
***Základné údaje o firme:***

- **PREVÁDZKOVATEĽ:** Andrea Neherová, Obrancov mieru 704/10, 96263 Pliešovce
- **IČO**: 52668142
- **ŠTATUTÁRNY ZÁSTUPCA:**
  - Andrea Neherová - Živnostník
- **ZA OCHRANU OS. ÚDAJOV ZODPOVEDÁ:**
  - Andrea Neherová - Živnostník

***IT smernica platí pre informačné systémy:***

- **IS01: Účtovné doklady**
- **IS02: Evidencia klientov na účely fakturácie**
- **IS03: Evidencia dodávateľov a odberateľov pri poskytovaní služieb a tovaru**
- **IS04: Evidencia prichádzajúcej a odosielanej pošty (papierová podoba-e-mail)**
- **IS05: Evidencia zmlúv**
- **IS06: Marketing**
- **IS07: Fotografie a videá**
- **IS08: IT podpora pre klientov**

**Spracúvané osobné údaje:**

- meno, priezvisko, bydlisko zamestnancov / dotknutých osôb
- rodné číslo zamestnancov / dotknutých osôb
- telefónne číslo zamestnancov / dotknutých osôb
- meno, priezvisko, bydlisko rodinných príslušníkov zamestnancov
- rodné číslo rodinných príslušníkov zamestnancov
- ďalšie osobné údaje sú uvedené v Záznamoch o spracovateľských činnostiach v IS

Osobnyudaj.sk
PORADENSTVO A SLUŽBY V OBLASTI OCHRANY OSOBNÝCH ÚDAJOV

***Vypracoval:*** osobnyudaj.sk, s.r.o., DUETT Business Residence, Námestie osloboditeľov 3/A, 040 01, IČO: 50528041
www.osobnyudaj.sk

**OBSAH IT SMERNICE**

## 1. Politika používania IT

### 1.1 Správca siete IT

- Inštaluje systémové programy (predovšetkým operačné systémy).
- Manipuluje s diskovými médiami a tlačiarňami.
- Je zodpovedný za plnú prevádzkyschopnosť systémových prostriedkov a nástrojov.
- Na základe povolení zriaďuje nové používateľské kontá, prideľuje pre ne základné prístupové práva, preveruje oprávnenosť prístupových práv a používateľských kont a na základe povolenia ruší používateľské kontá.
- Zodpovedá za zálohovanie a archiváciu systémových a používateľských dát, za archív a vedenie evidencie záložných médií a ich bezpečné uloženie.
- Pravidelne kontroluje stav technických súčastí informačného systému.
- Raz týždenne nastavuje a kontroluje stav serverov.
- Podľa požiadaviek bezpečnostnej politiky nastavuje prístupové práva na aktívnych sieťových prvkoch a komunikačných zariadeniach.
- Pravidelne monitoruje stav siete pomocou programových nástrojov pre riadenie siete.
- Udržuje v aktuálnom stave informácie o topológii siete, aktívnych a pasívnych prvkoch, o ich parametroch a nastaveniach.
- Zriaďuje, eviduje a ruší kontá používateľov a skupín, pravidelne preveruje oprávnenosť používateľských kont, prípadne prístupových práv.
- Vykonáva pravidelný audit databáz a pravidelne ich vyhodnocuje a zálohuje.
- Uskutočňuje pravidelnú údržbu databáz, monitorovanie ich priestorových nárokov, optimálne nastavovanie parametrov databáz v závislosti od stavu operačného systému a od aktuálnej situácie v databázach.
- Rieši havarijné stavy podľa havarijného poriadku, obnovuje dáta, funkčnosť databáz a konzultuje neštandardné stavy s dodávateľskými firmami.
- Testuje a nasadzuje nové databázové softvéry, prípadne ich update a upgrade.
- Zálohuje databázy a kontroluje pravidelnosť a spoľahlivosť prevádzky z hľadiska obnovy databáz po poškodení dát a obnovy databáz k dátumu.
- Archivuje systémové a používateľské dáta databáz a vedie evidenciu záložných médií a archívu.
- Kontroluje v logovacích súboroch oprávnenosť vstupu do databázy (ochrana pred neoprávneným vstupom), zisťuje či bola prekonaná bezpečnostná brána a v prípade, že bola prekonaná bezpečnostná brána, preveruje postup jej prekonania.
- Spolupracuje s ostatnými oddeleniami pri testovaní, výberovom konaní pre nový softvér.
- Tvorí a spolupodieľa sa na tvorbe návrhov smerníc, upresnení a školení súvisiacich s bezpečnosťou informačných systémov.
- Nastavuje bezpečnostné charakteristiky pre jednotlivé komponenty informačného systému vrátane komunikačných prvkov.
- Vyhodnocuje a spravuje kontrolné záznamy.
- Vykonáva bezpečnostné školenia používateľov.
- Kontroluje fyzickú bezpečnosť počítačového vybavenia a hlavnej miestnosti (serverovne), archívnych médií a výstupných zariadení (tlačiarne, zapisovače, atď.).
- Kontroluje prístup k zariadeniam systému.
- Kontroluje bezpečné uloženia záložných médií a archívov.

