Dokumentácia
na ochranu osobných údajov

v podmienkach spoločnosti

Nehnuteľnosti Levice s. r.o.,

so sídlom Kpt. Nálepku 78, 934 01 Levice
IČO: 50 541 757

v zmysle zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

POLITIKA INFORMAČNEJ BEPEČNOSTI

Vyhlásenie prevádzkovateľa: Nehnuteľnosti Levice s. r.o.,
so sídlom Kpt. Nálepku 78, 934 01 Levice
IČO: 50 541 757

Vzhľadom na zákon o ochrane osobných údajov č. 18/2018 Z.z. a medzinárodné normy informačnej bezpečnosti, prijímame nasledovnú dokumentáciu.

Zabezpečíme, aby osobné údaje a iné citlivé údaje obsiahnuté v našich informačných systémoch boli chránené proti strate, zneužitiu a boli spracúvané len v súvislosti s poskytovaním účtovnej, personálnej, mzdovej agendy a za účelom predaja, nákupu či prenájmu nehnuteľnosti pre klienta.

Vyhlasujeme, že na dosiahnutie tohto cieľa využijeme všetky organizačné, personálne a informačné možnosti v súlade s dobrými mravmi a rozumnou mierou nákladovosti.

Zaväzujeme sa pracovať v súlade s rešpektovaním platných zákonov Slovenskej republiky a platných medzinárodných noriem a v maximálnej možnej miere chrániť osobné údaje v našich systémoch.

Všetky zlepšenia a postupy informačnej bezpečnosti budeme v budúcnosti zavádzať v súlade s medzinárodnými normami STN ISO 27001 a 27002.

Za účelom podpory tejto politiky prijímame túto dokumentáciu o ochrane osobných údajov so záväzkom neustáleho zlepšovania a zdokonaľovania našej práce.

Projekt je koncipovaný a zrealizovaný na základe zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a nariadenia Európskeho parlamentu a Rady (EÚ) č. 2016/679.

Za ochranu osobných údajov zodpovedá prevádzkovateľ a poučení zamestnanci.

Dňa 25.05.2018

prevádzkovateľ
Nehnuteľnosti Levice s.r.o.,

ÚVODNÉ USTANOVENIA

DOKUMENTÁCIE

vymedzujúce

obsah a účel dokumentácie, rozsah a účel spracúvania osobných údajov vo firme, zodpovednosť za bezpečnosť osobných údajov, definíciu pojmov a základnú terminológiu

ÚVODNÉ USTAVENIA

ZÁMER DOKUMENTÁCIE

1) Základné bezpečnostné zámery a ciele firmy potrebné dosiahnuť na ochranu informačných systémov patriacich firme v podmienkach firmy (ďalej len IS) pred ohrozením jeho bezpečnosti, ktorých je firma zriaďovateľom.

2) Určenie počiatočného skutkového stavu bezpečnosti IS.

3) Špecifikáciu opatrení na ochranu IS a zabezpečenie osobných údajov.

4) Vymedzenie okolia IS a jeho vzťah k možnému narušeniu bezpečnosti.

5) Možné zvyškové riziká.

6) Vyhodnotenie podkladov pre dokumentáciu

ANALÝZA BEZPEČNOSTI INFORMAČNÉHO SYSTÉMU

1) Ako podrobný rozbor stavu bezpečnosti informačných systémov firmy, obsahujúci kvalitatívnu analýzu rizík, v rámci ktorej sa identifikujú hrozby pôsobiace na jednotlivé aktíva IS spôsobilé narušiť jeho bezpečnosť, alebo funkčnosť, pričom výsledkom kvalitatívnej analýzy rizík je:
   a) Zoznam aktív IS
   b) Analýza a kvantifikácia možných ohrození a rizík
   c) Zoznam hrozieb, ktoré môžu ohroziť dôvernosť, integritu a dostupnosť spracúvaných osobných údajov vo firme
   d) Rozsah možného rizika, návrhov opatrení ktoré eliminujú alebo minimalizujú vplyv rizík s vymedzením súpisu nepokrytých rizík
   e) Návrhy na minimalizáciu a elimináciu nežiaducich vplyvov a rizík
   f) Použitie bezpečnostných štandardov na ochranu
   g) Posúdenie zhody použitých bezpečnostných opatrení s bezpečnostnými štandardami
   h) Systém hodnotenia zhody navrhnutých bezpečnostných opatrení a použitými bezpečnostnými štandardmi, metódami a prostriedkami

i) Vyhodnotenie zhody navrhnutých bezpečnostných opatrení podľa jednotlivých opatrení

2) Za bezpečnosť osobných údajov vo firme, v zmysle zákona zodpovedá prevádzkovateľ tým, že ich chráni pred náhodným, ako aj nezákonným poškodením a zničením, náhodnou stratou, zmenou, nedovoleným prístupom a sprístupnením, ako aj pred akýmikoľvek inými neprípustnými formami spracúvania.

3) Na tento účel prijme primerané technické, organizačné a personálne opatrenia na ochranu osobných údajov zodpovedajúce spôsobu spracúvania.

4) Ide najmä o tieto opatrenia:
   a) vykonanie inventúry všetkých osobných údajov, ktoré sa vo firme spracúvajú
   b) preskúmanie aktuálnosti a potrebnosti osobných údajov, ktoré sú vo firme zhromaždené
   c) evidencia informačných systémov
   d) určenie okruhu osôb, ktorým sa povolí spracúvať osobné údaje
   e) zaviazanie mlčanlivosťou osoby, ktoré budú spracúvať osobné údaje v zmysle zákona
   f) určenie priestorov, kde sa budú osobné údaje spracúvať a určenie technických prostriedkov na spracúvanie
   g) určenie osôb, ktoré budú poverené dohľadom nad ochranou osobných údajov vo firme
   h) prijatie adekvátnych opatrení na ochranu osobných údajov

1. ÚVOD

1) Jedným z cieľov každej z organizácie by mala byť bezpečnosť vo všeobecnom ponímaní. Patria sme napr. ochrana majetku, finančných prostriedkov, bezpečnosti a zdravia pri práci, ochrana dobrého mena organizácie, ochrana osobných údajov či utajovaných informácií.

2) Táto dokumentácia pojednáva o ochrane osobných údajov podľa zákona NR SR č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

2. PRÁVNA ÚPRAVA

1) **Ochrana osobných údajov sa rieši** v súlade so zákonom č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.
2) Nariadenia Európskeho parlamentu a Rady (EÚ) č. 2016/679 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)
3) **Ďalej vychádza z nasledujúcich zákonov**:
   * Zákon NS SR č. 300/2005 Z.z. Trestný zákon § 247 a § 374
   * Zákon NR SR č. 215/2002 Z.z. o elektronickom podpise
   * Zákon NR SR 301/1995 Z.z. o rodnom čísle
   * Zákon NR SR č. 395/2002 Z.z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení zmien a doplnkov
4) **STN**
   * STN ISO/IE TR 13335-1 - Informačné technológie. Návod na manažérstvo bezpečnosti IT. Koncepcie a modely bezpečnosti IT.
   * STN ISO/IE TR 13335-2 - Informačné technológie. Návod na manažérstvo bezpečnosti IT. Riadenie a plánovanie bezpečnosti IT
   * STN ISO/IEC 27005 - Informačné technológie. Bezpečnostné metódy. Riadenie rizík informačnej bezpečnosti.

3. ÚČEL A CIEĽ

1) Cieľom dokumentácie je vymedziť rozsah a spôsob technických, organizačných a personálnych opatrení potrebných na eliminovanie a minimalizovanie hrozieb pôsobiacich na informačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti, funkčnosti a ochrany osobných údajov.

