osobných údajov,
- Opatrenia na zamedzenie nekontrolovaného prijímania zamestnancov do spoločnosti a ich nekontrolovaného pôsobenia v spoločnosti,
- Opatrenia na zamedzenie neoprávneného prístupu do priestorov prevádzkovateľa,
- Opatrenie na zamedzenie neoprávneného prístupu k chráneným osobným údajom,
- Opatrenia na zamedzenie nežiaducim dôsledkom požiaru, úniku vody či živelnej pohrome,

## 7.1. Vymedzenie bezpečnostných opatrení pre všetky účely spracovania osobných údajov

Bezpečnostné opatrenia aplikované na ochranu informačných systémov používaných prevádzkovateľom Bilčík, spol. s r. o. sú vymedzené troma oblasťami, na základe konkrétnych podmienok spracovania jednotlivých skupín osobných údajov, a to:

- Technické opatrenia
- Personálne opatrenia
- Organizačné opatrenia

### 7.1.1. Technické opatrenia

Hlavným poslaním technických opatrení je:

- Odstrašiť
- Zabrániť
- Spomaliť
- Detegovať
- Donútiť zanechať stopy a umožniť rekonštrukciu

Vymenované operátory sú voči potenciálnemu útočníkovi, ale aj voči procesom, ktorých dôsledok predstavuje ohrozenie osobných údajov.

Technické opatrenia vytvárajú veľmi dobré predpoklady na ochranu osobných údajov a vo významnej miere sa podieľajú na eliminácii nežiaduceho prístupu neoprávnených osôb k informačným systémom, na ktorých sa spracúvajú ochraňované osobné údaje.

Technické opatrenia na ochranu osobných údajov pozostávajú z nasledovných skutočností:

- Prevádzkovateľ disponuje súborom prostriedkov fyzickej povahy zabezpečujúcom ochranu spracúvaných údajov, a to:
  a) Zabezpečenie objektu pomocou mechanických zábranných prostriedkov je realizované prostredníctvom FAB zámkov,
  b) Zabezpečenie objektu pomocou kamerového systému,
  c) Informačné systémy sú umiestnené v priestore chránenom pred fyzickým prístupom neoprávnených osôb a taktiež pred nepriaznivými vplyvmi okolia.
  d) Fyzické nosiče osobných údajov sú uložené v uzamykateľných miestnostiach prevádzkovateľa.
  e) Fyzické nosiče osobných údajov sú zničené po uplynutí doby ich povinnej archivácie skartáciou.
- Ochrana pred neoprávnených prístupom k osobným údajom je zabezpečená prostredníctvom sústavy hesiel, potrebných pre vstup do systému údajov.
- Zabezpečiť šifrovú ochranu obsahu dátových nosičov a šifrovú ochranu dát premiestňovaných prostredníctvom počítačových sietí.
- Vylúčiť prístup tretích strán k informačným systémom, resp. vytvoriť pravidlá prístupu tretích strán k informačnému systému, ak k takému prístupu dochádza.
- Prístup oprávnených osôb k osobným údajom je ošetrený prostredníctvom identifikačných a autorizačných hesiel, jedinečných pre každý PC vo vlastníctve prevádzkovateľa.
- Ochrana PC proti škodlivému kódu zahŕňa nasledovné opatrenia:
  a) Oprávnené osoby sú povinné detegovať prítomnosť škodlivého kódu v prichádzajúcej elektronickej pošte, teda majú povinnosť pravidelne vykonávať aktualizáciu antivírusového systému PC.
  b) Prevádzkovateľ IS je povinný používať na všetkých PC prepojených vo vnútornej počítačovej sieti spoločnosti iba legálny a schválený Software.
- Sieťová bezpečnosť predpokladá:
  a) Kontrolu a obmedzenie prepojenia informačného systému, v ktorom sú spracúvané osobné údaje s verejne prístupnou počítačovou sieťou
  b) Ochranu vonkajšieho a vnútorného prostredia prostredníctvom nástroja sieťovej bezpečnosti (aktualizácia firewall)
  c) Pravidlá stanovené pre prístup do verejne prístupnej počítačovej siete vo forme zamedzenia pripojenia k určitým webovým sídlam, potenciálne obsahujúcim škodlivý kód - prevádzkovateľ vytvorí zoznam takýchto webových sídel.
- Povinnosť zálohovania osobných údajov predstavuje:
  a) Vytváranie záloh s periodicitou jeden týždeň, odosielanú do zabezpečeného úložiska dát (server).
  b) Test obnovy informačného systému zo zálohy, minimálne štyrikrát za kalendárny rok.
- Likvidácia osobných údajov a dátových nosičov sa uskutočňuje:
  a) Bezpečným vymazaním osobných údajov z dátových nosičov,
  b) Zariadením na likvidáciu dátových nosičov osobných údajov.

- Oprávnené osoby a všetci zamestnanci spoločnosti sú povinní pravidelne aktualizovať operačný systém a programové aplikačné vybavenie každého PC vo vlastníctve spoločnosti.

### 7.1.2. Personálne opatrenia

Personálne opatrenia riešia otázky výberu, riadenia a kontroly ľudských zdrojov zainteresovaných do procesu spracúvania a následnej ochrany osobných údajov dotknutých zákonom.

Personálne opatrenia na ochranu osobných údajov pozostávajú z nasledovných skutočností:

- Vzdelávanie poverených osôb o právach a povinnostiach vyplývajúcich zo všeobecným nariadením Európskeho parlamentu a rady (EU) 2016/679 o ochrane fyzických osôb pri spracovaní osobných údajov a o voľnom pohybe takýchto údajov a zodpovednosti za ich porušenie.
- Vymedzenie zakázaných postupov alebo operácií s osobnými údajmi.
- Poučenie oprávnených osôb o postupoch spojených s automatizovanými prostriedkami spracúvania .
- Oboznámenie oprávnených osôb s bezpečnostnými a internými smernicami prevádzkovateľa.

### 7.1.3. Organizačné opatrenia

Hlavným poslaním organizačných opatrení prevádzkovateľa je:

- Vypracovať a zaviesť účinné a efektívne preventívne opatrenia
- Zabezpečiť správny výber a trvalú prípravu oprávnených osôb na prácu s ochraňovanými údajmi
- Definovať režimové opatrenia pohybu osôb a manipulácie s ochraňovanými údajmi
- Vypracovať účinný kontrolný režim

Organizačné opatrenia na ochranu osobných údajov pozostávajú z nasledovných skutočností:

- Určenie postupov likvidácie osobných údajov s vymedzením súvisiacej zodpovednosti jednotlivých oprávnených osôb (bezpečné vymazanie osobných údajov z dátových nosičov, likvidácia dátových nosičov a fyzických nosičov osobných údajov).
- Evidencia bezpečnostných incidentov a použitých riešení
- Prevádzkovateľ vykonáva kontrolnú činnosť, ktorá je zameraná na dodržiavanie prijatých bezpečnostných opatrení, a to minimálne raz za kalendárny rok formou neohlásenej kontroly, pričom jej predmetom môže byť ktorákoľvek súčasť prijatých opatrení.

# 8. Základne bezpečnostne ciele pre pravá dotknutých osôb

- Pred začatím spracúvania jednoznačne a konkrétne vymedzí účel spracúvania
- Povinnosť oznámenia incidentu dotknutej osobe v závažných prípadoch

- Právo na prenosnosť údajov dotknutých osôb
- Právo na výmaz dotknutej osoby (ak sú dáta protizákonne spracúvané)
- Možnosť odvolať súhlas dotknutej osoby kedykoľvek
- Na rozdielne účely získavať osobné údaje osobitne
- Osobné údaje získané na rôzne účely nezdružovať
- Spracúvať osobné údaje v súlade s dobrými mravmi
- Nevynucovať súhlas dotknutej osoby hrozbou odmietnutia zmluvného vzťahu, dodania služieb alebo tovaru
- Vo všeobecne zrozumiteľnej forme poskytnúť informácie o stave spracúvania osobných údajov v rozsahu: názov, sídlo alebo trvalý pobyt, právnu formu a identifikačné číslo prevádzkovateľa; meno a priezvisko štatutárneho orgánu prevádzkovateľa; identifikačné označenie informačného systému; účel spracúvania, zoznam osobných údajov a okruh dotknutých osôb; okruh príjemcov, ktorým sú alebo budú údaje sprístupnené, tretie strany, ktorým osobné údaje sú alebo budú poskytnuté; tretie krajiny, do ktorých sa uskutočňuje prenos osobných údajov; právny základ informačného systému; formu zverejnenia, ak sa zverejnenie osobných údajov vykonáva; všeobecnú charakteristiku opatrení za zabezpečenia ochrany osobných údajov a dátum začatia a dobu spracúvania
- Vo všeobecne zrozumiteľnej forme presné informácie o zdroji, z ktorého boli osobné údaje získané
- Spracúvať len správne, úplné a aktualizované osobné údaje
- Nesprávne a neúplné osobné údaje blokovať, opraviť alebo doplniť
- Nesprávne údaje, ktoré nie je možné opraviť alebo doplniť zlikvidovať
- Zabezpečiť, aby osobné údaje boli spracúvané vo forme umožňujúcej identifikáciu dotknutých osôb počas doby nie dlhšej, ako je nevyhnutné na dosiahnutie účelu spracúvania
- Zlikvidovať osobné údaje, ktorých účel spracúvania sa skončil
- Vo všeobecne zrozumiteľnej forme odpis osobných údajov
- Opraviť nesprávne, neúplné alebo neaktuálne osobné údaje
- Archivovať písomné dokumenty tak, aby bol vedený zoznam dokumentov, miesto ich uloženia a zabezpečiť vhodné podmienky na archivovanie v súlade zo zákonom č. 395/2002 Z. z. O archívoch a registratúrach v znení neskorších predpisov
- Likvidovať osobné údaje po splnení účelu spracúvania; vrátiť úradné doklady, ak boli predmetom spracúvania
- Likvidáciu osobných údajov, ak došlo k porušeniu zákona
- Bezodkladné písomné oznámenie dotknutej osobe a úradu na ochranu osobných údajov SR, že na základe písomnej žiadosti oprávnenej osoby, ktorej práva boli obmedzené, boli jej nesprávne, neúplné alebo neaktuálne osobné údaje opravené
- Prípadne zlikvidované; ak boli predmetom spracúvania úradné doklady obsahujúce osobné údaje, že jej boli vrátené
- Realizáciu technických, personálnych a organizačných opatrení a dohliada na ich aplikáciu v praxi
- Dohľad pri výbere sprostredkovateľa a prípravu písomnej zmluvy alebo poverenia pre sprostredkovateľa; preveruje dodržiavanie dohodnutých podmienok
- Dohľad nad cezhraničným tokom osobných údajov

## 8.1. Zásady ochrany osobných aktív

Legislatívne predpisy upravujú ochranu osobných údajov dotknutých osôb. Možnosti spracúvania a prenosu údajov elektronickou cestou postupne zvyšujú úroveň rizík, ktoré pôsobia na jedno z najdôležitejších aktív.

Každý zamestnanec prevádzkovateľa je zaviazaný ochraňovať osobné údaje dotknutých osôb pred prezradením, zničením, poškodením alebo stratou. Rovnako je zaviazaný ochraňovať aj hmotné hodnoty prevádzkovateľa. Bezpečnosť aktív prevádzkovateľa je jednou z prvoradých úloh a všetci zamestnanci prevádzkovateľa majú individuálnu zodpovednosť pri jej zabezpečovaní:

- Zásada ochrany dôležitých systémov a komponentov informačného systému. Dôležité systémy a komponenty informačného systému sú tie časti, ktorých zlyhanie, zničenie alebo iný dôvod nedostupnosti by mal dopad na strategické záujmy prevádzkovateľa. Cieľom prevádzkovateľa je dosiahnuť minimalizáciu rizika zlyhania dôležitých súčastí informačného systému, komunikačnej a bezpečnostnej infraštruktúry.
- Zásada ochrany údajov v informačných systémoch. Údaje musia byť chránené vo všetkých formách - hlasovej, písomnej, elektronickej, počas ich spracovania a prenosu pomocou počítačov, faxov, telefónnej alebo počítačovej siete a počas ich archivácie. Cieľom je dosiahnuť ekonomicky primeranú a pritom spoľahlivú ochranu osobných údajov.
- Zásady a ciele ochrany osôb a personálnej bezpečnosti. Osoby sú uchádzači o zamestnanie, zamestnanci, manželia alebo manželky zamestnancov, vyživované deti zamestnancov, rodičia vyživovaných detí zamestnancov, blízke osoby, bývalí zamestnanci, klienti. Prevádzkovateľ musí chrániť práva osôb, ktorých údaje sú spracúvané, zároveň podniknúť opatrenia na ochranu informačného systému pred neautorizovanou činnosťou osôb a možným nátlakom na zamestnancov s prístupom k strategickým údajom.
- Zásada ochrany dobrého mena. Náležitá pozornosť bude venovaná ochrane dobrého mena prevádzkovateľa. Jej cieľom je udržanie a skvalitňovanie dobrého mena prevádzkovateľa.
- Zásada priradenia zodpovednosti za bezpečnosť. Každý zamestnanec musí mať definované práva a povinnosti, ktoré mu umožnia zabezpečiť spoľahlivý systém bezpečnostných opatrení na ochranu aktív v informačnom systéme, za ktoré je zodpovedný. Cieľom je presné vymedzenie práv a povinností zamestnancov majúce za následok zvýšenie zodpovednosti a skvalitnenie kontroly.
- Zásada správnej organizačnej štruktúry riadenia bezpečnosti. Podmienkou funkčnosti bezpečnostného systému je existencia primeranej organizačnej štruktúry bezpečnosti organizácie. Organizačná zložka bezpečnosti musí byť vybavená dostatočnými kompetenciami pre zabezpečenie požadovaných úloh. Cieľom organizácie je poveriť vybraných zamestnancov úlohami na úseku bezpečnosti a ochrany a vydať vnútorné nariadenia vymedzujúce ich povinnosti a kompetencie.
- Zásada hlásenia stavu bezpečnostného systému. Vedenie prevádzkovateľa a zamestnanci musia byť pripravení primerane reagovať na krízovú situáciu tak, aby sa minimalizovali jej následky. Činnosť bezpečnostného systému a užívateľov informačného systému bude monitorovaná, bezpečnostné incidenty budú sledované a pravidelne vyhodnocované. Proti narušiteľom bezpečnostného systému budú zavedené primerané opatrenia v súlade s platnou legislatívou.
- Zásada postupu implementácie bezpečnostného systému. Bezpečnostný systém prevádzkovateľa musia byť realizovaný na základe rozpracovaných zásad tak, aby boli rešpektované jej možnosti a potreby.
- Bezpečnostné mechanizmy, ktoré budú realizované v prostredí prevádzkovateľa na ochranu aktív, musia mať takú bezpečnostnú úroveň, aby vyhoveli požiadavkám legislatívy Slovenskej republiky týkajúcej sa oblasti ochrany osobných údajov, prevádzky a bezpečnosti informačných systémov, ochrany autorských práv, bezpečnosti pri práci, bezpečnosti osôb a majetku. Reálny stav bezpečnostnej úrovne bude pravidelne sledovaný a vyhodnocovaný.

## 8.2. Požiadavky na mechanizmy ochrany aktív

### 8.2.1. Ochrana systémová komponentov IS

Systémy sa musia rozvíjať v súlade s najnovšími trendmi tak, aby bol zabezpečená spoľahlivosť a požadovaná výkonnosť. V systémoch budú implementované také bezpečnostné mechanizmy, ktoré zabezpečia predovšetkým ich dostupnosť a integritu. Použité informačné technológie musia vyhovovať požiadavke kompatibility so zámermi rozvoja organizácie a vzájomnej kompatibility medzi jednotlivými používanými systémami.

- Operačné systémy, databázové systémy
  a) Prístup k službám jednotlivých systémov musí byť zabezpečený prostredníctvom bezpečného prihlásenia sa. Musí byť znemožnené neautorizované (nepovolené) zavedenie systému z nepovoleného média a jeho používanie neautorizovanou osobou. Z bezpečnostného hľadiska je potrebné aplikovať také operačné a databázové systémy, ktoré spĺňajú požiadavky schválenej bezpečnostnej úrovne. Je potrebné minimalizovať rôznorodosť technologických platforiem operačných a databázových systémov.

- Komunikačná infraštruktúra
  a) Aj keď organizácia má vybudovanú IT komunikačnú infraštruktúra, musí v prípade jej ďalšieho rozvoja aplikovať oddelenie citlivých častí komunikačnej infraštruktúry, ktoré umožní oddelenie vnútornej siete od vonkajšej siete, alebo oddelenie vnútorných sietí tak, aby bolo možné kontrolovať a riadiť tok údajov medzi oddelenými časťami. Kritické časti komunikačnej infraštruktúry musia byť navrhnuté tak, aby umožnili vytvoriť záložné (redundantné) spojenia.
  b) Vstupy do systému budú kontrolované na prítomnosť vírusov. Každý vstupný bod bude vybavený mechanizmom, ktorý bude robiť pravidelné prehliadky systému.
  c) Komunikačné rozvody (počítačové siete, telekomunikačné siete) musia byť chránené pred poškodením, zničením a zneužitím. Pripojovanie zariadení ku komunikačnej infraštruktúre musí byť centrálne riadené a kontrolované, musí sa zamedziť pripojovaniu nepreverených systémov a systémov, ktoré neboli schválené príslušnými bezpečnostnými orgánmi organizácie.

- Archivácia a zálohovanie
  a) Technológie zálohovania, archivácie a obnovy musia byť implementované tak, aby Čas obnovy zodpovedal požiadavkám na zabezpečenie kontinuity funkcií.
  b) Musia byť navrhnuté a implementované procedúry, upravujúce zálohovanie údajov a programového vybavenia.

- Evidencia a správa porúch
  a) U prevádzkovateľa musí byť navrhnutý a implementovaný primeraný systém podpory používateľov a systém správy porúch, ktorý zabezpečí detekciu, izolovanie, opravu a dokumentovanie chýb systémov a komponentov informačného systému.

### 8.2.2. Ochrana údajov

V rámci prevádzkovateľa existuje niekoľko typov údajov, ktorých prezradenie, strata, alebo zničenie by mali za následok negatívny dopad na strategické záujmy prevádzkovateľa a na pravá dotknutých osôb. Patria sem predovšetkým údaje spracovania finančných hotovostí, strategické údaje prevádzkovateľa, osobné údaje partnerov, obchodných klientov a zamestnancov.

- Klasifikácia údajov
  a) Požiadavky na ochranu pre všetky údaje nie sú rovnaké, preto bude potrebné stanoviť kategórie údajov podľa stupňa ich citlivosti a tiež kritériá zaraďovania údajov do jednotlivých kategórií. Pre každú kategóriu údajov sa určia také bezpečnostné mechanizmy, ktoré zaručia požadovanú dôvernosť, integritu a dostupnosť údajov počas celého ich životného cyklu.
  b) Každý údaj, ktorý je spracúvaný, uložený alebo prenášaný prostredníctvom informačného systému bude zaradený do jednej z kategórií citlivosti, ktorá určuje bezpečnostné požiadavky na jeho ochranu a pravidlá prístupu pre všetkých užívateľov. Klasifikácia je zaradenie údajov do jednej z kategórií citlivosti. Za klasifikáciu je zodpovedný vlastník.

- Aplikácia voliteľného riadenia prístupu k údajom
  a) Prístup k údajom bude založený na princípe voliteľného riadenia. Každý vlastník, v spolupráci s útvarom bezpečnosti, určí pravidlá pre priradenie prístupových práv všetkým užívateľom oprávneným používať údaje v jeho správe. Aplikácia týchto pravidiel bude regulovaná príslušnými procedúrami a praktikami.

