Technické a organizačné opatrenia k informačným systémom

Prevádzkovateľ:

Obchodné meno: **Marián Žuffa - MyŽu**
Miesto podnikania: 10. apríla 683/11, 91101 Trenčín
IČO: 53774680
Právna forma: živnosť
Číslo živnostenského registra: 350-46150
Registrový úrad: Okresný úrad Trenčín

Účinnosť od:		
Schválil:	**Marián Žuffa**	..... podpis

Obsah

Preambula....3
Skratky, pojmy a ich výklad 6
Bezpečnostné opatrenia č.1.....8
Bezpečnostné opatrenia č. 2....11
Bezpečnostné opatrenia č.3.....12
Bezpečnostné opatrenia č. 4....13
Bezpečnostné opatrenia č.5....14
Bezpečnostné opatrenia č.6....15
Bezpečnostné opatrenia č.7.... 16
Bezpečnostné opatrenia č. 8.... 21
Bezpečnostné opatrenia č.9....23
Bezpečnostné opatrenia č.10....23

Preambula

Prevádzkovateľ, na základe náležitého posúdenia spracúvania osobných údajov dotknutých osôb v zmysle 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, ktorým sa zrušuje smernica 95/46/ES (ďalej tiež ako „Nariadenie GDPR“) a v zmysle zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej tiež ako „zákon o OOÚ“) prijal so zreteľom na najnovšie poznatky, na náklady na vykonanie opatrení, na povahu, rozsah, kontext a účel spracúvania osobných údajov a na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva fyzických osôb primerané technické a organizačné opatrenia na zaistenie úrovne bezpečnosti primeranej tomuto riziku.

Tieto primerané technické a organizačné opatrenia zahŕňajú zabezpečenie trvalej dôvernosti, integrity, dostupnosti a odolnosti systémov spracúvania osobných údajov; proces obnovy dostupnosti osobných údajov a prístup k nim v prípade fyzického incidentu alebo technického incidentu; proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania osobných údajov.

Prevádzkovateľ zabezpečil, aby osoby poverené prevádzkovateľom, ktoré majú prístup k osobným údajom, spracúvali tieto údaje len na základe pokynov prevádzkovateľa, týchto technických a organizačných opatrení alebo podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná.

Zoznam informačných systémov

Prevádzkovateľ zatriedil spracúvané osobné údaje do nasledovných informačných systémov:

a)

názov informačného systému	**skratka používaná pre účely tohto posúdenia**
Informačný systém Účtovné doklady	IS ÚD

b)

názov informačného systému	**skratka používaná pre účely tohto posúdenia**
Informačný systém Zákazníci	IS Zákazníci

c)

názov informačného systému	**skratka používaná pre účely tohto posúdenia**
Informačný systém Marketing	IS Marketing

Zoznam osobných údajov

Prevádzkovateľ spracúva nasledovné osobné údaje:

a) v IS ÚD:

- meno, priezvisko
- adresa
- emailová adresa,
- ďalšie osobné údaje vyžadované osobitnými zákonmi na plnenie povinností zo zmluvy so zákazníkmi.

b) v IS Zákazníci:

- meno, priezvisko
- adresa
- telefón,
- emailová adresa,
- ďalšie osobné údaje vyžadované osobitnými zákonmi na plnenie povinností zo zmluvy so zákazníkmi.

c) v IS Marketing:

- meno, priezvisko
- emailová adresa

Skratky, pojmy a ich výklad

PC	Pracovná stanica
LAN	Local Area Network (vnútorná sieť výpočtovej techniky)
Prevádzkovateľ	**Marián Žuffa - MyŽu, 10. apríla 683/11, 91101 Trenčín, IČO:53774680**
IS	Informačným systémom 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 základe alebo geografickom základe.
Nariadenie GDPR	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
Zákon č. 18/2018 Z. z.	Zákon o OOÚ
Osobné údaje	Osobnými údajmi sú údaje týkajúce sa identifikovanej fyzickej osoby alebo identifikovateľnej 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.
Spracúvanie osobných údajov	Spracúvaním osobných údajov je 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.
Zodpovedná osoba	Zodpovednou osobou je osoba určená prevádzkovateľom alebo sprostredkovateľom, ktorá plní úlohy podľa zákona č. 18/2018 Z.z.
Súhlas dotknutej osoby	Súhlasom dotknutej osoby je akýkoľvek vážny a slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby vo forme vyhlásenia alebo jednoznačného potvrdzujúceho úkonu, ktorým dotknutá osoba vyjadruje súhlas so spracúvaním svojich osobných údajov.
Profilovanie	Profilovaním je akákoľvek forma automatizovaného spracúvania osobných údajov spočívajúceho v použití osobných údajov na vyhodnotenie určitých osobných znakov alebo charakteristík týkajúcich sa fyzickej osoby, najmä na analýzu alebo predvídanie znakov alebo charakteristík dotknutej osoby

	súvisiacich s jej výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom.
Pseudonimizácia	Pseudonymizáciou je spracúvanie osobných údajov spôsobom, že ich nie je možné priradiť ku konkrétnej dotknutej osobe bez použitia dodatočných informácií, ak sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia na zabezpečenie toho, aby osobné údaje nebolo možné priradiť identifikovanej fyzickej osobe alebo identifikovateľnej fyzickej osobe.
Šifrovanie	Šifrovaním je transformácia osobných údajov spôsobom, ktorým opätovné spracúvanie je možné len po zadaní zvoleného parametra, ako je kľúč alebo heslo.
Porušenie ochrany OÚ	Porušením ochrany osobných údajov je porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene alebo k neoprávnenému poskytnutiu prenášaných, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov, alebo k neoprávnenému prístupu k nim.
Dotknutá osoba	Dotknutou osobou je každá fyzická osoba, ktorej osobné údaje sa spracúvajú.
Prevádzkovateľ	Prevádzkovateľom 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.
Sprostredkovateľ	Sprostredkovateľom je každý, kto spracúva osobné údaje v mene prevádzkovateľa.
Príjemca	Príjemcom je každý, komu sa osobné údaje poskytnú 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.
Tretia strana	Treťou stranou je každý, kto nie je dotknutou osobou, prevádzkovateľ, sprostredkovateľ alebo inou fyzickou osobou, ktorá na základe poverenia prevádzkovateľa alebo sprostredkovateľa spracúva osobné údaje.

Bezpečnostné opatrenia IS ÚD, IS Zákazníci, IS Marketing č. 1

Povinnosti prevádzkovateľa pri uplatňovaní práv dotknutej osoby

§ 1
Práva dotknutej osoby

1. Podľa § 21 až § 28 zákona o OOÚ medzi základné práva dotknutej osoby patrí:

I. Právo na prístup k osobným údajom

Dotknutá osoba má právo získať od prevádzkovateľa potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú. Ak prevádzkovateľ takéto osobné údaje spracúva, dotknutá osoba má právo získať prístup k týmto osobným údajom a informácie o

a) účele spracúvania osobných údajov,
b) kategórii spracúvaných osobných údajov,
c) identifikácii príjemcu alebo o kategórii príjemcu, ktorému boli alebo majú byť osobné údaje poskytnuté, najmä o príjemcovi v tretej krajine alebo o medzinárodnej organizácii, ak je to možné,
d) dobe uchovávania osobných údajov; ak to nie je možné, informáciu o kritériách jej určenia,
e) práve požadovať od prevádzkovateľa opravu osobných údajov týkajúcich sa dotknutej osoby, ich vymazanie alebo obmedzenie ich spracúvania, alebo o práve namietať spracúvanie osobných údajov,
f) práve podať návrh na začatie konania podľa § 100 zákona o OOÚ,
g) zdroji osobných údajov, ak sa osobné údaje nezískali od dotknutej osoby,
h) existencii automatizovaného individuálneho rozhodovania vrátane profilovania podľa § 28 ods. 1 a 4 zákona o OOÚ; v týchto prípadoch poskytne prevádzkovateľ dotknutej informácie najmä o použitom postupe, ako aj o význame a predpokladaných dôsledkoch takéhoto spracúvania osobných údajov pre dotknutú osobu.