2) **Bezpečnostné vlastnosti**, ktoré informačný systém musí mať:
   a) **dôvernosť** – vlastnosť, že informácia nie je dostupná alebo prístupná neautorizovaným jednotlivcom, entitám, alebo procesom,
   b) **integrita dát** – ochrana dát pred zmenou alebo zničením neautorizovaným spôsobom,
   c) integrita systému – vlastnosť, že systém vykonáva svoju zamýšľanú funkciu nenarušeným spôsobom, bez zámernej alebo náhodnej neautorizovanej manipulácie so systémom,
   d) **dostupnosť** – vlastnosť, že niečo je na požiadanie prístupné a použiteľné autorizovanou entitou,
   e) **individuálna zodpovednosť** – vlastnosť zaručujúca, že činnosti určitej entity môžu byť sledované jedinečne pre túto entitu,
   f) **autenticita** – vlastnosť zaručujúca, že identita subjektu alebo zdroja je taká, za akú je prehlasovaná,
   g) **autenticita** – je aplikovaná na entity ako sú používatelia, procesy, systémy a informácie,
   h) **spoľahlivosť** – vlastnosť zaručujúca konzistentný režim práce, zamýšľané správanie a jeho výsledky

informačná bezpečnosť

vnútorná	vonkajšia
- komunikačná bezpečnosť	- fyzická bezpečnosť
- dátová bezpečnosť	- personálna bezpečnosť
- programová bezpečnosť	- režimová bezpečnosť

3) **Zodpovednosť** za bezpečnosť osobných údajov:
   a) spoločnosť na čele s prevádzkovateľom spoločnosti zodpovedá za bezpečnosť spracovaných osobných údajov v IS spoločnosti, pred odcudzením, stratou, poškodením, neoprávneným prístupom, zmenou a neoprávneným rozširovaním.

b) **dohľad nad ochranou osobných údajov** vykonáva prevádzkovateľ.

PREVÁDZKOVATEĽ

V súlade so zákonom č.18/2018 Z.z. o ochrane osobných údajov prevádzkovateľ s ohľadom na povahu, rozsah a účel spracúvania osobných údajov a na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva fyzickej osoby je prevádzkovateľ povinný prijať vhodné technické a organizačné opatrenia na zabezpečenie a preukázanie toho, že spracúvanie osobných údajov sa vykonáva v súlade s týmto zákonom. Uvedené opatrenia je prevádzkovateľ povinný podľa potreby aktualizovať.

4. DEFINÍCIA POJMOV

1) **Osobné údaje (OÚ)** – sú údaje týkajúce sa identifikovanej fyzickej osoby, ktorú možno identifikovať priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, iného identifikátora, ako je napríklad meno, priezvisko, identifikačné číslo, lokalizačné údaje, alebo online identifikátor, alebo na základe jednej alebo viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú identitu, fyziologickú identitu, genetickú identitu, psychickú identitu, mentálnu identitu, ekonomickú identitu, kultúrnu identitu alebo sociálnu identitu.
2) **Spracúvanie osobných údajov** – spracovateľská operácia alebo súbor spracovateľských operácií s osobnými údajmi alebo so súbormi osobných údajov, najmä získavanie, zaznamenávanie, usporadúvanie štruktúrovanie, uchovávanie, zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie, bez ohľadu na to, či sa vykonáva automatizovanými prostriedkami alebo neautomatizovanými prostriedkami.
3) **Zodpovedná osoba** – osoba určená prevádzkovateľom alebo sprostredkovateľom, ktorá plní úlohy podľa tohto zákona.
4) **Dotknutá osoba** – každá fyzická osoba, ktorej osobné údaje sa spracúvajú.
5) **Súhlas dotknutej osoby** – je akýkoľvek vážny a slobodne daný, konkrétny, informovaný a daný prejav vôle dotknutej osoby vo forme vyhlásenia alebo jednoznačného potvrdzujúceho úkonu, ktorým dotknutá osoba vyjadruje súhlas so spracovaním svojicj osobných údajov.

6) **Informačný systém** – akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom základe alebo geografickom základe
7) **Prevádzkovateľ** – je každý, kto sám alebo spoločne s inými vymedzí účel a prostriedky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene; prevádzkovateľ alebo konkrétne požiadavky na jeho určenie môžu byť ustanovené v osobitnom predpise alebo medzinárodnej zmluve, ktorou je Slovenská republika viazaná, ak takýto predpis alebo táto zmluva ustanovuje účel a prostriedky spracúvania osobných údajov.
8) **Zástupca** – fyzická alebo právnická osoba so sídlom, miestom podnikania, organizačnou zložkou, prevádzkarňou alebo trvalým pobytom v členskom štáte, ktorú prevádzkovateľ alebo sprostredkovateľ písomne poveril podľa § 35.
9) **Sprostredkovateľ** – každý, kto spracúva osobné údaje v mene prevádzkovateľa.
10) **Tretia strana** – je každý, kto nie je dotknutou osobou, prevádzkovateľ, sprostredkovateľ alebo inou fyzickou osobou, ktorá na základe poverenia prevádzkovateľa alebo sprostredkovateľa spracúva osobné údaje.
11) **Príjemca** – je každý, komu sú osobné údaje poskytnutú bez ohľadu na to, či je treťou stranou, za príjemcu sa nepovažuje orgán verejnej moci, ktorý spracúva osobné údaje na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, v súlade s pravidlami ochrany osobných údajov vzťahujúcimi sa na daný účel spracúvania osobných údajov.
12) **Logom** – záznam o priebehu činnosti používateľa v automatizovanom informačnom systéme.
13) **Šifrovaním** – transformácia osobných údajov spôsobom, ktorým opätovné spracúvanie je možné len po zadaní zvoleného parametra, ako je kľúč alebo heslo.
14) **Online identifikátorom** – identifikátor poskytnutý aplikáciou, nástrojom alebo protokolom, najmä IP adresa, cookies, prihlasovacie údaje do online služieb, rádiofrekvenčná identifikácia, ktoré môžu zanechať stopy, ktoré sa najmä v kombinácii s jedinečnými identifikátormi alebo inými informáciami môžu použiť na vytvorenie profilu dotknutej osoby a na jej identifikáciu.
15) **Obmedzením spracúvania OÚ** – označenie uchovávaných osobných údajov s cieľom obmedziť ich spracovanie v budúcnosti.
16) **Porušením ochrany OÚ** – porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene alebo k neoprávnenému poskytnutiu prenášaných,

uchovávaných osobných údajov alebo inak spracúvaných osobných údajov alebok neoprávnenému prístupu k nim.

17) **Účel spracúvania OÚ** – je vopred jednoznačne vymedzený alebo ustanovený zámer spracúvania osobných údajov, ktorý sa viaže na určitú činnosť.
18) **Biometrický údaj** – osobné údaje, ktoré sú výsledkom osobitného technického spracúvania osobných údajov týkajúcich sa fyzických charakteristických znakov fyzickej osoby, fyziologických charakteristických znakov fyzickej osoby alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú jedinečnú identifikáciu alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby, ako najmä vyobrazenie tváre alebo daktyloskopické údaje.
19) **Genetický údaj** – osobné údaje týkajúce sa zdedených genetických charakteristických znakov fyzickej osoby 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.
20) **Členský štát** – štát, ktorý je členským štátom Európskej únie alebo zmluvnou stranou Dohody o Európskom hospodárskom priestore.
21) **Tretia krajina** – krajina, ktorá nie je členským štátom.
22) **Integrita** – je definovanie metód a postupov pri spracúvaní informácií, vymedzenie obsahu informácie, zaistenie presnosti informácie a vymedzených možnosti zmien.
23) **Firewall** – kombinácia hardwaru tvoriaca systém zabezpečenia, obvykle brániaci neoprávnenému prístupu k internej sieti, či intranetu z vonkajšieho prostredia.
24) **Antivírový softwar** – špeciálne vyvinutý softwar, ktorý slúži na detekciu a prevenciu pred známymi a novými infiltráciami.
25) **Server** – počítač, ktorý poskytuje službu pre ďalšie počítače.
26) **Aktíva** – čokoľvek čo má pre organizáciu hodnotu.
27) **Hrozba** – potenciálna príčina nežiaduceho incidentu.
28) **Riziko** – potenciálna možnosť, že daná hrozba využije zraniteľnosť aktív alebo skupiny aktív a spôsobí tak stratu alebo zničenie aktív.
29) **Zvyškové riziko** – riziko, ktoré zostáva po implementácii bezpečnostných opatrení.
30) **Dopad** – výsledok nežiaduceho incidentu.
31) **Bezpečnostné opatrenie** – vykonávaná prax, pracovný postup alebo zriadenie, ktoré znižujú rizika.
32) **Bezpečnostné ciele** – identifikujú, čo je potrebné dosiahnuť.