- Aplikácia princípu minimaxu
  a) Každému zamestnancovi bude priradený minimálny rozsah prístupových práv, aký je možný na plnenie jeho pracovných úloh. Aplikovaním minimaxového pravidla je možné zaručiť prístup zamestnancov k údajom, ktoré sú potrebné pre výkon ich práce a zároveň zabezpečiť vysokú úroveň dôvernosti údajov

- Identifikácia a autentizácia
  a) Identifikácia a autentizácia užívateľa sa bude vyžadovať pri prístupe k údajom. Každý používateľ pristupujúci k údajom musí mať jedinečné identifikačné údaje, na základe ktorých bude môcť získať oprávnenia pre prístup k údajom a funkciám systémov, zdieľanie identifikačných údajov viacerými osobami nie je povoľované, bude sa monitorovať a vinníci budú postihnutí podľa platných predpisov organizácie. Rozdelenie kompetencií pri prístupe k zdrojom bude zároveň slúžiť aj k ochrane citlivých údajov, čím sa má zabrániť úniku údajov.

- Definovanie zodpovedností zamestnancov
  a) Zamestnanci prevádzkovateľa, ktorí prichádzajú alebo môžu prísť do styku s citlivými údajmi a informáciami počas výkonu svojej pracovnej funkcie, musia byť prevádzkovateľom zmluvne zaviazaní zachovávať mlčanlivosť o týchto údajoch a skutočnostiach. Súčasťou pracovnej zmluvy zamestnanca bude zoznam práv a povinností týkajúcich sa ochrany údajov vyplývajúcich z jeho pracovného zaradenia. Zamestnanci budú poučení o svojich právach a zodpovednostiach prostredníctvom výchovno-vzdelávacieho programu,

- Monitorovanie prístupu k citlivým údajom
  a) Prístup alebo pokus o prístup k citlivým údajom bude kontinuálne monitorovaný zodpovedajúcimi bezpečnostnými mechanizmami a vyhodnocovaný útvarom bezpečnosti. Neautorizované prístupy a pokusy o prístup, ktoré sú v rozpore s definovanými pravidlami, budú vyšetrené a proti narušiteľom budú zavedené nápravné postihy. V prípade výskytu takýchto narušení budú prijaté opatrenia na zvýšenie úrovne bezpečnosti.

- Obmedzenie prístupu externých subjektov k citlivým údajom
  a) Prístup zamestnancov externých subjektov k citlivým údajom bude obmedzený len na tie údaje, ktoré externí dodávatelia potrebujú pre svoju prácu. Riadenie prístupu zamestnancov dodávateľských firiem bude upravené špecifickými procedúrami a technickými opatreniami.
  b) Zamestnanci externých subjektov sa v priestoroch organizácie, v ktorých sa nachádzajú citlivé údaje, budú môcť pohybovať len na základe odôvodnených potrieb, predchádzajúceho súhlasu zodpovedného zamestnanca a v sprievode povereného zamestnanca prevádzkovateľa.
  c) Zmluvy s dodávateľmi musia byť koncipované tak, aby zohľadňovali platnú slovenskú legislatívu z oblasti ochrany údajov, podmienky ochrany a bezpečnosti informačného systému stanovené riadiacimi dokumentmi prevádzkovateľa. Rovnaké opatrenia sa týkajú aj systémov technickej a technologickej bezpečnosti.
  d) Citlivé údaje nesmú bezdôvodne opustiť priestory prevádzkovateľa. Ak je nevyhnutné, aby citlivé údaje opustili priestory prevádzkovateľa, musia byť dodržané príslušné vnútorné predpisy a musia byť vhodným spôsobom chránené pred zničením, modifikáciou, alebo iným zneužitím.
  e) Citlivé údaje v IT zariadeniach, na médiách a dokumentácia obsahujúca citlivé údaje musí byť pri vyradení z používania spoľahlivo zlikvidovaná.

- Ochrana údajov prenášaných elektronicky
  a) Elektronicky prenášané citlivé údaje budú chránené v súlade s požiadavkami na ochranu citlivých údajov v informačnom systéme. Citlivé údaje sa môžu prenášať len v odôvodnených prípadoch.

### 8.2.3. Kvalitný a efektívny vývoj, ochrana autorských práv

- Integrácia bezpečnostných požiadaviek
  a) Pri rozvoji informačného systému alebo systémov technickej ochrany budú zohľadňované bezpečnostné požiadavky vlastníkov a požiadavky útvaru bezpečnosti a budú v súlade s vnútornými predpismi prevádzkovateľa. Bezpečnostné požiadavky vyplývajúce z Bezpečnostnej politiky a ďalších riadiacich dokumentov budú zakomponované do vyvíjaných častí informačného systému tak, aby sa eliminovali náklady na ich dodatočné zapracovanie po ukončení procesu vývoja. Na vývoji sa budú podieľať aj špecialisti zodpovední za bezpečnosť

- Bezpečnosť dokumentácie
  a) Dokumentácia projektov informačného systému (tj. zdrojové a vykonateľné kódy, implementačné postupy) alebo systémov technickej ochrany bude chránená pred prístupom neautorizovaných osôb a pred neautorizovanými zmenami.

- Testovanie
  a) Pred distribúciou nakúpeného alebo vyvíjaného programového vybavenia budú vykonané zodpovedajúce testy v testovacom prostredí tak, aby sa zamedzilo následným škodám v ostrej prevádzke. Rovnako aj systémy technickej ochrany budú podrobené zodpovedajúcim testom).

- Ochrana autorských práv
  a) Distribúcia softvéru musí byť riešená tak, aby nedochádzalo k nelegálnemu kopírovaniu softvéru. Cieľom pravidelných kontrol je odhaliť nelegálne používanie softvéru, z ktorého budú vyvodené sankcie voči osobám, ktoré konali úmyselne alebo nedbalo.

### 8.2.4. Ochrana osôb a personálna bezpečnosť

Jedným z kľúčových aktív prevádzkovateľa sú osoby. Osoby sú zamestnanci, návštevy a partneri, ktorí sa nachádzajú v priestoroch prevádzkovateľa s jej súhlasom. Všetky systémy prevádzkovateľa musia byť chránené pred nelegálnou alebo neautorizovanou činnosťou osôb.

U každého prevádzkovateľa existujú vysoké hrozby zo strany vlastných zamestnancov, prípadne tretích osôb, ktoré sa môžu podieľať na útokoch na informačný systém, alebo pri realizovaní inej trestnej činnosti s cieľom získania finančného prospechu. Ľudia sú najslabším článkom bezpečnostnej štruktúry, a preto je potrebné venovať tomuto problému zvýšenú pozornosť. V nasledujúcej časti sú stanovené základné zásady a bezpečnostné požiadavky, ktoré bude prevádzkovateľ aplikovať v oblasti personálnej bezpečnosti.

- Zamedzenie neautorizovanému zhromažďovaniu a poskytovaniu údajov
  a) IT zariadenia (počítače) prevádzkovateľa obsahujú osobné údaje zamestnancov, údaje o službách a prácach realizovaných na prospech prevádzkovateľa, ako aj ďalšie citlivé údaje. Pre prevádzkovateľa je neprijateľná strata dôvernosti, neautorizované sprístupnenie a zneužitie údajov a znalostí. Činnosť zamestnancov, neautorizované akcie a pokusy o narušenie bezpečnostného systému budú monitorované a vyhodnocované. Záznamy budú analyzované útvarom zodpovedným za bezpečnosť, V prípade, že sa zistí narušenie bezpečnosti, bude vykonané vyšetrovanie s cieľom objasniť príčiny, pôvod incidentu, eliminovať jeho následky a vyvodiť dôsledky.

- Reakcia prevádzkovateľa pri nátlaku na zamestnancov
  a) Zamestnanci organizácie musia mať istotu, že táto podnikne všetky legálne akcie v prípadoch, keď budú vystavení tlaku nútenej nelegálnej spolupráce, alebo vydierania. Vedenie organizácie musí vyvinúť maximálne úsilie s cieľom mať prehľad o počte a dôležitosti prípadov vydierania, ktorým môžu čeliť zamestnanci na jednotlivých pracoviskách. Vedenie organizácie je zodpovedné za účinnú a citlivú reakciu na tieto incidenty, pričom bude využitý systém hlásenia bezpečnostných incidentov.

- Zníženie pravdepodobnosti omylu zamestnanca
  a) Problémom, ktorý vyplýva z prístupu osôb k údajom a informáciám, je riziko náhodného omylu. Na ochranu pred týmto rizikom budú v organizácii navrhnuté a uplatňované bezpečnostné a kontrolné mechanizmy a organizačné opatrenia, ktoré obmedzia pravdepodobnosť vzniku omylu a zabezpečia odhalenie omylu, ktorý

môže spôsobiť značné škody. Tieto opatrenia budú navrhované a testované v štádiu vývoja a testovania informačných systémov alebo systémov technickej bezpečnosti. Kontrolné mechanizmy budú zavedené aj v procesoch poskytovaných služieb tak, aby sa zabránilo možnému narušeniu alebo podvodu predovšetkým zo strany zamestnancov, ale aj zo strany verejnosti.

- Výchovno-vzdelávací program bezpečnostné povedomie
  a) Zodpovednosť a bezpečnostné povedomie zamestnancov organizácie sa bude zvyšovať primeraným komplexom výchovno-vzdelávacích aktivít. Zamestnanci musia mať pocit zodpovednosti za ochranu hmotných aj nehmotných aktív prevádzkovateľa. Cieľom výchovno- vzdelávacieho programu je stotožnenie sa zamestnancov s realizovanými bezpečnostnými opatreniami a vytvorenie bezpečnostného povedomia. Výchovno-vzdelávací program má umožniť zníženie rizík predovšetkým zo strany zamestnancov a rozvíjať prirodzenú lojalitu zamestnancov k prevádzkovateľa.

- Stanovenie zodpovedností a právomocí zamestnancov
  a) Každému zamestnancovi budú priradené také zodpovednosti a právomoci, aby mohol vykonávať úlohy, ktoré mu vyplývajú z jeho pracovnej náplne. Každý zamestnanec musí mať stanovený rozsah fyzického prístupu do budovy a jej častí, kde sa nachádzajú chránené aktíva prevádzkovateľa. Každý zamestnanec bude mať stanovený rozsah prístupu k zdrojom informačného systému.
  b) Poučenie zamestnancov o ich zodpovednostiach a právomociach v rámci organizačnej štruktúry bezpečnosti sa bude vykonávať v rámci výchovno-vzdelávacích aktivít. Každý zamestnanec bude ručiť za dôvernosť svojich autentizačných prostriedkov alebo identifikačných údajov, ktoré mu majú umožniť na vstup do kontrolovaných častí objektov resp. do informačného systému. Každý zamestnanec, ktorý poruší povinnosti, bude postihnuteľný sankciami definovanými v interných predpisoch prevádzkovateľa, prípadne v legislatíve SR. Informovanosť o postihoch za porušenie bezpečnostných pravidiel sa dosiahne prostredníctvom výchovno-vzdelávacieho programu.

- Aplikácia pravidla čistého stola
  a) Zamestnanci musia dodržiavať tzv. „pravidlo čistého stola". Všetky dokumenty, materiály, elektronické nosiče údajov, autentizačné prostriedky a pod. sa budú na stole nachádzať len v čase, ktorý je potrebný na prácu s nimi. Po ukončení práce sa tieto materiály presunú na určené bezpečné miesto.
  b) Všetky nepotrebné údaje a elektronické a papierové nosiče týchto údajov sa znehodnotia spôsobom, ktorý bude stanovený vnútornými predpismi prevádzkovateľa.

- Preverenie osôb s prístupom k citlivým údajom
  a) Pre proces prijímania nových zamestnancov, ktorí môžu prísť do styku s citlivými údajmi budú aplikované také pravidlá a postupy, ktoré vylúčia možnosť prijatia nespoľahlivých osôb alebo osôb s kriminálnou minulosťou. Tieto pravidlá a postupy budú použité aj pre preverenie zamestnancov dodávateľov, ktorí môžu prísť do styku s citlivými údajmi, alebo dôležitými komponentmi informačného systému. Prípadný odchod zamestnanca bude podmienený poučením o zachovaní dôvernosti citlivých údajov aj po skončení pracovno-právneho vzťahu.

- Motivovanie zamestnancov
  b) Dôležitým prvkom bezpečnostného systému je stabilizácia pracovného kolektívu, predovšetkým kľúčových zamestnancov. Bude použitý systém motivovania a odmeňovania kľúčových zamestnancov prevádzkovateľa, ktorých odchod môže vážne ohroziť funkčnosť bezpečnostných systémov.

- Kontrola pohybu partnerov a návštev v objektoch prevádzkovateľa
  a) Pohyb partnerov a návštev v priestoroch prevádzkovateľa musí byť riadený a kontrolovaný.
  b) Každej osobe budú prístupné len tie priestory, ktoré potrebuje na vybavenie svojich oprávnených požiadaviek.
  c) Pri sprístupňovaní priestorov bude dodržaná zásada ochrany zdravia a života osôb. Na riadenie a kontrolu pohybu cudzích osôb a ochranu ich zdravia budú využité mechanizmy technickej bezpečnosti a organizačné opatrenia.

- Pravidlá pre výber a prácu dodávateľov
  a) Pri výbere dodávateľov prevádzkovateľa bude potrebné zároveň s kritériami kvality brať do úvahy aj bezpečnostné požiadavky. Poskytované služby musia vyhovoval bezpečnostným požiadavkám prevádzkovateľa.
  b) Pre prístup externých dodávateľov do priestorov prevádzkovateľa musia byť aplikované také metódy a postupy, ktoré umožnia dodávateľom vykonávať svoje povinnosti a práva súvisiace s predmetom dodávky, ale neumožnia im neoprávnený prístup.

### 8.2.5. Technická bezpečnosť objektov a priestorov

Ochrana budov a hmotného majetku prevádzkovateľa je dôležitým bezpečnostným prvkom ochrany osôb, údajov a zabezpečenia všetkých jeho funkcií.

- Cieľ ochrany
  a) Ochrana priestorov má umožniť dosiahnutie požiadaviek, ktoré sú kladené na ochranu osôb v priestoroch prevádzkovateľa a na ochranu údajov zaradených do všetkých tried citlivosti údajov.
  b) Bezpečnostné mechanizmy zabezpečia ochranu priestorov pred neoprávneným vniknutím do nich a ochranu hmotného majetku pred stratou, zničením a krádežou

- Bezpečnostné požiadavky
  a) Jednotlivé priestory prevádzkovateľa sa podľa úrovne rizika a potreby ochrany zaradia do jednej z bezpečnostných zón. Aplikujú sa opatrenia, ktoré zaručia bezpečnosť osôb, informácií a majetku v bezpečnostných zónach. Bezpečnostné mechanizmy schopné identifikovať vznik požiaru predtým, ako sa rozrastie do väčších rozmerov, sa implementujú všade tam, kde je to potrebné. Systémy na automatickú likvidáciu požiaru sa nainštalujú do tých priestorov, kde sú ohrozené dôležité aktíva, alebo sa v nich pohybuje veľa osôb. Technické zariadenia, ktoré umožnia efektívny protipožiarny zásah zamestnancov, sa rozmiestnia v priestoroch na to určených.
  b) Bezpečnostné zóny, ktoré to vyžadujú, budú vybavené technickými prostriedkami umožňujúcim identifikovať ich narušenie aj v dobe neprítomnosti zamestnancov. Príjmu sa účinné opatrenia, ktoré minimalizujú riziká spojené s neoprávneným

vniknutím do bezpečnostných zón prevádzkovateľa.

c) Hmotné aktíva sa poistia proti najvýznamnejším rizikám, ktoré boli identifikované a ohodnotené rizikovou analýzou, všade, kde je to potrebné a vhodné. Za hodnotenie rizík zodpovedá útvar zodpovedný za bezpečnosť. Budú vyvinuté, pravidelne testované a udržiavané plány kontinuity funkcií, ktoré zaručia funkčnosť prevádzkovateľa v prípade krízovej situácie.
d) Obnova funkčnosti bude členená do krokov:
   - havária - ochrana životov a minimalizácia Škôd,
   - zotavenie - kroky na podporu kritických funkcií,
   - obnova funkčnosti - návrat do normálneho stavu.
e) Plány kontinuity funkcií budú zostavené z havarijných plánov a plánov obnovy po havárii. Každý z uvedených plánov bude obsahovať minimálne:
   - špecifikáciu havarijného tímu, požiadavky na jeho materiálne zabezpečenie,
   - spôsob vyrozumenia zodpovedných osôb v prípade kritického narušenia,
   - opis konkrétnych krokov a činností po vzniku havarijnej situácie,
   - obnova funkcie použitím záložných alebo iných náhradných riešení,
   - nácviky zotavenia,
   - cvičné poplachy

- Vytvorenie bezpečnostných zón
  a) Priestory a budovy, v ktorých sa nachádzajú dôležité aktíva sa klasifikujú a zaradia do bezpečnostných zón podľa toho, akú úroveň ochrany vyžadujú aktíva, ktoré sa v nich nachádzajú. Zavedú sa pravidlá prístupu a pohybu zamestnancov, partnerov a návštev v jednotlivých typoch.

- Aplikácia mechanizmov protipožiarnej ochrany
  a) Vo všetkých priestoroch, v ktorých ukáže riziková analýza za potrebné, budú naprojektované a nainštalované systémy elektronickej požiarnej signalizácie (EPS), ktoré budú pripojené na jeden, alebo viacero centrálnych kontrolných (signalizačných) pultov. Technické zariadenia, ktoré umožnia efektívny zásah proti požiaru (hasiace prístroje a pod.) budú umiestnené všade tam, kde to vyžadujú normy, legislatíva, alebo bezpečnostné a protipožiarne požiadavky.

### 8.2.6. Ochrana fyzického prístupu ku kritickým komponentov IS a ostatných dôležitých aktív

Prístup k dôležitým komponentom informačného systému alebo ostatným dôležitým aktívam bude riadený technickými prostriedkami. Riadenie prístupových práv budú upravovať praktiky a procedúry vypracované počas implementácie Bezpečnostnej politiky a modifikované podľa miestnych podmienok.

Pracovný priestor, v ktorom sa nachádzajú komponenty informačného systému alebo ostatné dôležité aktíva bude v neprítomnosti zamestnancov chránený vhodnými bezpečnostnými mechanizmami, ktoré budú vybrané v závislosti od druhu komponentu a spôsobu umiestnenia. Každý pokus o narušenie bezpečnostného mechanizmu bude hlásený, zaznamenaný a vyhodnotený útvarom bezpečnosti.

Používanie, uchovávanie a správu kľúčov alebo iných prostriedkov, ktoré umožňujú vstup do chránených priestorov, budú upravovať praktiky a procedúry vypracované počas implementácie Bezpečnostnej politiky a modifikované podľa miestnych podmienok. Tieto musia upravovať aj spôsob prístupu mimo pracovných hodín pre prípad havárie, alebo práce mimo bežnej pracovnej doby

- Budovanie vhodných priestorov
  a) Komponenty IS alebo iné dôležité aktíva, ktoré to vyžadujú, sa budú nachádzať v priestoroch, ktoré spĺňajú špeciálne požiadavky na ich technickú a režimovú bezpečnosť. Pri projektovaní priestorov alebo objektov musia byť akceptované odborné požiadavky zamestnancov zodpovedných za bezpečnosť a ochranu aktív.

### 8.2.7. Plány kontinuity funkcií - havarijné plány

Pre obnovu funkčnosti činnosti prevádzkovateľa v prípade krízovej situácie budú vyvinuté a nepretržite udržiavané a testované plány na zachovanie kontinuity funkcií. Krízovou situáciou sa pre účely tohoto bezpečnostného dokumentu myslí také narušenie funkcií, jeho komunikačnej a informačnej infraštruktúry, údajov a pracovných tímov, ktoré vedú alebo môžu viesť k zastaveniu alebo výraznému obmedzeniu činnosti prevádzkovateľa. Plány na zachovanie kontinuity funkcií pozostávajú:

- z havarijných plánov,
- plánov na obnovu funkčnosti.