II. Právo na opravu osobných údajov

Dotknutá osoba má právo na to, aby prevádzkovateľ bez zbytočného odkladu opravil nesprávne osobné údaje, ktoré sa jej týkajú. So zreteľom na účel spracúvania osobných údajov má dotknutá osoba právo na doplnenie neúplných osobných údajov.

III. Právo na výmaz osobných údajov

Dotknutá osoba má právo na to, aby prevádzkovateľ bez zbytočného odkladu vymazal osobné údaje, ktoré sa jej týkajú.

IV. Právo na obmedzenie spracúvania osobných údajov

Dotknutá osoba má právo na to, aby prevádzkovateľ obmedzil spracúvanie osobných údajov, ak

a) dotknutá osoba namieta správnosť osobných údajov, a to počas obdobia umožňujúceho prevádzkovateľovi overiť správnosť osobných údajov,

b) spracúvanie osobných údajov je nezákonné a dotknutá osoba namieta vymazanie osobných údajov a žiada namiesto toho obmedzenie ich použitia,
c) prevádzkovateľ už nepotrebuje osobné údaje na účel spracúvania osobných údajov, ale potrebuje ich dotknutá osoba na uplatnenie právneho nároku, alebo
d) dotknutá osoba namieta spracúvanie osobných údajov podľa § 27 ods. 1 zákona o OOÚ, a to až do overenia, či oprávnené dôvody na strane prevádzkovateľa prevažujú nad oprávnenými dôvodmi dotknutej osoby.

V. Právo na prenosnosť osobných údajov

Dotknutá osoba má právo získať osobné údaje, ktoré sa jej týkajú a ktoré poskytla prevádzkovateľovi, v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte a má právo preniesť tieto osobné údaje ďalšiemu prevádzkovateľovi, ak je to technicky možné a ak
a) sa osobné údaje spracúvajú podľa § 13 ods. 1 písm. a), § 16 ods. 2 písm. a) alebo § 13 ods. 1 písm. b) zákona o OOÚ a
b) spracúvanie osobných údajov sa vykonáva automatizovanými prostriedkami.

VI. Právo namietať spracúvanie osobných údajov

Dotknutá osoba má právo namietať spracúvanie jej osobných údajov z dôvodu týkajúceho sa jej konkrétnej situácie vykonávané podľa § 13 ods. 1 písm. e) alebo písm. f) zákona o OOÚ vrátane profilovania založeného na týchto ustanoveniach. Prevádzkovateľ nesmie ďalej spracúvať osobné údaje, ak nepreukáže nevyhnutné oprávnené záujmy na spracúvanie osobných údajov, ktoré prevažujú nad právami alebo záujmami dotknutej osoby, alebo dôvody na uplatnenie právneho nároku.

VII. Automatizované individuálne rozhodovanie vrátane profilovania

Dotknutá osoba má právo na to, aby sa na ňu nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní osobných údajov vrátane profilovania a ktoré má právne účinky, ktoré sa jej týkajú alebo ju obdobne významne ovplyvňujú.

§ 2
Oznamovacia povinnosť prevádzkovateľa v súvislosti s opravou, vymazaním alebo obmedzením spracúvania osobných údajov

1. Prevádzkovateľ oznámi príjemcovi opravu osobných údajov, vymazanie osobných údajov alebo obmedzenie spracúvania osobných údajov uskutočnené podľa § 22, § 23 ods. 1 alebo § 24 zákona o OOÚ, ak sa to neukáže ako nemožné alebo si to nevyžaduje neprimerané úsilie. Prevádzkovateľ o príjemcoch podľa predchádzajúcej vety informuje dotknutú osobu, ak to dotknutá osoba požaduje.

§ 3
Povinnosti prevádzkovateľa pri uplatňovaní práv dotknutej osoby

1. Prevádzkovateľ prijal vhodné opatrenia a zaviazal sa poskytnúť dotknutej osobe informácie podľa § 19 a 20 a oznámenia podľa § 21 až 28 a 41 zákona o OOÚ, ktoré sa týkajú spracúvania jej osobných údajov, v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme, formulované jasne, a to najmä pri informáciách určených osobitne dieťaťu. Prevádzkovateľ poskytne informácie v listinnej podobe alebo elektronickej podobe, spravidla v rovnakej podobe, v akej bola podaná žiadosť. Ak o

to požiada dotknutá osoba, informácie môže prevádzkovateľ poskytnúť aj ústne, ak dotknutá osoba preukáže svoju totožnosť iným spôsobom.

2. Prevádzkovateľ poskytne súčinnosť dotknutej osobe pri uplatňovaní jej práv podľa § 21 až 28 zákona o OOÚ. V prípadoch uvedených v § 18 ods. 2 zákona o OOÚ nemôže prevádzkovateľ odmietnuť konať na základe žiadosti dotknutej osoby pri výkone jej práv podľa § 21 až 28, ak nepreukáže, že dotknutú osobu nie je schopný identifikovať.

3. Prevádzkovateľ poskytne dotknutej osobe informácie o opatreniach, ktoré sa prijali na základe jej žiadosti podľa § 21 až 28 zákona o OOÚ, do jedného mesiaca od doručenia žiadosti. Uvedenú lehotu môže prevádzkovateľ v odôvodnených prípadoch s ohľadom na komplexnosť a počet žiadostí predĺžiť o ďalšie dva mesiace, a to aj opakovane. Prevádzkovateľ je povinný informovať o každom takomto predĺžení dotknutú osobu do jedného mesiaca od doručenia žiadosti spolu s dôvodmi predĺženia lehoty. Ak dotknutá osoba podala žiadosť v elektronickej podobe, prevádzkovateľ poskytne informácie v elektronickej podobe, ak dotknutá osoba nepožiadala o poskytnutie informácie iným spôsobom.

4. Ak prevádzkovateľ neprijme opatrenia na základe žiadosti dotknutej osoby, je povinný do jedného mesiaca od doručenia žiadosti, informovať dotknutú osobu o dôvodoch nekonania a o možnosti podať návrh podľa § 100 zákona o OOÚ na Úrad na ochranu osobných údajov.