33) **Bezpečnostné stratégie** – definujú ako dosiahnuť bezpečnostné ciele.

34) **VPN – Virtual private network** – je privátna dátová sieť využívajúca verejnú komunikačnú infraštruktúru, v ktorej je privátnosť (vo význame dôvernosť) zabezpečená „bezpečným tunelom" a bezpečnostnými procedúrami. Základným cieľom VPN je poskytnúť firmám bezpečnú „vlastnú" sieť za nízke náklady zdieľaním verejnej infraštruktúry. VPN využívajú metódu šifrovania údajov pred ich odoslaním do verejných (alebo nechránených) sietí a ich dešifrovania po prijatí. Ďalším bezpečnostným stupňom je využitie šifrovania nielen pre obsah (údaje) ale aj hlavičky paketov.

4.1. ZÁSADY SPRACÚVANIA OSOBNÝCH ÚDAJOV

a) osobné údaje možno spracúvať len spôsobom ustanoveným zákonom NR SR č. 18/2018 Z.z. o ochrane osobných údajov a v jeho medziach tak, aby nedošlo k porušeniu základných práv a slobôd dotknutých osôb, najmä k porušeniu ich práva na zachovanie ľudskej dôstojnosti alebo k iným neoprávneným zásahom do ich práva na ochranu súkromia,
b) osobné údaje môže spracúvať iba prevádzkovateľ a sprostredkovateľ,
c) prevádzkovateľom na účely spracúvania osobných údajov v registri trestov podľa osobitného zákona (zák.č. 330/2007 Z.z. o registri trestov), môže byť len štátny orgán.

4.2. ZOZNAM SKRATIEK

AIS - automatizovaný informačný systém

BOZP – bezpečnosť ochrany zdravia pri práci

EÚ – európska únia

EZS - elektronicky zabezpečovací systém

HDD - harddisk drive

IS - informačný systém

IT - informačné technológie

OÚ - osobné údaje

PaM - personalistka a mzdy

PC - pracovná stanica (Personal Computer)

PP – pracovná pozícia

OPP – ochrana pred požiarmi

SBS – súkromná bezpečnostná služba

TP – technický prostriedok

ŽV – životné prostredie

LAN – miestna počítačová sieť pre komunikáciu medzi pracovnými stanicami (Local Area Network)

5. ROZSAH A ÚČEL SPRACOVANIA OSOBNÝCH ÚDAJOV

5.1. PREDBEŽNÉ ROZČLENENIE OSOBNÝCH ÚDAJOV

1) V spoločnosti sa spracúvajú osobné údaje dotknuté zákonom, nasledovne:

Skupina údajov	spracúva
Personálne údaje	prevádzkovateľ
Účtovníctvo a účtovné doklady	sprostredkovateľ
Mzdové údaje	sprostredkovateľ
Údaje o klientoch	prevádzkovateľ

2) Metodické usmernenie
   - Sprostredkovateľ je oprávnený spracúvať osobné údaje len v rozsahu, za podmienok a na účel dojednaný s prevádzkovateľom v zmluve a spôsobom podľa tohto zákona. Pri výbere musí prevádzkovateľ dbať na jeho odbornú, technickú, organizačnú a personálnu spôsobilosť a jeho schopnosť zaručiť bezpečnosť spracúvaných OÚ.
   - Prevádzkovateľ pri spracúvaní osobných údajov dbá o ich bezpečnosť. Osobné údaje spracúva len za účelom predaja, kúpy alebo prenájmu nehnuteľnosti pre klienta a/alebo záujemcu.

5.2. TYPICKÉ PROCESY SPRACÚVANIA OSOBNÝCH ÚDAJOV

1) Typické procesy spracúvania osobných údajov sú identifikované nasledovne:

Proces	Podľa	Prebieha
Spracúvanie osobných údajov	§ 5 písm. e)	áno
Poskytovanie osobných údajov	§ 34 ods. 1	áno
Sprístupňovanie osobných údajov		nie
Zverejňovanie osobných údajov		nie
Cezhraničný tok osobných údajov		nie

2) Osobné údaje zamestnanca budú v súlade s osobitnými zákonmi poskytované nasledujúcim tretím stranám:
   - Zdravotné poisťovne
   - Sociálna poisťovňa

- Daňový úrad
- Úrad práce sociálnych vecí a rodiny
- Doplnkové dôchodkové spoločnosti
- Dôchodkové správcovské spoločnosti
- BOZP
- Iné (banky, komerčné poisťovne, exekútor ...)

Spracovanie osobných údajov zo strany prevádzkovateľa:

- rokovanie o uzavretí zmluvy, predzmluvné vzťahy, uzavretie zmluvy medzi prevádzkovateľom a Dotknutou osobou, resp. medzi dotknutou osobou a predávajúcim a/alebo kupujúcim, ako aj plnenie zmlúv – uzavretie zmluvy o budúcej kúpnej zmluve a/alebo kúpnej zmluvy, vykonanie zápisu vlastníckeho práva a iných práv účastníkov zmluvného vzťahu na príslušný okresný úrad, katastrálny odbor, evidencia platieb a zabezpečenie spôsobu platenia kúpnej ceny, odovzdanie nehnuteľnosti do užívania.

a) Externá účtovníčka je oprávnené spracovávať osobné údaje zamestnanca spoločnosti manuálne a v elektronickej podobe, údaje je oprávnená poskytovať bankovým a iným inštitúciám.
b) Zamestnanca, ktorého osobné údaje budú takýmto spôsobom poskytnuté, je potrebné informovať a zároveň zamestnanec musí poskytnúť súhlas dotknutej osoby. Súhlas musí obsahovať názov subjektu, ktorému budú osobné údaje poskytnuté a účel.

3) Osobné údaje nebudú postupované do tretích krajín a rovnako nebudú zverejňované.

4) Typickými dotknutými osobami podľa § 5 písmeno n) sú:
   a) vlastní zamestnanci firmy
   b) klienti spoločnosti

5.3. TECHNICKÉ PROSTRIEDKY

Popis dotknutých technických prostriedkov

Súpis predbežne identifikovaných technických prostriedkov, na ktorých sa automatizovaným a neautomatizovaným spôsobom spracúvajú osobné údaje:

1. **Personálny informačný systém**

   Komerčne bežne dostupný personálny evidenčný software, z údajov sa vyhotovujú listinné formy voľným spôsobom alebo do formulárov predpísaných inou autoritou.

Prevádzkuje sa na pracovných staniciach, ktoré sú pripojené do firemnej LAN. Prístupy sú na základe prístupových práv.

2. **Mzdový informačný systém**

   Komerčne bežne dostupný mzdový evidenčný software, z údajov sa vyhotovujú listinné formy voľným spôsobom alebo do formulárov predpísaných inou autoritou.

   Prevádzkuje sa na pracovných staniciach, ktoré sú pripojené do firemnej LAN. Prístupy sú na základe prístupových práv.

3. **Ekonomický informačný systém**

   Špecializovaný ekonomický informačný systém v režime klient a aplikačný server.

   Prevádzkuje sa na PC staniciach pripojených na LAN a WAN firmy. K osobným údajom majú prístup určené osoby podľa prístupových práv nastavovaných v systéme správcami.

4. **LAN a WAN sieť**

   LAN firmy je pripojená na Internet od jedného prevádzkovateľa. Prípojné body sú chránené firewallom a prenášané dáta sú kryptované.

5. **Zmluvy s klientmi**

   Zmluvy sú ukladané v skriniach v uzamknutej miestnosti. Do týchto priestorov majú prístup dvaja konatelia a jeden zamestnanec.

6. **Mzdové a personálne údaje zamestnancov**

   Formuláre predpísané inou autoritou, výkazníctvo ukladané v skriniach v tlačenej podobe u externej účtovníčky na základe Zmluvy o sprostredkovaní mzdovej agendy a účtovnej agendy.