Havarijné plány popisujú spôsob reakcie na incident hneď ako vznikne, postup zvládnutia incidentu a obnovu základných funkcií - činností. Aplikácia plánov na obnovu funkčnosti zabezpečí úplnú obnovu funkčnosti po tom, ako bola zvládnutá havarijná situácia. Činnosť zamestnancov zainteresovaných na incidente počas krízovej situácie budú popisovať špecifické procedúry.

### 8.2.8. Ochrana dobrého mena prevádzkovateľa

Nehmotné aktíva, ktoré musí organizácia chrániť, sú predovšetkým jej dobré meno, kredit u verejnosti, partnerských organizácii a etický štandard zamestnancov. Nehmotné aktíva sú neoddeliteľnou a veľmi dôležitou súčasťou vlastníctva prevádzkovateľa.

Pre oblasť ochrany aktív budú prijaté také technické a organizačné opatrenia, ktoré majú vplyv aj na ochranu týchto nehmotných aktív.

Budú vypracované také procedúry, ktoré znemožnia alebo sťažia konanie zamestnancov a iných osôb, ktoré by mohli poškodiť dobré meno organizácie.

### 8.2.9. Organizačná štruktúra bezpečnosti

Pre spoľahlivý a efektívny výkon bezpečnosti prevádzkovateľa je dôležité vytvorenie

stabilnej organizačnej štruktúry, ktorá zahrnie bezpečnosť informačného systému, bezpečnosť technickú a personálnu, ako aj bezpečnosť technologickú.

- Organizačná Štruktúra bezpečnosti musí byť navrhnutá tak, aby plnila nasledujúce úlohy :
  a) špecifikácia potrebných metodických, technických a organizačných opatrení,
  b) návrh, schválenie a implementácia opatrení,
  c) prevádzka implementovaných opatrení,
  d) monitorovanie dodržiavania implementovaných opatrení.

Základným krokom k návrhu stabilnej a fungujúcej organizačnej štruktúry bezpečnosti je pochopenie všeobecného modelu funkčnej štruktúry bezpečnosti (ďalej len „všeobecný model").

Základným krokom k návrhu stabilnej a fungujúcej organizačnej štruktúry bezpečnosti je pochopenie všeobecného modelu funkčnej štruktúry bezpečnosti (ďalej len „všeobecný model").

Všeobecný model funkčnej štruktúry organizácie bezpečnosti

Všeobecný model definuje jednotlivé organizačné zložky bezpečnostného systému a významné funkčné väzby medzi nimi. Úlohou všeobecného modelu nie je navrhnúť, akým spôsobom budú jednotlivé organizačné zložky začlenené do organizačnej štruktúry prevádzkovateľa, ale stanoviť zásady odborne a metodicky správnych a úplných organizačných vzťahov.

- Všeobecný model funkčnej štruktúry bezpečnosti systému je založený na dvoch princípoch:
  a) na princípe vlastníctva, t. j. zodpovednosti za funkčnosť,
  b) na princípe centrálnej správy bezpečnosti a centrálne riadenej metodiky bezpečnosti.

- Všeobecný model má tri úrovne riadenia:

a) úroveň stratégie a auditu,
b) úroveň operačného riadenia (implementácie),
c) úroveň prevádzky a realizácie (aplikácie/administrácie).

Na úrovni stratégie a auditu sa riešia koncepčné otázky týkajúce sa bezpečnosti informačného systému, technickej a režimovej bezpečnosti, personálnej bezpečnosti a technologickej bezpečnosti. Organizačné zložky tejto úrovne rozhodujú o riadení rizík a globálnych bezpečnostných opatreniach, autorizujú implementované bezpečnostné mechanizmy a kontrolujú dodržiavanie Bezpečnostnej politiky.

Úroveň operačného riadenia bezpečnosti metodicky riadi zložky, ktoré sa nachádzajú na úrovni prevádzky a realizácie. Priamo riadi výkon niektorých kritických bezpečnostných činností na úrovni prevádzky a realizácie. Organizačné zložky tejto úrovne riadia návrh a implementáciu konkrétnych bezpečnostných mechanizmov a zodpovedajú za ich dodržiavanie.

Rovnako sa podieľajú na príprave vnútropodnikovej legislatívnej základne bezpečnosti.

Zložky na úrovni prevádzky a realizácie zodpovedajú za implementáciu a správu konkrétnych bezpečnostných mechanizmov a vykonávajú ostatné činnosti týkajúce sa bezpečnosti podľa platných metodických postupov, štandardov a projektovej dokumentácie.

- Všeobecný model funkčnej štruktúry prevádzkovateľa bezpečnosti informačného systému má dve logicky oddelené časti:
  a) funkčnú časť, ktorá zabezpečuje služby a funkcie prevádzkovateľa (útvary užívateľov),
  b) časť, ktorá zabezpečuje bezpečnostné funkcie (útvar bezpečnosti).

- Prevádzkovateľ zavedie také organizačné opatrenia:
  a) ktoré umožnia efektívne riadiť bezpečnostný systém,
  b) umožňujúce monitorovanie incidentov a narušení,
  c) umožňujúce naplnenie cieľov stanovených týmto projektom,
  d) definuje jasné práva a povinnosti svojich zamestnancov,
  e) v súlade s platnou legislatívou menuje zamestnanca zodpovedného za bezpečnosť, stanoví jeho povinnosti a vymedzí jeho kompetencie.

Útvar bezpečností by mal pracovať (byť organizačne začlenený) nezávisle od správcu informačného systému. Útvar bezpečnosti a správa informačného systému sa zodpovedá vedeniu organizácie. Stav bezpečnostného systému, analýza bezpečnostných incidentov a ich zvládnutie bude pravidelne vyhodnocované

### 8.2.10. Poznávanie stavu bezpečnostného systému a hlásenie bezpečnostných incidentov

Významným faktorom efektívneho bezpečnostného systému je jeho schopnosť poskytnúť informácie o aktuálnom stave bezpečnostných opatrení implementovaných na ochranu aktív.

Stav bezpečnostného systému bude monitorovaný zamestnancami z útvaru bezpečnosti využitím automatizovaných prostriedkov s centrálnou správou. Monitorovanie stavu bezpečnostného systému musí byť zamerané na sledovanie neautorizovaných činností užívateľov, odhaľovanie prienikov do informačného systému a predikciu bezpečnostných incidentov. Monitorovací systém nesmie byť zneužitý na sledovanie zamestnancov. V prípade, že sa zistí narušenie bezpečnosti, bude vykonané vyšetrovanie s cieľom objasniť príčiny, pôvod incidentu, eliminovať jeho následky a vyvodiť dôsledky.

Bezpečnostné incidenty, ktoré nie je možné monitorovať automatizovanými prostriedkami, budú monitorované doterajšími zaužívanými metódami. Rovnako aj riešenie takýchto incidentov bude prebiehať zavedenými metódami vlastného vyšetrovania, pokiaľ to situácia dovoľuje. Všetky takto zistené bezpečnostné incidenty budú zaznamenané a budú pravidelne vyhodnocované.

**„Bezpečnostný incident je akákoľvek udalosť s cieľom narušiť bezpečnosť informačného systému, technickú bezpečnosť priestoru alebo objektu, bezpečnostný mechanizmus aplikovaný v rámci prevádzkovaných technológií. Bezpečnostný incident môže byť vyvolaný náhodným faktorom, neúmyselným činom alebo úmyselným útokom alebo**

**podvodom"**

- Každý bezpečnostný incident bude zaradený do jednej z kategórií, podľa naliehavosti jeho riešenia:
  a) **okamžitý zásah** - incidenty, ktoré pravdepodobne spôsobia škody alebo ich už spôsobili, ohrozujú bezpečnosť alebo plynulosť spracovania údajov v informačnom systéme, prípadne sa môžu rozšíriť (požiar, nedostupnosť zdrojov, komunikácií a pod.),
  b) **prioritný zásah** — incidenty, ktoré svojou podstatou porušili platnú legislatívu SR alebo interné normy prevádzkovateľa a následne môžu spôsobiť narušenie bezpečnosti (podozrenie zo zneužívania údajov a porušenia práv a slobody fyzických osôb, neštandardné akcie dodávateľa, porušenie autorských práv,.)
  c) **rutinný zásah** - incidenty, ktoré sú očakávané alebo existuje podozrenie z ich výskytu (vírusy, opakované zablokovanie a pod.)

# 9. Vymedzenie okolia IS a jeho vzťah k možnému narušenie bezpečnosti

Pre kvalitný návrh Bezpečnostnej politiky je nevyhnutné dobré poznanie okolia, ktoré vplýva na fungovanie prevádzkovateľa. Okolie prevádzkovateľa je možné rozčleniť do nasledujúcich kategórií:

- Ľuďmi (pracovníkmi, návštevníkmi, zamestnancami dodávateľov servisných a iných služieb, cudzími osobami, útočníkmi, narušiteľmi)
- Fyzickým okolím - lokalitou (mestská časť, ulica, bezprostredné okolie informačného systému)
- Prírodnými vplyvmi (klimatické podmienky, počasie, prírodné energetické polia, vyššia moc)

## 9.1. Popis okolia IS tvoreného ľuďmi

Všetky systémy organizácie musia byť chránené pred nelegálnou alebo neautorizovanou činnosťou osôb. Osoby, ktoré sa v priestoroch prevádzkovateľa môžu nachádzať, možno rozdeliť do nasledovných kategórií:

- Vlastní zamestnanci.
- Osoby, respektíve zamestnanci prevádzkovateľa, ktorí zmluvne zabezpečujú výkon špecifických činností súvisiacich s problematikou IS a bezpečnosti.
- Osoby, ktoré sa nachádzajú v priestoroch prevádzkovateľa s jej súhlasom.
- Cudzie osoby - návštevy sprevádzané vlastnými zamestnancami.
- Cudzie osoby - osoby pohybujúce sa bez dozoru, narušitelia zvonka.

### 1. Vlastní zamestnanci

U každého prevádzkovatelia existujú hrozby zo strany vlastných zamestnancov, ktorí sa môžu podieľať na útokoch na informačný systém. Ľudia sú najslabším článkom bezpečnostnej štruktúry a preto je potrebné venovať tomuto problému zvýšenú pozornosť. Zo Stany vlastných

zamestnancov môže dôjsť jednak k neúmyselnému konaniu (omyl, strata údajov, nedbanlivosť, neúmyselné prezradenie prístupových hesiel a pod.), ktoré môže viesť k narušeniu ochrany osobných údajov v IS, a jednak k úmyselnému konaniu (neautorizovaný prístup do IS s následnou možnosťou manipulácie s údajmi v plnom rozsahu, vrátane ich zničenia, modifikovania, odcudzenia, poskytnutia tretím subjektom a pod.). Prevenciou proti prípadným incidentom je kvalitný a stabilný kolektív s jasne definovanou organizačnou - riadiacou štruktúrou, precízne spracovanými vnútornými predpismi a korektnými pracovnými aj medziľudskými vzťahmi zamestnancov na pracovisku.

V rámci organizačnej štruktúry prevádzkovateľa majú k osobným údajom prístup nasledovní pracovníci:

| ***Funkcia*** | ***Použitie technického prostriedku*** | ***Stupeň prístupu*** | ***Stupeň oprávnenia*** |
|---|---|---|---|
| *Konateľ* | automatizovane<br>neautomatizovane | prístup ku všetkým OÚ | vytvorenie<br>prezeranie<br>zmena<br>postúpenie |
| *Externá mzdová a účtovnícka kancelária* | automatizovane<br>neautomatizovane | prístup k časti OÚ na základe sprostredkovateľskej zmluvy | vytvorenie<br>prezeranie<br>zmena<br>postúpenie |
| *Externý IT správca* | automatizovane<br>neautomatizovane | prístup k časti OÚ na základe sprostredkovateľskej zmluvy | vytvorenie<br>prezeranie<br>kopírovanie<br>zmena<br>postúpenie<br>archivácia<br>skartácia |
| *Prijímací technik* | automatizovane<br>neautomatizovane | prístup k časti OÚ v rámci svojej pracovnej náplne | vytvorenie<br>prezeranie<br>zmena<br>postúpenie<br>kopírovanie<br>archivácia<br>skartácia |

**2. Osoby, ktoré zmluvne zabezpečujú výkon špecifických činností**

Súvisiacich s problematikou IS a bezpečnosti - z hľadiska bezpečností a ochrany OÚ v automatizovaných IS prevádzkovateľa je veľmi dôležitý zmluvný vzťah s poskytovateľom servisných služieb. Vzhľadom na možnú administrátorskú úroveň prístupu k počítačom, napr. pri servisných zásahoch alebo aktualizácii programového vybavenia, môžu títo zamestnanci

získať náhodný alebo aj zámerný prístup k citlivým údajom prevádzkovateľa. Z tohto dôvodu je nevyhnutné zmluvne zakotviť požiadavky na ochranu všetkých interných údajov, ku ktorým sa servisní pracovníci môžu dostať pri vykonávaní svojej práce. Tieto požiadavky platia aj v prípade pracovníkov poskytujúcich servis zabezpečovacej protipožiarnej techniky, bezpečnostného technika a pod.

Prevádzkovateľ nemá zriadenú pozíciu informatika alebo správcu IT, tieto činnosti zabezpečuje na základe zmluvy o servisných službách externá firma.

**3. Osoby, ktoré sa nachádzajú v priestoroch organizácie s jej súhlasom**

Tieto osoby (napr. fyzické osoby, dodávatelia a odberatelia tovaru a služieb, dodávatelia a odberatelia klientov) sa pohybujú v objekte prevádzkovateľa len v pracovnom čase a ich pohyb by mal byť kontrolovaný vlastnými zamestnancami. Možnosť prístupu týchto osôb k osobným údajom je obmedzený a dôsledným dodržiavaním pravidiel uvedených v tomto dokumente ju možno prakticky vylúčiť.

**4. Cudzie osoby - návštevy sprevádzané vlastnými zamestnancami**

Návštevy by nemali mať možnosť priameho prístupu do kancelárií a ostatných miestností s OÚ a voľného pohybu po objekte. Možnosť prístupu týchto osôb k osobným údajom je obmedzená, ale nie je úplne vylúčená.

**5. Cudzie osoby**

Osoby pohybujúce sa bez dozoru, narušitelia zvonku. Tieto osoby predstavujú reálnu hrozbu z hľadiska ochrany osobných údajov, pretože v prípade úspešného nespozorovaného prieniku do priestorov, kde sa nachádzajú IS, môže dôjsť k narušeniu bezpečnosti v plnom rozsahu možných nežiadúcich aktivít. Pohybu takýchto osôb v areáli prevádzkovateľa je potrebné zabrániť spoľahlivým fungovaním organizačných opatrení, existenciou zabezpečovacieho systému a v pracovnom čase aj aktívnym spolupôsobením vlastných zamestnancov prevádzkovateľa.

## 9.2. Popis okolia záznamov tvoreného fyzickým okolím

Narušenie bezpečnosti osobných údajov je možná tak z vnútra informačného systému zo strany zamestnancov ako aj z okolia systému a to vo forme úmyselného alebo neúmyselného vplyvu okolia. Na zabezpečenie eliminácie alebo minimalizácie týchto rizík sú prijaté technické, organizačné a personálne opatrenia.

### 9.2.1. Popis a prijate bezpečnostné opatrenia- priestory prevádzkarne

Miera možného narušenia IS: nízka, priestory prevádzkarne sú zabezpečené pomocou zábranných prostriedkov:

a) Zabezpečenie pomocou mechanických zábranných prostriedkov
   - uzamykateľné dvere pri vstupe do prevádzkarne aj pri vstupe do chráneného priestoru,

- dvere kde sa spracúvajú osobne údaje majú plnú vyplň, FAB zámka,
- chránený priestor je zabezpečený pred fyzickým prístupom neoprávnených osôb,
- oddelenie chráneného priestoru od ostatných častí prevádzkarne,
- umiestnenie informačného systému v chránenom priestore,
- rozmiestnenie nábytku a počítačov vylučuje odpozeranie osobných údajov z monitora, pripadne z písomnosti dokumentov zo stola,
- fyzické nosiče sú bezpečne uložené v uzamykateľných na to zvlášť určených priestoroch,
- zobrazovacie jednotky sú umiestnené tak, aby bolo zamedzené náhodnému odpozeraniu,
- v praxi je zavedená aplikácia tzv. „ pravidlo čistého stola „. Všetky dokumenty, materiály, elektronické nosiče údajov, autentizačné prostriedky a pod. sa nachádzajú na stole len v čase, ktorý je potrebný na prácu s nimi,
- v budove je zavedený a trvalo udržiavaný protipožiarny režim (pravidlá, hasiace prístroje, evakuačné plány, signalizácia). Vzhľadom na kvalitu stavebných častí a umiestnenie informačných systémov, je minimalizované ich ohrozenie unikajúcou vodou z vodovodného a odpadového systému,

b) Registratúrne stredisko
   - dokumenty určené na archiváciu sú uložené na povale objektu, vstup majú povolene oprávnené osoby. Kľúče od archívu sú uložene u poverenej osoby,

c) Zariadenie na likvidáciu dátových nosičov osobných údajov
   - V likvidáciu osobných údajov vykonávajú oprávnené osoby skartovaním a fyzickou likvidáciou (roztrhaním), tak aby tieto údaje sa stali nečitateľnými a nemohli byť zneužité inou neoprávnenou osobou,

d) Správa kľúčov (individuálne prideľovanie kľúčov, bezpečné uloženie rezervných kľúčov)
   - kľúče sú oprávneným osobám a iným zamestnancom prevádzkovateľa prideľované v závislosti na ich funkčnom zaradení individuálne na základe preberacieho protokolu;
   - S rezervné kľúče sú uložené v zapečatenej obálke, ktorou je oprávnený disponovať len poverený člen štatutárneho orgánu prevádzkovateľa;

e) Režim údržby a upratovania chránených priestorov
   - údržba a upratovanie chránených priestorov je zabezpečovaná prevádzkovateľom individuálne určenou osobou, ktorá môže byť zastúpená len osobou odsúhlasenou prevádzkovateľom;

f) Zabezpečenie pomocou technických zabezpečovacích prostriedkov
   - prevádzkovateľ na zabezpečenie objektu využíva aj technické opatrenie - kamerový systém monitorujúci vyhradené priestory. Používanie kamerového systému, monitorujúceho vyhradené priestory, sa nevyhnutne riadi pravidlami stanovenými interným predpisom - smernicou o používaní informačného systému,

### 9.2.2. Popis a prijaté bezpečnostné opatrenia- Budova

Miera možného narušenia IS: nízka, budova je zabezpečená pomocou zábranných prostriedkov:

a) zabezpečenie pomocou mechanických zábranných prostriedkov
   - uzamykateľné dvere pri vstupe do budovy,

- dvere kde sa spracúvajú osobne údaje majú plnú vyplň, FAB zámka,

b) zabezpečenie pomocou technických zabezpečovacích prostriedkov:
   - prevádzkovateľ na zabezpečenie objektu, využíva aj technické opatrenie - kamerový systém monitorujúci vyhradene priestory. Používanie kamerového systému, monitorujúceho vyhradene priestory, sa nevyhnutne riadi pravidlami stanovenými interným predpisom - smernicou o používaní informačného systému.