5. Prevádzkovateľ poskytuje informácie podľa § 19 a 20 zákona o OOÚ a oznámenia a opatrenia prijaté podľa § 21 až 28 a 41 zákona o OOÚ bezodplatne. Ak je žiadosť dotknutej osoby zjavne neopodstatnená alebo neprimeraná, najmä pre jej opakujúcu sa povahu, prevádzkovateľ môže

   a) požadovať primeraný poplatok zohľadňujúci administratívne náklady na poskytnutie informácií alebo primeraný poplatok zohľadňujúci administratívne náklady na oznámenie alebo primeraný poplatok zohľadňujúci administratívne náklady na uskutočnenie požadovaného opatrenia, alebo
   b) odmietnuť konať na základe žiadosti.

6. Zjavnú neopodstatnenosť žiadosti alebo neprimeranosť žiadosti preukazuje prevádzkovateľ. Prevádzkovateľ môže požiadať o poskytnutie dodatočných informácií potrebných na potvrdenie totožnosti dotknutej osoby, ak má oprávnené pochybnosti o totožnosti fyzickej osoby, ktorá podáva žiadosť podľa § 21 až 27 zákona o OOÚ; ustanovenie § 18 zákona o OOÚ tým nie je dotknuté. Informácie, ktoré má prevádzkovateľ poskytnúť dotknutej osobe podľa § 19 a 20 zákona o OOÚ, možno podať v kombinácii so štandardizovanými ikonami s cieľom poskytnúť dobre viditeľný, jasný a zrozumiteľný prehľad zamýšľaného spracúvania osobných údajov. Štandardizované ikony musia byť strojovo čitateľné, ak sú použité v elektronickej podobe.

§ 4
Poverené osoby

1. Prevádzkovateľ za účelom splnenia povinností uvedených v § 2 a v § 3 týchto opatrení, poverí na základe písomných pokynov, svojich zamestnancov ich výkonom. Prevádzkovateľ o tomto poverení vyhotoví písomný záznam pre každého zamestnanca individuálne.

§ 5
Prijaté dokumenty

1. Prevádzkovateľ v zmysle týchto opatrení vypracuje Záznam o poverení osoby a oboznámení sa s opatreniami na ochranu osobných údajov a Oznámenie porušenia ochrany osobných údajov Úradu na ochranu osobných údajov.

Bezpečnostné opatrenia IS ÚD, IS Zákazníci, IS Marketing, č. 2

Spracúvanie, uschovávanie a likvidácia osobných údajov z informačných systémov

§ 1
Spracúvanie osobných údajov

1. Spracúvať osobné údaje u prevádzkovateľa má právo a povinnosť len poverená osoba, písomne poverená a poučená a to len v zmysle pokynov prevádzkovateľa a na základe Nariadenia GDPR a zákona o OOÚ.

2. Poverená osoba zodpovedná za vedenie osobných údajov v listinných informačných systémoch a taktiež v automatizovaných informačných systémov v zmysle poverenia prevádzkovateľa. Rozsah povinností jednotlivých poverených osôb, určí prevádzkovateľ a vyhotoví o tom písomný záznam. Poverená osoba okrem iného zabráni, aby jednotlivé písomnosti v informačných systémoch nevypadávali pri bežnej práci s nimi (lepením, zošívaním, vložením do obalov).

§ 2
Uschovávanie a likvidácia osobných údajov

1. Písomnosti obsahujúce osobné údaje sa v priestoroch prevádzkovateľa ukladajú do uzamykateľných miestností resp. priestorov na to určených, resp. v uzamykateľnej skrini v priestoroch na prízemí na adrese 10. apríla 683/11, 91101 Trenčín, ktorej je prevádzkovateľ vlastníkom.

2. Za úschovu písomnosti obsahujúcej osobné údaje zodpovedá poverená osoba v zmysle poverenia prevádzkovateľa, ktorej bola písomnosť zverená. Táto poverená osoba je povinná po skončení používania písomnosti obsahujúcej osobné údaje uložiť ju do uzamykateľných miestností na to určených, uzamykateľných kontajnerov alebo zásuviek kancelárskeho stola, alebo do iných uzamykateľných zariadení alebo ju odovzdať osobe, od ktorej písomnosť získala.

3. Písomnosti, obsahujúce osobné údaje, ktorých účel spracúvania sa skončil, musia byť zlikvidované.

4. Likvidáciu nepotrebných písomností, ktoré obsahujú osobné údaje, zabezpečí prevádzkovateľ prostredníctvom poverenej osoby. Dokumenty resp. iné nosiče osobných údajov musia byť zlikvidované skartovacím zariadením, spálením alebo inou metódou zamedzujúcou čitateľnosť.

5. Prevádzkovateľ je v zmysle § 9 zákona o OOÚ povinný bez zbytočného odkladu vymazať osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú.

6. Prevádzkovateľ na základe žiadosti dotknutej osoby podľa § 23 ods. 1 zákona o OOÚ, bez

zbytočného odkladu vymaže osobné údaje, ktoré sa jej týkajú, ak je splnený čo i len jeden predpoklad v zmysle § 23 ods. 2 zákona o OOÚ.

§ 3
Prijaté dokumenty

1. Prevádzkovateľ v zmysle týchto opatrení vypracuje Záznam o poverení osoby.

Bezpečnostné opatrenia IS ÚD, IS Zákazníci, IS Marketing č. 3

Popis povolených spracovateľských činností a podmienky spracúvania osobných údajov

§ 1
Rozsah a popis povolených spracovateľských činností a oprávnení

1. Rozsah oprávnení a povolených spracovateľských operácií poverenej osoby súvisiacich so spracúvaním osobných údajov je vymedzený záznamom o poverení osoby, opisom pracovných činností konkrétnej poverenej osoby, ktorá je neoddeliteľnou súčasťou jej pracovnej zmluvy alebo inej zmluvy, všeobecne záväznými právnymi predpismi, ako aj platnými internými riadiacimi aktmi prevádzkovateľa.

2. Prevádzkovateľ je prostredníctvom poverených osôb povinný osobné údaje chrániť pred zneužitím treťou osobou. Pokiaľ bezprostredne nepracujú s osobnými údajmi, prevádzkovateľ je povinný listiny s osobnými údajmi držať v uzamykateľnej skrini, priestore resp. v inom zabezpečenom priestore.

§ 2
Podmienky spracúvania osobných údajov prostredníctvom neautomatizovaných prostriedkov spracúvania (listinný forma spracúvaných osobných údajov)

1. Pri spracúvaní osobných údajov neautomatizovaným spôsobom prevádzkovateľ najmä

a) zachováva obozretnosť pri podávaní chránených informácií, vrátane osobných údajov, pred návštevníkmi prevádzkovateľa alebo inými nepoverenými osobami,
b) neponecháva osobné údaje voľne dostupné na chodbách, stoloch a v iných neuzamknutých miestnostiach alebo na iných miestach, vo verejne prístupných miestach, opustených dopravných prostriedkoch a pod.,
c) odkladá písomnosti, spisy a iné listinné materiály na určené miesto a neponecháva ich po skončení pracovnej doby, resp. opustení priestorov prevádzkovateľa voľne dostupné (napr. na pracovnom stole),
d) zaobchádza s tlačenými materiálmi obsahujúcimi osobné údaje podľa ich citlivosti; je potrebné aplikovať všetky relevantné opatrenia, ktoré zabezpečia ochranu vytlačených informácií obsahujúcich osobné údaje pred neoprávnenými osobami,
e) pri skončení pracovného pomeru alebo obdobného vzťahu poverená osoba je povinná odovzdať prevádzkovateľovi pracovnú agendu vrátane listín, ktoré obsahujú osobné údaje,

f) v prípade tlače dokumentov obsahujúcich osobné údaje zabezpečuje, aby sa počas tlačenia neoboznámila s nimi nepoverená osoba; tlačené materiály obsahujúce osobné údaje musia byť ihneď po ich vytlačení odobraté poverenou osobou a uložené na zabezpečené miesto; to sa uplatňuje aj pri kopírovaní dokumentov - nadbytočné a chybné dokumenty poverená osoba bez zbytočného odkladu zlikviduje skartovaním,
g) uzamyká priestory pri každom opustení v prípade, že v miestnosti už nie je iná poverená osoba prevádzkovateľa,