5.4. PRACOVNÉ POZÍCIE POVERENÝCH OSÔB

1) **Vymedzenie pracovných pozícií, ktoré spracúvajú osobné údaje**

   - Zamestnanci spoločnosti sú dotknutou osobou, teda fyzickou osobou, ktorej osobné údaje sa spracúvajú.

   - Klienti spoločnosti alebo záujemcovia sú dotknutou osobou, teda fyzickou osobou, ktorej osobné údaje sa spracúvajú.

2) **Metodické usmernenie**

   - Dotknutá osoba - zamestnanec udelí súhlas prevádzkovateľovi o spracovaní jej osobných údajov za účelom mzdovej a účtovnej agendy.
   - Dotknutá osoba - klient/záujemca udelí súhlas prevádzkovateľovi o spracovaní svojich osobných údajov za účelom predaja, kúpy či prenájmu nehnuteľnosti

5.5. TYPICKÉ OPRÁVNENIA OSÔB PRACUJÚCICH S OSOBNÝMI ÚDAJMI

Typickými oprávneniami osôb sú tieto operácie:

- **Vytváranie**
  Vytvorí sa nová informácia obsahujúca chránený osobný údaj (záznam, databázy, vytvorenie súboru, zoznamu a pod.)
- **Modifikovanie**
  Existujúca informácia, existujúci záznam sa zmení – modifikuje (znateľným spôsobom – prečiarknutie, dopísanie, vyhotovenie novej verzie, pričom stará je dostupná tiež, alebo neznateľným spôsobom – nie je možné zistiť pôvodný obsah informácie, vytvorí sa iný obsah existujúcej informácie)
- **Prezeranie**
  Existujúca informácia sa používa na ďalšie spracovanie, pričom sa nekopíruje, iba prezerá (nedôjde k fyzickej zmene informácie)
- **Kopírovanie**
  Existujúca informácia sa rozmnoží za účelom ďalšieho spracovania, poskytnutia (vyhotoví sa kópia listinnej formy alebo elektronickej formy)
- **Poskytovanie**
  Existujúca informácia sa poskytne v akejkoľvek forme – nahliadnutie, kopírovanie – inej osobe (nedochádza k zmene informácie)
- **Archivácia**
  Uloženie informácie na akomkoľvek nosiči do archívu (musí byť vyhotovený záznam)
- **Likvidácia**
  Fyzické zlikvidovanie informácie (musí byť vyhotovený záznam)

BEZPEČNOSTNÝ ZÁMER
Dokumentácie

NA OCHRANU OSOBNÝCH ÚDAJOV V PODMIENKACH SPOLOČNOSTI

vymedzujúci

základné bezpečnostné ciele, ktoré je potrebné dosiahnuť na ochranu osobných údajov systému firmy pred ohrozením jeho bezpečnosti

6. BEZPEČNOSTNÝ ZÁMER

1) Dokumentácia je zameraná na ochranu osobných údajov získaných za účelom personálnej a mzdovej agendy. Je vypracovaná podľa súčasne používaných prostriedkov výpočtovej techniky, ich umiestnenia, konfigurácie a zapojenia.

2) Pri zmene podmienok je potrebné dokumentáciu prepracovať, prípadne doplniť dodatkom o vykonanej zmene.

6.1. ZÁKLADNÉ BEZPEČNOSTNÉ CIELE PRE OCHRANU OSOBNÝCH ÚDAJOV STANOVENÉ VEDENÍM SPOLOČNOSTI

1) Základnými cieľmi v bezpečnosti informačných systémov sú skutočnosti v oblasti:
   a) vybudovať a trvalo udržiavať vysokú úroveň ochrany osobných údajov,
   b) zabezpečiť osobné údaje pred prístupom nepovolaných osôb,
   c) pri získavaní osobných údajov zabezpečiť súhlas so spracovávaním a následne archiváciu súhlasu, súhlas zapracovať do pracovnej zmluvy, zmluvy o sprostredkovaní predaja nehnuteľnosti, rezervačnej zmluvy,
   d) pri automatizovanom spracovávaní osobných údajov zabezpečiť antivírovú ochranu a zálohovanie,
   e) zabezpečiť osobné údaje pred sprístupnením a zverejnením prostredníctvom zneužitia počítačovej siete a pripojenia na internet,
   f) zabezpečiť vhodné podmienky na archivovanie všetkých dokumentov,
   g) zabezpečiť dôslednú likvidáciu údajov, ktoré už nie je potrebné spracovávať,
   h) v pravidelných časových intervaloch analyzovať použité bezpečnostné opatrenia, posúdiť zvyškové riziká a prípadne navrhnúť ďalšie bezpečnostné opatrenie,

2) Vychádzajúc z týchto cieľov boli vypracované minimálne požadované bezpečnostné opatrenia.

6.2. ZÁKLADNÉ POŽADOVANÉ BEZPEČNOSTNÉ OPATRENIA

1) Bezpečnostné opatrenia by mali chrániť všetky cenné dáta i majetok organizácie.

2) Spoločnosť spĺňa nasledujúce minimálne požiadavky vyplývajúce zo zákona o ochrane osobných údajov:

a) pri získavaní osobných údajov zamestnancov zabezpečiť písomný súhlas so spracúvaním osobných údajov,
b) pri automatizovanom spracovávaní osobných údajov používať programové vybavenie, ktoré vyžaduje meno a heslo používateľa,
c) správne nastaviť a obmedziť prístupové práva k adresárom a súborom, ktoré obsahujú osobné údaje,
d) údaje pravidelne zálohovať,
e) používať antivírovú ochranu na všetkých vstupoch do automatizovaného informačného systému,
f) priestory určené pre spracovávanie osobných údajov zamykať i pri dočasnej neprítomnosti prevádzkovateľa alebo zamestnanca,
g) písomné dokumenty archivovať v uzamykateľnej miestnosti,
h) nepotrebné písomné dokumenty likvidovať v súlade so zákonom č. 18/2018 Z.z. o ochrane osobných údajov,
i) dôkladne odstrániť dáta z dátových nosičov pred ich vyradením z používania.

6.3. ŠPECIFIKÁCIA REALIZOVANÝCH BEZPEČNOSTNÝCH OPATRENÍ

Špecifikácia je rozdelená do troch kategórií:

6.3.1. TECHNICKÉ OPATRENIA
6.3.2. ORGANIZAČNÉ OPATRENIA
6.3.3. PERSONÁLNE OPATRENIA

6.3.1. TECHNICKÉ OPATRENIA

1) Technické opatrenia sú realizované najmä použitím technických prostriedkov na zabránenie postupu osôb do chránených priestorov.
2) V oblasti informačných technológií sa tieto opatrenia vykonávajú využitím funkcií operačných systémov a jednotlivých aplikácií.

Ochrana priestorov

- Zabezpečená a strážená budova, 1. poschodie
  (spôsob využitia: obmedzenie a riadenie prístupu osôb)
- hasiace prístroje, požiarno-evakuačný plán
  (spôsob využitia: ochrana pred živelnou pohromou)

- uloženie písomných dokumentov personalistiky a miezd obsahujúcich osobné údaje v zabezpečenej drevenej skrini uzamykateľnej na kľúč v kancelárii účtovníčky, archivovanie v regáloch. Uloženie zmlúv s klientmi obsahujúce osobné údaje v zabezpečenej skrini, v zabezpečenej miestnosti mimo sídla spoločnosti.
  (spôsob využitia: obmedzenie a riadenie prístupu osôb)

Informačné technológie

- používané nové verzie operačných systémov, ktoré poskytujú vyššiu úroveň bezpečnosti
- aplikácie používané na spracúvanie osobných údajov pre spustenie vyžadujú meno a heslo používateľa
- definované prístupové práva na jednotlivé časti AIS (súbory, priečinky, ...)
  (spôsob využitia: uplatňovaná povinnosť identifikácie a autentizácie pri prístupe k informačnému systému, využívaná možnosť nastaviť oprávnenia pre jednotlivé časti AIS, riadenie prístupu k aktívam)
- inštalované opravné programové balíčky pre operačné systémy i aplikácie
  (spôsob využitia: zvyšovanie bezpečnosti programového vybavenia)
- šifrovanie uložených dát – súbory, ktoré obsahujú osobné údaje sa nedajú samostatne, bez spustenia príslušnej aplikácie, ktorá vyžaduje heslo a meno používateľa, zobraziť alebo tlačiť
  (spôsob využitia: ochrana údajov v prípade získania prístupu k súborom)
- ochrana proti škodlivým programom, kontrola všetkých vstupov do AIS – všetky PC, e-mail, www stránky, pravidelne aktualizované antivírové programy, update i upgrade na jednotlivých počítačoch
  (spôsob využitia: ochrana proti počítačovým vírusom, pred poškodením údajov, prípadne pred ich sprístupnením)
- zriadené bezpečné pripojenie na internet
  (spôsob využitia: ochrana pred prienikom do siete zvonku)

6.3.2. ORGANIZAČNÉ OPATRENIA

1) Zahŕňajú postupy a vzťahy pri ochrane a prevádzke informačného systému, definujú podmienky a priebeh bezpečného spracovania OÚ v informačnom systéme, napr. musia zabrániť neoprávneným osobám prečítať vytlačený dokument, obsahujúci osobné údaje alebo dokument zobrazený na monitore.