c) zabezpečenie pomocou organizačných a personálnych zabezpečovacích prostriedkov:
   - Kontroluje sa príchod cudzích osôb do objektu tak, aby nedošlo k nekontrolovateľnému pohybu nepovolaných osôb do priestorov prevádzkovateľa,

d) Lokalizácia prevádzkovateľa v záplavovom území:
   - spoločnosť nie je lokalizovaná v záplavovom území, informačný systém nie je ohrozený zvýšenou hladinou riek ani prípadnou záplavou

## 9.3. Popis okolia IS tvoreného prírodným okolím

V tejto podkapitole sú popísané potenciálne ohrozenia zo strany okolia, ktoré môžu za určitých okolností nastať a návrh možných účinných opatrení.

a) Priamy vplyv prírodných energetických polí na infraštruktúru LAN

Predstavuje ohrozenie elektrických a elektronických podsystémov najmä prepätím v rozvodnej sústave počas atmosférických výbojov. Elimináciu dosahujeme inštaláciou prepäťových ochrán v napájacích sieťach a zálohovaním napájania (UPS) rozhodujúcich prvkov. Dôležitým prvkom je zabezpečenie núdzového osvetlenia dôležitých priestorov, kde sa spracúvajú osobné údaje. Narušenie bezpečnosti je možné v plnom rozsahu škály možných narušení,

b) Vplyvy počasia

Ohrozenie môže predstavovať zatekanie strechy, priamy zásah blesku a následný požiar, prípadne guľový blesk. Narušenie bezpečnosti je možné v plnom rozsahu škály možných narušení,

c) Nevhodné prostredie v kanceláriách, serverovni a v archíve

Ohrozenie predstavuje unikajúca voda pri poruche vodovodného a odpadového potrubia, prípadne kondenzát klimatizačných jednotiek. Ďalej prítomnosť hlodavcov, priame slnečné svetlo a pod. Narušenie bezpečnosti je možné v plnom rozsahu škály možných narušení,

d) Vyššia moc

Nie je možné definovať zdroje ohrozenia. Narušenie bezpečnosti je možné v plnom rozsahu škály možných narušení,

## 9.4. Popis realizácie hardvérovej a softvérovej bezpečnosti IS

### 9.4.1. Popis záznamu spracovateľských činnosti „Mzdy a Personalistika"

Automatizovaná forma spracovania sa realizuje prostredníctvom pracovných staníc, ktoré sú pripojene na internet.

a) Charakteristika

Typom dotknutých osôb pre tento informačný systém

- Sú zamestnanci prevádzkovateľa, rodinní príslušníci v prípade iných vyživovaných osôb. Súhlas so spracovaním osobných údajov nie je potrebný. Spracovanie osobných údajov je povolene zákonom č.311/2001 Z. z. Zákonník prace;
- Ak prevádzkovateľ poveril spracúvaním osobných údajov sprostredkovateľa až po získaní osobných údajov, je povinný zabezpečiť oznámenie tejto skutočnosti dotknutým osobám.
- Počet zamestnancov, ktorých sa spracovanie osobných údajov tyká, je približne 15

b) Dochádzka zamestnancov

- Je realizovaná prostredníctvom dochádzkovej knihy, do ktorej sa eviduje čas príchodu a odchodu z pracoviska;

c) Informačný systém prevádzkovateľa

- Záznam spracovateľských činnosti Mzdy a personalistika slúži na spracovanie mzdových dokladov spoločnosti.
- Spoločnosť využíva na spracovanie miezd, externú spoločnosť, z ktorou ma podpísanú sprostredkovateľskú zmluvu podľa nariadenia Európskeho parlamentu a rady (EU) 2016/679- konkrétny článok/články 28/ 2,3 Nariadenia EP a R (EÚ) o ochrane fyzických osôb pri spracovaní osobných údajov a o voľnom pohybe takýchto údajov
- Záznam spracovateľských činnosti Mzdy a personalistika sa aktuálne pracúva na jednom počítači s operačným systémom MS Windows, ktorý je pripojene do lokálnej siete, s inými počítačmi a s pripojením do internetu;
- Prístup do počítača; je podmienený zadaním prihlasovacieho mena a hesla;

d) Ochrana proti škodlivému kódu

- PC sú chránené antivírovým programom, ktorý sa automaticky aktualizuje. Antivírový program je denne niekoľkokrát aktualizovaný a kontroluje všetky vstupy do informačného systému. Riziko prieniku počítačových vírusov a ohrozenia bezpečnosti osobných údajov je malé;

e) Sieťová bezpečnosť

- Užívatelia lokálnej počítačovej siete využívajú pripojenie do internetu na elektronickú poštu a na prístup k www stránkam. V počítačovej sieti je inštalovaný HW prvok Firewall. Sieťové služby sú nastavené na vysokú mieru bezpečnosti, prienik z vonkajšej siete je málo pravdepodobný;

f) Zálohy IS dát

- V sú realizované denne na externé zariadenie : externý server;

g) Správca systému

- Spracúvané osobné údaje v hore uvedenom zaznáme o spracovateľských činnostiach zabezpečuje servis a údržbu externá spoločnosť;

h) Tlač dokumentov

- Osobne údaje sú tlačene priamo s tlačiarni , ktorá je pripojená na počítač oprávnenej

osoby. Tato osoba je prítomná priamo pri tlači. Preto zneužitie dokumentov s tlačiarni je malo pravdepodobne. Na tlač citlivých údajov sa nevyužíva tlačiareň, ktorá je umiestnená mimo kancelárii;
- Používanie kopírok nie je podmienene prístupovým kódom;

i) Poskytovanie OU
- Osobné údaje, nachádzajúce sa v hore uvedenom zaznáme o spracovateľských činnostiach, poskytuje: externá spoločnosť
  sociálnej poisťovni,
  zdravotnej poisťovni,
  daňovému úradu,
  DDS /Doplnkové dôchodkové spoločnosti/

j) Likvidácia papierových nosičov s OU
- Likvidáciu osobných údajov vykonávajú poverene osoby skartovaním, tak aby tieto údaje sa stali nečitateľnými a nemohli byť zneužité inou neoprávnenou osobou.

k) Zodpovedná osoba
- v zmysle § 44 zákona č.18/2018 Z. z. o ochrane osobných údajov pre záznam Mzdy a personalistika, nebola určená;
- Za prevádzku tohto záznamu o spracovateľských činnosti zodpovedá: Konateľ;

### 9.4.2. Popis záznamu spracovateľských činnosti „Účtovné doklady"

Automatizovaná forma spracovania sa realizuje prostredníctvom pracovných staníc, ktoré sú pripojene na internet.

a) Charakteristika
Typom dotknutých osôb pre tento informačný systém
- Sú dodávatelia a odberatelia tovaru a služieb, zamestnanci, zamestnanci klientov, dodávatelia a odberatelia klientov;
-

b) Informačný systém prevádzkovateľa
- Záznam spracovateľských činnosti Účtovné doklady slúži na spracovanie účtovných dokladov spoločnosti; Spoločnosť využíva na spracovanie účtovníctva, externú spoločnosť, z ktorou ma podpísanú sprostredkovateľskú zmluvu podľa nariadenia Európskeho parlamentu a rady (EU) 2016/679- konkrétny článok/články 28/ 2,3 Nariadenia EP a R (EÚ) o ochrane fyzických osôb pri spracovaní osobných údajov a o voľnom pohybe takýchto údajov
- Záznam spracovateľských činnosti Účtovné sa aktuálne pracúva na jednom počítači s operačným systémom MS Windows, ktorý je pripojene do lokálnej siete, s inými počítačmi a s pripojením do internetu;
- Prístup do účtovného programu je podmienený zadaním prihlasovacieho mena a hesla

c) Ochrana proti škodlivému kódu

- PC sú chránené antivírovým programom, ktorý sa automaticky aktualizuje. Antivírový program je denne niekoľkokrát aktualizovaný a kontroluje všetky vstupy do informačného systému. Riziko prieniku počítačových vírusov a ohrozenia bezpečnosti osobných údajov je malé;

d) Sieťová bezpečnosť
   - Užívatelia lokálnej počítačovej siete využívajú pripojenie do internetu na elektronickú poštu a na prístup k www stránkam. V počítačovej sieti je inštalovaný HW prvok Firewall. Sieťové služby sú nastavené na vysokú mieru bezpečnosti, prienik z vonkajšej siete je málo pravdepodobný;

e) Zálohy IS dát
   - V sú realizované denne na externé zariadenie : externý server;

f) Správca systému
   - Spracúvané osobné údaje v hore uvedenom zaznáme o spracovateľských činnostiach zabezpečuje servis a údržbu externá spoločnosť

g) Poskytovanie údajov externou spoločnosťou
   - Údaje, nachádzajúce sa v hore uvedenom zaznáme o spracovateľských činnostiach, poskytujú daňovému úradu;

h) Zodpovedná osoba
   - V zmysle § 44 zákona č.18/2018 Z. z. o ochrane osobných údajov pre záznam Účtovne doklady, nebola určená;
   - Za prevádzku tohto záznamu o spracovateľských činnosti zodpovedá: konateľ;

### 9.4.3. Popis záznamu spracovateľských činnosti „Kamerový systém"

Automatizovaná forma spracovania sa realizuje prostredníctvom pracovných staníc, ktoré sú pripojene na internet.

a) Charakteristika

Typom dotknutých osôb pre tento informačný systém
- sú dodávatelia a odberatelia tovaru a služieb, zamestnanci klientov, dodávatelia a odberatelia klientov zamestnanci;

b) Účel kamerového systému
- Monitorovanie pre zvýšenie bezpečnosti, ochrana zdravia, majetku a osôb pred krádežami, vandalizmom, prevencia pred páchaním trestných činov, porušovaním verejného poriadku, bezpečnosť a odhaľovania kriminality;

c) Informačný systém prevádzkovateľa
- Spoločnosť využíva na monitorovanie vyhradených priestorov kamerový systém s pripojením do internetu;
- Používané kamery sú digitálne;
- Zaznamenávanie beží nepretržite 24 hodín, sedem dní v týždni, 365 dní v roku, pričom je zaznamenávaný len obraz. Zvuková stopa nie je zaznamenávaná;

- Osobne údaje sú spracovane v IS, ktorého softwarové komponenty sú nainštalované v PC stanici, chránené heslom. S USB a LAN rozhraním pre účel vytvárania kópie spracovaného obrazového obsahu. Záznamové zariadenie ma vlastnú IP adresu, prostredníctvom routera je pripojená do LAN prevádzkovateľa do siete Internet. Záznamové zariadenie sa nachádza v kancelárii konateľa.

d) UPS - zdroj záložného napájania*
- S Záznamník je napojený na zdroj záložného napájania;

e) Sieťová bezpečnosť
- V počítačovej sieti je inštalovaný HW prvok Firewall;

f) Likvidácia záznamu
- Likvidácia kamerových záznamov urobených kamerovým systémom je zabezpečená automaticky, programovou činnosťou systému časovej slučke 72 hodín.

g) Správca systému
- Spracúvané osobné údaje v hore uvedenom zaznáme o spracovateľských činnostiach, zabezpečuje servis a údržbu externá spoločnosť,

h) Požiarna ochrana
- Je zabezpečená hasiacimi prístrojmi;

i) Poskytovanie audio/video záznamu
- Záznamy z KIS sa poskytujú vo veciach podozrení alebo konaní o priestupkoch a trestných činoch len príslušníkovi Policajného zboru;

j) Zodpovedná osoba
- v zmysle § 44 zákona č.18/2018 Z.z. o ochrane osobných údajov pre kamerový systém, nebola určená;
- Za prevádzku tohto záznamu o spracovateľských činnosti zodpovedá: konateľ;

**identifikácia snímacích zariadení:**

| IDENTIFIKÁCIA SNÍMACÍCH ZARIADENÍ : |
|---|
| Kamera 01 – Predajňa – Showroom: vnútorná časť |
| Kamera 02 – Dvor – parkovisko pred predajňou |
| Kamera 03 – Strojovňa umyvárky |
| Kamera 04 – umývacie boxy umyvárky |
| Kamera 05 - Vysávač |

## 9.5. Vymedzenie hraníc určujúcich množinu zvyškových rizík

Hranicu zostatkových rizík stanovuje súbor všetkých opatrení pomocou ktorých je zabezpečený normálny chod informačného systému a sú splnené všetky podmienky na

dodržiavanie zásad ochrany IS. Množina zostatkových rizík je ohraničená nepredvídateľnými udalosťami, alebo činnosťami, ktoré sa nedajú ovplyvniť.

Zostatkovým rizikom sa rozumie bezpečnostné riziko, ktoré zostane úplne alebo čiastočne nepokryté bezpečnostnými opatreniami z dôvodu, že jeho miera je pre prevádzkovateľa akceptovateľná, alebo cena technických opatrení je vzhľadom k hodnote chránených aktív neprimerane vysoká.

Ide o rizika z nasledujúcich oblasti hrozieb:

1) Teroristický útok
- Cieľom terorizmu je násilné poškodenie organizácie, čo najväčšie narušenie jej činnosti, vznik neistoty medzi zamestnancami, môže sa prejaviť uložením výbušniny, vydieraním, bratím rukojemníka, výhražnými telefonátmi, poštovými a listovými bombami.

- Pravdepodobnosť hrozieb spojených s terorizmom je nízka, rovnako miera ohrozenia osobných údajov týmto spôsobom, preto zaradujeme teroristicky útok do zostatkových rizík.

# 10. Analýza bezpečnosti

## 10.1. Analýza rizík

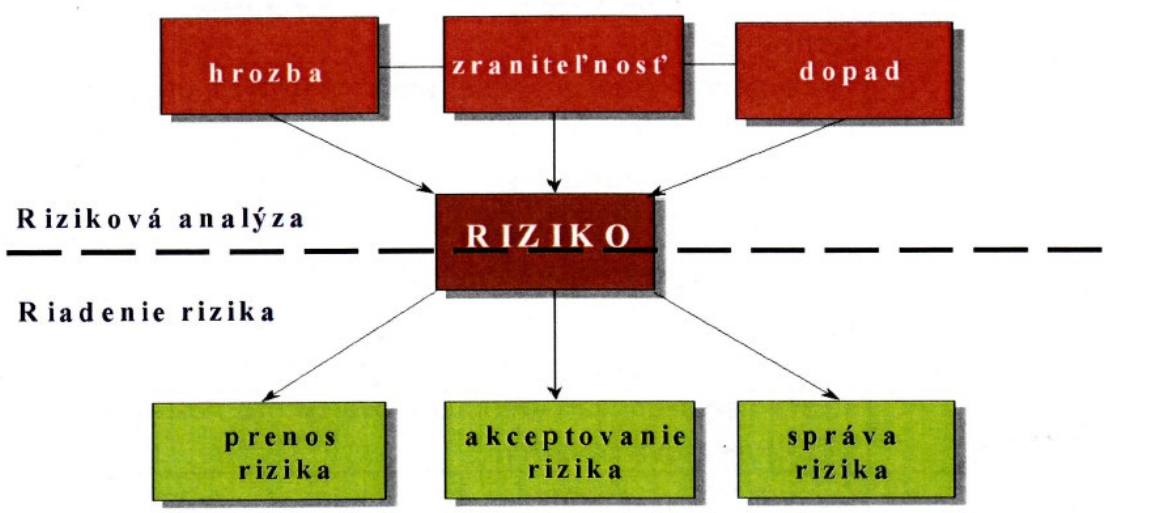
Aktíva prevádzkovateľa a jej informačného systému boli hodnotené z pohľadu možného ohrozenia rôznymi hrozbami. Výsledkom tohto hodnotenia je riziková analýza aktív informačného systému prevádzkovateľa.

1) Cieľom analýzy rizík je:
- identifikovať a ohodnotiť riziká, ktorým sú alebo môžu byť osobné údaje v skutočnosti vystavené,
- odhadnúť negatívne dopady (veľkosť ujmy), ktoré môžu vzniknúť pri neoprávnenej manipulácii s osobnými údajmi,
- identifikovať rozsah potrebných ochranných opatrení na zaistenia fyzickej bezpečnosti a objektovej bezpečnosti.

2) Základný obsah analýzy tvorí:
- identifikácia a ohodnotenie osobných údajov, ktoré majú byť chránené (určenie

veľkosti dopadu neoprávnenej manipulácie)',
- identifikácia a ohodnotenie hrozieb,
- ohodnotenie zraniteľnosti,
- stanovenie miery rizika,

3) Riziková analýza aktív informačného systému:




### 10.1.1. Hrozby

Pre potreby tvorby funkcionálnej analýzy je potrebné vytvoriť zoznam reálnych hrozieb voči aktívam, ktoré budú posudzované. Pre jednotlivé aktíva nemusia byť posudzované všetky hrozby, hodnotené budú len hrozby relevantné danému aktívu a časovému obdobiu

| ***Hrozba*** | ***Popis*** |
|---|---|
| Chyby a nekvalita údržby | Chybná prípadne nekvalitná údržba z dôvodov nedostatočnej odbornej pripravenosti pracovníkov, nedostatku náhradných dielov, materiálu a pod. |
| Chyby prenosu | Chyby vzniknuté pri prenose dát, ktorých výsledkom môže byť modifikácia údajov. |
| Ohrozenie práv a slobody fyzických osôb | Chybne spracovanie osobných údajov môže viest ujme na zdraví, majetkovej alebo nemajetkovej ujme, a to najmä ak spracúvanie môže viesť k diskriminácii, krádeži totožnosti alebo podvodu, finančnej strate, poškodeniu dobrého mena, strate dôvernosti osobných údajov chránených profesijným tajomstvom. |
| Chyby úmyselné a neúmyselne | Činnosť zamestnanca alebo inej osoby, ktorá nie je v súlade s internými a právnymi predpismi a jej výsledkom nie je snaha získať osobný prospech. |

| | |
|---|---|
| Neautorizovaná činnosť | Taká činnosť zamestnancov alebo externých návštevníkov, na ktorú nemajú oprávnenie a ktorou môžu spôsobiť organizácii škody. |
| Poruchy a chyby zariadení | Nefunkčnosť, nedostatočná alebo nesprávna funkčnosť zariadenia, chyby technických komponentov, softvéru, nedostatočnej, prípadne neodbornej údržby, nevyhovujúceho prevádzkového prostredia (vysoká teplota, vlhkosť a pod.), dosiahnutia životnosti komponentov a súčiastok. |
| Nedokumentované postupy | Vykonávanie činností bez odsúhlaseného metodického postupu len na základe overených alebo získaných skúseností. |
| Nedostatočná príprava | Nedostatočná odborná príprava zamestnancov, ktorí zabezpečujú prevádzku, správu a údržbu zariadení, systémov a aplikácii z dôvodu nedostatku školení zamestnancov. |
| Podvod alebo komplot | Cieľavedomá činnosť jednej alebo viacerých osôb (interných zamestnancov, externých spolupracovníkov a pod.), ktorej cieľom je nelegálne obohatenie sa na úkor organizácie, prípadne jej partnerov. |
| Zničenie údajov a konfigurácií | Strata, zničenie údajov spracúvaných aplikáciami, potrebných pre plynulé poskytovanie služby alebo pre správne vyúčtovanie poplatkov. Strata alebo zničenie konfigurácie operačných systémov, APV, databázových systémov, strata nastavení zariadení. Obnova týchto nastavení si môže vyžiadať veľké ľudské a časové kapacity. |

| ***Hrozba*** | ***Popis*** |
|---|---|
| Krádež | Odcudzenie zariadení, komponentov výpočtovej techniky, softvéru, dokumentácie, peňažných prostriedkov, cenín z dôvodu ich nedostatočnej fyzickej ochrany a bez použitia násilia. Krádež hmotného majetku. |
| Nespokojnosť | Nespokojnosť zamestnancov s pracovnými podmienkami, finančným ohodnotením, podporou nadriadených. Odchod kľúčových zamestnancov z dôvodu nespokojnosti. |
| Nelegálne zhromaždenie údajov | Nelegálne, neautorizované zhromažďovanie údajov. Kombináciou niektorých typov údajov, ktoré nie sú označené ako dôverné, môžu vzniknúť údaje citlivé z hľadiska prezradenia. |
| Neidentifikateľnosť vstupu | Samostatný, nekontrolovaný vstup zamestnancov do aplikácií, operačných a databázových systémov, priestorov alebo objektov bez možnosti spätne zistiť, kto a kedy sa v nich pohyboval. Nekontrolovaný pohyb zamestnancov. |