§ 3
Podmienky spracúvania osobných údajov prostredníctvom úplne alebo čiastočne automatizovaných prostriedkov spracúvania

1. Pri spracúvaní osobných údajov prostredníctvom úplne alebo čiastočne automatizovaných prostriedkov spracúvania prevádzkovateľ najmä

a) využíva služby Internetu (povolené je využívanie iba verejných služieb WWW - worldwide web) za účelom plnenia pracovných úloh, pričom dodržiava bezpečnostné opatrenia prijaté prevádzkovateľom za účelom zabezpečenia ochrany osobných údajov pri využívaní služieb Internetu,
b) nepoužíva verejné komunikačné systémy na rýchly prenos správ (Facebook, WhatsApp, Messenger, Viber, Instagram, AOL, IRC a pod.),
c) informačnú techniku (počítače, notebooky, USB kľúč, a pod.) umiestňuje iba v uzamykateľných priestoroch; miestnosť, v ktorej sa nachádza informačná technika, musí byť pri každom odchode poverenej osoby uzamknutá a po skončení pracovnej doby je poverená osoba povinná vypnúť počítač a uzamknúť skrine a priestory s materiálmi obsahujúcimi osobné údaje,
d) dbá na antivírusovú ochranu pracovných staníc sledovaním toho, či správne funguje primárne určený softvérový systém, ktorý je automaticky pravidelne aktualizovaný,
e) berie do úvahy zákaz odinštalovania, zablokovania alebo zmenu konfigurácie antivírusovej ochrany,

§ 4
Prijaté dokumenty

1. Prevádzkovateľ v zmysle týchto opatrení vypracuje Záznam o poverení osoby a Záznam o spracovateľských činnostiach.

Bezpečnostné opatrenia IS ÚD, IS Zákazníci, IS Marketing č. 4

Rozmnožovanie písomností obsahujúcich osobné údaje

§ 1
Rozmnožovanie písomností obsahujúcich osobné údaje

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

2. Rozmnožovať písomnosti môže len poverená osoba v zmysle poverenia prevádzkovateľa.

§ 2
Prijaté dokumenty

1. Prevádzkovateľ v zmysle týchto opatrení vypracuje Záznam o poverení osoby.

Bezpečnostné opatrenia IS ÚD, IS Zákazníci, IS Marketing č. 5
Rozsah zodpovednosti poverených osôb

§ 1
Povinnosti poverených osôb

1. Prevádzkovateľ je povinný v zmysle § 79 zákona o OOÚ zachovávať mlčanlivosť o osobných údajoch, ktoré spracúva. Povinnosť mlčanlivosti trvá aj po ukončení spracúvania osobných údajov.

2. Prevádzkovateľ zaviaže mlčanlivosťou o osobných údajoch fyzické osoby resp. zamestnancov, ktorí prídu do styku s osobnými údajmi u prevádzkovateľa. Povinnosť mlčanlivosti podľa prvej vety musí trvať aj po skončení pracovného pomeru, štátnozamestnaneckého pomeru, služobného pomeru alebo obdobného pracovného vzťahu tejto fyzickej osoby.

3. Povinnosť mlčanlivosti podľa odsekov § 1 a § 2 týchto opatrení neplatí, ak je to nevyhnutné na plnenie úloh súdu a orgánov činných v trestnom konaní podľa osobitného zákona; tým nie sú dotknuté ustanovenia o mlčanlivosti podľa osobitných predpisov.

4. Poverené osoby budú prevádzkovateľom oboznámené s obsahom bezpečnostných opatrení, sú povinné ich dodržiavať a zachovať mlčanlivosť vzhľadom na osobné údaje zákazníkov a ostatných zamestnancov prevádzkovateľa.

5. Osoby poverené spracovávať osobné údaje sú najmä
a) zodpovedné za komplexné, pravdivé, aktuálne údaje a vkladanie týchto údajov do IS
b) sú zodpovedné za uchovávanie, ochranu a manipuláciu s nimi v prípade, že tieto údaje sú v textovej forme
c) zodpovedné za preukázateľnosť súhlasu na spracovanie osobného údaju, a to tak, že možno o ňom predložiť dôkaz
d) zodpovedné za poriadok v priestoroch prevádzkovateľa a odloženie všetkých písomností obsahujúcich osobné údaje a iných dokumentov, ktoré by mohli viesť k slobodnému prístupu k osobným údajom, do uzamykateľných odkladacích políc
e) zodpovedné za dodržiavanie zásad práce; podľa príkazu sú povinné včas informovať osobu zodpovednú za dohľad nad ochranou osobných údajov o pripravovanom začatí spracovania osobných údajov a o všetkých skutočnostiach, ktoré by mohli viesť k zneužitiu týchto údajov

6. Osoby, ktoré prevádzkujú informačný systém

a) zodpovedajú za archiváciu údajovej základne a aplikačného programového vybavenia
b) sú zodpovedné za antivírovú ochranu
c) spoluzodpovedajú s užívateľmi pracovných staníc za antivírovú ochranu
d) zodpovedajú za modernizáciu hmotných a nehmotných aktív
e) sú zodpovedné za riadny chod IS

7. Osoby zodpovedné za dohľad nad ochranou osobných údajov
a) zodpovedajú za dozeranie na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov
b) posúdia pred začatím spracúvania osobných údajov v informačnom systéme, či ich spracúvaním nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb. Zistenie narušenia práv a slobôd dotknutých osôb pred začatím spracúvania alebo porušenia zákonných ustanovení v priebehu spracúvania osobných údajov poverená alebo zodpovedná osoba bezodkladne písomne oznámi prevádzkovateľovi; ak prevádzkovateľ po upozornení bezodkladne nevykoná nápravu, oznámi to poverená alebo zodpovedná úradu na ochranu osobných údajov
c) kontrolujú zásady spracúvania osobných údajov

§ 2
Prijaté dokumenty

1. Prevádzkovateľ v zmysle týchto opatrení vypracuje Záznam o poverení osoby a Zoznam poverených osôb.

Bezpečnostné opatrenia IS ÚD, IS Zákazníci, IS Marketing č. 6
Kľúčový režim prevádzkovateľa a povinnosti držiteľov kľúčov

§ 1
Úvodné ustanovenie

1. Kľúče slúžiace na zabezpečenie vstupu do priestorov prevádzkovateľa a otváranie zariadení v ktorých sa uschovávajú počítače, počítačové média alebo otváranie uzamykateľných skríň v ktorých sa uschovávajú písomností obsahujúce osobné údaje (ďalej „evidované kľúče") sa prideľujú len osobám, ktoré určí a poverí prevádzkovateľ. Evidované kľúče prideľuje prevádzkovateľ, alebo osoba ním poverená zodpovednosťou za ochranu osobných údajov.