2) Sú zamerané hlavne na oblasti:
   a) bezpečné umiestnenie prvkov AIS a prvkov manuálneho spracúvania,
   b) protipožiarna ochrana a ochrana zdravia pri práci, ohrozenie zaplavenia priestoru vodou,
   c) prívod elektrickej energie do organizácie, rozvody a napájanie AIS,
   d) káblové a telefónne rozvody,
   e) kľúčový poriadok, elektronický zabezpečovací systém, ochrana pred vstupom nepovolaných osôb do budovy, určenie podmienok vstupu osôb do priestorov so sústredenými osobnými údajmi,
   f) podmienky pre výkon práce, zariadenie, umiestnenie monitorov, okná kúrenie,
   g) sledovanie a implementácia zákonov a vyhlášok do vnútropodnikovej legislatívy,
   h) finančné zabezpečenie rozvoja aktív informačného systému – plánovanie rozpočtu,

OCHRANA PRIESTOROV

Priestory v sídle spoločnosti sú chránené alarmom a kamerovým systémom. Vstup do budovy je možný len s kľúčom a kódom. Dvere sú uzavreté do budovy, bez kľúča vstup do budovy nie je možný. Kancelária sa nachádza na 1. poschodí, vstupné dvere do kancelárie uzamykateľné. Kľúčom disponuje prevádzkovateľ a jeden zamestnanec spoločnosti.
Budova je chránená pred požiarom, ochrana pred živelnou katastrofou

- o alarm sa stará administrátor – externá firma
  (spôsob využitia: organizácia si môže voči nej uplatniť náhradu prípadnej škody)

6.3.3. PERSONÁLNE OPATRENIA

1) Personálne opatrenia predstavujú najmä poučenie zamestnancov o jednotlivých interných smerniciach a ich vzdelávanie:
   - poučené všetky osoby, ktoré majú alebo môžu mať prístup k informačnému systému

   (spôsob využitia: splnenie zákonných požiadaviek, zvyšovanie povedomia o bezpečnosti a o potrebe dodržiavať bezpečnostné opatrenia)

6.4. OKOLIE INFORMAČNÉHO SYSTÉMU

- **Sídlo**

  Nehnuteľnosti Levice s. r.o.,
  Kpt. Nálepku 78, 934 01 Levice

- **Ochrana priestorov**
  - Zabezpečená a uzamknutá budova, osvetlená
  - hasiace prístroje, požiarno – evakuačný plán

- **Počet zamestnancov**
  - 1 zamestnanec, 2 konatelia

- **Osoby, ktoré sa dostávajú do kontaktu s OÚ**
  - Účtovníčka, mzdárka – externá osoba
  - zamestnanec spoločnosti Nehnuteľnosti Levice s.r.o., dvaja konatelia

- **Zabezpečenie miestnosti kde sú spracúvané OÚ - kancelária**
  - uzamykateľné dvere
  - v administratívnej časti budovy

- **Kde sú uložené OÚ v miestnosti kde sa spracúvajú**
  - OÚ sú zabezpečené v drevenej skrini uzamykateľnej na kľúč

- **Prístup a kľúče od miestnosti**
  - prístup a kľúče do miestnosti majú dvaja konatelia

- **Dokumenty s OÚ v MS Office**
  - spracovanie kúpnych zmlúv, návrhov na vklad vlastníckeho práva na príslušný okresný úrad, katastrálny odbor, súhlas dotknutej osoby, zmluva o sprostredkovaní predaja nehnuteľnosti, rezervačná zmluva, záznam o vykonanej obhliadke, súhlas so zaradením nehnuteľnosti do ponuky
- **Archivovanie dokumentov, kde sú uložené**
  - dokumenty určené na archiváciu sa archivujú na adrese bydliska konateľov: Pivničná ul. 3995/96, 934 01 Levice
  - samostatná uzamykateľná miestnosť, ktorá slúži ako kancelária zamestnanca, zabezpečená budova s alarmom
  - prístup a kľúče majú konatelia

- **Preberanie pošty**
  - poštu sú oprávnení preberať obaja konatelia

- **Upratovanie miestností kde sa spracúvajú OÚ**
- upratovanie kancelárskych priestorov – zabezpečujú konatelia
- **Protipožiarna ochrana**
  - požiarno – evakuačný plán
  - hasiace prístroje – umiestnené na presne určených miestach

- **Automatizované informačné systémy**
  - spoločnosť má vo vlastníctve 1ks notebook a 1ks počítača. Poskytovateľom internetových služieb je spoločnosť Orange Slovensko a.s., mobilné pripojenie, ktorá spoločnosti poskytuje služby internetového prístupu a pripojenie prostredníctvom technológie DSL.
  - prístup k dátam je obmedzený heslom
  - vstup do systémov je zabezpečený menom a heslom

- **Súčasný stav ochrany proti napadnutiu IS**
  - antivírová ochrana na PC – program ESET
  - bezpečnostná brána,
  - prístup zabezpečený heslami,
  - automatická aktualizácia scanovacieho programu aj databázy vírusov vykonávaná denne
  - úschova médií v sídle spoločnosti a v mieste bydliska konateľov

- **Prevádzku informačných systémov a výpočtovej techniky spoločnosti**
  - ich vybavenosť, zabezpečovanie opráv, inováciu technického stavu a sledovanie nákladovosti riadi IT technik (externá spoločnosť).

- **Zabezpečenie prevádzky informačných systémov a výpočtovej techniky**
  - údržby, opráv a odstránených porúch, inštaláciu hardwarového a softwarového vybavenia, operačných systémov ako i nastavenie bezpečnostných a technických opatrení na určených technických prostriedkoch spoločnosti, lokálnej a internetovej siete spoločnosti, vykonáva externý systémový administrátor automatizovaných informačných systémov spoločnosti, t.j. osoba zodpovedná za prevádzku informačných systémov v spoločnosti (ďalej len IT technik)

- **Tlačiareň**
  - Spoločnosť disponuje 1 tlačiarňou

6.5. ZVYŠKOVÉ RIZIKÁ

Odhad zvyškových rizík

1) Spoločnosť je pripravená realizovať relevantné a primerané opatrenia v oblasti technických prostriedkov, organizačných opatrení a v systéme riadenia ľudských zdrojov na zabránenie a elimináciu ohrození informačných systémov na spracúvanie osobných údajov.

2) Rozsah a kvalita prijatých opatrení bude determinovaná najmä:
   a) technickou (skutočnou) realizovateľnosťou opatrení,
   b) finančnými nákladmi na opatrenia,
   c) stupňom dodržiavania prijatých opatrení pracovníkmi organizácie

3) Zvyškové riziká sú všetky tie, ktoré ešte ostali napriek existujúcim bezpečnostným opatreniam.