| | |
|---|---|
| Nesúlad s internou legislatívou | Nedodržiavanie, prípadne obchádzanie interných pravidiel platných v rámci prevádzkovateľa, ktoré sú vydávané v podobe smerníc, príkazov, metodických usmernení a pod. |
| Nedostatok finančných zdrojov | Nedostatok finančných zdrojov sa môže prejavovať rôznymi spôsobmi: nedostatkom zdrojov na vnútornú správu a prevádzku organizácie, nedostatkom zdrojov na rozvoj systému, aplikácií, HW komponentov, nedostatkom zdrojov na rozvoj technológií, nedostatočným finančným ohodnotením pracovníkov, slabým zabezpečením _ bezpečnostnými systémami. |
| Nejasná alebo nesprávne interpretovaná legislatíva | Nedostatočne prepracované zákony, časté zmeny zákonov a ich pomalá alebo žiadna implementácia do legislatívneho prostredia organizácie. |
| Nedostatočná centrálna správa | Nedostatočná centrálna správa môže spôsobiť nedostatočný prehľad o fungovaní zariadení, stratu hlásení o narušení bezpečnosti, nekonsolidovaným stavom databáz a pod. |
| Nedostatočné kompetencie | Nedostatok kompetencií, prekrývanie kompetencií. Problémy v komunikácii medzi jednotlivými zamestnancami. |
| Nejasná stratégia a koncepcia | Nedostatočné koncepčné riadenie zo strany vedenia, nejasná stratégia rozvoja organizácie, systémov, technickej infraštruktúry, bezpečnosti, technologickej nevyrovnanosti. |
| Odmietnutie služby | Neposkytnutie požadovanej služby, nezískanie požadovaného výstupu zo systému z dôvodu nefunkčnosti zariadení, softvéru alebo hardvéru, preťaženia alebo nedostatočnej prenosovej kapacity liniek, štrajku, nedodržanie zmluvy a pod. |
| Špionáž | Nekontrolovaná činnosť cudzích osôb, zamestnanci iných organizácií nie sú dostatočne kontrolovaní a voľne sa pohybujú v dôležitých priestoroch. |
| ***Hrozba*** | ***Popis*** |
| Poškodenie úmyselné a neúmyselné | Poškodenie zariadení, komponentov, hardvéru, softvéru, médií, hmotného majetku a pod. neúmyselne z dôvodu chybnej manipulácie, nedostatočného zaškolenia obsluhy, chyby údržby a obsluhy alebo úmyselne (snaha poškodiť organizáciu). |
| Prerušenie dodávok elektrickej energie | Prerušenie dodávky elektrickej energie do objektu kritického z hľadiska prevádzky. Môže byť spôsobené prírodnými vplyvmi (búrka, blesk, prerušenie vedenia) alebo preťažením vedenia, prípadne pripojením ďalšieho odberateľa na rozvod, ktorý nie je dostatočne dimenzovaný. Neexistencia záložného napájania s dostatočnou kapacitou. |
| Únik údajov | Získanie údajov neautorizovanými aj autorizovanými osobami a ich využitie neschváleným spôsobom s cieľom obohatenia sa. |

| | |
|---|---|
| Prinútenie k spolupráci | Prinútenie zamestnanca k neautorizovanej činnosti, podvodu alebo komplotu s externými subjektami vydieraním, prisľúbením finančného zisku a pod. |
| Nevhodné umiestnenie | Umiestnenie dôležitých aktív alebo ich častí na miestach s vysokým rizikom poškodenia požiarom, zatopením a pod., prípadne na miestach s častým pohybom osôb. |
| Výtržnosť | Náhodné narušenia objektov alebo systémov v dôsledku neplánovaných aktivít (demonštrácie v okolí, kultúrne a športové podujatia) s následným narušením priestoru, vniknutie do objektu, prerušenie normálnej práce, vandalizmus. |
| Ohrozenie osôb | Pomsta, vydieranie alebo psychologický nátlak s možnosťou ohrozenia zdravia alebo života zamestnancov, partnerov, návštev a iných osôb nachádzajúcich sa v priestoroch prevádzkovateľa. |
| Prírodné katastrofy a priemyselné nehody | Pod prírodné katastrofy a priemyselné nehody spadá zaplavenie, skrat na vedení, zanedbanie protipožiarnych opatrení, úmyselné založenie požiaru, neúmyselné založenie požiaru, havária vo výrobe, zosuvy pôdy a pod. |
| Single point of failture | Existencia jedného miesta (komponentu, zamestnanca), v ktorom sú koncentrované kritické aktíva organizácie bez adekvátnej náhrady, napr. sústredenie významných komponentov potrebných pre zabezpečenie niekoľkých služieb organizácie do jedného objektu, koncentrácia viacerých funkcií jednému zamestnancovi. |
| Terorizmus | Cieľom terorizmu je násilné poškodenie prevádzkovateľa, čo najväčšie narušenie jej činnosti, vznik neistoty medzi zamestnancami. Môže sa prejaviť uložením výbušniny, vydieraním, bratím rukojemníka, výhražnými telefonátmi, poštovými a listovými bombami. |

Sila hrozieb je hodnotená troma stupňami:

- (V) - vysoká sila hrozby,
- (S)-stredná sila hrozby,
- (N) - nízka sila hrozby.

### 10.1.2. Zraniteľnosť

Zraniteľnosť je slabé miesto v systéme, ktoré môže spôsobiť realizáciu hrozby a narušenie bezpečnosti systému. Zraniteľnosť je hodnotená troma stupňami: 1

- (V) - vysoká zraniteľnosť,
- (S) - stredná zraniteľnosť,
- (N) - nízka zraniteľnosť.

### 10.1.3. Strategické osi

Strategické osi predstavujú zovšeobecnený súbor hlavných záujmov, činností a cieľov organizácie, ktorých zachovanie a ochrana je z nejakých dôvodov nutná. V rizikovej analýze bol vyhodnotený dopad jednotlivých hrozieb na strategické osi (kritické funkcie), ktoré sú relevantné pre hodnotený systém v dôsledku realizácie niektorej z hrozieb.

| *Kód* | **Strategická os** | **Popis** | **Váha** |
|---|---|---|---|
| *1* | Poskytovanie služieb | Zabezpečenie poskytnutia prezentovaných služieb fyzickým osobám, ale aj ostatným partnerom. | 1 |
| *2* | Pružne reagovať na požiadavky verejnosti | Zabezpečenie služieb na úrovni, podriadenie sa neustálemu vývoju | 1 |
| *3* | Poskytovanie kvalitných služieb | Zabezpečenie realizovania služieb, ktoré sú deklarované najmä z časového hľadiska, dodržiavanie zákonom stanovených podmienok | 1 |
| *4* | Ochrana dobrého mena | Poškodenie dobrého mena, resp. jeho strata, strata dôvery partnerov, vládnych orgánov. Posudzované s ohľadom možných negatívnych ohlasov verejnosti a médií na potenciálne krízy (havarijné stavy) v poskytovaných službách. | 1 |
| *5* | Transparentné a jasne definované vzťahy s externými subjektami | Zabezpečenie vzťahov so všetkými partnermi. Jedná sa nielen o partnerov, pre ktorých sa služby realizujú, ale aj o externé subjekty. | 1 |
| *6* | Ekonomická stabilita | Zabezpečenie vstupného toku financií.<br>Zabezpečenie a sprehľadnenie toku financií pre zabezpečenie bežných prevádzkových činností. | 1 |
| *7* | Riadenie a rozvoj ľudských zdrojov | Zabezpečenie kvalitného, odborne vzdelaného a stabilného personálu schopného podporovať základné funkcie. | 1 |

### 10.1.4. Dopad

Je výsledok pôsobenia realizovanej hrozby na strategickú os. Dopad sa môže prejaviť znížením integrity, dostupnosti alebo dôvernosti hodnoteného aktíva. Veľkosť dopadu je priamoúmerná počtu zasiahnutých strategických osí a ich váham. Hodnotu dopadu bude tvoriť súčet váh strategických osí zasiahnutých hodnotenou hrozbou.

| **Suma dopadov** | Hodnotenie |
|---|---|
| **0** | 0 |
| **1-2** | 1 |

| | |
|---|---|
| **3-4** | 2 |
| **5-7** | 3 |
| **8 a viac** | 4 |

### 10.1.5. Hodnotenie rizika

Katalóg rizík definuje všetky možné ohrozenie, ktoré môžu pôsobiť na aktíva alebo chránené osobné údaje. Pre účely vyhodnotenia možnosti ohrozenia osobných údajov boli riziká rozdelené do nasledujúcich skupín:

- priemyselné havárie
- teroristické útoky alebo ohrozenie
- cudzie osoby
- vlastní zamestnanci - neoprávnené osoby
- vlastní zamestnanci - oprávnené osoby
- priemyselná špionáž, konkurencia
- prírodné katastrofy
- ohrozenia vzniknuté činnosťou technických prostriedkov - informačných systémov,
- ohrozenia vzniknuté používaním a prevádzkovaním prostriedkov fyzickej bezpečnosti
- sociologické ohrozenie
- pravá slobôd fyzických osôb

Riziko je definované ako funkcia nasledujúcich faktorov:

- hodnoty aktív
- hrozieb, ktorým môžu byť osobné údaje v skutočnosti vystavené,
- zraniteľnosti, ktorá môže byť využitá hrozbami na neoprávnenú manipuláciu s osobnými údajmi,
- existujúcich alebo plánovaných bezpečnostných opatrení.

Veľkosť rizika sa určovala „stupňami hodnotenia rizika" (v časti Analýza rizík príloha - tabuľka č. 1 Miera rizika) nasledovne:

a) Nízka pravdepodobnosť, že príslušné ohrozenie nastane znamená, že toto ohrozenie môže nastať iba výnimočne a je dostatočne eliminované základnými opatreniami, požitím mechanických zábran a základných režimových opatrení
b) Stredná pravdepodobnosť znamená takú intenzitu hrozby, ktorej je potrebné venovať zvýšenú pozornosť a eliminovať dôsledky je možné špecifickými opatreniami
c) Vysoká pravdepodobnosť je tak závažná, že vyžaduje relatívne časté preverenie všetkých opatrení na elimináciu. Opatrenia na elimináciu vyžadujú nadštandardné aktivity.

Výška rizika je číselná hodnota v rozpätí 0-8, ktorá sa určuje podľa sily hrozby, výšky

zraniteľnosti a hodnoty dopadov.

Z tabuľky vyplýva, že najvyššia hodnota rizika je 8 a najnižšia je 0. Pre prijatie zodpovedajúcich opatrení a ľahšiu orientáciu môžeme zaviesť pomocné hodnotenie rizika v štyroch kategóriách.

| ***Názov*** | **Hodnotenie podlá tabuľky** | **Opatrenia** |
|---|---|---|
| *Zostatkové riziko* | 0 až 1 | Nemusia byť prijaté opatrenia. Riziko je potrebné sledovať a pravidelne |
| *Nízke riziko* | 2 až 4 | Plánovať aplikáciu opatrení v období nad jeden rok. |
| *Vážne riziko* | 5 až 6 | Plánovať aplikáciu opatrení v blízkom období (jednotky mesiacov). |
| *Kritické riziko* | 7 až 8 | Prijať okamžité opatrenia proti identifikovanej hrozbe. |

**Popis položiek funkčných rizík**

V nasledujúcej tabuľke je uvedený prehľad položiek katalógu funkčných rizík.

| ***Položka*** | **Popis** |
|---|---|
| *Aktívum - POPIS* | Aktíva uvedené v tabuľke boli identifikované počas funkcionálnej analýzy rizík. |
| *Hrozba - popis* | V tomto stĺpci sú uvedené hrozby zo zoznamu hrozieb, ktoré sú relevantné pre dané aktívum. Ak je hrozba aplikovateľná na aktívum, ale spôsobuje len nízke riziko, neuvádza sa |
| *Hrozba - C, 1, A* | V týchto stĺpcoch je uvedené, ktoré z bezpečnostných potrieb - C - dôvernosť (Confidentality), 1 - integrita (Integrity), A - dostupnosť (Availability) - môže hrozba ovplyvniť. |
| *Hrozba - sila.* | Tento stĺpec udáva silu hrozby voči aktívu za predpokladu, že nie sú implementované žiadne bezpečnostné opatrenia. Sila hrozieb je v súlade s metodikou hodnotená troma stupňami: (V) -vysoká, (S) -stredná a (N) - nízka sila hrozby |

| | |
|---|---|
| *Zraniteľnosť - popis* | Stĺpec určuje zraniteľnosť v zmysle dôvernosti, dostupnosti a integrity. Nevzťahuje sa len na súčasnú zraniteľnosť organizácie, ale odráža aj jej predpokladaný vývoj |
| *Zraniteľnosť- hodnota* | Stĺpec udáva veľkosť zraniteľnosti aktív. Zraniteľnosť je hodnotená troma stupňami (V) - vysoká, (S) - stredná a (N) - nízka. |
| *Dopady na strategické osi - popis* | V stĺpcoch je zoznam strategických osí. U tých osí u ktorých je možné očakávať dopady v dôsledku realizácie hrozieb je vyznačená váha týchto zasiahnutých osí, u osí u ktorých sa zasiahnutie nepredpokladá je prázdne pole. |
| *Dopady na strategické osi - hodnota* | V tomto stĺpci je ohodnotená veľkosť dopadov. Spôsob určenia hodnoty dopadov je popísaný vyššie. |
| *Riziko - hodnota* | Tento stĺpec určuje úroveň rizík pre jednotlivé aktíva. Riziká sa hodnotia v súlade s metodikou v škále od 0 po 8. Po odsúhlasení bude kritériom implementácie bezpečnostných mechanizmov. |
| *Riadenie rizika* | V tomto stĺpci sa nachádza návrh konzultantov na riadenie rizika. Do úvahy prichádzajú tri možnosti (S) - správa, (P) - prenesenie, (A) - akceptovanie. |

V súlade s požiadavkami zákona bola vyhodnotená možnosť narušenia (ohrozenia) týchto vlastností osobných údajov:

- Dôvernosť je vlastnosť informácie, ktorá zabezpečuje, že informácie sú dostupné len tým subjektom, ktoré majú k nim autorizovaný prístup. Informácie nebudú poskytnuté neoprávneným subjektom, pričom subjektom sa rozumie nielen používateľ, ale aj technické prostriedky a softvér.
- Integrita je definovaná ako zabezpečenie presnosti a úplnosti informácií a metód spracovania. Zaisťuje, aby informácia nebola zmenená neautorizovaným subjektom.
- Dostupnosť je definovaná ako zabezpečenie toho, aby autorizovaní používatelia mali prístup k informáciám a súvisiacim aktívam vtedy, keď to potrebujú. Zaisťuje ochranu proti odmietnutiu alebo zadržaniu služieb a zdrojov systému. Je to teda vlastnosť, ktorá zaisťuje, aby dáta boli v správnom čase na správnom mieste.

V tabuľke č. 1 je z hľadiska narušenia dôvernosti, integrity a dostupnosti osobných údajov vyhodnotená a v stĺpci „Miera rizika" uvedená celková hodnota miery rizika pri každom jednotlivom riziku.

### 10.1.6. Hodnotenie aktív informačného systému

V tejto časti analýzy sú popísané aktíva so zameraním sa na automatizované a neautomatizované prostriedky spracúvania osobných údajov. Z hľadiska bezpečnosti osobných údajov sa vyhodnocuje miera možného narušenia bezpečnosti a funkčnosti, resp. narušenie dôvernosti, integrity a dostupnosti. Narušenie bezpečnosti osobných údajov môže byť spôsobené tiež stratou funkčnosti informačného systému, stratou alebo odcudzením osobných údajov.

Identifikácia aktív umožňuje definovať hmotné a nehmotné aktíva, dáta, informácie a ďalšie hodnoty vyskytujúce sa v informačnom systéme alebo v prostredí, v ktorom je informačný systém prevádzkovaný. Na základe identifikácie je možné podľa významu stanoviť stupne citlivosti a adekvátne potreby ochrany jednotlivých aktív.

Pri vykonávaní bezpečnostnej analýzy jednotlivých aktív prevádzkovateľa, identifikácii hrozieb na tieto aktíva bola vyhodnotená miera možného narušenia a identifikácia hrozieb ohrozujúcich bezpečnosť alebo funkčnosť nasledujúcich aktív:

- klientske stanice, samostatné PC, firewall),
- sieť LAN (sieť LAN, prepojenie sietí LAN),
- programové prostriedky, dáta, súbory (operačný systém Windows, programové prostriedky MS Office (WORD, EXCEL), antivírový program,
- pamäťové médiá, na ktorých sú uložené dáta s osobnými údajmi (server, HDD, CD, DVD, externé pamäte),
- papierové dokumenty s osobnými údajmi (formuláre, spisy, dokumenty),
- priestory, v ktorých sa spracúvajú osobné údaje automatizovaným a neautomatizovaným spôsobom,
- objekt, v ktorom sú umiestnené priestory určené na spracúvanie osobných údajov
- ceniny, finančné prostriedky,
- zdroje elektrickej energie,
- dobré meno,
- ľudské zdroje,
- citlivé informácie,
- činnosť prevádzkovateľa
- komunikačné prostriedky,
- elektronický zabezpečovací systém, zábranné prostriedky
- heslá
- iné aktíva

V tabuľke č. 1 „Identifikácia aktív“ (v časti Analýza rizík viď. Príloha) je vykonaná detailná analýza možnosti ohrozenia jednotlivých aktív hrozbami, ktoré môžu narušiť ich bezpečnosť alebo funkčnosť (dôvernosť, integritu alebo dostupnosť).

Všeobecným ohrozením je odcudzenie, zničenie a strata, t. j. ukradnutie, úmyselné zničenie, neúmyselné zničenie, zničenie vplyvom vonkajších faktorov, vyhodenie, zabudnutie a pod. Takéto ohrozenie znamená ohrozenie dôvernosti, integrity aj dostupnosti. Eliminácia je možná v prípade, že sa riziko zistí dostatočne skoro a vykonajú sa opatrenia, napríklad prostredníctvom zablokovania, výmeny hesiel, vykonania protiopatrení a pod.

U niektorých aktív je dôležitý faktor narušenia autentickosti, t. j. keď aktívum generuje

nepravdivé informácie (zneužitie podpisu, doplnenie databázy o fiktívnu položku, vetu, nepravdivé podklady a pod.).

Identifikácia dopadov na aktíva (osobné údaje, informačné systémy) v dôsledku straty dôvernosti, integrity a dostupnosti spracúvaných osobných údajov - miera možného narušenia je uvedená v tabuľke č. 2 (v časti Analýza rizík viď. Príloha)

Analýza a ohodnotenie rizík založených na určení dopadov, ktoré môžu vyplynúť zo zlyhania bezpečnosti - v tejto časti analýzy sa vyhodnocuje konkrétna miera rizika pre prevádzkovateľa, miera možných následkov (dopadov) v prípade, ak zo zlyhania bezpečnosti potenciálne riziko nastane. Na základe týchto predpokladov sa vyhodnotila celková miera rizika, ktorá predstavuje kvalitatívny odhad možnosti, že riziko vznikne a ako bude reálne pôsobiť na aktíva prevádzkovateľa.