- Povoľuje zavedenie nových používateľov.
- Kontroluje a spravuje systém prihlasovania užívateľov a stanovuje maximálnu dobu životnosti hesiel podľa bezpečnostnej politiky.
- Riadi a zabezpečuje päťročnú archiváciu súborov týkajúcich sa bezpečnostných záznamov operačného systému a dôležitých aplikácií.
- Analyzuje prieniky do informačných systémov, vytvára, optimalizuje a spravuje bezpečnostnú politiku .
- Odstraňuje technické poruchy a závady na zariadeniach IT a to buď svojpomocne (napr. výmenou súčiastky, časti dielu alebo celého dielu za nový v rámci záručných podmienok), alebo formou doručenia chybného zariadenia do príslušného servisného strediska alebo dohovoru o oprave cez dodávateľa daného zariadenia.
- Realizuje technické prepojenia lokálnych počítačových sietí na súčastiach a pracoviskách
- Pripája zariadenia IT do elektrickej siete napájania a do počítačovej siete.
- Prepája jednotlivé zariadenia IT medzi sebou.
- Vykonáva previerku zariadení IT, ktoré podliehajú pravidelnému technickému auditu.

### 1.2 Používateľ IT

- Používa PC, operačný systém na ňom nainštalovaný, ako aj všetky aplikácie, na ktoré dostal oprávnenie.
- Prihlasuje sa do počítačovej siete a používa zdieľané súbory, databázy, aplikácie, tlačiarne, či iné zariadenia podľa práv, ktoré mu boli pridelené jeho priamym nadriadeným.
- Je preukázateľne poučený o povinnosti dodržiavať túto smernicu a riadiť sa ňou pri svojej práci.
- Riadi sa pokynmi zamestnancov útvaru IT a obracia sa na nich v prípade závad, porúch a mimoriadnych situácií.
- Dbá na ochranu spracovávaných dát.
- PC a ostatné zariadenia IT používa výhradne na služobné účely vyplývajúce z jeho opisu pracovnej činnosti. Na iné účely použitia zariadení IT potrebuje písomný súhlas priameho nadriadeného.
- Používatelia sú povinný chrániť prístupové heslá k informačnému systému (IS), operačnému systému (OS), pošte, vzdialenému prístupu a iným heslom chráneným prístupom.
- IT zariadenia sú k perifériám zverené bez obmedzovania prístupu a bez obmedzenia internetu, pričom sa predpokladá, že používateľ si je po zaškolení vedomý rizík vyplývajúcich z používania tohto zariadenia.
- IT technika obsahuje antivírový softvér (SW), ktorý sa sám aktualizuje a aktualizácie OS sa preberajú a inštalujú automaticky
- V prípadne upozornia používateľa na spustenie aktualizácie OS, je nutné túto aktualizáciu v čo najbližšom možnom čase vykonať.
- Zálohovanie zariadení na PC sa spúšťa automaticky, v prípade notebookov je nutné odovzdať zariadenie IT technikovi, ktorý ho odzálohuje.