2. Každý evidovaný kľúč je označený jedinečným znakom, pod ktorým je zapísaný v evidencii.

3. Prevádzkovateľ, alebo osoba ním poverená zodpovednosťou za ochranu osobných údajov vedie o evidovaných kľúčoch evidenciu, ktorá obsahuje najmä:
a) identifikačný znak kľúča,
b) označenie dverí, zariadenia alebo zámku, ktorý sa kľúčom otvára,
c) identifikačné údaje osoby (meno, priezvisko, podpis), ktorej bol kľúč pridelený,
d) dátum prebrania (odovzdania) kľúča a podpis osoby, ktorá preberá (odovzdáva) kľúč.

4. Osoba, ktorá nie je poverená na spracúvanie osobných údajov, môže mať pridelené a samostatne

používať evidované kľúče od priestorov prevádzkovateľa iba s podmienkou, že pamäťové média IS a iné dokumenty obsahujúce osobné údaje sú uzamykané v zariadeniach na úschovu prístupných iba držiteľom evidovaných kľúčov.

5. Držiteľ evidovaných kľúčov je povinný:

a) zaobchádzať s kľúčmi tak, aby nedošlo k ich krádeži alebo strate,
b) osobne dohliadať nad prácou nepoverených osôb v priestoroch prevádzkovateľa, zabrániť im prístup k osobným údajom a zabezpečiť, aby sa v priestoroch, v ktorých sa spracovávajú osobné údaje nezdržiavali nepoverené osoby z iných ako pracovných dôvodov,
c) uzamykať okná, dvere a zariadenia, od ktorých má pridelené evidované kľúče vždy, keď sa vzďaľuje z priestorov prevádzkovateľa,
d) pred uzamknutím a opustením priestorov prevádzkovateľa uschovať všetky pamäťové média a písomnosti obsahujúce osobné údaje, ktoré sú voľne položené v priestoroch pracoviska,
e) bez omeškania oznámiť prevádzkovateľovi krádež alebo stratu evidovaných kľúčov,
f) na výzvu prevádzkovateľa v stanovenom termíne odovzdať evidované kľúče.

§ 2
Prijaté dokumenty

1. Prevádzkovateľ v zmysle týchto opatrení vypracuje Evidenciu pridelených kľúčov.

Bezpečnostné opatrenia IS ÚD, IS Zákazníci, IS Marketing č. 7
Povinnosti prevádzkovateľa pri práci s automatizovanými IS

§ 1
Poverená osoba za automatizované informačné systémy

1. Za bezpečnosť osobných údajov v priestoroch prevádzkovateľa zodpovedá prevádzkovateľ, ktorý na to môže poveriť osobu, ktorá musí byť bezúhonná.

2. Za chod automatizovaných informačných systémov zodpovedá prevádzkovateľ, alebo na to určená osoba, ktorá musí byť písomne poučená a poverená na prácu s osobnými údajmi.

3. Prevádzkovateľ určí rozsah oprávnení podľa nasledujúcich pravidiel:
a) poverená resp. zodpovedná osoba má neobmedzený prístup k celým informačným systémom,
b) získavať osobné údaje od dotknutých osôb môže len osoba poverená, toto oprávnenie vydá prevádzkovateľ a príslušná osoba ho potvrdí svojím podpisom,
c) osoby poverené pracovať s IS musia byť poučené. Svoj záväzok o diskrétnosti a mlčanlivosti potvrdí príslušná osoba svojím podpisom,
d) v súvislosti s možnosťou prieniku do počítačového systému sa každá poverená osoba prezentuje svojím prístupovým heslom, ktoré určí, alebo schváli zodpovedná osoba (dĺžka hesla musí mať minimálne 8 znakov),

e) prístupové heslá pravidelne mení.

§ 2
Opatrenia

1. Poverená alebo zodpovedná osoba na základe poverenia prevádzkovateľa zabezpečí technické a organizačné opatrenia, formu a periodicitu kontrol.

§ 3
Manipulácia s technickými prostriedkami IS na základe poverenia prevádzkovateľa

1. Pracovné stanice IS musia byť umiestnené tak, aby vplyvom okolia nedošlo k neúmyselnému poškodeniu alebo poruche zariadenia (pádom pracovnej stanice, teplom, vodou, priamym slnečným svetlom a pod.). Pracovné stanice neumiestňovať na podlahu.

2. Poverená alebo zodpovedná smie manipulovať s pracovnými stanicami IS (zapínať, používať, vypínať) len v súlade s inštrukciami výrobcu, resp. dodávateľa zariadenia.

3. Poverená alebo zodpovedná osoba nesmie znižovať životnosť pracovných staníc IS hrubým zaobchádzaním a ich znečisťovaním.

4. V blízkosti technických zariadení IS je zakázané jesť, piť a fajčiť, ale aj vykonávať iné činnosti hroziace znečistením technických zariadení (pestovanie kvetov v blízkosti technických zariadení a pod.).

5. Opravy a úpravy pracovnej stanice môže vykonávať len prizvaný kvalifikovaný špecialista. Kvalifikovaný špecialista pritom môže zasahovať do pracovnej stanice iba s preukázateľným súhlasom prevádzkovateľa. Používateľ pracovnej stanice je povinný odmietnuť prístup k pracovnej stanici osobe, ktorá sa nepreukáže takýmto súhlasom.

6. Čistenie povrchu technických zariadení pracovnej stanice od prachu je povinný vykonávať používateľ pracovnej stanice vhodnými čistiacimi prostriedkami pri vypnutom stave zariadenia. Vnútorné čistenie zariadení IS môže vykonávať len kvalifikovaný špecialista pri dodržaní podmienok odseku 5 týchto opatrení.

7. Do mechaník prenosných pamäťových médií (DVD, CD, USB porty, externý harddisk, atď.) nesmú byť vkladané znečistené alebo poškodené médiá.

8. Pri zapínaní a reštartovaní počítača nesmie byť v CD, DVD, USB mechanike zapojené pamäťové médium.

§ 4
Technické opatrenia na základe poverenia prevádzkovateľa

1. Poverená alebo zodpovedná osoba zabezpečí najmä nasledovné technické opatrenia:

a) priebežne počas práce s IS sleduje ich činnosť a prípadné nekorektné správanie konzultuje s ich dodávateľom

b) 1x za 12 mesiacov zabezpečí kontrolu počítačového systému špecializovaným servisným technikom.