Ujma (dopad) je definovaná v jednotlivých stupňoch nasledovne:

- žiadna ujma - aktíva nebudú ohrozené (numerická hodnota =0)
- nízka ujma - dopad spôsobený na prevádzkovateľa je malého významu, spôsobí len minimálne straty bez dodatočných následkov a prejavuje sa krátkodobo - aktíva môžu byť nasledovne ohrozené (numerická hodnota = 1):

| ***Aktívum*** | **Možný dopad na aktíva (ujma)** |
|---|---|
| *Osoby - zamestnanci, návštevy, fyzická ochrana* | Nízke ohrozenie zdravia bez potreby lekárskeho zásahu |
| *Informačné systémy (sieť, HW, SW, komunikačné prostriedky)* | Nízke poškodenie, odcudzenie, strata integrity, strata dostupnosti, prípadne odcudzenie niektorých častí, ktoré nespôsobí dlhšie ohrozenie prevádzkovateľa (len niekoľko hodín) |
| *Osobné údaje, iné citlivé informácie (dáta, dokumenty s osobnými údajmi)* | Strata dôvernosti, strata integrity, strata dostupnosti s nízkou ujmou pre prevádzkovateľa |
| *Technológie* | Čiastočné poškodenie, prípadne odcudzenie niektorých častí, ktoré nespôsobí dlhšie ohrozenie prevádzky prevádzkovateľa |
| *Objekt, chránené priestory* | Poškodenie objektu |
| *Bezpečnostný systém (TZP, MZP, EZS)* | Strata dôvernosti, strata integrity, strata dostupnosti |
| *Iné* | Ohrozenie dobrého mena prevádzkovateľa |

- stredná ujma - dopad spôsobený na prevádzkovateľa je znateľný, prevádzkovateľ sa môže dostať do ekonomických alebo iných ťažkostí, ktoré sa prejavujú dlhšiu dobu - znamená takú intenzitu hrozby, ktorej je potrebné venovať zvýšenú pozornosť a eliminovať

dôsledky je možné špecifickými opatreniami, pričom môžu byť nasledovne ohrozené (numerická hodnota = 2):

| ***Aktívum*** | **Možný dopad na aktíva (ujma)** |
|---|---|
| *Osoby - zamestnanci, návštevy, fyzická ochrana* | Ohrozenie zdravia, pri ktorom môže byť potrebné lekárske ošetrenie, prípadne krátkodobá hospitalizácia, ohrozenie dobrého mena riadiacich manažérov, čo môže ohroziť čiastočne aktivity prevádzkovateľa |
| *Informačné systémy (sieť, HW, SW, komunikačné prostriedky)* | Poškodenie, odcudzenie, strata integrity, strata dostupnosti, ohrozenie, ohrozenie činnosti pri riadení a spravovaní prevádzkovateľa, ktoré spôsobí dlhodobejšie prerušenie činnosti prevádzkovateľa a následné zvýšené náklady na odstránenie následkov |
| *Osobné údaje, iné citlivé informácie (dáta, dokumenty s osobnými údajmi)* | Strata dôverností, strata integrity, strata dostupnosti citlivých informácií alebo osobných údajov, ohrozenie dobrého mena |
| *Technológie* | Poškodenie, odcudzenie, dlhodobé ohrozenie činnosti |
| *Objekt, chránené priestory* | Ohrozenie poškodenie objektu, ohrozenie regulárnej činnosti |
| *Bezpečnostný systém (TZP, MZP, EZS)* | Strata dôvernosti, strata integrity, strata dostupnosti, pričom dôjde k čiastkovému ochromeniu systému alebo obmedzenie činnosti bezpečnostného manažmentu a fyzickej resp. objektovej ochrany |
| *Iné* | Ohrozenie dobrého mena, ohrozenie regulárnej činnosti |

- vysoká ujma - dopad spôsobený na prevádzkovateľa je veľkého rozsahu, môže sa dostať do závažných ekonomických ťažkostí pôsobiacich dlhú dobu - je tak závažná, že vyžaduje relatívne časté preverenie všetkých opatrení na elimináciu. Opatrenia na elimináciu vyžadujú nadštandardné aktivity (numerická hodnota = 3):

| ***Aktívum*** | **Možný dopad na aktíva (ujma)** |
|---|---|

| | |
|---|---|
| *Osoby - zamestnanci, návštevy, fyzická ochrana* | Ohrozenie zdravia, pri ktorom je potrebné lekárske ošetrenie s následnou dlhodobou hospitalizáciou, vážne ohrozenie dobrého mena riadiacich manažérov, čo môže ohroziť aktivity prevádzkovateľa závažným spôsobom |
| *Informačné systémy (sieť, HW, SW, komunikačné prostriedky)* | Vážne poškodenie, odcudzenie, strata integrity, strata dostupnosti, ohrozenie, ohrozenie činnosti pri riadení a spravovaní prevádzkovateľa, ktoré spôsobí dlhodobé prerušenie činnosti prevádzkovateľa a následné vysoké náklady na odstránenie následkov |
| *Osobné údaje, iné citlivé informácie (dáta, dokumenty s osobnými údajmi)* | Strata dôvernosti, strata integrity, strata dostupnosti citlivých informácií alebo osobných údajov, vážne ohrozenie dobrého mena a následné vysoké náklady |
| *Technológie* | Vážne poškodenie, odcudzenie, ohrozenie činnosti prevádzkovateľa |
| *Objekt, chránené priestory* | Vážne poškodenie objektu a dlhodobé ohrozenie regulárnej činnosti prevádzkovateľa |
| *Bezpečnostný systém (TZP, MZP, EZS)* | Strata dôvernosti, strata integrity, strata dostupnosti, pričom dôjde k celkovému zlyhaniu bezpečnostných systémov dlhodobejšie ohrozenie alebo obmedzenie činnosti bezpečnostného manažmentu a fyzickej resp. objektovej ochrany |
| *Iné* | Vážne ohrozenie dobrého mena a dlhodobejšie ohrozenie regulárnej činnosti prevádzkovateľa |

V analýze miery možných následkov je takisto spracovaný opis možných následkov v prípade, ak nastane riziko a definované kľúčové miesta objektu, na ktoré môže byť smerované predpokladané riziko resp. smerovaný útok.

Vyhodnotenie ohrozenia aktív vychádza z analýzy aktív, definovaním najdôležitejších aktív školy, vyhodnotením veľkosti miery možnej ujmy, ohrozenia každého aktíva vo vzťahu ku každému riziku a efektívnosti realizovaných bezpečnostných opatrení-v časti Analýza rizík viď. Tabuľka č. 3 Vyhodnotenie miery možných následkov.

Určenie reálnej pravdepodobnosti výskytu zlyhania bezpečnosti a odhad úrovne rizík vymedzujúcim, či je riziko akceptovateľné alebo vyžaduje prijatie ďalších opatrení za využitia vopred určených kritérií na akceptáciu rizika a identifikovaných prijateľných úrovní rizika.
Vymedzenie, či je riziko akceptovateľné, alebo vyžaduje prijatie ďalších opatrení je definované

(určené) nasledovne:

- riziko pokryté
- riziko čiastočne pokryté
- nepokryté riziko

Na základe vyhodnotenia rizík, ohrozenia aktív a prijatých bezpečnostných opatrení sú odporučené protiopatrenia eliminujúce predpokladané riziká, ktoré sa realizujú v rámci fyzickej bezpečnosti a objektovej bezpečnosti, personálnej, informačnej a administratívnej bezpečnosti (bezpečnostné opatrenia sú definované v bezpečnostnom zámere).
Reálna pravdepodobnosť výskytu zlyhania bezpečnosti (možnosť, nebezpečenstvo straty, neúspechu, škody) býva definované ako určitý druh neistoty, ktorý je kvantifikované prostredníctvom štatistických metód s cieľom predpovedať vznik nepriaznivých skutočností. Predstavuje tiež označenie možnosti vzniku straty, škody alebo dosiahnutie iného výsledku oproti pôvodne predpokladanému, resp. nedosiahnutia očakávaných výsledkov, pričom odchýlky môžu byť buď priaznivé (zisk) alebo nepriaznivé (strata). Riziko však poväčšine v sebe skrýva náboj potenciálneho nebezpečenstva nepriaznivého vývoja.

Reálna pravdepodobnosť výskytu zlyhania bezpečnosti je definovaná ako funkcia nasledujúcich faktorov:

- hodnoty aktív,
- hrozieb, ktorým môžu byť aktíva v skutočnosti vystavené vrátane využitia databázy bezpečnostných rizík a jej analýzy (početnosť rizík),
- zraniteľnosti, ktorá môže byť využitá hrozbami na neoprávnenú manipuláciu s osobnými údajmi,
- existujúcich alebo plánovaných bezpečnostných opatrení.

Reálna pravdepodobnosť výskytu zlyhania bezpečnosti (v časti Analýza rizík viď. Tabuľka č. 4) je definovaná nasledovne:

- Nízka pravdepodobnosť (0,1) znamená, že toto zlyhanie môže nastať iba výnimočne a je dostatočne eliminované len základnými opatreniami použitím bezpečnostných opatrení. Početnosť týchto zlyhaní na základe databázy bezpečnostných rizík je nízke

- Stredná pravdepodobnosť (0,3) znamená, že toto zlyhanie môže nastať častejšie a je eliminované definovanými štandardnými bezpečnostnými opatreniami. Následky na aktíva môžu byť rovnako vážne. Početnosť týchto zlyhaní na základe databázy bezpečnostných rizík je stredné.

- Vysoká pravdepodobnosť (0,5) znamená, že toto zlyhanie môže nastať pomerne často a následky na aktíva môžu byť vysoké, zlyhanie nie je dostatočne eliminované bezpečnostnými opatreniami. Početnosť týchto zlyhaní na základe databázy bezpečnostných rizík je nízke.

Pokrytie rizík, určenie reálnej pravdepodobnosti je kvantifikované na základe reálnej pravdepodobnosti výskytu zlyhania bezpečnosti, mierou ohrozenia rizík, možnými následkami a súčasným riešením bezpečnostného systému - v časti Analýza rizík viď tabuľka č. 4 Reálna pravdepodobnosť výskytu zlyhania bezpečnosti.

# 11. Opatrenia na riešenie bezpečnostných rizík a mechanizmy na zabezpečenie ochrany osobných údajov na preukázanie súladu s týmto nariadením

Za bezpečnosť spracúvaných údajov zodpovedá prevádzkovateľ. Prevádzkovateľ je povinný chrániť spracúvané osobné údaje pred ich poškodením, zničením, stratou, zmenou, neoprávneným prístupom a sprístupnením, poskytnutím alebo zverejnením, akýmikoľvek inými neprípustnými formami spracúvania. Na tento účel príjme primerané technické, organizačné a personálne opatrenia zodpovedajúce spôsobu spracúvania osobných údajov, pričom berie do úvahy najmä použiteľné technické prostriedky, dôvernosť a dôležitosť spracúvaných osobných údajov ako aj rozsah možných rizík, ktoré sú spôsobilé narušiť bezpečnosť alebo funkčnosť informačného systému.

Opatrenia na riešenie bezpečnostných rizík sú súhrn pravidiel pre nastavenie bezpečnostných prvkov pri využívaní informačného systému v praxi. Spresňujú a aplikujú závery vyplývajúce z bezpečnostného projektu na konkrétne podmienky prevádzkovaného informačného systému. Je to základný dokument pre všetkých užívateľov informačného systému. Tieto pravidlá je potrebné rešpektovať pre zachovanie bezpečného chodu informačného systému v praxi.

## 11.1. Popis technických, organizačných a personálnych opatrení pre všetky účely spracovanie osobných údajov

Pre zabezpečenie bezpečnosti osobných údajov, ktoré sa spracúvajú v informačných systémoch u prevádzkovateľa prijal prevádzkovateľ nasledovné personálne, technické, organizačné a opatrenia:

### 11.1.1. Popis personálnych bezpečnostných opatrení

V oblasti personálnych bezpečnostných opatrení implementovaných za účelom minimalizácie rizík zneužitia OÚ sa uplatňujú uvedené bezpečnostné opatrenia:

1) Zabezpečiť komplexné poučenie o právach a povinnostiach vyplývajúcich zo všeobecným nariadením Európskeho parlamentu a rady (EU) 2016/679 o ochrane fyzických osôb pri spracovaní osobných údajov a o voľnom pohybe takýchto údajov.
2) Vzdelávanie zamestnancov prevádzkovateľa o právach a povinnostiach vyplývajúcich zo Zákona o ochrane osobných údajov.
3) Poučenie o podmienkach spracúvania osobných údajov v automatizovanej a neautomatizovanej forme;
4) Oboznámenie s internými riadiacimi aktmi prevádzkovateľa;
5) Prevádzkovateľ opätovne poučí poverenú 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 spracúvania osobných údajov alebo rozsah spracúvaných osobných údajov v rámci jej pracovného, služobného alebo funkčného zaradenia.
   a) Vymedzenie osobných údajov, ku ktorým má mať konkrétna poverená osoba prístup na účel plnenia jej povinností alebo úloh

- dokumentácia stanovuje rozsahu osobných údajov, ktoré sú oprávnené osoby oprávnené spracúvať;
- poverená osoba má prístup len k informačným systémom, ktoré v rámci pracovnej náplne využíva.

b) Určenie postupov, ktoré je poverená osoba povinná uplatňovať pri spracúvaní osobných údajov
   - V prevádzkovateľ vymedzil postupy, ktoré je poverená osoba povinná uplatňovať pri spracúvaní osobných údajov v internom riadiacom akte prevádzkovateľa označenom ako „Hlavné zásady ochrany osobných údajov" a v internom riadiacom akte prevádzkovateľa označenom ako „Zásady bezpečnosti pre poverene osoby -používateľov 15 ", „Zásady bezpečnosti pri správe databáz a aplikácií IS ", „Zásady bezpečnosti pri prevádzke informačných a komunikačných technológií na pracovisku IS ", „Informačná povinnosť prevádzkovateľa dotknutým osobám "a „Zásady bezpečnosti pre poverene osoby - používateľov IS kamerových systémov "
   - Z poverená osoba je povinná pri spracúvaní osobných údajov uplatňovať základné zásady ochrany osobných údajov, ktoré sú vymedzené v internom riadiacom akte prevádzkovateľa označenom ako „Hlavné zásady ochrany osobných údajov";
   - Z poverená osoba je povinná pri spracúvaní osobných údajov uplatňovať postupy, ktoré sú vymedzené v internom riadiacom akte prevádzkovateľa označenom ako „Zásady bezpečnosti pre poverene osoby -používateľov IS ", „Zásady bezpečnosti pri správe
   - databáz a aplikácií IS ", „Zásady bezpečnosti pri prevádzke informačných a komunikačných technológií na pracovisku IS ", „Informačná povinnosť prevádzkovateľa dotknutým osobám "a „Zásady bezpečnosti pre poverene osoby - používateľov IS kamerových systémov "
   - Z poverená osoba je povinná rešpektovať podmienky spracúvania osobných údajov zvlášť pre automatizovanú formu spracúvania a zvlášť pre neautomatizovanú formu spracúvania osobných údajov, o ktorých bola poučená;

c) Vymedzenie zakázaných postupov alebo operácií s osobnými údajmi
   - Z prevádzkovateľ vymedzil zakázané postupy alebo operácie s osobnými údajmi, v internom riadiacom akte prevádzkovateľa označenom ako „Hlavné zásady ochrany osobných údajov" a v internom riadiacom akte prevádzkovateľa označenom ako „Zásady bezpečnosti pre poverene osoby -používateľov IS ", „Zásady bezpečnosti pri správe databáz a aplikácií IS ", „Zásady bezpečnosti pri prevádzke informačných a komunikačných technológií na pracovisku IS ", „Informačná povinnosť prevádzkovateľa dotknutým osobám "a „Zásady bezpečnosti pre poverene osoby - používateľov IS kamerových systémov "
   - Z poverená osoba je povinná pri spracúvaní osobných údajov zdržať sa zakázaných postupov, ktoré sú vymedzené v internom riadiacom akte prevádzkovateľa označenom ako „Hlavné zásady ochrany osobných údajov";
   - Z poverená osoba je povinná pri spracúvaní osobných údajov zdržať sa zakázaných postupov, ktoré sú vymedzené v internom riadiacom akte prevádzkovateľa označenom ako „Zásady bezpečnosti pre poverene osoby -používateľov IS ", „Zásady bezpečnosti pri správe databáz a aplikácií IS ", „Zásady bezpečnosti pri prevádzke informačných a komunikačných technológií na pracovisku IS ", „Informačná povinnosť prevádzkovateľa dotknutým osobám "a „Zásady bezpečnosti pre poverene osoby - používateľov IS kamerových systémov "

6) Poučenie oprávnených osôb o postupoch spojených s automatizovanými a neautomatizovanými prostriedkami spracúvania a súvisiacich právach a povinnostiach (v priestoroch prevádzkovateľa a mimo týchto priestorov)
   - Z prevádzkovateľ poučí oprávnenú osobu o postupoch spojených s automatizovanými a neautomatizovanými prostriedkami spracúvania a súvisiacich právach a povinnostiach;
   - Z oprávnená osoba je povinná rešpektovať podmienky spracúvania osobných údajov zvlášť pre automatizovanú formu spracúvania a zvlášť pre neautomatizovanú formu spracúvania osobných údajov,
7) Zabezpečiť písomné poverenie zodpovednej osoby vyplývajúce v zmysle Článku 37 ods. l všeobecného Nariadenia EP a R (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov v prípade
   - Z prevádzkovateľ poverí zodpovednú osobu, ak tento postup bude z hľadiska zabezpečenia adekvátnej ochrany osobných údajov nevyhnutný
   - Z pokaľ splna podmienky poverenia zmysle Nariadenia EP a R (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov v prípade
8) Oboznámenie poverených osôb s bezpečnostnými smernicami
   - Z prevádzkovateľ oboznámi poverene osoby s v internými riadiacimi aktmi prevádzkovateľa v oblasti ochrany osobných údajov, a to s dokumentmi označenými ako „Zásady bezpečnosti pre poverene osoby -používateľov IS ", „Zásady bezpečnosti pri správe databáz a aplikácií IS ", „Zásady bezpečnosti pri prevádzke informačných a komunikačných technológií na pracovisku IS ", „Informačná povinnosť prevádzkovateľa dotknutým osobám "a „Zásady bezpečnosti pre poverene osoby - používateľov IS kamerových systémov "
9) Vzdelávanie poverených osôb (napr. právna oblasť, oblasť informačných technológií)
   - prevádzkovateľ kontinuálne oboznamuje
10) Postup pri ukončení pracovného alebo obdobného pomeru poverenej osoby (napr. odovzdanie pridelených aktív, zrušenie prístupových práv, poučenie o následkoch porušenia zákonnej alebo zmluvnej povinnosti mlčanlivosti)
   - pri ukončení pracovného alebo obdobného pomeru poverenej osoba odovzdá pridelené aktíva;
   - pri ukončení pracovného alebo obdobného pomeru poverenej osoby prevádzkovateľ zruší prístupové práva oprávnenej osoby;
   - pri ukončení pracovného alebo obdobného pomeru poverenej osoby prevádzkovateľ poučí o následkoch porušenia zákonnej a zmluvnej povinnosti mlčanlivosti,

### 11.1.2. Popis informačno-technických bezpečnostných opatrení

1) Technické opatrenia realizované prostriedkami fyzickej povahy
   a) Zabezpečenie pomocou mechanických zábranných prostriedkov
      - budova, v ktorej sa nachádza prevádzkareň, je zabezpečená uzamykateľnými dverami;
      - priestory prevádzkarne sú zabezpečené uzamykateľnými dverami;
      - chránené priestory sú zabezpečené uzamykateľnými dverami.
   b) Zabezpečenie pomocou technických zabezpečovacích prostriedkov
      - priestory prevádzkarne sú zabezpečené kamerovým systémom.

c) Zabezpečenie chráneného priestoru jeho oddelením od ostatných častí objektu
   - chránené priestory nie sú prístupné iným osobám ako zamestnancom prevádzkovateľa
d) Umiestnenie informačného systému v chránenom priestore
   - informačné systémy sú umiestnené v chránenom priestore zabezpečujúcom ochranu pred fyzickým prístupom neoprávnených osôb ako aj nepriaznivými vplyvmi okolia; uvedené sa vzťahuje na automatizované aj neautomatizované informačné systémy.
e) Bezpečné uloženie fyzických nosičov osobných údajov
   - uloženie fyzických nosičov osobných údajov je zabezpečené uložením v policiach nachádzajúcich sa v chránených priestoroch;
f) Zamedzenie náhodného odpozerania osobných údajov zo zobrazovacích jednotiek informačného systému
   - náhodnému odpozeraniu osobných údajov zo zobrazovacích jednotiek informačného systému je zabránené vhodným umiestnením zobrazovacích jednotiek;
   - prevádzkovateľ poučí oprávnené osoby o nutnosti dbať na zvýšenú ochranu proti odpozeraniu osobných údajov zo zobrazovacích jednotiek.
g) Zariadenie na ničenie fyzických nosičov osobných údajov
   - prevádzkovateľ zabezpečí zariadenie na skartovanie listín;
   - s prevádzkovateľ dohliada na efektívne využívanie zariadenie na skartovanie listín a jeho neustálu funkčnosť; v prípade potreby bezodkladne zabezpečí servis zariadenia.