Ohrozenie:

- **Odcudzenie, rozširovanie** – nie je možné, zamestnanec je zároveň aj konateľ,
- Pravdepodobnosť rizika ohrozenia – malá
  Pravdepodobný negatívny dopad – vysoký
- **Zneužitie právomoci s následkom negatívneho dopadu** – prezradenie prístupových kódov, prenechanie identifikačného predmetu, nedodržanie stanovených postupov
  Pravdepodobnosť rizika ohrozenia – nízka
  Pravdepodobný negatívny dopad - vysoký
- **Vandalstvo, terorizmus, sabotáž** – zničujúci požiar, výbuch nástražného systému v blízkosti alebo priamo v budove a pod.
  Pravdepodobnosť rizika ohrozenia – nízka
  Pravdepodobný negatívny dopad - vysoký

- **Pôsobenie vyššej moci** – nerozpoznané
  Pravdepodobnosť rizika ohrozenia – nízka
  Pravdepodobný negatívny dopad - vysoký

ANALÝZA BEZPEČNOSTI

NA OCHRANU OSOBNÝCH ÚDAJOV V PODMIENKACH SPOLOČNOSTI

vymedzujúca

rozbor stavu bezpečnosti informačného systému

7. ANALÝZA BEZPEČNOSTI INFORMAČNÉHO SYSTÉMU

7.1. POPIS INFORMAČNÉHO SYSTÉMU

1) V informačnom systéme sa spracúvajú údaje, ktoré môžeme rozdeliť na:
   a) údaje o zamestnancovi a jeho rodinných príslušníkoch
   b) údaje o klientoch

7.2. AUTOMATIZOVANÉ INFORMAČNÉ SYSTÉMY

1) Spoločnosť spracováva osobné údaje v informačnom systéme (IS):
   a) „POHODA" – účtovníctvo
   b) „POHODA" – PaM
   c) CMS Joomla, program na nehnuteľnosti: OS Property
      Spoločnosť nezbiera dáta o návštevnosti a nemá registráciu užívateľov. Osobné údaje, ktoré posielajú spoločnosti zákazníci len formou kontaktného formulára: meno, priezvisko, e-mail, telefón.

Do kategórie osobných údajov sú podľa zákona č. 18/2018 Z.z. o ochrane osobných údajov a zmien a doplnení zaradené údaje o zamestnancovi ako aj údaje o klientoch. Údaje sú zhromažďované v písomnej forme na základe zmluvy, návrhov na vklad vlastníckeho práva na príslušný okresný úrad, katastrálny odbor, súhlas dotknutej osoby, zmluva o sprostredkovaní predaja nehnuteľnosti, rezervačná zmluva, záznam o vykonanej obhliadke, súhlas so zaradením nehnuteľnosti do ponuky.

2) Účelom spracovávania osobných údajov je viesť jednotlivé informačné systémy v súlade so zákonnými ustanoveniami.

3) Pre naplnenie databáz je určený technický prostriedok (PC), na ktorom sa automatizovaným spôsobom vedú osobné údaje.

4) Vstup do systémov je zabezpečený menom a heslom.

5) Spoločnosť disponuje tlačiarňou.

6) Na počítači je nainštalovaný operačný systém, Windows 7, chránený nainštalovaným Firewallom a antivírusovým programom ESET.

7.3. ELEKTRONICKÁ FORMA

Zoznam spracovávaných údajov v automatizovaných informačných systémoch pre dotknuté osoby s uvedením kategórií osobných údajov, ktoré sa v jeho aplikáciách a databázach spracovávajú:

1) **Platy a mzdy – IS**
   a) *Dotknuté osoby*: zamestnanec
   b) *Kategória osobných údajov*: osobitnej kategórie (OK)
   c) *Kategória osobných údajov*: ostatné

   Zoznam osobných údajov: meno, priezvisko – aj rodné a predchádzajúce, titul, adresa, dátum narodenia, miesto narodenia, mzda, rodinní príslušníci, rodinný stav, invalidita, dôchodok, číslo OP, štátna príslušnosť, zdravotná poisťovňa, dátum nástupu, dátum výstupu

2) **Personalistika – IS**
   a) *Dotknuté osoby*: zamestnanec
   b) *Kategória osobných údajov*: osobitnej kategórie (OK)

   Zoznam osobných údajov: rodné číslo
   c) *Kategória osobných údajov*: ostatné

   Zoznam osobných údajov: meno, priezvisko – aj rodné a predchádzajúce, titul, dátum a miesto narodenia, číslo OP, rodinný stav, bydlisko, národnosť, štátna príslušnosť, najvyššie ukončené vzdelanie, rok ukončenia vzdelania, dátum 1. nástupu do zamestnania, zmenená prac. schopnosť, mzda/plat, zdravotná poisťovňa, vodičský preukaz, jazykové znalosti, začiatok pracovného pomeru (PP), funkcia, dôchodok, dátum a spôsob ukončenia PP, rodinní príslušníci

3) **MS Office (MS Word, MS Excel, MS Otlook)**
   a) *Dotknuté osoby*: klienti
   b) *Kategória osobných údajov*: osobitnej kategórie (OK)
   c) *Kategória osobných údajov*: ostatné

   Zoznam osobných údajov: meno, priezvisko, titul, číslo OP, bydlisko, v prípade predaja/kúpy nehnuteľnosti medzi klientom a záujemcom, za účelom spracovania kúpnych zmlúv : meno, priezvisko, rodné priezvisko, bydlisko, dátum narodenia, rodné číslo, štátna príslušnosť

7.4. ŠPECIFIKÁCIA INFORMAČNÝCH SYSTÉMOV

a) Spoločnosť má vo vlastníctve PC, ktoré sú pripojené na internet.
b) Poskytovateľom internetových služieb je spoločnosť Orange Slovensko a.s., ktorá spoločnosti poskytuje služby internetového prístupu a pripojenie s garantovanou rýchlosťou v licencovanom pásme.

7.5. SÚČASNÝ STAV OCHRANY PROTI NAPADNUTIU IS

a) antivírová ochrana PC – ESET
b) bezpečnostná brána
c) prístup zabezpečený heslami
d) automatická aktualizácia scanovacieho programu aj databázy vírusom vykonávaná denne
e) úschova médií v sídle spoločnosti

7.6. ANTIVÍRUSOVÉ OPATRENIA

Počítače, na ktorých sa spracúvajú osobné údaje sú zabezpečené antivírusovým systémom spoločnosti.

- Používané programy: ESET
- Základné nastavenia programov: rezidentná kontrola všetkých programov
- Spôsob práce s programami: automatické spúšťanie
- Perióda vykonávaná rezidentnej kontroly: týždenné

7.7. ZABEZPEČENIE PREVÁDZKY INFORMAČNÝCH SYSTÉMOV A VÝPOČTOVEJ TECHNIKY

a) Osoba zodpovedná za prevádzku informačných systémov v spoločnosti (správca IT technik – externá spoločnosť.

7.8. ELEKTRONICKÁ POŠTA

a) Cieľom je zabezpečiť, aby údaje prenášané a prijímané prostredníctvom elektronickej pošty boli chránené takým stupňom ochrany, aký vyžaduje pôvodca údajov. Údaje musia byť chránené proti porušeniu, strate, omeškaniu a neautorizovanému odhaleniu.

8. NÁVRH OPATRENÍ

1) Konkrétne bezpečnostné opatrenia pre jednotlivé aktíva informačného systému závisia na podrobnom popise a analýze hrozieb, ktoré môžu na ne pôsobiť. Pri každom návrhu na realizáciu konkrétneho opatrenia by mali byť jasné nasledujúce informácie.
   a) identifikácia problému
   b) možné varianty riešenia vrátane nákladov a možných prínosov
   c) doporučené riešenie problému a dôvody preň
   d) návrh, kto realizuje riešenie, termín realizácie
   e) dôsledky, ak s problém nevyrieši.

2) Výsledkom kvalitatívnej analýzy rizík má byť zoznam hrozieb, ktoré môžu ohroziť dôvernosť, integritu a dostupnosť spracúvaných osobných údajov, s uvedením rozsahu možného rizika a návrhov opatrení, ktoré eliminujú alebo minimalizujú vplyv rizík.

8.1. BEZPEČNOSTNÉ OPATRENIA ŠPECIFIKÁCIE PRE SYSTÉM IT

8.1.1. Identifikácia a autentizácia

1) Identifikácia je prostriedok, ktorým užívateľ poskytuje systému požadovanú identitu.

2) Autentizácia je prostriedok, ako preukázať platnosť tohto tvrdenia. Najtypickejšou metódou identifikácie a autentizácie sú heslá. Vytváranie hesiel a ich pravidelná zmena musí byť pravidelne kontrolovaná.

3) Kópie hesiel musia byť bezpečne uschované, aby bola zachovaná možnosť autorizovaného prístupu, keď je užívateľ nedostupný alebo heslo zabudol.

8.1.2. Ochrana účtu

1) Užívateľské mená a heslá nesmú byť uložené ako súčasť informácií užívateľského účtu, inak môže ľubovoľná osoba s prístupom k tomuto účtu nahliadať tiež do týchto uložených informácií.

2) Užívatelia musia svoje účty nevyhnutne chrániť pred zneužitím. Uzamykanie počítačov alebo odhlasovanie užívateľov počas ich neprítomnosti, ochrana šetričom obrazovky, heslom a používanie silných hesiel sú metódy, ktoré prispievajú k ochrane účtu.

3) Používať silné heslá pre všetky účty. Hoci môže silné heslo prispieť k ochrane pred neoprávnenými užívateľmi, existujú možnosti, ako heslo daného zdroja uhádnuť alebo odcudziť.

4) Z týchto dôvodov je nutné uskutočňovať pravidelnú výmenu hesiel.

8.1.3. Vytváranie silných hesiel

1) Používanie silných hesiel pre prihlásenie

2) Silné heslá sú dôležité, pretože nástroje k odhaleniu hesiel sú stále zlepšované a výkon počítačov používaných k tomuto účelu, sa stále zvyšuje.

3) Software odhaľujúci heslá používa jednu z troch nasledujúcich metód: inteligentné odhadovanie, zisťovanie pomocou slovníka a automatizovaný postup, ktorým možno vyskúšať všetky možné kombinácie znakov.

4) Automatizovanou metódou sa dá odhaliť akékoľvek heslo, pokiaľ je k dispozícii dostatok času. Odhalenie silného hesla však môže trvať i niekoľko mesiacov.

5) Heslá systému Windows môžu obsahovať až 127 znakov. Pokiaľ je však používaný systém Windows XP v sieti, ku ktorej sú pripojené PC so systémom Windows 95 alebo Windows 98, je vhodné používať heslá najviac so 14 znakmi. Systémy Windows 95 a Windows 98 podporujú heslá obsahujúce maximálne 14 znakov.

6) Z dôvodu zabezpečenia je treba používať heslá obozretne.

7) Odporúča sa dodržiavať nasledovné zásady: heslo nikdy nezapisovať, nikdy nesprístupniť heslo iným osobám, heslo na prihlásenie k sieti nikdy nepoužívať k inému účelu, používať iné heslo pre prihlásenie k sieti a iné pre prihlásenie k účtu správcu počítača, heslo pre prihlásenie k siet meniť každých 60 – 90 dní, alebo tak často, ako to zodpovedá konkrétnym potrebám. V prípade, že je podozrenie z prezradenia hesla, treba ho okamžite zmeniť,, nevyužívať možnosť uloženia alebo zapamätania si hesla systémom.

8) Príklady zlých hesiel: svoje meno, 123456, 0000, 1111, meno z kalendára,

8.1.4. Riadenie logického prístupu

1) Prístupové práva sú udeľované podľa požiadaviek vykonávanej činnosti.

2) Riadenie prístupu k počítačom musí byť zabezpečené tak, aby sa zamedzilo akémukoľvek neautorizovanému prístupu.

3) Riadenie prístupu k počítaču musí byť podporované použitím konkrétneho hesla. Všetky prístupové práva musia byť pravidelne revidované aby sa zamedzilo ich zneužitiu.

8.1.5. Ochrana pred škodlivým programovým kódom

1) Škodlivý programový kód môže byť zavedený do systému prostredníctvom externých spojení a prostredníctvom súborov a softvérov zavádzaných z prenosných diskov.
2) Škodlivý programový kód môže byť jedným z nasledovných typov: vírusy, červy, trójske kone. Nositeľom škodlivého programového kódu sú: spustiteľný program, dátové súbory, aktívny obsah www stránok.

3) Škodlivý programový kód sa môže šíriť: prenosnými médiami, elektrickou poštou, sieťami, sťahovaním.

4) Ochrana pred škodlivým programovým kódom musí obsahovať viac ochranných opatrení. Skenery – antivírové programy. Spolu s kontrolou integrity detegujú a odstraňujú rôzne formy škodlivého programového kódu. Nemožno sa však spoliehať, že skenery detegujú každý škodlivý programový kód, pretože neustále vznikajú nové formy škodlivého programového kódu.

8.1.6. Kontrolovanie integrity

1) Nesmie prebiehať nekontrolovateľný obeh médií (hlavne diskov), čo by mohlo viesť k zvýšenému riziku zavedenia škodlivého programového kódu do systému IT organizácie.

2) Riadenie obehu médií môže byť dosiahnuté použitím špeciálneho softvéru alebo procedurálnymi ochrannými opatreniami.

8.1.7 Správca siete

1) Vhodná konfigurácia a správa siete je účinným prostriedkom na zníženie rizika.

8.1.8. Prevádzkové postupy

1) K zaisteniu správnej a bezpečnej činnosti siete je potrebné stanoviť prevádzkové postupy a zodpovednosť.

2) Toto zahŕňa dokumentáciu prevádzkových postupov a stanovenie postupov, ako reagovať na incidenty týkajúce sa bezpečnosti.

8.1.9. Konfigurácia siete

1) Vhodná konfigurácia siete je podstatná pre jej spoľahlivé fungovanie.

8.1.10. Oddelenie siete

1) Aby sa znížilo riziko a zamedzilo možnému zneužitiu v prevádzkovej sieti s osobnými údajmi, mali by byť tieto zariadenia logicky alebo fyzicky oddelené.

8.1.11. Monitorovanie siete

1) Monitorovanie siete musí byť používané pre rozpoznávanie slabých miest v rámci existujúcej konfigurácie siete. To umožňuje zmenu konfigurácie v dôsledku analýzy prevádzky a pomáha rozpoznať narušiteľov.

8.1.12. Detekcia prienikov

1) Pokusy o získanie prístupu k systému alebo celej siete musí byť detekovaný, aby organizácia mohla reagovať primeraným účinným spôsobom.

8.1.13. Vzdialený prístup do systému

1) Každý používateľ systému musí byť identifikovaný a autentizovaný pred tým, ako je mu povolený prístup do systému. Na autentizáciu musí byť použitý technický prostriedok autentizácie alebo jednorazové prístupové heslo.
2) Musia byť použité také opatrenia, aby bola zachovaná integrita a dôvernosť prenášaných údajov.
3) Používateľovi, ktorému bude na základe žiadosti garanta umožnený takýto prístup do systému, môže byť pridelený len autorizovaný prístupový profil.

4) V prípade, keď sú vzdialené prístupy používané len občas, prípadne v definovaných časových rozmedziach, je možné prístup otvoriť len na požiadanie. Prístupy, ktoré sú bežne uzatvorené, budú otvorené iba na predchádzajúcu žiadosť.

8.1.14. Vzdialená údržba systému

1) Mnohé systémy po nainštalovaní umožňujú neobmedzený prístup pre vzdialenú údržbu. Ak je potrebné umožniť prístup do systému pre vzdialenú údržbu, musia byť dodržiavané nasledujúce pravidlá:
   a) Vzdialená údržba bude autentizovaná technickým prostriedkom autentizácie alebo jednorazovým prístupovým heslom
   b) na konci spojenia bude prístup znovu zablokovaný.

9. BEZPEČNOSTNÉ ŠTANDARDY

9.1. BEZPEČNOSTNÉ ŠTANDARDY OCHRANY INFORMAČNÝCH SYSTÉMOV

1) Na ochranu osobných údajov budú primerane použité štandardy, ktoré sa používajú na ochranu utajovaných skutočností, vydaných Národným bezpečnostným úradom SR (opäť v primeranej miere) a v súlade so zákonom č. 18/2018 Z.z. o ochrane osobných údajov v znení zmien a doplnení.

2) Na základe týchto podkladov, boli pre účely ochrany osobných údajov vypracované účelové štandardy. Pre informačné systémy s použitím automatizovaných prostriedkov spracúvania sa použijú štandardy všetkých skupín, t.j.:
   a) Fyzické opatrenia
   b) Technické opatrenia
   c) Programové opatrenia
   d) Režimové opatrenia
   e) Personálne opatrenia

3) Pre informačné systémy s použitím neautomatizovaných prostriedkov spracúvania sa používajú štandardy:
   a) Fyzické opatrenia
   b) Technické opatrenia

c) Režimové opatrenia

d) Personálne opatrenia

4) Základom ochrany je použitie záväzných opatrení. O použití doplnkových opatrení rozhoduje prevádzkovateľ. Doplnkové opatrenia sa odporúčajú najmä pri ohrozeniach, ktorých miera negatívneho dopadu je vysoká.

9.2 FYZICKÉ OPATRENIA

1) Úlohou fyzických opatrení je zabezpečenie priestorov, v ktorých sú aktíva umiestnené, ochrana pred prírodnými vplyvmi a opatrenia proti neoprávnenému vniknutiu osôb do týchto priestorov.
2) Ďalej riešia bezpečné uloženie dátových nosičov s informáciami a výstupov z tlačiarní, spôsoby ničenia už nepotrebných informácií a médií, ochranu pred prírodným živlom a požiarmi.

Záväzné opatrenia (fyzické)

1) miestnosti, v ktorých sú umiestnené informačné systémy, na ktorých sa spracúvajú osobné údaje, musia mať pevné dvere so zámkovým systémom,
2) zámkový systém do miestností, v ktorých sa spracúvajú osobné údaje nesmie používať skupinový alebo generálny kľúč,
3) okná do miestností, v ktorých sa spracúvajú osobné údaje musia byť pevné, nesmú sa dať otvoriť bez použitia násilia,
4) úschovne objekty musia mať zámkové systémy,
5) zámkový systém úschovných objektov nesmie používať skupinový alebo generálny kľúč,
6) osobné údaje uložené v elektronickej forme musia byť zálohované min. 1x mesačne. Doba archivácie záložných údajov je min. 7 dní,
7) záložné médiá sa musia ukladať v kovovej schránke,
8) všetky informačné systémy, na ktorých sa vykonáva automatizované spracúvanie osobných údajov musia mať antivírovú ochranu,
9) na likvidáciu osobných údajov sa používa skartovač.

Doplnkové opatrenia (fyzické)

1) dvere do miestností, v ktorých sú umiestnené informačné systémy, na ktorých spracúvajú osobné údaje musia byť bezpečnostné, alebo vybavené mrežou,
2) úschovné objekty, v ktorých s uchovávajú osobné údaje (v listinnej alebo elektronickej podobe) musia byť kovové,
3) v budove, kde sú miestnosti, v ktorých sa spracúvajú osobné údaje, je napojená na alarm. Ochranu objektu vykonáva externá firma.
4) antivírový program musí byť pravidelne aktualizovaný,
5) osobné údaje obsahujúce musia byť po opustení informačného systému zaheslované.

9.3 TECHNICKÉ OPATRENIA

Predstavujú nasadenie technických prostriedkov do informačného systému – elektrická požiarna signalizácia, elektronická zabezpečovacia signalizácia, videokamery, rušičky vyžarovaných signálov, skartovacie zariadenia, hardvérové identifikátory, záložné zdroje, diskové polia, bezpečnostné karty, ochrana proti vizuálnemu pozorovaniu a odpočúvaniu, ochrana pred elektromagnetickým vyžarovaním, a pod.

Záväzné opatrenia (technické)

1) Elektronické systémy, na ktorých sa spracúvajú osobné údaje (samostatný počítač, súborový server, databázový server) musia byť vybavené záložným zdrojom v prípade dočasného výpadku elektrickej energie.

Doplnkové opatrenia (technické)

1) Miestnosť v ktorej sa spracúvajú osobné údaje musí byť vybavená poplachovou signalizáciou na hlásenie narušenia.
2) Budova, v ktorej sa nachádza miestnosť, v ktorej sa spracúvajú osobné údaje musí byť vybavená protipožiarnou signalizáciou.
3) Elektronické systémy, na ktorých sa spracúvajú osobné údaje sú vybavené zariadením nepretržitého napájania.

9.4 PROGRAMOVÉ OPATRENIA

Programové opatrenia umožňujú chrániť informácie priamo v počítači pomocou bezpečnostných prostriedkov. Tieto sa rozdeľujú do troch skupín:

- kontrola prístupu (napr. heslo do aplikácie, heslo pre prístup do siete)
- monitorovanie činnosti
- hlásenie o narušení

Záväzné opatrenia (programové)

1) Prístup do informačného systému automatizovaného spracovania údajov je chránený prostredníctvom hesla.
2) Prístup do aplikácie musí byť chránený prostredníctvom hesla.
3) Heslo musí byť reťazec alfanumerických znakov min. dĺžky 6 znakov, z ktorých minimálne dva znaky musia byť zo skupiny tzv. ostatných znakov 0123456789. Zakazuje sa požívať meno, priezvisko. Je zakázané zapisovať si heslo na prístupné miesto, heslo je vhodné uložiť v zalepenej obálke do trezora.

Doplnkové opatrenia (programové)

1) Technické zariadenie musí byť schopné odoprieť opakované použitie prístupového hesla.

9.5 REŽIMOVÉ OPATRENIA

Režimové opatrenia sú realizované formou interných predpisov.

Zahrňujú hlavne tieto oblasti:

a) zásady a pravidlá pre prácu s výpočtovou technikou v rámci organizácie,
b) pravidlá pre prácu s heslami a šifrovacími kľúčmi, vytvorenie režimových pracovísk,
c) definovanie bezpečnostných zón,
d) pravidlá riadenia vstupu do nich, postup pri hlásení podozrivých udalostí a pod.

Doplnkové opatrenia (režimové)

1) O likvidácii sa vypracuje zápis. V zápise musia byť zlikvidované údaje vymenované a musí byť uvedený fyzický spôsob likvidácie v súlade so zákonom č. 18/2018 Z.z. o ochrane osobných údajov

2) Priestory budovy sú chránené alarmom, ktorý je napojený na externú firmu, ktorá vykonáva ochranu celého
3) Prístup osôb do priestorov - budovy, v ktorých sa spracúvajú osobné údaje, je chránený elektronickým prístupovým systémom ovládaným číselným kódom alebo identifikačným predmetom.

9.6 PERSONÁLNE OPATRENIA

Riadia výber. Prvotnú prípravu a zdokonaľovacie tréningy personálu zainteresovaného do procesu spracúvania ochrany osobných údajov.

Záväzné opatrenia (personálne)

1) Spoločnosť musí mať vypracované pravidlá pre sankcie v prípade porušenia pravidiel ochrany osobných údajov. Pravidlá musia byť verejné.
2) Každý pracovník, ktorý bude vykonávať spracúvanie osobných údajov, musí byť preukázateľne poučený v zmysle zákona.

10. NEPOKRYTÉ RIZIKÁ

1) Voči hrozbe víchrice, zemetrasenia a terorizmu nie sú priamo vykonané žiadne bezpečnostné opatrenia. Tieto hrozby sú veľmi málo pravdepodobné.

10.1 VÍCHRICA

1) Môže spôsobiť výpadok elektrickej energie a tým dočasnú nedostupnosť osobných údajov, prípadne poškodiť okná a následne technické zariadenie.
Možné bezpečnostné opatrenia: náhradný zdroj elektrickej energie – generátor

10.2 ZEMETRASENIE

1) Môže spôsobiť nedostupnosť prípadne zničenie osobných údajov.
Možné bezpečnostné opatrenia: archivácia záloh
V našej zemepisnej oblasti, kde je lokalizovaná organizácia, je nízke riziko zemetrasenia.

10.3 TERORIZMUS

1) 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.

V našej zemepisnej oblasti je pravdepodobnosť hrozieb spojených s terorizmom nízka, rovnako miera ohrozenia osobných údajov týmto spôsobom.