Tento zrealizuje overenie integrity pevného disku s verifikáciou povrchu, antivírusový scan a kontrolu technického stavu všetkých hardvérových komponentov

c) zabezpečí správne nastavenie brány FireWall
d) zabezpečí správne nastavenie antivírusového programu
e) zakáže použitie cudzích pamäťových nosičov a prezeranie a inštaláciu akýchkoľvek programov z internetu
f) podľa opatrení pre zálohovanie zabezpečí bezchybný stav zálohovacích mechaník a nosičov

§ 5
Organizačné opatrenia na základe poverenia prevádzkovateľa

1. Poverená alebo zodpovedná osoba zabezpečí najmä nasledovné organizačné opatrenia:
a) počas pracovnej doby zamedzí prístup nepovereným osobám k počítaču a iným aktívam IS
b) nepoverené osoby nesmú mať prístup k informačným systémom. V neprítomnosti poverených alebo zodpovedných osôb musí byť priestor s IS uzamknutý a prístup do počítača musí byť chránený heslom
c) pri krátkodobom odchode z priestorov prevádzkovateľa sa uvedie počítač do stavu, kedy na pokračovanie v programe je potrebné zadať heslo
d) pri odchode z priestorov prevádzkovateľa na záver pracovnej doby vykonaná zálohy databáz na prenosný nosič a pevný disk, vypne počítač a uzamkne priestory

§ 6
Antivírusové opatrenia na základe poverenia prevádzkovateľa

1. Akýkoľvek zásah do nastavenia rezidentnej antivírusovej ochrany pracovnej stanice používateľom počítača je zakázaný.

2. Poverená alebo zodpovedná osoba je povinná pred použitím pamäťových nosičov dát otestovať ich na prípadný výskyt vírusov.

3. Používateľ počítača (poverená alebo zodpovedná) je povinný v prípade podozrenia na výskyt vírusu otestovať pracovnú stanicu.

4. V prípade, že sa na pracovnej ploche používateľa počítača zobrazí varovanie, že sa na disku, USB kľúči, CD, atď. nachádza vírus, používateľa počítača nesmie toto varovanie ignorovať. V prípade, že zavírený pamäťový nosič patrí inému subjektu, používateľ počítača ho viditeľne a výrazne označí ako zavírený a vráti ho jej vlastníkovi. V prípade zavírenia pevného disku, vlastného USB kľúča, CD, atď. používateľ počítača túto skutočnosť bezodkladne oznámi prevádzkovateľovi a predmetný pamäťový nosič viditeľne a výrazne označí ako zavírený.

5. V prípade ak používateľ počítača objaví vírus v prijatej elektronickej pošte, bezodkladne o tejto udalosti upovedomí prevádzkovateľa, ako aj odosielateľa predmetnej elektronickej pošty. V žiadnom prípade zavírenú elektronickú poštu neposiela inému adresátovi.

6. Je zakázané otvárať prílohy správ elektronickej pošty prijaté od nedôveryhodného odosielateľa alebo podozrivého obsahu správy od známeho odosielateľa. Používateľ počítača (poverená alebo zodpovedná) je povinný hodnovernosť obsahu správy overiť u odosielateľa.

§ 7
Forma a periodicita kontrol na základe poverenia prevádzkovateľa

1. Prevádzkovateľ priebežne, minimálne však 1x za 6 mesiacov, skontroluje náhodným výberom kompletnosť databázy v počítačovom systéme.

2. Prevádzkovateľ v prípade pripájania PC na internet zabezpečí permanentnú antivírovú a antispamovú kontrolu.

3. Pri nekorektnom správaní systému poverená alebo zodpovedná osoba skontroluje, alebo špecializovaným technikom zabezpečí kontrolu logových súborov v zobrazovači udalostí operačného systému /EventViewer/.

4. Minimálne 1x za 6 mesiace, alebo po nekorektnom ukončení alebo výpadku energie vykoná poverená alebo zodpovedná osoba systémovú kontrolu disku (scandisk), ak operačný systém takúto voľbu povoľuje.

5. Minimálne 1x za 6 mesiace vykoná poverená alebo zodpovedná osoba systémový scandisk a defragmentáciu disku, ak operačný systém takéto voľby povoľuje.

6. Pri údržbe a údržbových funkciách jednotlivých programov poverená alebo zodpovedná osoba dodržiava zásady podľa návodu na použitie (tieto služby, ako napr. defragmentácia, kompresia a kontrola integrity databáz sa odporúča vykonať 1x za 6 mesiace).

7. Pri výzve na aktualizáciu systému poverená alebo zodpovedná osoba zabezpečí spustenie stiahnutých aktualizácií v čo najkratšom termíne s dôrazom na bezpečnostné aktualizácie.

§ 8
Bezpečnostný incident a preventívne opatrenia

1. Bezpečnostným incidentom je udalosť (porucha, havária, vírusová infiltrácia a pod.), ktorá spôsobila narušenie bezpečnosti informačného systému, t.j. došlo ku strate diskrétnosti, integrity alebo dostupnosti dát. Za bezpečnostný incident treba považovať aj odhalený pokus o prekonanie bezpečnostných opatrení.

2. Každý bezpečnostný incident poverená alebo zodpovedná osoba poznačí do príslušnej evidencie.

3. Pri havárii, nefunkčnosti alebo neštandardnom správaní poverená alebo zodpovedná osoba zváži a rozhodne, či kontaktovať počítačový servis, alebo softvérovú spoločnosť, ktorá počítačový systém dodala.

4. Po konzultácii poverená alebo zodpovedná osoba postupuje podľa inštrukcií dodávateľskej firmy.

5. V prípade nechceného vymazania databáz poverená alebo zodpovedná osoba v žiadnom prípade nepokračuje v práci. Je bezpodmienečne nutné vypnúť počítač a kontaktovať dodávateľa informačného systému (ak sa po vymazaní súborov neuskutočňujú žiadne ďalšie inštalácie, obnovy,

kopírovanie, atď., možno odborným prístupom tieto vymazané údaje obvykle obnoviť).

6. Podľa doporučení dodávateľa informačných systémov poverená alebo zodpovedná osoba vykonáva pravidelný servis databáz a operačného systému počítača.

§ 9
Postup pri riešení bezpečnostného incidentu na základe poverenia prevádzkovateľa

1. Pokiaľ poverená alebo zodpovedná osoba nepostupuje podľa inštrukcií dodávateľskej firmy, riešenie jednotlivých typov bezpečnostných incidentov môžeme rozdeliť do týchto fáz: Príprava, Detekcia a analýza, Vymedzenie a odstránenie incidentu a obnova po incidente, Post-incidentné aktivity. Riešenie a nápravu bezpečnostného incidentu zabezpečí dodávateľská spoločnosť na základe zmluvného záväzku s prevádzkovateľom.

Príprava
Dbá sa na prevenciu pred incidentmi. Cieľom je udržanie nízkeho počtu incidentov. Odporúčané praktiky na zabezpečenie sietí, systémov a aplikácií je manažment záplat, bezpečnosť počítačov, sieťová bezpečnosť, prevencia pred škodlivým kódom, tréning a povedomie zamestnancov.

Detekcia a analýza
- profilujú sa siete a systémy
- použije sa centralizovaný zber záznamov
- vykoná sa korelácia udalostí
- udržujú sa hodiny všetkých počítačov synchronizované
- udržuje a využíva sa znalostná báza informácií
- používajú sa internetové vyhľadávacie nástroje na skúmanie
- berie sa do úvahy filtrovanie údajov

Vymedzenie a odstránenie incidentu a obnova po incidente
Incident sa vymedzí. Po vymedzení incidentu nastúpi odstránenie incidentu, ktoré spočíva v eliminácii komponentov incidentu, ako je vymazanie škodlivého kódu alebo zablokovanie napadnutých používateľských účtov atď. Procedúry odstránenia incidentu a obnova po incidente sú typicky závislé na operačnom systéme a na aplikáciách. Ochrana osobných údajov je zabezpečená ich uložením na zálohovacie zariadenia. Pri obnove sa znova zavedie systém do normálnej prevádzky. Obnova zahrňuje:
- obnova systému
- náhrada kompromitovaných súborov z čistých verzií
- zmena hesiel
- zúženie bezpečnostného perimetra siete (prestavenie konfiguračného súboru bezpečnostnej brány, filtrovacích pravidiel)

Post-incidentné aktivity
Z incidentu sa treba poučiť. Zhodnotí sa, čo sa presne stalo a kedy sa to stalo. Hodnotia sa nasledovné skutočnosti:
- ako dobre si počínali poverené alebo zodpovedné osoby pri riešení incidentu
- či sa postupovalo sa podľa schválených procedúr
- či sú procedúry adekvátne
- aké boli vykonané kroky alebo akcie, ktoré by mohli zabrániť obnove
- čo by mali robiť poverené alebo zodpovedné osoby na riešenie incidentov v budúcnosti

inak v prípade, že sa vyskytne podobný incident
- aké opravné akcie zabránia podobným incidentom v budúcnosti
- aké ďalšie nástroje alebo zdroje sú potrebné na detekciu, analýzu a zníženie budúcich incidentov

§ 10
Využívanie sieťových služieb (Internet) na základe poverenia prevádzkovateľa

1. Poverená alebo zodpovedná osoba, ak má umožnený prístup do siete Internet, je povinná rešpektovať nasledovné zásady:

a) prístup do siete Internet využívať predovšetkým v súlade so svojou pracovnou náplňou a činnosťou príslušného organizačného útvaru
b) svojou činnosťou v sieti Internet reprezentuje nielen seba ale aj prevádzkovateľa, ktorý mu prístup do siete umožnil. Preto je povinná rešpektovať etické zásady a zdržať sa činností, ktoré by viedli k poškodeniu dobrého mena prevádzkovateľa alebo k iným škodám
c) komunikácia na Internete (napríklad elektronická pošta) spravidla nie je chránená pred "odpočúvaním". V prípade potreby prenosu dôverných údajov sieťou Internet je nevyhnutné tieto riadne zabezpečiť ich zašifrovaním. Šifrovanie, resp. kryptovanie súborov, pseudonymizovanie súborov obsahujúcich osobné údaje aj pri ich prenosoch cez verejne prístupnú počítačovú sieť v rámci elektronickej komunikácie je potrebné zabezpečiť
d) elektronická pošta môže byť pozmenená – „sfalšovaná“. V prípade, že na základe údajov (obsahu) prijatej elektronickej pošty by mala poverená alebo zodpovedná osoba realizovať závažné kroky, je povinná si overiť, či predmetnú elektronickú poštu naozaj poslal v nej uvedený odosielateľ

§ 11
Prijaté dokumenty

1. Prevádzkovateľ v zmysle týchto opatrení vypracuje Záznam o poverení osoby, Zoznam aktív a všetkých miest prepojenia sietí, Evidenciu o zistených bezpečnostných incidentoch a prijaté opatrenia.

Bezpečnostné opatrenia IS ÚD, IS Zákazníci, IS Marketing č. 8

Zálohovanie údajov v počítačovom systéme

§ 1
Zálohovanie databáz

1. Zálohovaním databáz počítačového systému rozumieme proces, ktorým sa vytvorí kópia všetkých databázových súborov IS resp. len jej časť, nevyhnutná na obnovu všetkých databáz a to v prípade poruchy, alebo odcudzenia počítačového systému. Na vytvorenie zálohových súborov sa vo väčšine prípadov používajú štandardné komprimačné algoritmy (ZIP, CAB,ARJ, RAR, atď.).

2. Tieto opatrenia platia pre každý používaný IS osobitne.

§ 2
Typy zálohovania

1. Zálohovaním na iný pevný disk, alebo na iný PC v sieti je bezpečnejší spôsob, ktorý lepšie eliminuje riziká technickej, alebo inej poruchy pevného disku. Nerieši však problém odcudzenia počítačov. Na druhej strane je vyššie riziko narušenia údajov, nakoľko údaje sú uložené na viacerých počítačoch.

2. Zálohovanie na ten istý pevný disk počítača, na ktorom je umiestnený IS je najlacnejším a najrýchlejším spôsobom zálohovania. Princíp je založený na vytvorení kópie databáz do iného adresára, ako je IS resp. nainštalovaný program. Zálohovanie rieši stratu integrity databáz, ako aj poškodenie údajových štruktúr vplyvom výpadku napájania. Nerieši však stratu a poškodenie údajov spôsobenú neopraviteľnou poruchou pevného disku alebo odcudzením počítačového systému.

3. Zálohovanie na externé nosiče je najbežnejším spôsobom prenosu a uchovávania údajov. Treba uplatňovať zásadu nezálohovania stále na tie isté nosiče. Ideálnym riešením je pravidelne používať iný súbor zálohovacích nosičov a tieto striedať (zálohovanie s cirkuláciou média).

4. Zálohovanie na iný prenosný nosič akým je napríklad USB kľúč, CDR, CDRW, DVDR, MemoryCard, prenosný pevný disk atď. je taktiež účinným spôsobom zálohovania. Z hľadiska ceny, kompatibility a spoľahlivosti je najvýhodnejším spôsobom zálohovania USB kľúč.

§ 3
Zásady, postupy a periodicita pri zálohovaní

1. Každý deň vykonať bezpečnostnú zálohu na pevný disk vášho počítača. Minimálne 1 x za 6 mesiace vykonať zálohu na prenosný nosič.

2. Minimálne 1x za 12 mesiacov vykonať úplné formátovanie pamäťových médií a to z dôvodu overenia ich funkčnosti.

3. Minimálne 1x za 12 mesiacov overiť možnosť obnoviť informačný systém z vykonanej zálohy.

4. V žiadnom prípade nenechávať zálohové nosiče neuzamknuté v priestoroch prevádzkovateľa, nakoľko je potrebné si uvedomiť, že prípadný narušiteľ môže odcudziť nielen počítač, ale aj predmetné nosiče. V tomto prípade sú údaje nenávratne stratené.

5. Pri prenose údajov na zálohovacích nosičoch na iné miesto treba dodržiavať zásady bezpečnosti a ani v domácom prostredí ich nenechávať voľne prístupné.

6. Osobné údaje, ktorých účel spracúvania skončil je z pamäťového nosiča treba vymazať formátovaním alebo fyzickou likvidáciou nosiča a to spálením, mechanickým rozbitím alebo použitím špecializovaného zariadenia na likvidáciu pamäťových nosičov.

7. Čo sa týka dlhodobého skladovania databázových údajov, je potrebné minimálne 1x za 24 mesiacov zálohovať všetky databázy počítačových informačných systémov a zálohy uložiť na "nový" zapisovateľný veľkokapacitný nosič akým je napríklad Externý hardisk, USB, BlueRAY, atď. Tieto zálohy je potrebné uložiť na bezpečné miesto t. j. uzamykateľná miestnosť atď.