2) Ochrana pred neoprávneným prístupom
   a) Šifrová ochrana obsahu dátových nosičov a šifrová ochrana dát premiestňovaných prostredníctvom počítačových sietí
      - šifrová ochrana je v súčasnosti využívaná
   b) Pravidlá prístupu tretích strán k informačnému systému, ak k takému prístupu dochádza
      - pravidlá sú určené nastavením firewallu a pridelením obmedzeným konkrétnym druhom prístupov

3) Riadenie prístupu oprávnených osôb
   a) Identifikácia, autentizácia a autorizácia oprávnených osôb v informačnom systéme
   b) Zaznamenávanie vstupov jednotlivých oprávnených osôb do informačného systému
      - záznam je v logoch jedn. systémov resp. databáz

4) Ochrana proti škodlivému kódu
   a) Detekcia prítomnosti škodlivého kódu v prichádzajúcej elektronickej pošte a v iných súboroch prijímaných z verejne prístupnej počítačovej siete alebo z dátových nosičov
      - Detekcia je zabezpečená antivírusovým programom
   b) Ochrana pred nevyžiadanou elektronickou poštou
      - Ochranu zabezpečuje licencovaný antivírusový program
   c) Používanie legálneho a prevádzkovateľom schváleného softvéru
      - Zabezpečená priebežná kontrola administrátorom na prítomnosť nelegálneho softwaru
   d) Pravidlá sťahovania súborov z verejne prístupnej počítačovej siete
      - Vytvorená hierarchia práv možnosti inštalovania nového softwaru

5) Sieťová bezpečnosť
   a) Kontrola, obmedzenie alebo zamedzenie prepojenia informačného systému, v ktorom sú spracúvané osobné údaje s verejne prístupnou počítačovou sieťou y Obmedzenie je zabezpečené aktívnym sieťovým prvkom firewall
      - Evidencia všetkých miest prepojenia sietí vrátane verejne prístupnej počítačovej siete y Zabezpečené aktívnym sieťovým prvkom firewall
   b) Ochrana vonkajšieho a vnútorného prostredia prostredníctvom nástroja sieťovej bezpečnosti (napr. firewall)
      - Zabezpečené aktívnym sieťovým prvkom firewall
   c) Pravidlá prístupu do verejne prístupnej počítačovej siete (napr. zamedzenie pripojenia k určitým webovým sídlam)
      - Zabezpečené aktívnym sieťovým prvkom firewall
   d) Ochrana proti iným hrozbám pochádzajúcim z verejne prístupnej počítačovej siete (napr. hackerský útok)
      - Zabezpečené aktívnym sieťovým prvkom firewall

6) Zálohovanie
   a) Test funkcionality dátového nosiča zálohy
      - Priebežne kontrolovaný správcom siete
   b) Vytváranie záloh s vopred určenou periodicitou
      - Pravidelne zálohovanie dát servera na dátové úložisko za pomoci softvérového riešenia
   c) Test obnovy informačného systému zo zálohy
      - Priebežne kontrolovaný správcom siete
   d) Bezpečné ukladanie záloh
      - Dáta uložené v samostatnom zariadení v zabezpečenej miestnosti

7) Likvidácia osobných údajov a dátových nosičov
   a) Bezpečné vymazanie osobných údajov z dátových nosičov
      - Mazanie zabezpečené za pomoci softwaru
   b) Zariadenie na likvidáciu dátových nosičov osobných údajov
      - Využitie skratkovacieho stroja
8) Aktualizácia operačného systému a programového aplikačného vybavenia
      - Automatická aktualizácia operačného systému + priebežná kontrola správcom siete

### 11.1.3. Popis organizačných bezpečnostných opatrení

V oblasti organizačných bezpečnostných opatrení implementovaných za účelom minimalizácie rizík zneužitia OÚ sa uplatňujú uvedené bezpečnostné opatrenia:

1) Vedenie zoznamu aktív a jeho aktualizácia
   - prevádzkovateľ vedie prehľadný zoznam aktív;
   - zoznam aktív je priebežne prevádzkovateľom aktualizovaný.

2) Riadenie prístupu oprávnených osôb k osobným údajom
   a) Kontrola vstupu do budovy, prevádzkarne a chránených priestorov prevádzkovateľa

- budova je zabezpečená pomocou zábranných prostriedkov:
  - zabezpečenie pomocou mechanických zábranných prostriedkov: uzamykateľné dvere pri vstupe do budovy, mreže na oknách a vstupových dverách
  - zabezpečenie pomocou technických zabezpečovacích prostriedkov: kamerový systém
- priestory prevádzkarne sú zabezpečené pomocou zábranných prostriedkov:
  - zabezpečenie pomocou mechanických zábranných prostriedkov
    - uzamykateľné dvere pri vstupe do prevádzkarne aj pri vstupe do chráneného priestoru
    - oddelenie chráneného priestoru od ostatných častí prevádzkarne umiestnenie informačného systému v chránenom priestore
    - chránený priestor je zabezpečený pred fyzickým prístupom neoprávnených osôb
    - chránený priestor je zabezpečený pre nepriaznivými vplyvmi okolia
    - fyzické nosiče sú bezpečne uložené v trezore alebo v uzamykateľných na to zvlášť určených priestoroch
    - zobrazovacie jednotky sú umiestnené tak, aby bolo zamedzené náhodnému odpozeraniu
    - likvidácia osobných údajov v IS je zabezpečené formou zariadenia na to určeného (zariadenie na skartovanie listín)
  - zabezpečenie pomocou technických zabezpečovacích prostriedkov
    - kamerový systém
    - chránené priestory sú zabezpečené uzamykateľnými dverami.

b) Správa kľúčov (individuálne prideľovanie kľúčov, bezpečné uloženie rezervných kľúčov)
- S kľúče sú oprávneným osobám a iným zamestnancom prevádzkovateľa prideľované v závislosti na ich funkčnom zaradení;
- rezervné kľúče sú uložené v zapečatenej obálke, ktorou je oprávnený disponovať len poverený člen štatutárneho orgánu prevádzkovateľa

c) Prideľovanie prístupových práv a úrovní prístupu (rolí) poverených osôb
- pri ukončení pracovného alebo obdobného pomeru oprávnenej osoby, resp. iného zamestnanca, prevádzkovateľ" zruší prístupové práva oprávnenej osoby, resp., iného zamestnanca;

d) Správa hesiel
- Každému oprávnenému používateľovi je pridelené jednoznačné náhodne vygenerované heslo. Heslo pre prihlásenie do počítača nemôže oprávnená osoba zmeniť. Heslo do IS môže si oprávnená osoba zmeniť. Pridelené heslá nie je možné spätne zistiť. Po štarte hesla musí byť vygenerovane nové heslo.
- Každému oprávnenému používateľovi je pridelene heslo, ktoré pozná len používateľ. Toto heslo nie je možné zistiť tretou osobou.

e) Vzájomné zastupovanie poverených osôb
- v prípade nehody, dočasnej pracovnej neschopnosti, ukončenia pracovného alebo obdobného pomeru je chýbajúcu oprávnenú osobu oprávnená zastúpiť len iná oprávnená osoba, a to na základe poverenia prevádzkovateľa;
- v prípade nemožnosti zastúpenia oprávnenej osoby inou oprávnenou osobou, prevádzkovateľ určí na zastupovanie inú poverenú osobu,

3) Organizácia spracúvania osobných údajov

a) Pravidlá spracúvania osobných údajov v chránenom priestore
- Z poverená osoba je povinná pri spracúvaní osobných údajov uplatňovať základné

zásady ochrany osobných údajov, ktoré sú vymedzené v internom riadiacom akte prevádzkovateľa označenom ako „Hlavné zásady ochrany osobných údajov";
- Z poverená osoba je povinná pri spracúvaní osobných údajov uplatňovať postupy, ktoré sú vymedzené v internom riadiacom akte prevádzkovateľa označenom ako „Zásady bezpečnosti pri správe databáz a aplikácií IS ", „Zásady bezpečnosti pri prevádzke informačných a komunikačných technológií na pracovisku IS ", „Informačná povinnosť prevádzkovateľa dotknutým osobám "a „Zásady bezpečnosti pre poverene osoby - používateľov IS kamerových systémov "
- Z poverená osoba je povinná rešpektovať rozsah povolených činností a oprávnení pri spracúvaní osobných údajov a to vždy vo vzťahu k svojmu funkčnému zaradeniu;
- oprávnená osoba je povinná rešpektovať podmienky spracúvania osobných údajov zvlášť pre automatizovanú formu spracúvania a zvlášť pre neautomatizovanú formu spracúvania osobných údajov;

b) Nepretržitá prítomnosť poverenej osoby v chránenom priestore, ak sa v ňom nachádzajú aj iné ako poverene osoby
   - Z v prípade, že je nevyhnutná prítomnosť tretej osoby v chránených priestoroch, poverená osoba je povinná byť počas celej doby prítomnosti tretej osoby v chránených priestoroch taktiež prítomna;

c) Režim údržby a upratovania chránených priestorov
   - Z údržba a upratovanie chránených priestorov je zabezpečovaná prevádzkovateľom individuálne určenou osobou, ktorá môže byť zastúpená len osobou odsúhlasenou prevádzkovateľom;

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

4) Likvidácia osobných údajov
   a) Určenie postupov likvidácie osobných údajov s vymedzením súvisiacej zodpovednosti jednotlivých poverených osôb
      - prevádzkovateľ zabezpečuje bezpečné vymazanie osobných údajov z dátových nosičov formátovaním
      - prevádzkovateľ zabezpečuje bezpečnú likvidáciu dátových nosičov mechanickým poškodením
      - prevádzkovateľ zabezpečuje bezpečnú likvidáciu fyzických nosičov osobných údajov - mechanickým poškodením

5) Bezpečnostné incidenty
   a) Postup pri ohlasovaní bezpečnostných incidentov a zistených zraniteľných miest informačného systému na účel včasného prijatia preventívnych alebo nápravných opatrení
      - poverene osoby prevádzkovateľa sú povinní dodržiavať postup pri ohlasovaní bezpečnostných incidentov
   b) Evidencia bezpečnostných incidentov a použitých riešení

- prevádzkovateľ vedie zoznam nahlásených bezpečnostných incidentov s uvedením prijatého riešenia;

c) Postup pri riešení jednotlivých typov bezpečnostných incidentov
   - postup pri riešení jednotlivých bezpečnostných incidentov určuje podľa závažnosť a možnosti nápravy oprávnená osoba alebo prevádzkovateľ;;

d) Identifikácia, evidencia a odstraňovanie následkov bezpečnostných incidentov
   - všetci zamestnanci prevádzkovateľa sú povinní dbať na včasnú identifikáciu bezpečnostných incidentov;
   - poverene osoby sú povinné venovať zvýšenú pozornosť identifikácii bezpečnostných incidentov v rámci sprístupnených informačných systémov;

e) Oznámenie bezpečnostného incidentu úradu do 72 hodín, ak sa preukaze , že ide o porušenie ochrany OU a či to viedlo , alebo môže viest k riziku pre fyzické osoby
   - prevádzkovateľ by mal ihneď, ako sa dozvie, že došlo k porušeniu ochrany osobných údajov, bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín od okamihu, ako sa dozvedel, že došlo k porušeniu ochrany osobných údajov, toto porušenie oznámiť dozornému orgánu s výnimkou prípadov, keď vie prevádzkovateľ v súlade so zásadou zodpovednosti preukázať, že nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb.
   - ak nie je možné oznámenie podať do 72 hodín, malo by sa k oznámeniu pripojiť odôvodnenie omeškania, pričom informácie možno poskytnúť vo viacerých etapách bez ďalšieho zbytočného odkladu.

f) Postupy pri haváriách, poruchách a iných mimoriadnych situáciách
   - zamestnanci prevádzkovateľa sú povinní bezodkladne oznamovať bezpečnostné incidenty povereným osobám;
   - poverene osoby sú povinné bezodkladne oznamovať bezpečnostné incidenty prevádzkovateľovi;
   - zamestnanci a poverene osoby sú povinní v rámci povolených činností a v súlade s bezpečnostnými opatreniami vykonať opatrenia za účelom ochrany osobných údajov, ktoré neznesú odklad, predovšetkým sú povinní vykonať opatrenia s cieľom minimalizovať riziko zneužitia osobných údajov a ich sprístupnenia tretím osobám

g) Postup pri poruche, údržbe alebo oprave automatizovaných prostriedkov spracúvania (napr. ochrana osobných údajov na pevnom disku opravovaného počítača)
   - nosič informácií je potrebné po demontovaní z TP servisným pracovníkom dopraviť na užívateľský útvar,
   - ak je možné z takéhoto nosiča informácie niektoré údaje zachrániť, vykonajú sa potrebné kroky na užívateľskom útvare v prítomnosti zamestnanca, ktorý má pridelený TP,
   - informácie, ktoré nie je možné získať z pôvodného nosiča informácie sa obnovia zo záložných nosičov, o obnovení súborov sa vykoná zápis do prevádzkového zošita TP

6) Kontrolná činnosť

a) Kontrolná činnosť prevádzkovateľa zameraná na dodržiavanie prijatých bezpečnostných opatrení s určením spôsobu, formy a periodicity jej realizácie
   - prevádzkovateľ vykonáva pravidelné kontroly prístupov k informačnému systému 1 krát ročné.
   - výsledok kontroly zdokumentuje v protokole „EVIDENCIA KONTROLNÝCH

ČINNOSTI,, ( prílohe BP )

## 12. Kontrolné činnosti spôsob, forma a periodicita výkonu kontrolných činností

Spôsob kontroly:

kontrolu vykonáva poverený zamestnanec na pracovisku oprávnených osôb, kladením otázok, praktických porovnávaním predpokladaného stavu so stavom skutočným, kontrolou dokumentácie a riešením modelových situácii.

Forma kontroly a periodicita výkonu kontroly:

- Minimálne jedenkrát za rok skontroluje náhodným výberom kompletnosť databázy v počítačovom systéme.
- V prípade pripájania PC na internet zabezpečí permanentnú antivírovú a antispamovú kontrolu.
- Pri nekorektnom správaní systému skontroluje, alebo špecializovaným technikom zabezpečí kontrolu logových súborov v zobrazovači udalostí operačného systému /Event Viewer/.
- V prípade použitia nosičov, ktoré sa vrátia od iných prevádzkovateľov, aplikuje pred použitím v systéme minimálne rýchle formátovanie. (Pri neznámych nosičoch platí zásada, že ich obsah sa neprezerá, nespúšťajú sa z nich žiadne aplikácie, iba sa prevedie ich formátovanie, ktoré odstráni prípadnú vírusovú nákazu.)
- Minimálne jedenkrát týždenne, alebo po nekorektnom ukončení alebo výpadku energie vykoná systémovú kontrolu disku (scandisk), ak operačný systém takúto voľbu povoľuje.
- Minimálne jedenkrát za 6 mesiacov vykoná systémový scandisk a defragmentáciu disku, ak operačný systém takéto voľby povoľuje.
- Pri údržbe a údržbových funkciách jednotlivých programov dodržiava zásady podľa návodu na použitie (tieto služby, ako napr. defragmentácia, kompresia a kontrola integrity databáz sa odporúča vykonať l x mesačne).
- Pri výzve na aktualizáciu systému zabezpečí spustenie stiahnutých aktualizácií v čo najkratšom termíne s dôrazom na bezpečnostné aktualizácie.

Z vykonanej kontroly oprávnená osoba vyhotoví zápis vzor Príloha .

## 13. Postupy pri haváriách, poruchách a iných mimoriadnych udalostiach

Táto kapitola všeobecne sumarizuje obsah krízového plánu, resp. tých jeho častí, ktoré bezprostredne súvisia s ochranou a bezpečnosťou osobných a iných citlivých údajov. Spoločnosť vypracuje svoj krízový plán tak, aby postihoval aj tie situácie, ktoré sú zovšeobecnené v tejto kapitole. Predpokladom účinného fungovania krízového plánu je harmonizácia všetkých ňou zavedených opatrení, ktoré sa majú aplikovať v prípade niektorej z krízových situácií v ňom uvedených. Táto kapitola neuvádza všetky opatrenia, ktoré má obsahovať krízový plán, pretože jeho súčasťou sú aj opatrenia vyplývajúce z iných všeobecne záväzných predpisov.

Krízový plán okrem iného určuje:

- Organizačné opatrenia určujúce činnosti pri narušení objektu a priestorov, v ktorých sa spracúvajú osobné údaje a pri pokuse o narušenie objektu
- Organizačné opatrenia pri zistení narušenia fungovania IS
- Organizačné opatrenia určujúce činnosti v prípade vzniku mimoriadnych udalostí
- Spôsob výkonu kontroly opatrení krízového štábu.