### 1.3 Používateľ Internetu

Používateľom internetu je zamestnanec prevádzkovateľa, ktorému bolo pridelené používateľské konto a na základe toho umožnený prístup do celosvetovej počítačovej siete Internet (www).

### 1.4 Používateľ Intranetu

Používateľom intranetu je zamestnanec prevádzkovateľa, ktorému bolo pridelené používateľské konto a na základe toho umožnený prístup do Intranetu počítačovej siete (tzv. vnútro-podnikovej siete).

### 1.5 Používateľ elektronickej pošty

Používateľom elektronickej pošty je zamestnanec prevádzkovateľa, ktorému bolo pridelené používateľské konto a na základe toho umožnené používanie elektronickej pošty (e-mailu).

### 1.6 Zamestnanec

Pre účely tejto smernice sa za zamestnanca považujú všetci kmeňoví zamestnanci prevádzkovateľa, ale aj externí zamestnanci, ktorí majú s prevádzkovateľom pracovno-právny vzťah, prípadne iný zmluvný vzťah.

## 2. Používanie hardvéru

- Na pracoviskách prevádzkovateľa sa používa iba taký hardvér, ktorý je schválený príslušnými vedúcimi zamestnancami a je evidovaný v evidencii majetku na oddelení správy majetku ekonomického odboru.
- Akýkoľvek iný hardvér sa zakazuje používať.
- Zakazuje sa akýkoľvek zásah do hardvéru alebo jeho konfigurácie a jeho svojvoľné premiestňovanie či výmena. Touto činnosťou je poverený technik príslušného útvaru IT, ktorý túto činnosť vykoná.
- Používatelia IT, ktorým boli zverené alebo zapožičané prenosné notebooky, telefóny, prípadne akékoľvek iné zariadenia IT, sú povinní s nimi nakladať tak, aby nedošlo k ich strate, zneužitiu či krádeži, nesmú ich požičať, prenechať, odovzdať tretej osobe, či u tretej osoby takéto zariadenie založiť formou záložného práva.
- Poruchu hardvéru treba nahlásiť útvaru IT. Pracovník oddelenia IT sa okamžite, prípadne podľa dohody postará o nápravu, opravu alebo výmenu poruchového hardvéru.

## 3. Používanie softvéru

- Pri práci s PC je zakázané pracovať s iným softvérom, než aký bol nainštalovaný, resp. schválený (unifikovaný).
- Používateľ IT používa len taký softvér, na ktorého používanie má podľa schválenia nárok.

- Pri akejkoľvek zmene týkajúcej sa používateľa IT, ktorá má vplyv na používanie softvéru, je Používateľ IT povinný požiadať príslušného nadriadeného o vykonanie takejto zmeny.
- Po zakúpení softvéru tento nový softvér inštaluje zamestnanec útvaru IT, alebo zamestnanci dodávateľskej firmy za prítomnosti zamestnanca útvaru IT.
- Poruchu softvéru treba nahlásiť útvaru IT.
- Pracovník IT sa okamžite, prípadne podľa dohody postará o nápravu poruchy softvéru.
- Zakazuje sa používať, uchovávať alebo distribuovať akýkoľvek pirátsky softvér a údaje na hardvérovom vybavení.

## 4. Používanie služieb Internetu, intranetu a elektronickej pošty

- Prevádzkovateľ používa alebo môže používať softvér a systémy, ktoré umožňujú monitorovať a zaznamenávať všetky použitia celosvetovej počítačovej siete Internet a elektronickej pošty. Systémy môžu zaznamenávať prístup na webové stránky, diskusné skupiny, použitie elektronickej pošty, prenos súborov medzi prevádzkovateľom a inými subjektami.
- Používateľ Internetu a elektronickej pošty musí vedieť, že prevádzkovateľ má právo v súlade s platnou legislatívou preverovať použitie týchto prístupov.
- Prevádzkovateľ má právo nariadiť kontrolu všetkých dát a akýchkoľvek súborov, ktoré sú uložené na lokálnych diskoch PC používateľov IT, alebo v ich domovských adresároch na serveroch prevádzkovateľa.
- Zakazuje sa zobrazovanie, archivovanie, uchovávanie, rozširovanie, spracovávanie alebo zaznamenávanie akéhokoľvek obrázku, či dokumentu s jednoznačným sexuálnym obsahom.
- Prístup na Internet a elektronickú poštu sa nesmú vedome použiť na porušenie všeobecne záväzných právnych predpisov Slovenskej republiky alebo medzinárodných zmlúv, ktorými je Slovenská republika viazaná.
- Akýkoľvek softvér alebo súbor získaný prostredníctvom Internetu a uložený na lokálnej siete prevádzkovateľa, alebo na lokálnom disku používateľa IT, sa stáva majetkom prevádzkovateľa. Všetky takéto súbory, dokumenty alebo softvér, sa môžu používať výhradne spôsobom, ktorý je v súlade s udelenými licenciami, autorskými právami, resp. ich odsúhlasil útvar IT a musia priamo súvisieť s pracovnými povinnosťami používateľa IT.
- Zakazuje sa získavanie a následné ukladanie zábavného softvéru alebo hier, videí, obrázkov a zvukových súborov z Internetu alebo prostredníctvom elektronickej pošty, hranie hier na Internete. Takisto sa zakazuje rozširovanie akéhokoľvek softvéru či údajov, ktoré sú majetkom prevádzkovateľa bez jeho predchádzajúceho písomného súhlasu.
- Používateľom Internetu a elektronickej pošty sa zakazuje využívať svetovú počítačovú sieť Internet a elektronickú poštu na zámerné rozširovanie akýchkoľvek vírusov, červíkov, trójskych koňov alebo iného škodlivého softvéru. Takisto používateľ nesmie využiť či zneužiť prístup na Internet či elektronickú poštu na vyradenie, preťaženie alebo oklamanie akéhokoľvek počítačového systému alebo počítačovej siete a tým narušiť súkromie alebo bezpečnosť iného používateľa či spoločnosti.
- Vyjadrovať sa v mene prevádzkovateľa, alebo jeho súčastí do akýchkoľvek diskusných skupín môžu len zamestnanci, ktorí sú riadne poverení komunikáciou s médiami.

Ostatní používatelia Internetu a elektronickej pošty sa môžu zúčastňovať na diskusiách a fórach v priebehu pracovnej doby, ak sa to vzťahuje na ich odbornú činnosť, ale v tom prípade vystupujú ako jednotlivci vo vlastnom mene a sú povinní informovať ostatných zúčastnených, že nie sú oprávnení vystupovať v mene prevádzkovateľa, alebo jeho súčastí. Pri účasti v týchto diskusiách a fórach je používateľ Internetu a elektronickej pošty povinný zdržať sa akýchkoľvek politických, náboženských, rasových prejavov, prejavov neznášanlivosti a prejavov urážajúcich ľudskú dôstojnosť, či prejavov týkajúcich sa trestnej činnosti. Používateľ Internetu a elektronickej pošty nesmie zverejňovať údaje a dôverné informácie o prevádzkovateľovi.

- Používatelia Internetu a elektronickej pošty môžu počas obedovej alebo inej prestávky, alebo po pracovnej dobe využívať prístup na Internet a elektronickú poštu pre prieskum alebo prezeranie informačných zdrojov nesúvisiacich s náplňou práce len za predpokladu, že budú dodržané všetky ustanovenia tejto smernice.
- Prevádzkovateľ je v zmysle príslušných zákonných ustanovení povinný poskytnúť orgánom činným v trestnom konaní všetky dostupné záznamy týkajúce sa prístupu na Internet a elektronickú poštu príslušného používateľa Internetu a elektronickej pošty.
- Používateľ Internetu a elektronickej pošty sa musí riadiť všeobecne záväznými právnymi predpismi, autorským právom, či obchodnými značkami.
- Komerčné používanie Internetu na podporu vedľajšej podnikateľskej činnosti prevádzkovateľa alebo jeho súčastí mimo jeho pracovnej náplne nie je možné.

## 5. Všeobecné pravidlá bezpečnosti IT

- Používateľ IT je oprávnený pracovať s počítačom, softvérom a údajmi potrebnými pre výkon jeho činnosti iba v súlade s pridelenými právami a oprávneniami iba.
- Je zakázané poskytovať tretím osobám špecifické informácie o používateľoch IS , ktoré by mohli byť zneužité pre neoprávnený prístup k údajom a programom, najmä identifikácie a autentifikácie, rozsah oprávnení a práv a heslá používateľov IT.
- Každý používateľ IT má pridelené svoje prihlasovacie meno a heslo, ktoré musí zachovať v tajnosti. Tieto mená a heslá pomáhajú stanoviť osobnú zodpovednosť. Zakazuje sa spoločné používanie prihlasovacích mien a hesiel viacerými používateľmi IT. V prípade nebezpečia prezradenia je potrebné tieto heslá okamžite zmeniť.
- Používateľ IT je plne zodpovedný za svoje heslo, nesmie byť ľahko uhádnuteľné, alebo odvoditeľné. V prípade zabudnutia hesla používateľom IT, si používateľ IT v súčinnosti so zamestnancom útvaru IT nastaví nové heslo.
- V záujme zaistenia bezpečnosti svojich počítačov, počítačových sietí a softvérového vybavenia majú zamestnanci nainštalované rôzne programy (napr. firewall, proxy server, antivírusové prostriedky), monitorovacie systémy pre Internet a elektronickú poštu a bezpečnostné systémy. Zamestnancom sa zakazuje vyraďovať z činnosti, narúšať, prekonávať alebo obchádzať ktorékoľvek bezpečnostné zariadenie alebo systém.
- Súbory, ktoré obsahujú citlivé (dôverné) údaje, musia byť pri akomkoľvek prenose prostredníctvom Internetu zašifrované. V tomto smere bude používateľovi IT nápomocný útvar IT. O takomto prenose musí byť vopred informovaný bezpečnostný manažér IT.
- Pri opustení pracoviska je potrebné vylúčiť akúkoľvek možnosť neoprávneného prístupu tretích osôb k dátam a manipuláciu s nimi. V prípade, že používateľ IT, či

zamestnanec útvaru IT zistí pokus o narušenie bezpečnosti IT týkajúce sa ochrany dát, je povinný takémuto pokusu podľa svojich schopností a možností zabrániť a okamžite o tom informovať svojho nadriadeného.

- V prípade prítomnosti zástupcu servisnej alebo dodávateľskej firmy je zodpovedný vedúci zamestnanec povinný určiť zamestnanca, ktorý bude zodpovedný za dohľad nad dodržiavaním ustanovení tejto smernice zo strany zástupcu alebo zástupcov servisných alebo dodávateľských firiem.
- V prípade poruchy zariadenia IT, ktoré by mohlo obsahovať dáta, musí technik IT pred odovzdaním tohto zariadenia do opravy odstrániť všetky možné médiá, na ktorých by sa dáta mohli nachádzať (pevné disky, CD, DVD média a pod.).
- Ak je poškodený pevný disk, technik IT je povinný dať zástupcovi servisnej firmy podpísať čestné prehlásenie o mlčanlivosti, ktoré bude súčasťou zmluvy, prípadne objednávky.
- Bez predchádzajúceho písomného súhlasu bezpečnostného manažéra IT je zakázané poskytovať v akejkoľvek forme akékoľvek údaje, dáta, databázy či prehľady o informačných systémoch iným osobám, organizáciám.
- Zamestnanec IT zabezpečí inštaláciu, prevádzku a priebežnú aktualizáciu antivírusového systému pre všetky PC, ktoré používajú zamestnanci prevádzkovateľa.
- Každý bezpečnostný incident, ktorý sa vyskytne na hardvéri, softvéri alebo zariadeniach počítačovej siete, musí byť okamžite ohlásený podľa jeho povahy buď správcovi siete, správcovi aplikácie, databázovému administrátorovi, systémovému administrátorovi, alebo bezpečnostnému manažérovi IT. Dokumentáciu o všetkých bezpečnostných incidentoch, ktoré sa vyskytli, vedie bezpečnostný manažér IT v denníku incidentov.

## 6. Zálohovanie údajov serverov informačného systému

Z pohľadu charakteru záloh sa zálohy delia na Operatívne a Bezpečnostné.

### 6.1 Operatívna záloha

- Zálohovanie databáz databázového servera SQL .
- Denne je automaticky vykonávaný logický backup databázy pomocou exportnej utility databázového servera **SQL**, ktorá vykonáva logickú zálohu databázy. Zálohovací skript, ktorý túto utilitu využíva, sa nazýva OS.
- Exportovaná je celá databáza. Denne sú kontrolované log súbory z exportu databázy pre prípad výskytu chýb pri exporte. Výsledný súbor takto vytvorenej zálohy databázy, ktorý vo svojom názve obsahuje názov databázy a dátum vykonania jej zálohy, je umiestnený na diskovom zariadení. Druhá kópia je pre prípad požiaru alebo iného nebezpečenstva umiestnená mimo objektu serverovne.
- Dodatočne sa vykonáva záloha databázy pomocou fyzickej zálohy databázových súborov, ktorú smie vykonať ktorýkoľvek zamestnanec bez obmedzenia práv.

### 6.2 Bezpečnostná záloha

- Zálohovanie súborov OS aj s dátami.
- Raz denne sa vykonáva záloha operačného systému a súborov databázového servera pomocou na to zakúpeného softvéru.
- Výsledný súbor takto vytvorenej zálohy databázy, ktorý vo svojom názve obsahuje názov databázy a dátum vykonania jej zálohy, je umiestnený na serveri. Druhá kópia je pre prípad požiaru alebo iného nebezpečenstva umiestnená mimo objektu serverovne.

## 7. Práca s citlivými dátami firmy

Všetci zamestnanci sú povinní manipulovať s dátami a dátovými nosičmi obsahujúcimi citlivé informácie o firme, firemných aktivitách, odberateľoch, dodávateľoch a pod. tak, aby sa nedostali do rúk nepovolaných osôb.

Táto časť smernice tvorí neoddeliteľnú súčasť bezpečnostnej dokumentácie.

Bezpečnostná dokumentácia je evidovaná pod číslom osvedčenia: . Validitu dokumentu možno overiť na **www.osobnyudaj.sk.** Kopírovanie týchto dokumentov sa považuje za porušenie autorských práv vypracovateľa.

# Oboznámenie s „IT smernicou“
# Prezenčná listina

| **Meno a Priezvisko zamestnanca** | Dátum | Podpis |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

**Hore uvedené osoby svojim podpisom prehlasujú, že Zamestnávateľ - Andrea Neherová, so sídlom Obrancov mieru 704/10, 96263 Pliešovce, IČO: 52668142 ich oboznámil s „IT smernicou“, tejto porozumeli a budú ju pri výkone svojej činnosti rešpektovať.**