Bezpečnostné opatrenia IS ÚD, IS Zákazníci, IS Marketing č. 9

Spôsob, forma a periodicita výkonu kontrolných činností zameraných na dodržiavanie bezpečnostných opatrení

§ 1
Kontrolná činnosť bezpečnostných opatrení na základe poverenia prevádzkovateľa

1. Kontrolná činnosť sa zabezpečuje neustále. Poverené osoby kontrolujú informačné systémy neustále. Akékoľvek incidenty a nekorektnosti chodu sú zaznamenávané do príslušnej evidencie bezpečnostných incidentov.

2. Prevádzkovateľ resp. ním poverená osoba uskutočňuje kontrolu zásad spracovávania osobných údajov a dodržiavanie bezpečnostných opatrení, o čom sa vyhotoví písomný záznam v evidencii kontrolných činností.

3. Pred začatím kontroly je o kontrole upovedomený príslušný vedúci pracovník zodpovedný za danú agendu. Kontrolná činnosť zameraná na dodržiavanie prijatých bezpečnostných opatrení sa uskutočňuje minimálne 1x za 12 mesiacov. Kontrola prevádzky automatizovaných IS sa prevádza nepretržite a to technickými a programovými prostriedkami. Kontrola zabezpečenia miestností pred nedovoleným prístupom v pracovnej dobe ale i v mimopracovnom čase je vykonávaná náhodne a to poverenými osobami.

4. Záznam o vykonanej kontrolnej činnosti obsahuje najmä nasledovné údaje:
a) dátum, čas a poradové číslo
b) druh a zameranie kontroly
c) zistené nedostatky
d) názov informačného systému
e) osoba ktorá kontrolu vykonala a zaznamenala.

§ 2
Prijaté dokumenty

1. Prevádzkovateľ v zmysle týchto opatrení vypracuje Záznam o vykonanej kontrolnej činnosti.

Bezpečnostné opatrenia IS ÚD, IS Zákazníci, IS Marketing č. 10

Postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení

§ 1
Postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení

1. Odporúčaný postup pri haváriách IS spôsobených technickou chybou niektorého komponentu počítača

- monitorovať činnosť počítača, kontrolovať chybové hlásenia
- zabezpečiť dostatok finančných prostriedkov na obnovu IS
- vybrané poverené osoby by mali byť vybavené hlásičmi stavu IS prostredníctvom telekomunikačnej techniky aby mohli zabezpečiť protiopatrenia

2. Odporúčaný postup pri poruche počítača spôsobenej vírusom, neautorizovaným programom

- zabezpečiť antivírovú ochranu
- inštalovať len autorizované programy
- preverovanie cudzích nosičov (FD, CD ROM atď.)
- nepripájať nepreverené PC do siete
- neotvárať nevyžiadané e-mailové prílohy
- nespúšťať programy z prostredia internetu
- nesťahovať neautorizované programy z prostredia internetu
- sledovať aktuálne dianie v sieti internet
- vybrané osoby by mali byť vybavené hlásičmi stavu IS prostredníctvom telekomunikačnej techniky aby mohli zabezpečiť protiopatrenia
- odpojiť každého užívateľa
- spustiť antivírový program s aktuálnou databázou známych vírusov
- detekovať spôsob narušenia
- odstrániť príčinu poruchy
- opraviť narušenú funkčnosť
- opätovne skontrolovať systém antivírovým programom
- prekontrolovať všetky počítače
- nájsť zdroj infiltrácie a zabezpečiť jeho eliminovanie
- znovu spustenie systému a pripojenie užívateľov

3. Odporúčaný postup pri poruche napájania, strata dodávky elektrickej energie

- vybrané osoby by mali byť vybavené hlásičmi stavu IS prostredníctvom telekomunikačnej techniky aby mohli zabezpečiť protiopatrenia
- po nábehu elektrickej energie je potrebné spustiť počítače a prekontrolovať ich funkčnosť

4. Odporúčaný postup pri poruche aktívnych prvkov siete

- monitorovať činnosť, používať menežovateľné aktívne prvky
- zabezpečiť dostatočnú kapacitu
- zabezpečiť dostatočnú ochranu pred nepovolaným prístupom
- vymeniť vadnú časť

5. Odporúčaný postup pri poruche v pasívnej časti siete

- premeranie kabeláže, zásuviek a konektorov
- opraviť, prípadne vymeniť vadnú časť

6. Odporúčaný postup pri havárii databáz
- sledovať konfiguračné súbory
- monitorovať hlásenia a včas na ne reagovať
- denne kontrolovať chybové hlásenia aplikácie a databázy

7. Odporúčaný postup pri havárii aplikácie
- sledovať hlásenia aplikácie a zaznamenávať postrehy užívateľov
- sledovať konfiguračné súbory
- monitorovať hlásenia a včas na ne reagovať
- denne kontrolovať chybové hlásenia aplikácie a databázy
- nainštalovať novšiu verziu aplikácie
- konzultovať chyby s dodávateľom

8. Odporúčaný postup pri poruche pracovných staníc
- používať len autentizované programy
- inštalovať antivírové programy
- inštalovať nové programy smie len poverená osoba
- užívatelia nesmú zasahovať do konfiguračných súborov
- chybové hlásenia treba hlásiť, zálohovať dáta na externé preverené médiá
- za zálohy, prevádzku a bezpečnosť zodpovedá poverená osoba

technická chyba:
- zabezpečiť opravu vadnej časti

softvérová chyba:
- identifikovať príčiny
- obnoviť súbory zo zálohy, alebo preinštalovať operačný systém
- aktualizovať antivírovú ochranu

9. Odporúčaný postup pri narušení dverí, okien
- pravidelne sledovať funkčnosť
- neodkladne zabezpečiť opravu

10. Odporúčaný postup pri mimoriadnych udalostiach spôsobených vplyvom zvyškových rizík
- zabezpečiť niekoľkonásobné záložné kópie
- kontrolovať či sú splnené protipožiarne opatrenia
- kontrolovať osoby pri vstupe do priestorov prevádzkovateľa
- vo vytipovaných priestoroch inštalovať bezpečnostné mreže, dvere
- zabezpečiť autentizáciu osôb pri vstupe do chránených priestorov
- vybrané osoby by mali byť vybavené hlásičmi stavu IS prostredníctvom telekomunikačnej techniky aby mohli zabezpečiť protiopatrenia

v prípade vyradenia IS z činnosti:
- aktivovať záložnú kópiu
- skontrolovať úplnosť systému
- spustenie prevádzky
- odstránenie škôd na pôvodnom pracovisku
- po obnovení funkčnosti vrátenie činností

v prípade napadnutia len časti IS:
- presunúť aktíva do vyhovujúcich priestorov
- obnoviť IS zo zálohy

- spustiť prevádzku
- po odstránení dôsledkov vrátiť činnosti do stavu pred udalosťou.

§ 2
Odborná pomoc

2. Postupy uvedené v § 1 týchto opatrení vykoná prevádzkovateľ resp. poverená osoba len v tom prípade, ak sa jedná o naliehavú a neodkladnú situáciu; v ostatných prípadoch sa havárie, poruchy a iné mimoriadne situácie odvrátia a napravia prostredníctvom kvalifikovaného a odborne zdatného subjektu v tejto oblasti a to na základe zmluvného záväzku.

V ....., Dňa: .....

Štatutárny orgán prevádzkovateľa/poverená osoba: .....

.....
podpis