## 13.1. Organizačné opatrenia určujúce činnosti pri narušenie objektu a chráneného priestoru a pri pokuse o narušenie objektu a chráneného priestoru

Za narušenie objektu a chráneného priestoru a pokus o narušenie objektu a chráneného priestoru sa pre účely krízového štábu rozumie:

- krádež obyčajná,
- krádež vlámaním,
- pokus krádeže,
- teroristický útok
- sabotáž, poškodzovanie cudzej veci, výtržnosť,
- hrozba uložením výbušného systému.
- hrozba pre pravá a slobody fyzických osôb

**Krádeže a pokusy krádeží**

Krádežou sa rozumie trestný čin krádeže alebo jeho pokusu (§ 247 trestného zákona) a to aj v prípade, že došlo ku krádeži údajov bez rozdielu ich dôležitosti. Pri krádeži v objekte a chránenom priestore spôsobenej vlastným zamestnancom, pracovníkom iných servisných dodávateľských firiem, návštevou v pracovnej dobe, sa vykonajú tieto organizačné opatrenia:

| ***Por.*** | ***Popis opatrenia*** | ***Kto vykoná*** | ***Spôsob*** |
|---|---|---|---|
| *1.* | Zadržanie páchateľa krádeže a pokusu o krádež - ak je to možné | Každý pracovník prevádzkovateľa | Znemožnením úniku z priestorov prevádzkovateľa. O zadržaní ihneď informovať nadriadeného a zodpovednú osobu/štatutára |
| *2.* | Oznámenie zistenej krádeže v objekte | Zamestnanec, ktorý krádež zistil<br>Zodpovedná osoba/štatutár | Oznámiť skutočnosť svojmu nadriadenému a zodpovednej osobe/štatutár a vyčkať na ich pokyny.<br>Oznámiť skutočnosť orgánom činným v trestnom konaní (Policajnému zboru SR na tel. č. 158) |

| | | | |
|---|---|---|---|
| *3.* | Zabezpečenie miesta krádeže pred vniknutím neoprávnenej osoby a pre uchovanie dôkazného materiálu pre ďalšie vyšetrovanie | Zodpovedná osoba/štatutár a v prípade jej neprítomnosti vedúci pracovník pracoviska, na ktorom sa stala krádež, určí jedného z prítomných zamestnancov | Fyzickým strážením, vytvorením účinnej prekážky vstupu do priestorov, v ktorých je možné predpokladať, že ku krádeži došlo |

Pri teroristickom útoku na objekt, sú na objekte prijaté tieto organizačné opatrenia, zamestnanci a osoby zadržiavané v priestoroch organizácie a priamo ohrozované na životoch

| ***Por.*** | ***Popis opatrenia*** | ***Kto vykoná*** | ***Spôsob*** |
|---|---|---|---|
| *1.* | Zabezpečenie bezpečnosti zadržiavaných osôb | Každý zadržiavaný pracovník prevádzkovateľa | Primeranou spoluprácou s páchateľmi s cieľom navodiť kľud, neprovokovať k činom vedúcim k stratám na životoch |
| *2.* | Únik z ohrozeného priestoru | Každý zadržiavaný pracovník prevádzkovateľa | Únik realizovať len za asistencie privolanej ozbrojenej pomoci, účinne spolupracovať s tímom realizujúcim oslobodenie zadržiavaných osôb |
| ***Zamestnanci priamo neohrozovaní teroristickým útokom*** | | | |
| *3.* | Oznámenie zistenej skutočnosti | Každý pracovník prevádzkovateľa, ktorý skutočnosť zistil | Bezodkladne informovať orgány policajného zboru, potom nadriadeného pracovníka a štatutára |
| *4.* | Sledovanie a stráženie ohrozeného priestoru | Do príchodu príslušníkov polície a vedenia prevádzkovateľa každý pracovník prevádzkovateľa | Pozorovaním miesta teroristického útoku z bezpečnej vzdialenosti, sledovanie pohybu osôb a vozidiel. |
| *5.* | Zamedzenie vstupu ďalších osôb do ohrozeného priestoru | Do príchodu príslušníkov polície a vedenia prevádzkovateľa každý pracovník prevádzkovateľa | Podaním informácie vhodným spôsobom |
| *6.* | Súčinnosť s policajným zborom | Každý pracovník prevádzkovateľa | Podľa pokynov a požiadaviek poskytne každý pracovník policajnému zboru účinnú pomoc. |
| ***Cieľ zvládnutia každého teroristického útoku je najprv ochrana života a zdravia a až následne majetku prevádzkovateľa*** | | | |

**Poškodzovanie cudzej veci, sabotáž a výtržnosť**

Za poškodzovanie cudzej veci (majetku prevádzkovateľa), sabotáž a výtržnosť sa všeobecne považujú činnosti, ktoré majú poškodiť majetok prevádzkovateľa alebo znemožniť jej ďalšie normálne fungovanie, pričom si páchateľ obvykle neprisvojuje majetok prevádzkovateľa. Za majetok prevádzkovateľa sa považuje hmotný ale aj nehmotný majetok. Pri zistení týchto činov sa postupuje rovnako ako pri krádežiach.

**Hrozba uloženia výbušného systému**

Pri hrozbe uloženia výbušného systému sú na objekte prijaté tieto organizačné opatrenia:

| *Por.* | *Popis opatrenia* | *Kto vykoná* | *Spôsob* |
|---|---|---|---|
| *1.* | Evakuácia zamestnancov prevádzkovateľa a osôb nachádzajúcich sa v priestoroch prevádzkovateľa | Štatutár alebo iná ňou poverená osoba | Hlasom, telefónom, osobne. Určiť miesto kam majú byť evakuované osoby. |
| *2.* | Informovať ostatné organizácie nachádzajúce sa v budove | Štatutár alebo iná ňou poverená osoba | Telefonickým vyrozumením, alebo vyslaním zamestnanca. |
| *3.* | Povinnosť oznámiť uloženie výbušného systému | Štatutár alebo iná ňou poverená osoba | Telefonicky policajnému zboru |
| *4.* | Zabránenie vstupu osôb do priestorov organizácie | Štatutár alebo iná ňou poverená osoba | Po spoľahlivom zistení, že všetky osoby opustili priestory uzamknúť vstupné dvere. |
| *5.* | Spolupráca s policajným zborom | Každý zamestnanec prevádzkovateľa | Podľa pokynov polície |

### 13.1.1. Organizačné opatrenia pri narušení fungovania IS

Narušením fungovania informačného systému prevádzkovateľa sa rozumie akákoľvek situácia, ktorá má za následok poškodenie, zničenie, modifikáciu, alebo únik údajov z počítačov. Narušením je takisto nežiadúce alebo nepredpokladané chovanie používaného softvéru, aj keď zdanlivo nevedie k narušeniu údajov, programových prostriedkov a operačných systémov (jedná sa hlavne o činnosť vírusov alebo obdobných infiltrácií). Za narušenie sa považuje aj porucha počítača, ktorá môže spôsobiť stratu údajov. Pre zvládnutie uvedených situácií sa stanovujú nasledovné opatrenia:

| *Por.* | Popis opatrenia | Kto vykoná | Spôsob |
|---|---|---|---|
| *1.* | Zamedzenie ďalších škôd | Zamestnanec, ktorý skutočnosť zistil | Bezodkladné bezpečné vypnutie počítača, odpojenie zdroja elektrickej energie, vrátane periférií. Odpojenie od komunikačných prostriedkov. Pri voľbe spôsobu vypnutia zvoliť malú stratu údajov (rozpracovanej práce) pred rozsiahlym poškodením zariadenia a údajov. |
| *2.* | Hlásenie narušenia | Zamestnanec, ktorý skutočnosť zistil | Informovať zodpovednú osobu/štatutára a zamestnanca zodpovedného za chod IS |
| *3.* | Poskytnutie účinnej pomoci pri odstraňovaní škôd a vyšetrení incidentu | Všetci zamestnanci prevádzkovateľa | Podľa pokynov zodpovednej osoby/štatutára a zamestnanca zodpovedného za chod IS |

### 13.1.2. Organizačné opatrenia určujúce činnosti v prípade vzniku iných mimoriadnych udalostí

Mimoriadnymi udalosťami sa pre účely krízového plánu v súvislosti s ochranou IS prevádzkovateľa rozumejú najmä:

- únos vedúcich pracovníkov a kľúčových zamestnancov s cieľom ohroziť prevádzkovateľa,
- vydieranie zamestnanca, nátlak na zamestnanca s cieľom prinútiť ho k spolupráci na poškodení prevádzkovateľa,
- živelná pohroma, prírodná katastrofa, priemyselná a ekologická havária.

1) Únos vedúcich pracovníkov a kľúčových zamestnancov

Únosom s cieľom ohroziť organizácie sa rozumie najmä trestný čin brania rukojemníka (§ 234a trestného zákona), ktorého cieľom je prinútiť prevádzkovateľa, aby konala proti svojim vlastným záujmom, resp. aby inak porušovala zákony SR. V prípade únosu sa vykonajú tieto opatrenia:

| *Por.* | Popis opatrenia | Kto vykoná | Spôsob |
|---|---|---|---|
| *1.* | Ohlásenie únosu policajnému zboru a nadriadenému pracovníkovi | Zamestnanec, ktorý bol únoscami kontaktovaný, alebo sa o únose inak dozvedel | Bezodkladne telefonicky informovať policajný zbor a štatutára |
| *2.* | Spolupráca s únoscami | Zamestnanec, ktorý je v kontakte s únoscami | Uposlúchnuť pokyny únoscov (okrem podmienky neinformovať políciu), pokúsiť sa odložiť plnenie podmienok na prepustenie. S únoscami nevyjednávať, navodiť zdanie účinnej spolupráce. |
| *3.* | Súčinnosť s políciou | Zamestnanec, ktorý je v kontakte s únoscami | Postupovať podľa pokynov polície |

2) Vydieranie a nátlak na zamestnanca

Vydieranie a nátlak na zamestnanca sú hrozby iných osôb alebo prevádzkovateľovi, smerujúce s tomu, aby vydieraný zamestnanec a zamestnanec, na ktorého je vyvíjaný nátlak konal proti záujmom prevádzkovateľa (najmä trestné činy podľa § 235 a § 235a trestného zákona). Pre prípad vydierania a nátlaku sa stanovujú tieto organizačné opatrenia:

| *Por.* | Popis opatrenia | Kto vykoná | Spôsob |
|---|---|---|---|
| *1.* | Ohlásenie vydierania a nátlaku. | Zamestnanec, ktorý je vydieraný, alebo zamestnanec, ktorý sa o takomto vydieraní dozvedel. | Bezodkladne telefonicky policajnému zboru a zodpovednej osobe/štatutárovi |
| *2.* | Spolupráca s vydieračmi. | Vydieraný zamestnanec. | Podľa pokynov polície spolupracovať, navodiť zdanie spolupráce a poskytnúť pomoc a informácie vedúce k odhaleniu vydierača. |
| *3.* | Izolovanie vydieraného. | Vedúci zamestnanec | Vydieranému znemožniť konanie proti záujmom prevádzkovateľa - znemožnením používania telefónu, faxu, kopírovacích zariadení a PC, prípadne aj nevpustením do priestorov. Izoláciu konzultovať s policajným zborom. |

3) Živelná pohroma, prírodná katastrofa, priemyselná a ekologická havária

Hrozby rozsiahlych živelných pohrôm, prírodných katastrof, alebo ekologických a priemyselných havárií sú nízke. Najpravdepodobnejšou živelnou pohromou je požiar. Pri ostatných pohromách a haváriách sa postupuje obdobne ako pri požiari. Pre zvládnutie požiaru je vypracovaný plán požiarnej ochrany, ktorý musí okrem iného stanoviť aj poradie evakuácie a záchrany majetku prevádzkovateľa.

### 13.1.3. Oznámenie bezpečnostných incidentov úradu do 72 hodín

Ak sa porušenie ochrany osobných údajov nerieši primeraným spôsobom a včas, môže fyzickým osobám spôsobiť ujmu na zdraví, majetkovú alebo nemajetkovú ujmu, ako je napríklad strata kontroly nad svojimi osobnými údajmi a pod., teda prevádzkovateľ zhodnotí , že bezpečnostný incident povedie k porušeniu práv a slobôd fyzickým osobám ma povinnosť tento incident nahlásiť dozornému úradu.
Keď vie prevádzkovateľ v súlade so zásadou zodpovednosti preukázať, že nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb tento bezpečnostný incident nemusí oznamovať dozornému organu.

| ***Por.*** | **Popis opatrenia** | **Kto vykoná** | **Spôsob** |
|---|---|---|---|
| *1.* | Systémová bezpečnosť<br>Fyzická bezpečnosť<br>Legislatívne opatrenia | Zodpovedná osoba/štatutár | Znemožnením úniku z priestorov prevádzkovateľa. O zadržaní ihneď informovať nadriadeného a zodpovednú osobu/štatutára |
| *2.* | Oznámenie o zistenom incidente | Zamestnanec, ktorý incident zistil | Oznámiť skutočnosť svojmu nadriadenému a zodpovednej osobe/štatutár a vyčkať na ich pokyny. |
| *3.* | Súčinnosť dozorným organom | Zodpovedná osoba/štatutár | Ak bezpečnostný incident povedie k riziku pre pravá a slobody fyzických osôb, oznámi tuto skutočnosť dozornému organu do 72 hodín od zistenia incidentu. Ak nie je možné oznámenie podať do 72 hodín, malo by sa k oznámeniu pripojiť odôvodnenie omeškania, pričom informácie možno poskytnúť vo viacerých etapách bez ďalšieho zbytočného odkladu. |

| | |
|---|---|
| | Dozorný orgán, ktorým je Úrad na ochranu osobných údajov Slovenskej republiky so sídlom na adrese Hraničná 12, 820 07 Bratislava 27. |

# 14. ZÁVEREČNÉ USTANOVENIA

Bezpečnostný projekt je výsledným produktom analytickej časti riešenia bezpečnosti IS obsahujúceho osobné údaje. Sumarizuje výsledky analýzy a s bezpečnostnými smernicami určuje spôsoby zabezpečenia ochrany osobných údajov s popisom bezpečnostných opatrení.

Bezpečnostný projekt sa považuje za dôverný dokument, ktorého obsah je chránený pred neoprávneným prístupom.

Sprístupnenie obsahu tohto projektu neoprávneným alebo nepovolaným osobám môže mať za následok ohrozenie jeho dôvernosti a bezpečnostných mechanizmov IS.

Bezpečnostný projekt informačných systémov nadobúda účinnosť 25. Mája 2018.

Súvisiace dokumenty k Bezpečnostnému projektu:
Nasledovné uvedené šablóny dokumentov a záznamov agendy ochrany osobných údajov sú spracované v elektronickom formáte MS Word a sú prístupné povereným osobám prevádzkovateľa pre spracúvanie osobných údajov:

- Evidencia kľúčov
- Evidencia kontrolných činnosti
- Oboznámenie o kontrolnom mechanizme
- Oboznámenie o sprostredkovateľovi
- Poverenie na spracovanie osobných údajov
- Súhlas dotknutej osoby
- Zákon a Nariadenie EU
- Dodatok do pracovnej zmluvy
- Záznam o oboznámení s Internými Riadiacimi aktami
- Zmluva o spracovaní osobných údajov
- Informácie na web ohľadne prvá dotknutých osôb pri spracovaní osobných údajov

Prílohy:

1. Evidencia bezpečnostných incidentov a použitých riešení
2. Evidencia bezpečnostných incidentov a použitých riešení - vzor
3. Identifikované typy incidentov a spôsob ich riešenia
4. Evidencia kontrolných činností
5. Evidencia kontrolných činností – vzor
6. Evidencia odovzdaných kľúčov

Súvisiace dokumenty:

- „Hlavné zásady ochrany osobných údajov"
- „Zásady bezpečnosti pre poverene osoby -používateľov IS"

- „Zásady bezpečnosti pri správe databáz a aplikácií IS "
- „Zásady bezpečnosti pri prevádzke informačných a komunikačných technológii na pracovisku IS "
- „Informačná povinnosť prevádzkovateľa dotknutým osobám "
- „Zásady bezpečnosti pre poverene osoby - používateľov IS kamerových systémov

Doložky:

- „Záznamy o spracovateľských činnostiach podľa všeobecného nariadenia Európskeho parlamentu a rady (EU) 2016/679- konkrétny článok/články 30/1 Nariadenia EP a R (EÚ) o ochrane fyzických osôb pri spracovaní osobných údajov a o voľnom pohybe takýchto údajov"

Príloha č. 1 Evidencia bezpečnostných incidentov a použitých riešení

Názov/Obchodné meno:
IČO:

| *dátum čas porad. č.* | bezpečnostný incident/popis | použité /riešenie | typ incidentu | zaznamenal / meno /podpis |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Príloha č. 2 Evidencia bezpečnostných incidentov a použitých riešení – vzor

| *dátum čas porad. č.* | bezpečnostný incident/popis | použité/ riešenie | typ incidentu | zaznamenal / meno/ podpis |
|---|---|---|---|---|
| 5.06.2018 16.00 001/2018 | program hlási poškodenie databázy /nejde spustiť | spustená služba reparácie databázy a následne služba opravy databázy z programu - hlásenie OK - správanie programu korektné | porucha DB | |
| 10.07.2018 14:00 002/2018 | nefunguje obnovenie zo zálohy na domácom počítači / OS hlási nemožnosť čítania z médií | kontrola obsahu média cez Windows prieskumník - médium je nečitateľné - z toho vyplýva poškodenie média -médium je nahradené a záloha vykonaná znovu na overené médium | porucha HW | |
| 13.7.2018 19:00 003/2018 | nejde vykonať UpGrade priamo z programu | kontaktovaná firma a problém riešený cez vzdialenú správu, identifikované zlé nastavenie antivírusového programu, aplikačný program bol pridaný do výnimiek ako dôveryhodný zdroj | konflikt OS / SW | |

## Príloha č. 3 Identifikovaná typy incidentov a spôsobov riešenia

Názov/Obchodné meno:
IČO:

Automatizovaný IS - AIS

| *bezpečnostný incident* | použité/ riešenie | typ incidentu |
|---|---|---|
| *poškodenie databázy* | reparácia OK - vyriešené | porucha SW/HW |
| *poškodenie databázy* | reparácia neprebehla - kontaktovať servisnú firmu a vylúčiť poškodenie HDD | porucha SW/HW |
| *nezálohuje* | kontrolovať médium - výmena média ak je médium OK - kontaktovať servisnú firmu | porucha HW/SW |
| *neštartuje PC* | žiadna kontrolka nesvieti skontrolovať napájanie - ak je OK, kontaktovať servisnú firmu, technika | porucha HW |
| *UpGrade priamo z programu nejde* | vykonať skontrolovať nastavenie antivírového programu - program sa musí zaviesť do výnimiek | porucha HW |
| *antivírusový program hlási infiltráciu* | súhlas s možnosťou opravy, alebo odloženie do karantény, v prípade znefunkčnenia nejakého modulu previesť reinštaláciu SW, ak sa problém nevyrieši, kontaktovať technika | vírová nákaza |
| *záloha nejde obnoviť* | kontrolovať médium - výmena média ak je médium OK - | porucha HW/SW |

Nearomatizovaný IS – NIS

| *bezpečnostný incident/popis* | použité riešenie | typ incidentu |
|---|---|---|
| *nevrátenie zapožičanej dokumentácie* | výzva na vrátenie | normál |
| *poškodenie živelnou pohromou* | oznámiť dotknutým osobám a následné zabezpečenie opisu | živel |
| *odcudzenie dokumentácie* | oznámiť dotknutej osobe a podľa citlivosti údajov zvážiť ohlásenie na polícii | krádež |
| *poškodenie dokumentácie* | zvážiť opravu dokumentu, prípadne vytvoriť opis a založiť do karty | poškodenie |

Príloha č. 4 Evidencia kontrolných činností

Názov/Obchodné meno:
IČO:

| *dátum čas porad. č.* | *kontrola / popis* | *zistené nedostatky informačný systém* | *zaznamenal* | *meno /podpis* |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Príloha č. 5 Evidencia kontrolných činností – vzor

Názov/Obchodné meno:
IČO:

| *dátum čas porad. č.* | kontrola / popis | zistené nedostatky informačný systém | AIS/NIS | zaznamenal /meno/ podpis |
|---|---|---|---|---|
| *14/06/2018 10:00 001/2018* | Kontrola zálohovacích médií Kontrola integrity databázy Defragmentácia | Žiadne | AIS | |
| *22.07.2018 14:00 002/2018* | Kontrola mzdovej evidencie, náhodný výber 1 ks | Žiadne | NIS | |

Príloha č. 6: Evidencia odovzdaných kľúčov

Názov/Obchodné meno:
IČO:

Kľúče odovzdal:

| *Meno* | *Priezvisko* | *Funkcia* |
|---|---|---|
| | | |

Prehlásenie
1. Preberám uvedené kľúče. Som si vedomá/ý zodpovednosti a v prípade straty alebo odcudzenia túto skutočnosť bezodkladne nahlásim vedúcemu zamestnancovi.

| *Číslo kľúča* | *Kľúč od miestnosti, budovy* | *Prebral podpis/dňa* | *Odovzdal podpis/dňa* |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |