Bezpečnostná smernica *V súlade s NARIADENÍM 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.*		
Platnosť od:	**1.2.2021**	**Verzia 02**
Predchádzajúca verzia:		
		Počet strán :32
Stupeň dôvernosti:	**Citlivý materiál**	Registratúrny znak:

Implementácia bezpečnostnej politiky

do podmienok prevádzkovateľa pri spracúvaní osobných údajov

Smernica „Princípy bezpečnosti pri spracúvaní osobných údajov“

Názov: Obec Nižné Ladičkovce

Právna forma: Obec

Sídlo: Nižné Ladičkovce 55, 067 11 Ľubiša

IČO: 00323306

Vypracoval: PP PROTECT s.r.o., info@ppprotect.sk,
Antona Bernoláka 2, 071 01 Michalovce

Schválil: Ing. Ján Hudák
Starosta

Podpis: .....

Obsah

1. ČASŤ 3
VŠEOBECNÉ USTANOVENIA 3
2. ČASŤ 5
INTERNET 5
3. ČASŤ 7
VÝMENA A ZVEREJŇOVANIE ÚDAJOV 7
4. ČASŤ 9
ŠIFROVANIE 9
5. ČASŤ 10
SIEŤOVÁ BEZPEČNOSŤ 10
6. ČASŤ 10
ORGANIZAČNÉ OPATRENIA 10
7. ČASŤ 11
FYZICKÁ BEZPEČNOST 11
8. ČASŤ 17
ANTIVÍRUSOVÁ OCHRANA 17
9. ČASŤ 18
RIADENIE PRÍSTUPU 18
10. ČASŤ 19
BEZPEČNOSTNÝ INCIDENT 19
11. ČASŤ 21
OCHRANA OSOBNÝCH ÚDAJOV 21
12. ČASŤ 25
KONTROLNÁ ČINNOSŤ 25
13. ČASŤ 27
ZÁSADY SPRACÚVANIA OSOBNÝCH ÚDAJOV 27
14. ČASŤ 29
HAVARIJNÝ PLÁN A PLÁN OBNOVY 29
Zoznam príloh 32

1. ČASŤ
VŠEOBECNÉ USTANOVENIA

Čl. 1
Úvodné ustanovenia

(1) Smernica upravuje princípy bezpečnosti pri spracúvaní osobných údajov v obci Nižné Ladičkovce (ďalej len „Úrad“ a/alebo „prevádzkovateľ“).

(2) Smernica je záväzná pre všetkých zamestnancov, zamestnancov externých subjektov alebo iné fyzické osoby, ktoré majú prístup k osobným údajom (ďalej len „zamestnanec“).

(3) Cieľom smernice je zabezpečenie ochrany osobných údajov Dotknutých osôb a ochrany prevádzkovateľa a iných osôb pred neoprávneným spracúvaním osobných údajov v rozpore s Nariadením[1].

Čl. 2

Základné pojmy

(1) Informačný systém je súborom technických prostriedkov (hardvér, softvér), prostredníctvom ktorých sú spracúvané osobné údaje, alebo ktoré slúžia na spracúvanie osobných údajov.

(2) Užívateľ informačného systému je každý zamestnanec, alebo zamestnanci externých subjektov alebo iné fyzické osoby, ktoré majú prístup k informačnému systému.

(3) Nadriadený užívateľa je vedúci organizačnej zložky, do ktorej je užívateľ zaradený.

(4) Žiadateľ o prístupové právo je užívateľ informačného systému alebo nadriadený užívateľa žiadajúci prístupové právo k informačnému systému pre seba alebo svojho podriadeného.

(5) Vlastník (odborný garant) systému je zamestnanec, ktorý v rozhodujúcej miere určuje spôsob a rozsah spracovania informácií v informačnom systéme a je zodpovedný za schvaľovanie a revíziu prístupových práv k informačnému systému.

(6) Prístupové právo užívateľa určuje spôsob a možnosti práce, ktoré môže užívateľ v konkrétnom informačnom systéme s dátami a informáciami vykonávať.

(7) Zvláštne prístupové právo je prístupové právo prideľované pre vývoj, testovanie a administráciu informačných systémov.

(8) Užívateľský prístupový profil je tvorený všetkými užívateľovi pridelenými prístupovými právami k informačným systémom a je viazaný k určitej pracovnej pozícii organizačnej štruktúry Úradu.

(9) Zrušenie prístupového práva je postup administrátora, pri ktorom odstráni dané prístupové právo z užívateľského profilu.

(10) Agenda Úradu je oblasť spracúvania osobných údajov, pre ktorú bol stanovený rozsah a účel spracúvania osobných údajov.

[1] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

(11) Zodpovedná osoba (ďalej len „ZO“) je štatutárom Úradu písomne určená fyzická osoba a/alebo právnická osoba v zmysle čl. 37 Nariadenia, ktorá je zodpovedná za plnenie úloh podľa čl. 39 Nariadenia, prípadne v rozsahu úloh nad rámec predmetného článku, ak sú tieto úlohy definované v písomnom určení podľa čl. 37 Nariadenia.

(12) Vlastník agendy je písomne menovaný zamestnanec, zodpovedný za spracúvanie a bezpečnosť osobných údajov v rámci určenej agendy, spravidla vedúci zamestnanec, v ktorého riadiacej pôsobnosti dochádza k spracúvaniu osobných údajov, a ktorý je na úseku agendy zodpovedný najmä za prijímanie bezpečnostných opatrení, ich revíziu a kontrolu nad ich dodržiavaním.

(13) Oprávnená osoba je zamestnanec, ktorý spracúva osobné údaje v Úrade, na základe písomného poverenia alebo ak spracúvanie osobných údajov jasne a zrozumiteľne vyplýva zamestnancovi z opisu pracovných činností alebo interných predpisov Úradu.

(14) Osobné údaje 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.

(15) Dotknutá osoba je každá fyzická osoba, ktorej sa spracúvané osobné údaje týkajú.

(16) Súhlas 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.

(17) Prevádzkovateľom je každý, kto sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov; v prípade, že sa účely a prostriedky tohto spracúvania stanovujú v práve Únie alebo v práve členského štátu, možno prevádzkovateľa alebo konkrétne kritériá na jeho určenie určiť v práve Únie alebo v práve členského štátu.

(18) Sprostredkovateľom je každý, kto spracúva osobné údaje v mene prevádzkovateľa.

(19) 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.

(20) Treťou stranou je fyzická osoba alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý nie je dotknutou osobou, prevádzkovateľom, sprostredkovateľom alebo osobou poverenou prevádzkovateľom alebo sprostredkovateľom spracúvaním osobných údajov.

(21) Porušenie ochrany osobných údajov je porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene alebo neoprávnenému poskytnutiu prenášaných, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov, alebo k neoprávnenému prístupu k nim, t.j. narušenie dôvernosti, dostupnosti alebo integrity dát, ktoré môže znamenať riziko alebo vysoké riziko pre práva a slobody fyzických osôb.

(22) Bezpečnostný incident je porušenie bezpečnostných zásad, alebo neštandardné zmeny alebo správanie informačného systému; porušenie integrity, dôvernosti alebo dostupnosti dát, pričom nemusí ísť o porušenie ochrany osobných údajov.

(23) Spracúvanie osobných údajov je spracovateľská operácia alebo súbor spracovateľských operácií s osobnými údajmi alebo 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.

(24) Subdodávateľ je každý, kto spracúva osobné údaje a zabezpečuje ich ochranu na zodpovednosť Sprostredkovateľa (subjekt v pozícii ďalšieho sprostredkovateľa podľa čl. 28 Nariadenia, ktorý spracúva osobné údaje podľa dojednaných podmienok so Sprostredkovateľom a v súlade s podmienkami dojednanými medzi Prevádzkovateľom a Sprostredkovateľom). Ustanovenia Nariadenia o Sprostredkovateľovi sa vzťahujú aj na Subdodávateľa. Na Subdodávateľa sa nahliada ako na Sprostredkovateľa.

(25) Dozorným orgánom je Úrad na ochranu osobných údajov Slovenskej republiky, ktorý je orgánom štátnej správy s celoslovenskou pôsobnosťou, ktorý vykonáva dozor nad ochranou osobných údajov a podieľa sa na ochrane základných práv a slobôd fyzických osôb pri spracúvaní ich osobných údajov.

2. ČASŤ
INTERNET

Čl. 3
Využívanie internetu

(1) Využívanie služieb internetu zamestnancami je určené výlučne pre plnenie pracovných úloh.

(2) Používanie verejných komunikačných systémov na rýchly prenos správ (ICQ, AOL, IRC a pod.) je zakázané. Je zakázané využívať internet na prenos softvéru alebo informácií, ktoré môžu spôsobiť porušenie autorských práv.

(3) Povolené je využívanie iba verejných služieb WWW (world wide web) a FTP (file transfer protocol).

(4) Na ochranu informačného systému pred škodlivými programami zavádza prevádzkovateľ opatrenia obmedzujúce niektoré typy internetovej komunikácie a sťahovanie niektorých typov súborov z internetu.

(5) V prípade, ak užívateľ nemôže využívať niektorú službu internetu alebo k svojej pracovnej činnosti potrebuje stiahnuť do počítača súbor potrebný pre výkon svojej práce, štatutár môže umožniť využívanie danej služby alebo stiahnutie súboru na základe písomnej žiadosti podpísanej užívateľom, ktorý danú službu alebo súbor požaduje. Povolenie môže mať, s ohľadom na vykonávaný charakter pracovnej činnosti, platnosť maximálne na jeden rok. Pred uplynutím lehoty platnosti udeleného povolenia je štatutár oprávnený povolenie obnoviť, ak podmienky jeho udelenia trvajú. Ak takéto povolenie nie je udelené, užívateľ je povinný z počítača službu alebo súbor odinštalovať, resp. bezpečne odstrániť.

(6) Prevádzkovateľ je oprávnený stanoviť obmedzenia pre používanie internetu zamestnancami.

(7) Zamestnanci majú povolené:

a) sťahovanie súborov z internetu iba v prípade keď je to potrebné pre vykonávanie ich pracovnej činnosti,

b) publikovať na internet iba informácie, ktoré nie sú informáciami internými alebo utajovanými skutočnosťami,
c) používať na prístup do internetu iba technológie (webový prehliadač, prepojenie sietí), ktoré sú na tento účel určené,
d) používať lokálne modemy pre prístup do internetu, registrovať sa na verejných internetových stránkach s použitím pracovnej adresy elektronickej pošty iba v prípadoch, keď ide o plnenie úloh súvisiacich s činnosťou a prevádzkou prevádzkovateľa.

(8) Zamestnanec je pri prístupe do internetu povinný dodržiavať nasledujúce zásady:
a) prístup do internetu využívať predovšetkým v súlade so svojou pracovnou náplňou a činnosťou príslušného organizačného útvaru,
b) rešpektovať všeobecné etické pravidlá slušného správania užívateľov na internete a zdržať sa činností, ktoré by viedli k poškodeniu dobrého mena prevádzkovateľa alebo k iným škodám,
c) komunikácia prostredníctvom Internetu (napríklad elektronická pošta) spravidla nie je chránená pred „odpočúvaním“. V prípade potreby prenosu osobných, dôverných a citlivých údajov sieťou Internet je nevyhnutné tieto riadne zabezpečiť ich zašifrovaním alebo uzamknutím,
d) riadiť sa hláseniami antivírusového programu,
e) nepripájať sa na neznáme internetové stránky s nepreverenym obsahom, ak to nie je potrebné na výkon pracovných úloh,
f) na prístup k verejným internetovým službám nepoužívať heslá, ktoré sa používajú pre prístup k vnútorným informačným systémom.

Čl. 4
Aktualizácia webového sídla úradu

(1) Aktualizáciu verejne prístupného webového sídla má oprávnenie vykonávať len určený zamestnanec, na základe pokynu nadriadeného, vrátane zverejňovania povinných údajov podľa osobitných predpisov.

(2) Oprávnenie na aktualizáciu webového sídla musí vyplývať z popisu pracovných činností zamestnanca, interných predpisov alebo iného písomného pokynu schváleného oprávnenou osobou.

Čl. 5
Elektronická pošta

(1) Elektronická pošta sa používa pre účely internej a externej komunikácie.

(2) Pre elektronickú komunikáciu zamestnanci používajú elektronickú poštu.

(3) Každý zamestnanec má pridelenú emailovú adresu bez diakritiky pred deliacim znakom @ v tvare „meno.priezvisko“. V prípade identického mena aj priezviska viacerých používateľov sa použije číslo za priezviskom (bez medzery).

(4) Použitie iných systémov elektronickej pošty (napr. verejné poštové servery) pre výmenu informácií pracovného charakteru a interných informácií je zakázané.

(5) Každý zamestnanec je zodpovedný za obsah správ, ktorý musí byť v súlade so všeobecnými etickými pravidlami slušného správania užívateľov na internete aj pri písomnom styku.

(6) Zamestnanci majú zakázané používanie elektronickej pošty na prenos softvéru alebo informácií, ktorými môže byť spôsobené porušenie autorských práv alebo právnych predpisov.

(7) Pre zaistenie bezpečnosti informačného systému pred škodlivými programami sú implementované opatrenia obmedzujúce odosielanie a prijímanie správ s určitými typmi príloh.

(8) Prevádzkovateľ je oprávnený zamestnancom príkazom stanoviť obmedzenia pre používanie elektronickej pošty.

(9) Správa s internou alebo chránenou informáciou musí byť uzamknutá alebo šifrovaná (napríklad uložiť informáciu do heslom chráneného ZIP archívu, zašifrovať súbor MS Office) v prípade jej posielania mimo lokálnej domény a heslo k rozšifrovaniu postúpiť adresátovi inými kanálmi (napr. SMS, telefonicky).

(10) Pri odosielaní správy elektronickej pošty sú zamestnanci povinní:
a) v texte správy identifikovať sa menom alebo prostredníctvom vizitky,
b) uviesť predmet správy,
c) pred odoslaním musia obsah správy, vrátane príloh posúdiť z hľadiska dôvernosti.

(11) Zamestnanci sú ďalej povinní:
a) pravidelne kontrolovať svoju poštovú schránku, s cieľom zabezpečiť včasné vybavenie prijatej pošty,
b) pravidelne vykonávať údržbu svojej poštovej schránky (mazať nepotrebné správy, presúvať správy do svojej osobnej schránky na pracovnej stanici.

(12) Zamestnanci majú zakázané:
a) falšovanie, zmenu alebo potláčanie identity odosielateľa správy,
b) čítať alebo posielať správy prostredníctvom používateľského účtu iného zamestnanca, okrem prípadov delegovania právomocí,
c) posielať prijaté správy internou informáciou ďalšiemu prijímateľovi, okrem prípadov, keď je to nevyhnutné na plnenie pracovných povinností alebo na pokyn priameho nadriadeného,
d) posielať hromadné správy, okrem prípadov, keď je to nevyhnutné na plnenie pracovných povinností alebo na pokyn priameho nadriadeného,
e) vytvárať a distribuovať falošné výstražné správy,
f) používať vulgárne a znevažujúce výrazy v komunikácii.

(13) Všetky prijaté a odoslané správy elektronickej pošty sú zálohované po dobu 1 roka. V prípade vymazania správ elektronickej pošty užívateľom alebo aj v prípade nedostupnosti užívateľskej schránky elektronickej pošty môže užívateľ požiadať určeného zamestnanca o obnovenie správ elektronickej pošty.

3. ČASŤ
VÝMENA A ZVEREJŇOVANIE ÚDAJOV

Čl. 6
Výmenné formáty pre textové súbory

(1) Pri výmene a zverejňovaní údajov pre textové dokumenty prevádzkovateľ používa jeden z nasledujúcich typov formátov súborov:
a) Rich Text Format (.rtf),
b) Text Format (.txt),

c) Hypertext Markup Language (.hmtl),
d) Portable Document Format (.pdf),
e) Extensible Markup Language (.xml),
f) Open Document Format (.odf).

(2) Odporúčané požiadavky:
a) používanie formátu Portable Document Format (.pdf) pri výmene údajov pre textové dokumenty,
b) obsah dokumentu vo formáte Portable Document Format (.pdf) spracúvať ako textový dokument,
c) používanie formátu (.doc) na internú potrebu, pokiaľ to technické podmienky umožňujú.

(3) Používatelia sú povinní vytvárať textové dokumenty vo formáte Rich Text Format (.rtf) pri výmene údajov. Táto povinnosť sa vzťahuje na odosielanie dokumentov v prílohách správ elektronickej pošty.

(4) Odosielať dokumenty elektronickou poštou vo formáte (.doc) je zakázané s výnimkou prípadov, ak druhá strana vopred súhlasí. Textové dokumenty vo formáte (.doc) je povolené používať iba na internú potrebu (intranet, výmena dokumentov).

(5) Na verejne prístupnom webovom sídle Úradu je povolené zverejňovať iba textové dokumenty vo formáte (.pdf) alebo (.rtf). Určený zamestnanec pred zverejnením dokumentov vo formáte (.pdf) vymaže z dokumentu informácie a vlastnosti popisujúce dokument.

Čl. 7
Výmenné formáty pre kompresiu dát

Pre kompresiu dát pri výmene údajov sú zamestnanci povinní používať formát Zip.

Čl. 8
Výmenné formáty pre grafiku a statické obrazy

(1) Povinnou požiadavkou je používanie jedného z nasledujúcich typov formátov pri výmene a zverejňovaní údajov pre grafiku a statické obrazy:
a) Portable Document Format (.pdf),
b) Graphics Interchange Format (.gif),
c) Joint Photographic Experts Group (.jpg),
d) Tagged Image File Format (.tif).

(2) Určený zamestnanec zverejňuje obrázky na verejne prístupnom webovom sídle iba vo formáte (.gif) alebo (.jpg).

Čl. 9
Výmenné formáty pre audio a video súbory

(1) Pre výmenu audio a video súborov je v Úrade povolené používanie formátov:
a) Moving Picture Experts Group (.mpg, mpeg., .mp4, .m4a a podobne),
b) OGG (.ogg, .oga, .ogv, .ogx),
c) Waveform Audio File Format s obsahom kódovaným pomocou Linear Pulse Code Modulation (.wav),
d) Audio Interchange File Format s obsahom kódovaným pomocou Linear Pulse Code Modulation (.aiff, .aif).

(2) Odporúčanou požiadavkou je podpora formátu MP3 pri výmene audio súborov.

Čl. 10
Výmenné formáty pre audio a video streaming

(1) Pre audio streaming pri výmene údajov je v Úrade povolené používanie formátov Ogg Vorbis (.ogg, .oga), MPEG-4 Advanced Audio Coding alebo MPEG-1 Audio Layer III (.mp3).

(2) Pre video streaming pri výmene údajov je v Úrade povolené používanie formátov MPEG-4 part 10, MPEG-4 part 2 alebo Ogg Theora (.ogv).

(3) Pre kontajnerové formáty streamingu je v Úrade povolené používanie formátov MPEG-4 part 14 alebo Ogg.

Čl. 11
Opatrenia pri výmene dátových súborov

(1) Prevádzkovateľ zabezpečí, aby nebolo možné odosielať a prijímať elektronickou poštou súbory vo formátoch, ktoré nie sú uvedené v uvedených výmenných formátoch s výnimkou niektorých bežne používaných proprietárnych dátových formátoch (.rar, .pps, .ppt, .xls, .mdb).

Čl. 12
Súbory obsahujúce tabuľky

(1) Pri výmene a používaní súborov s tabuľkami, ak nie je potrebné zachovať úplnú funkčnosť tabuľkových procesorov, je povinné používanie nasledujúcich formátov:

a) Rich Text Format (.rtf),
b) Text Format (.txt),
c) Hypertext Markup Language (.hmtl),
d) Portable Document Format (.pdf),
e) Extensible Markup Language (.xml),
f) Open Document Format (.odf).

(2) Ľubovoľný formát súboru obsahujúceho tabuľky je možné použiť len v prípade, ak má byť zachovaná úplná funkčnosť tabuľkových procesorov pri zverejňovaní na webovej stránke.

4. ČASŤ
ŠIFROVANIE

Čl. 13
Šifrovanie

(1) Šifrovanie informácií je povinným bezpečnostným opatrením pre účinnú ochranu dôverných informácií pred ich prezradením, prípadne zneužitím.

(2) Požiadavky na šifrovanie informačných aktív vyplývajú z ich klasifikácie.

(3) Za schvaľovanie šifrovacích prostriedkov do prevádzky, za implementáciu šifrovacích prostriedkov, ich údržbu, aktualizáciu, zaškolenie a servis používateľom zodpovedá prevádzkovateľ.

(4) Za požadovanie šifrovacích prostriedkov a ich aplikovanie zodpovedá vlastník informačného aktíva.

(5) Za inštalovanie a odovzdanie do používania schváleného šifrovacieho prostriedku používateľovi zodpovedá určený zamestnanec.

(6) Požiadavky tretej strany na používanie neschválených šifrovacích prostriedkov schvaľuje prevádzkovateľ.

5. ČASŤ
SIEŤOVÁ BEZPEČNOSŤ

Čl. 14
Sieťová bezpečnosť

(1) Cieľom ochrany sietí je implementovať opatrenia na zaistenie bezpečnosti dát a na ochranu pripojených služieb pred neautorizovaným prístupom.

(2) Prevádzkovateľ používa sieť typu Ethernet LAN.

(3) Interná sieť je prepojená do medzirezortnej vládnej siete Govnet, ktorá je prepojená do internetu.

(4) Interná sieť je od verejných sietí oddelená a je primerane chránená firewallom a aplikačnými proxy servermi.

(5) Pripojenie sieťových zariadení do internej siete je riadené a umožnené len sieťovým zariadeniam (počítače, notebooky, sieťové tlačiarne, servery), ktoré sú majetkom prevádzkovateľa a ktoré používajú zamestnanci výlučne na plnenie pracovných úloh.

(6) Je zakázané pripájať do internej počítačovej siete zariadenia, ktoré nie sú majetkom prevádzkovateľa. Takéto zariadenia môže v odôvodnených prípadoch pripájať do internej počítačovej siete len určený zamestnanec. Pripájanie zariadení ktoré nie sú majetkom prevádzkovateľa je povolené iba na WiFi sieť prevádzkovateľa so súhlasom určeného zamestnanca, ktorý poskytne prístupové heslo.

6. ČASŤ
ORGANIZAČNÉ OPATRENIA

Čl. 15
Personálne opatrenia

(1) Pri skončení pracovného alebo obdobného vzťahu je zamestnanec povinný odovzdať pracovnú agendu vrátane spisov, všetky pridelené inventárne predmety, zapožičané knihy a kľúče, výsledky práce v súvislosti s informačnými systémami prevádzkovateľa, ktorými sú najmä programy vrátane dokumentácie a vlastné elektronické dokumenty. Určený zamestnanec zruší prístupové práva odchádzajúceho zamestnanca v informačných systémoch najneskôr ku dňu skončenia pracovného alebo obdobného pomeru.

(2) Všetci zamestnanci musia byť poučení o základných bezpečnostných zásadách predtým, ako získajú prístup k osobným údajom. Poučenie je povinný vykonať štatutár Úradu alebo ním poverený zamestnanec v rozsahu tejto bezpečnostnej smernice a nadväzujúcich pravidiel pre

oblasť bezpečnosti IT. Poučenie musí byť vykonané preukázateľným spôsobom. Doklad o poučení podpísaný zamestnancom musí byť založený do osobného spisu zamestnanca.

(3) Prevádzkovateľ zabezpečí aspoň raz za rok školenie zamestnancov v oblasti informačnej bezpečnosti a odhaľovania bezpečnostných incidentov, s dôrazom na bezpečnostné incidenty, ktoré sú porušením ochrany osobných údajov s rizikom alebo vysokým rizikom pre práva a slobody fyzických osôb v zmysle čl. 33 a 34 Nariadenia.

(4) Pri vzniku pracovného pomeru alebo obdobného vzťahu podpisuje zamestnanec vyhlásenie o zachovávaní mlčanlivosti o osobných údajoch a o skutočnostiach, ktoré v záujme prevádzkovateľa nemožno oznamovať iným osobám. Povinnosť mlčanlivosti trvá aj po skončení pracovného alebo obdobného pomeru.

(5) Zamestnancovi môže byť pridelený technický prostriedok, ktorý je majetkom prevádzkovateľa a je potrebný pre výkon jeho pracovných činností. O prebraní alebo odovzdaní majetku zamestnancom musí byť spísaný Preberací/odovzdávací protokol, v ktorom musí byť uvedená presná identifikácia majetku, identifikácia zamestnanca, ktorý majetok preberá a aj to, či je zamestnanec oprávnený vynášať majetok mimo priestorov prevádzkovateľa. Originál preberacieho/odovzdávacieho protokolu ostáva u zamestnanca zodpovedného za evidenciu majetku, kópiu protokolu si prevezme zamestnanec.

(6) Osoby, ktoré vykonávajú pre prevádzkovateľa činnosti vyplývajúce zo zmluvných záväzkov (ďalej len "tretia strana") a majú prístup do informačných systémov prevádzkovateľa, musia byť poučené o schválenej bezpečnostnej politike prevádzkovateľa a o povinnostiach z nej vyplývajúcich. Poučenie musí byť vykonané preukázateľným spôsobom. Doklad o poučení je súčasťou zmluvy. Majetok prevádzkovateľa, elektronické dokumenty, databázy a prístupy do informačných systémov sa tretej strane zapožičiavajú alebo poskytujú na základe protokolu.

(7) Súčasťou zmluvy s treťou stranou je aj vyhlásenie o zachovávaní mlčanlivosti počas a po skončení zmluvného vzťahu o osobných údajoch a o skutočnostiach, o ktorých sa dozvedela v súvislosti s vykonávaním činností pre prevádzkovateľa a ktoré v záujme prevádzkovateľa nemožno oznamovať iným osobám.

(8) Pred skončením zmluvného vzťahu s treťou stranou je tretia strana povinná protokolárne odovzdať všetok zapožičaný majetok, kľúče a výsledky práce v súvislosti s informačnými systémami prevádzkovateľa, ktorými sú najmä programy vrátane dokumentácie a vlastné elektronické dokumenty. Správca IT zruší všetky prístupové práva tretej osoby do informačných systémov prevádzkovateľa po ukončení činností, najneskôr v posledný deň trvania zmluvného vzťahu. Súčasťou je vyhlásenie tretej osoby, že odstránila zo svojich zariadení všetky údaje získané z informačných systémov prevádzkovateľa a iné interné dokumenty prevádzkovateľa.

7. ČASŤ
FYZICKÁ BEZPEČNOST

Čl. 16
Používanie informačnej techniky

(1) Informačná technika (počítače, notebooky a pod.) musí byť umiestnená v uzamykateľných priestoroch. Miestnosť, v ktorej sa nachádza informačná technika, musí byť pri každom odchode zamestnanca uzamknutá. Po skončení pracovnej zmeny je zamestnanec povinný:

a) vypnúť osobný počítač alebo notebook,
b) uzamknúť skrine s materiálmi obsahujúcimi osobné údaje.

(2) Informácie prenášané prostredníctvom telekomunikačných zariadení (faxom, telefonicky) a nešifrovanej elektronickej pošty nie sú bezpečné a môžu byť odpočúvané.

(3) Pred prenosom informácií prostredníctvom faxu musí zamestnanec vykonávajúci prenos skontrolovať číslo, informovať prijímateľa o prenášaní informácií a overiť príjem informácií.

(4) Zamestnanci, ktorí zodpovedajú za používanie skenovacích zariadení musia zaistiť, že obsah naskenovaných materiálov je určený len na pracovné účely. Zamestnanci používajúci skenovacie zariadenia musia dodržiavať autorské práva na zdrojové materiály.

(5) Zamestnanec je povinný priebežne vymazávať nepotrebné súbory.

(6) Pri vyraďovaní a likvidácii softvéru, hardvéru a médií, je zamestnanec povinný zaistiť bezpečnú likvidáciu údajov na vyraďovaných zariadeniach a médiách. Rovnako sa postupuje aj v prípade preradenia pamäťových médií na iné využitie, ako na spracovanie (uloženie) osobných údajov alebo iných citlivých informácií, resp. preradenie zariadenia inému zamestnancovi.

Čl. 17
Ochrana prenosných počítačov (notebook)

(1) Každý používateľ, ktorému bol pridelený prenosný počítač (notebook), je zodpovedný za jeho ochranu pred poškodením, zničením, krádežou, zneužitím a prístupom neoprávnených osôb. Používateľ nesmie ponechať prenosný počítač bez dozoru na verejne dostupných miestach, v opustených dopravných prostriedkoch, neuzamknutých miestnostiach alebo na iných miestach, na ktorých môže prísť k ich zneužitiu, krádeži, poškodeniu, zničeniu.

(2) Prístup k zdrojom prenosného počítača musí byť chránený vstupným heslom užívateľa (uložené v systéme BIOS zariadenia); užívateľské dáta na internom disku prenosného počítača musia byť šifrované alebo aspoň pracovné dokumenty musia byť uložené v šifrovanom priečinku alebo šifrovanom virtuálnom disku.

(3) Prístup do prenosných počítačov musí byť chránený pomocou prístupového hesla (pri štarte systému, šetrič obrazovky chránený heslom a pod.).

Čl. 18
Ochrana prenosných médií

(1) Každý zamestnanec, z ktorého pracovnej činnosti vyplýva potreba uchovávania údajov na prenosnom médiu (netýka sa centralizovaného zálohovania) zodpovedá za aplikovanie ustanovení smernice. V prípade uchovávania niektorých interných a chránených informácií, mala by byť ich ochrana zabezpečená šifrovaním, ak to technické a programové prostriedky umožňujú (napr. šifrovaný virtuálny disk pomocou programu TrueCrypt).

(2) Prenosné médium musí byť pred použitím skontrolované na prítomnosť vírusov rezidentnou antivírusovou ochranou, nachádzajúcou sa na každej pracovnej stanici. Kontrolu vykonáva zamestnanec, ktorý dané médium používa.

(3) Každé vynesenie média s dôvernými informáciami alebo osobnými údajmi mimo priestorov prevádzkovateľa, musí zamestnanec oznámiť nadriadenému a podlieha jeho schváleniu. Výnimkou je iba opakovaný prenos toho istého média, v tom prípade však musí byť upovedomený nadriadený, že dôjde k viacnásobnému prenosu.

(4) Je zakázané odstraňovať z médií ochranu proti zápisu, pokiaľ boli pridelené na používanie s takouto ochranou.

(5) Zverenie a stráženie médií s osobnými údajmi je povolené len oprávnenej osobe.

(6) Zamestnanci sú po použití prenosného média povinní zlikvidovať jeho obsah vymazaním. Pri vymazávaní údajov z médií sú oprávnené osoby povinné riadiť sa týmito zásadami:

a) disky, musia byť preformátované úplným formátovaním,
b) prepisovateľné CD disky musia byť znovu inicializované v príslušnom zapisovacom programe,
c) flash disky, pamäťové karty, USB disky a pod. musia byť úplne vymazané, prípadne, ak to obslužný program dovoľuje, nanovo formátované,
d) v prípade chránených informácií musí byť informačný obsah prenosného média prepísaný.

(7) Nepotrebné súbory s osobnými údajmi na médiách zamestnanec bezodkladne vymaže.

(8) Nepotrebné a nepoužiteľné médiá zamestnanec fyzicky zlikviduje, v prípade potreby v súčinnosti so správcom IT. Nepotrebné a nepoužiteľné médiá, ktoré sú evidované, odovzdá zamestnanec na vyradenie alebo iné použitie určenému zamestnancovi. Zamestnanec, ktorý zodpovedá za vyradenie média, zabezpečí jeho fyzickú likvidáciu tak, aby údaje aj nosič boli nevratne znehodnotené.

(9) Fyzicky zlikvidované musia byť predovšetkým tie médiá, ktorých obsah sa nedá natrvalo vymazať.

Čl. 19
Pravidlo čistej obrazovky a čistého stola

(1) Na počítačoch a notebookoch musí byť nastavený šetrič obrazovky chránený heslom, ktorý sa spúšťa automaticky po určenom čase nečinnosti (10 min). Pred pridelením počítača alebo notebooku na prácu nastavuje šetrič obrazovky správca IT.

(2) Pri každom odchode od svojho počítača je používateľ povinný uzamknúť počítač systémovými prostriedkami (odhlásením sa z operačného systému alebo systémovým uzamknutím).

(3) Pri odchode z pracoviska po ukončení práce je používateľ počítača povinný ukončiť aplikáciu a vypnúť operačný systém a osobný počítač.

(4) Ak zamestnanec skončí pracovnú zmenu alebo odchádza z pracoviska na dlhšiu dobu, musí zabezpečiť, aby sa na jeho pracovnom stole nenachádzali žiadne materiály alebo médiá obsahujúce osobné údaje alebo citlivé informácie. Tieto materiály je povinný uložiť do uzamykateľnej skrine, resp. trezoru.

(5) Počas pracovnej doby je nutné:

a) v prítomnosti neoprávnených osôb mať materiály vždy pod dohľadom a neumožniť týmto osobám prístup k osobným údajom alebo k iným interným a citlivým materiálom alebo médiám,
b) pri odchode od počítača zabezpečiť informačný systém proti prístupu k údajom – zatvoriť aplikáciu, zabezpečiť heslom.

Čl. 20
Ochrana tlačených informačných aktív

(1) Zamestnanci sú povinní zachovávať obozretnosť pri podávaní chránených informácií (napr. osobných údajov) pred návštevníkmi.

(2) Informačné aktíva nesmú byť ponechávané bez dozoru voľne dostupné na chodbách a v iných neuzamknutých miestnostiach alebo na iných miestach. Informačné aktíva nesmú byť ponechané bez dozoru vo verejne prístupných miestach, opustených dopravných prostriedkoch a pod.

(3) S tlačenými materiálmi je potrebné zaobchádzať podľa ich citlivosti. Je potrebné aplikovať všetky relevantné opatrenia, ktoré zabezpečia ochranu vytlačených informácií pred neoprávnenými osobami.

(4) Zamestnanec je povinný v prípade tlače dokumentov obsahujúcich osobné údaje alebo iné chránené informácie zabezpečiť, aby sa počas tlačenia neoboznámila s nimi neoprávnená osoba. Tlačené materiály obsahujúce chránené informácie musia byť ihneď po ich vytlačení odobraté oprávnenou osobou, ktorá ich tlačila a uložené na zabezpečené miesto. To sa uplatňuje aj pri kopírovaní dokumentov. Nadbytočné a chybné dokumenty je zamestnanec povinný bez zbytočného odkladu zlikvidovať skartovaním.

Čl. 21
Správa kľúčov

(1) Všetky kľúče od kancelárií, vchodových dverí do priestorov prevádzkovateľa a ostatných miestností prevádzkovateľa spravuje určený zamestnanec. Duplikáty sa nachádzajú u správcu budovy.

(2) Kľúče od bezpečnostných schránok (trezor, bezpečnostná plechová skriňa) spravuje určený vedúci zamestnanec, alebo poverený zamestnanec a iba v prípadoch, keď si to vyžaduje bezpečnosť obsahu informácií uchovávaných v bezpečnostnej schránke môže byť správa (úschova) kľúčov zverená inému zamestnancovi.

(3) Každému zamestnancovi pri nástupe do zamestnania je pridelený jeden kľúč od dverí do kancelárie, v ktorej bude vykonávať pracovnú činnosť, a jeden kľúč od vchodových dverí do priestorov. Zamestnancovi je možné prideliť aj kľúče od iných dverí, ale len v prípade, že si to vyžaduje jeho pracovná náplň alebo zabezpečenie pracovných úloh a pridelenie kľúča schváli oprávnená osoba.

(4) Zamestnancovi môže byť pridelený aj kľúč od bezpečnostnej schránky, ak si to vyžaduje jeho pracovná náplň a pridelenie kľúča povolí oprávnená osoba.

(5) Kľúče od dverí do miestností alebo bezpečnostných schránok môžu byť pridelené aj iným osobám ako zamestnancom, a to iba v prípade, ak je to nevyhnutné na plnenie úloh prevádzkovateľa a pridelenie kľúča povolí štatutár.

(6) Kľúče sa preberajú a odovzdávajú oproti podpisu. O prevzatí a odovzdaní kľúča zamestnancovi alebo inej osobe vyhotoví písomný záznam zamestnanec poverený správou kľúčov.

(7) Kľúče od uzamykateľných miestností sú uložené aj u správcu budovy.

(8) V mimoriadnych a odôvodnených prípadoch s povolením prevádzkovateľa je možné zamestnancovi jednorazovo zapožičať nepridelené kópie kľúčov od kancelárií alebo sprístupniť kanceláriu:

a) zamestnancovi je možné krátkodobo zapožičať druhú kópiu kľúča, ktorý už má pridelený;

b) vedúcemu zamestnancovi je možné zapožičať kľúč od kancelárie jeho podriadeného zamestnanca.

(9) Zamestnancovi je možné sprístupniť uzamknutú kanceláriu iného neprítomného zamestnanca so súhlasom dotknutého zamestnanca alebo jeho nadriadeného, počas sprístupnenia musí byť v kancelárii prítomný aj iný určený zamestnanec.

(10) O zapožičaní alebo sprístupnení kancelárie je určený zamestnanec prítomný pri sprístupnení kancelárie povinný vyhotoviť písomný záznam s uvedením mena a priezviska vypožičiavateľa, resp. žiadateľa, v prípade sprístupnenia kancelárie, dátumu a času vypožičania kľúča, resp. sprístupnenia, dôvodu a dátumu a času vrátenia kľúča.

(11) Za kľúče zodpovedá zamestnanec, ktorému boli pridelené. Tieto kľúče je zamestnanec v prípade ukončenia pracovného alebo iného obdobného pomeru povinný odovzdať určenému zamestnancovi.

(12) Každú stratu kľúča, ktorý bol zamestnancovi pridelený, je zamestnanec povinný bezodkladne nahlásiť štatutárovi.

Čl. 22
Vstup do budovy a priestorov

(1) Vstup do priestorov prevádzkovateľa je umožnený zamestnancom alebo osobám, ktoré majú uzatvorenú dohodu o vykonaní práce mimo pracovného pomeru alebo inú zmluvu o pravidelnom výkone práce v priestoroch prevádzkovateľa pomocou kľúča a/alebo RFID karty, ktoré im boli pridelené.

(2) Osobám, ktoré nie sú zamestnancami alebo nemajú uzatvorenú dohodu o vykonávaní práce mimo pracovného pomeru ani inú zmluvu o pravidelnom výkone práce v priestoroch prevádzkovateľa (ďalej len „cudzia osoba“), môže byť umožnený vstup bez sprievodu zamestnanca len počas stránkových hodín. Zamestnanec je povinný dbať na to, aby cudzia osoba nezostala v kancelárii sama.

(3) Upratovacie, údržbárske a podobné práce v miestnostiach, kde sú uložené dôležité informačné aktíva (napr. serverovňa) sa vykonávajú len so súhlasom a vedomím určeného zamestnanca a za prítomnosti ním povereného zamestnanca. Osoby vykonávajúce tieto práce musia byť vopred riadne poučené o zákaze akokoľvek manipulovať s elektronickými zariadeniami bez predchádzajúceho súhlasu.

(4) Určený zamestnanec zabezpečí, že všetky opravy a úpravy a akýkoľvek iný zásah na informačných aktívach budú vykonávať len kvalifikované osoby, konajúce na základe platného, vopred daného poverenia, resp. súhlasu.

Čl. 23
Režimové pracovisko

(1) Režimové pracovisko je zabezpečená oblasť, na ktorú sa vzťahuje prísnejší režim (bezpečnostné opatrenia) ako na ostatné oblasti (pracoviská).

(2) Režimovým pracoviskom je technická miestnosť so servermi (ďalej len: „serverovňa“).

(3) Do serverovne majú prístup len určení zamestnanci, správca IT, bezpečnostný správca. Iné osoby sa môžu v serverovni zdržiavať len za prítomnosti poverených osôb.

(4) Náhradný kľúč od serverovne je uschovaný v zapečatenej obálke v kancelárii štatutára Úradu.

Čl. 24
Ostatné opatrenia

(1) Zamestnanec je povinný pri každom opustení kancelárie v prípade, že v miestnosti už nie je iný zamestnanec, kanceláriu uzamknúť a kľúč vziať so sebou.

(2) Pred odchodom je zamestnanec povinný uzamknúť bezpečnostné schránky a skontrolovať uzatvorenie oblokov vo svojej kancelárii.

(3) Svojvoľné premiestňovanie inventárnych predmetov medzi jednotlivými kanceláriami je zakázané. Všetky zmeny uvedeného charakteru musia byť vykonané so súhlasom štatutára Úradu.

(4) V prípade, že na plnenie predmetu zmluvy s treťou stranou (dodávatelia, externí spolupracovníci, orgány verejnej správy, fyzické osoby vykonávajúce pre prevádzkovateľa činnosť na základe zmluvných záväzkov) je potrebný prístup k aktívam (osobným údajom), pri uzatváraní zmluvného vzťahu medzi treťou stranou a prevádzkovateľom, musí byť:

a) menovaný zástupca tretej strany a zástupca prevádzkovateľa za informačnú bezpečnosť,
b) tretia strana informovaná o zásadách ochrany osobných údajov,
c) tretia strana informovaná o právach a povinnostiach, vyplývajúcich z bezpečnostných smerníc, a to predtým, ako získa prístup k informačným systémom v prípade, že si prístup vyžaduje plnenie predmetu zmluvy,
d) osobami poverenými prevádzkovateľom zabezpečené prijatie takých technických, organizačných a personálnych podmienok pre činnosť tretej strany tak, aby nebola narušená bezpečnosť spracúvania osobných údajov. Zástupca prevádzkovateľa je povinný zabezpečiť, aby boli v zmluve s treťou stranou o poskytovaní služieb súvisiacich s informačnými systémami uvedené bezpečnostné požiadavky na služby a zabezpečiť kontrolu bezpečnostných požiadaviek podľa bezpečnostných smerníc.

(5) Tretia strana pri plnení predmetu zmluvy s prevádzkovateľom je povinná dodržiavať zásady ochrany osobných údajov, s ktorými bola oboznámená, predovšetkým povinnosti oprávnených osôb zdržať sa akéhokoľvek konania, ktoré by poškodzovalo záujmy a dobré meno prevádzkovateľa.

(6) V prípade zistenia nebezpečenstva hroziaceho informačným systémom a citlivým údajom v nich, tretia strana počas plnenia predmetu zmluvy oznámi túto skutočnosť zástupcovi prevádzkovateľa. Po splnení predmetu zmluvy treťou stranou je tretia strana povinná:

a) dodržiavať mlčanlivosť o skutočnostiach a citlivých údajoch, s ktorými prišla do styku v spojitosti s plnením zmluvného vzťahu voči prevádzkovateľovi,
b) vrátiť pridelené zariadenia, ktorými sú najmä počítače, pamäťové médiá, a ďalšie informačné aktíva, ktorými sú najmä programy, dokumenty a údaje, v prípade, ak jej boli poskytnuté za účelom splnenia predmetu zmluvy,
c) odovzdať výsledky práce v súvislosti s informačnými systémami, ktorými sú najmä programy vrátane dokumentácie a vlastné elektronické dokumenty, ktoré boli predmetom zmluvy.

(7) Po splnení predmetu zmluvy treťou stranou zástupca prevádzkovateľa:

a) prevezme predmet plnenia zmluvy od tretej strany, zruší prístupové práva tretej strany k aktívam informačného systému/systémov, prevezme od tretej strany zariadenia, ktoré jej boli pridelené za účelom splnenia predmetu zmluvy,

b) vyhotoví písomný záznam o prevzatí predmetu zmluvy a technických zariadení, pridelených tretej strane na účely splnenia predmetu zmluvy. Záznam musí byť podpísaný obidvomi zmluvnými stranami a musí byť na ňom uvedený dátum prevzatia.

8. ČASŤ
ANTIVÍRUSOVÁ OCHRANA

Čl. 25
Všeobecné požiadavky na ochranu pred vírusmi

(1) Vírus alebo iný škodlivý softvér môže spôsobiť prevádzkovateľovi vážne škody od zničenia alebo poškodenia údajov spracúvaných v informačných systémoch až po prezradenie údajov.

(2) Na antivírusovú ochranu pracovných staníc je primárne určený softvérový systém, ktorý je automaticky pravidelne aktualizovaný. Používatelia majú zakázané odinštalovanie, zablokovanie alebo zmenu konfigurácie antivírusovej ochrany.

(3) Za inštaláciu, aktualizáciu, zmeny konfigurácie a previerky antivírusových systémov, ako aj za bezodkladné riešenie problémov spojených s existenciou vírusov, zodpovedá správca IT.

(4) Pokiaľ má zamestnanec podozrenie, že jeho antivírusový systém nepracuje alebo nepracuje správne, musí informovať správcu IT. Na vyzvanie správcu IT, resp. ním povereného zodpovedného informatika má používateľ povinnosť poskytnúť mu potrebnú súčinnosť a postupovať podľa pokynov zodpovedného informatika. Zamestnanci majú zakázané používať pracovné stanice, na ktorých antivírusový systém nepracuje, alebo nepracuje správne.

Čl. 26

Antivírusová ochrana pri používaní elektronickej pošty a internetu

(1) Zamestnanci môžu používať prehliadače internetu a softvér pre používanie elektronickej pošty len na takých pracovných staniciach, na ktorých je nainštalovaný antivírusový softvér.

(2) Každá prijatá správa elektronickej pošty vrátane príloh je kontrolovaná na prítomnosť vírusov, prípadne iného škodlivého softvéru. Zamestnanci majú zakázané otvárať poštu, ktorá je podozrivá z nákazy vírusom.

(3) Zamestnanci majú zakázané:
a) otvárať elektronickú poštu s podozrivým predmetom správy alebo s podozrivým pôvodom. Pred otvorením príloh musí príjemca správy aspoň rámcovo poznať ich obsah (napr. z podpisu uvedeného v tele správy),
b) otvárať a používať súbor alebo prílohu elektronickej pošty s podozrivým pôvodom. Majú povolené otvárať a používať len tie prílohy elektronickej pošty, ktoré boli prijaté z dôveryhodných a overených zdrojov.

Čl. 27
Postupy pri podozrení z nakazenia vírusom

(1) Ak zamestnanec zistí, že jeho pracovná stanica alebo iný prostriedok bol nakazený vírusom alebo má podozrenie z nákazy, je povinný to hlásiť ako bezpečnostný incident správcovi IT.

(2) Do príchodu správcu IT k nakazenému prostriedku IS majú používatelia zakázané jeho používanie.

(3) Používatelia sa nesmú pokúšať vymazať alebo inak odstrániť podozrivý súbor.

(4) V prípade zistenia vírusovej nákazy alebo pri podozrení z nej, zodpovedný informatik pošle správu elektronickej pošty alebo jej prílohu a informáciu o víruse odosielateľovi a môže ho požiadať o vysvetlenie jej pôvodu a významu.

(5) Opätovné používanie pracovnej stanice, alebo iného prostriedku je možné až na pokyn správcu IT.

9. ČASŤ
RIADENIE PRÍSTUPU

Čl. 28
Zriadenie a zmena prístupového práva

(1) Proces vystavenia žiadosti o prístupové práva, jej schvaľovanie a realizáciu označujeme ako zriadenie prístupového práva.

(2) Pri požadovaní zriadenia prístupového práva k informačným systémom sú všetci zamestnanci povinní uplatňovať zásadu prístupu iba k nevyhnutným informáciám potrebným pre výkon práce.

(3) Uplatňovanie zásady prístupu iba k nevyhnutným informáciám sa vzťahuje aj na všetkých zamestnancov tretích strán, ktorí majú prístup k informačným systémom.

(4) Prístupové práva pre iné osoby ako zamestnancov je možné žiadať iba na dobu určitú (s definovaným koncom platnosti prístupového práva) a na obdobie najviac 6 mesiacov.

(5) Ak potreba priradenia prístupových práv podľa ods. 4) trvá, resp. bude trvať aj po uplynutí doby, na ktorú boli priradené, v dostatočnom časovom predstihu je potrebné znovu požiadať o zriadenie prístupového práva.

Čl. 29
Schvaľovanie žiadosti o prístupové právo

(1) Žiadosti o prístupové práva do IS schvaľuje štatutár Úradu.

(2) Priradenie prístupového práva vykonáva zodpovedný informatik iba na základe správne vystaveného a schváleného formuláru v zmysle tejto smernice do 24 hodín od doručenia žiadosti.

(3) Administrátor po vytvorení prístupového práva pre daného užívateľa odošle elektronickou poštou oznámenie užívateľovi. Ak oznámenie nie je možné odoslať elektronickou poštou, oznámi mu to osobne. Oznámenie obsahuje informácie potrebné pre používanie prístupového práva.

(4) Všetci užívatelia sú povinní chrániť im priradené prístupové práva a dodržiavať pravidlá ochrany prístupových práv.

(5) Správca IT je povinný asistovať užívateľovi pri aktivovaní prístupového práva a zmene prvotného hesla.

(6) Zamestnanec nesmie používať priradené prístupové práva na inú činnosť, ako je stanovená jeho pracovnou zmluvou, inou zmluvou, funkčným zaradením a náplňou práce. Zamestnanec nesmie poskytnúť svoje prístupové práva a identifikátor prístupu inej osobe.

Čl. 30
Zmena prístupového práva

(1) O zmenu prístupového práva žiadajú zamestnanci a ich nadriadení s podrobným uvedením dôvodu zmeny.

(2) Pre realizáciu zmeny prístupového práva platia rovnaké postupy ako sú uvedené pre zriadenie alebo zrušenie prístupového práva.

Čl. 31
Zrušenie prístupového práva

(1) O zrušenie prístupového práva, alebo všetkých prístupových práv, pre konkrétneho užívateľa požiada písomne:
a) užívateľ, ak už nepotrebuje prístupové právo pre konkrétny výkon práce,
b) nadriadený užívateľa, ak už uplynuli dôvody, pre ktoré bolo prístupové právo priradené.

(2) O zrušenie prístupových práv užívateľovi môže mimo priameho nadriadeného požiadať aj vlastník IS alebo správca IS v prípade podozrenia z narušenia bezpečnosti IS, vlastníckych oprávnení a kompetencií.

(3) Žiadosť je možné podať elektronickou poštou priamo správcovi IT. Správca IT je povinný vykonať okamžité zrušenie prístupových práv užívateľa uvedených v žiadosti.

(4) Určený zamestnanec je povinný zaslať správcovi IT elektronickou poštou oznámenie o ukončení pracovného alebo obdobného pomeru zamestnanca najneskôr 3 dni pred jeho skončením. V oznámení je uvedené meno a priezvisko zamestnanca, dátum ukončenia pracovného alebo obdobného pomeru.

(5) Správca IT je povinný vykonať zrušenie prístupových práv pre užívateľov najneskôr do 16. hodiny v deň ukončenia pracovného alebo obdobného pomeru.

(6) V prípadoch ak ide o výpoveď z dôvodu porušenia pracovnej disciplíny určený zamestnanec bezodkladne vydá príkaz správcovi IT na okamžité zrušenie všetkých prístupových práv dotknutého zamestnanca.

(7) V prípade neprítomnosti správcu IT, ak ide o zrušenie prístupového práva je nutné zamedziť užívateľovi fyzický prístup k informačným systémom.

(8) Správca IT je oprávnený operatívne zrušiť prístupové právo užívateľa v prípade:
a) prešetrovania bezpečnostných incidentov v IS prevádzkovateľa,
b) zistenia porušenia bezpečnostnej politiky prevádzkovateľa.

(9) Správca IT je povinný vykonať záznam do prevádzkového denníka o vykonaných zrušeniach prístupových práv.

10. ČASŤ
BEZPEČNOSTNÝ INCIDENT

Čl. 32
Správa bezpečnostných incidentov

(1) Cieľom správy bezpečnostných incidentov je účinná prevencia a minimalizácia škôd, ktoré by mohli v informačnom systéme spôsobiť bezpečnostné incidenty.

(2) Každý zamestnanec je povinný akékoľvek podozrenie z porušenia bezpečnostných zásad, alebo neštandardné zmeny alebo správanie informačného systému nahlásiť správcovi IT alebo štatutárovi. Nenahlásenie sa považuje za porušenie pracovnej disciplíny.

(3) Pokiaľ zamestnanec v dôsledku chyby programových alebo technických prostriedkov alebo zlyhania ľudského faktora získa privilegovaný stav, ktorý mu nebol pridelený alebo prístupové práva, ktoré mu neboli pridelené, je povinný túto skutočnosť bezodkladne oznámiť zodpovednej osobe.

(4) Správca IT vedie prevádzkový denník IS, do ktorého zaznamenáva podstatné udalosti súvisiace so systémom, jeho prevádzkou a bezpečnosťou. Do prevádzkového denníka sa zaznamenávajú predovšetkým nasledujúce udalosti:

a) poruchy na kľúčových komponentoch (vrátane komunikácie a porúch na dodávke elektrickej energie na pracovisku),
b) opravy, údržby a zásahy do kľúčových komponentov IS,
c) zmeny prístupových hesiel privilegovaných používateľov (napr. správca systému),
d) vykonanie preventívnej prehliadky a testovania systému alebo jeho komponentov (vrátane kontroly čitateľnosti médií, so záložnými kópiami údajov IS),
e) inštalovanie novej verzie základného alebo aplikačného programového vybavenia,
f) bezpečnostné incidenty (vrátane výskytu počítačového vírusu a iného malware na pracovisku).

(5) Do prevádzkového denníka sa zapisujú minimálne nasledujúce údaje:

a) dátum a čas výskytu zaznamenávaných udalostí,
b) stručný, výstižný a zrozumiteľný popis zaznamenávanej udalosti,
c) meno, priezvisko a podpis osoby, ktorá vykonala záznam.

Čl. 33
Porušenie ochrany osobných údajov

(1) Každý bezpečnostný incident musí byť posúdený vo vzťahu k osobným údajom a súčasne vo vzťahu k dopadom na práva a slobody fyzických osôb.

(2) Každé posúdenie bezpečnostného incidentu z pohľadu ochrany osobných údajov musí byť vykonané za prítomnosti zodpovednej osoby.

(3) Pre identifikáciu dopadov pre práva a slobody fyzických osôb je potrebné použiť dopady definované v recitáli 75 Nariadenia v spojení s právami a slobodami definovanými Ústavou Slovenskej republiky.

(4) Osoba, ktorá sa dozvie o bezpečnostnom incidente je povinná nahlásiť bezpečnostný incident zodpovednému zamestnancovi podľa čl. 32 tejto smernice a Zodpovednej osobe obratom, najneskôr do 1 hodiny od momentu, kedy sa o bezpečnostnom incidente dozvedel.

(5) Zodpovedná osoba spoločne zo zamestnancom podľa čl. 32 vyhodnotí bezpečnostný incident a vykoná analýzu dopadu na práva a slobody fyzických osôb v zmysle Nariadenia.

(6) V prípade, že existuje riziko pre práva a slobody fyzických osôb, Zodpovedná osoba nahlási porušenie ochrany osobných údajov v lehote do 72 hodín od momentu, kedy identifikovala riziko pre práva a slobody fyzických osôb.

(7) V prípade, že existuje vysoké riziko pre práva a slobody fyzických osôb, Zodpovedná osoba zabezpečí oznámenie porušenia ochrany osobných údajov všetkým dotknutým osobám v súlade a v rozsahu podľa čl. 34 Nariadenia.

(8) Oznámenie dotknutým osobám musí byť formulované jasne a jednoducho, musí obsahovať opis povahy porušenia ochrany osobných údajov, informácie a opatrenia minimálne v rozsahu:
a) kontaktné údaje zodpovednej osoby,
b) opis pravdepodobných následkov porušenia ochrany osobných údajov,
c) opis opatrení prijatých alebo navrhovaných prevádzkovateľom s cieľom napraviť porušenie ochrany osobných údajov, vrátane opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov, ak je primerané informáciu o opatreniach poskytnúť (informácia o prijatých opatreniach nesmie ohroziť bezpečnosť informácií).

(9) Oznámenie dotknutej osobe je potrebné vykonať najneskôr v čase nahlásenia porušenia ochrany osobných údajov dozornému orgánu.

11. ČASŤ
OCHRANA OSOBNÝCH ÚDAJOV

Čl. 34
Oprávnená osoba

(1) Spracúvať osobné údaje môže len osoba, ktorá bola poverená prevádzkovateľom, na základe pokynov podľa tejto smernice, iných interných predpisov a právnych predpisov.

(2) Oprávnená osoba je v zmysle § 79 zákona č. 18/2018 Z. z. o ochrane osobných údajov povinná zachovávať mlčanlivosť o osobných údajoch, ktoré spracúva a s ktorými príde do styku.

(3) Povinnosť mlčanlivosti platí aj pre tretie strany a ich zamestnancov, ktorí v rámci svojej činnosti môžu prísť do styku s osobnými údajmi spracúvanými prevádzkovateľom.

(4) Povinnosť mlčanlivosti trvá aj po zániku funkcie oprávnenej osoby alebo po skončení jej pracovného pomeru, obdobného pracovného vzťahu alebo zmluvného vzťahu.

(5) Povinnosť mlčanlivosti neplatí, ak je to nevyhnutné na plnenie úloh súdu a orgánov činných v trestnom konaní podľa osobitného zákona, alebo vo vzťahu k prevádzkovateľovi pri plnení jeho úloh podľa zákona o ochrane osobných údajov; ustanovenia o povinnosti mlčanlivosti podľa osobitných predpisov tým nie sú dotknuté.

(6) Oprávnená osoba môže v súvislosti s protiprávnym nakladaním s osobnými údajmi čeliť trestnému stíhaniu za trestné činy podľa § 247 a § 374 zákona č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov alebo môže voči nej byť vedené disciplinárne konanie.

(7) Osobné údaje sa nesmú poskytovať v telefonickej komunikácii alebo na základe telefonického vyžiadania.

(8) Podrobné informácie o každej spracovateľskej činnosti vedie Zodpovedná osoba formou Záznamov o spracovateľských činnostiach v zmysle čl. 30 Nariadenia.

(9) Oprávnená osoba nesmie osobné údaje spracúvané prevádzkovateľom využiť pre osobnú potrebu, či potrebu inej osoby alebo na iné, než služobné účely podľa tohto záznamu.

(10) Rozsah oprávnení a povolených činností oprávnenej osoby súvisiacich so spracúvaním osobných údajov je vymedzený poučením, opisom pracovných činností zamestnanca, ktorý je neoddeliteľnou súčasťou jeho pracovnej zmluvy, všeobecne záväznými právnymi predpismi, ako

aj platnými internými predpismi prevádzkovateľa. Úroveň prístupových práv k jednotlivým informačným systémom osobných údajov a vymedzenie spracovateľských operácií, ktoré môže oprávnená osoba v rámci jednotlivých informačných systémov osobných údajov vykonávať je predmetom pokynov prevádzkovateľa.

(11) Pri spracúvaní osobných údajov neautomatizovaným spôsobom oprávnená osoba najmä:

a) zachováva obozretnosť pri podávaní chránených informácií, vrátane osobných údajov, pred návštevníkmi prevádzkovateľa alebo inými neoprávnenými osobami,
b) neponecháva osobné údaje voľne dostupné na chodbách a v iných neuzamknutých miestnostiach alebo na iných miestach, vo verejne prístupných miestach, opustených dopravných prostriedkoch a pod.,
c) odkladá spisy a iné listinné materiály na určené miesto a neponecháva ich po skončení pracovnej doby, resp. opustení pracoviska 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 oprávnená osoba je povinná odovzdať prevádzkovateľovi pracovnú agendu vrátane spisov obsahujúcich osobné údaje,
f) v prípade tlače dokumentov obsahujúcich osobné údaje zabezpečuje, aby sa s nimi počas tlačenia neoboznámila neoprávnená osoba; tlačené materiály obsahujúce osobné údaje musia byť ihneď po ich vytlačení odobraté oprávnenou osobou a uložené na zabezpečené miesto; to sa uplatňuje aj pri kopírovaní dokumentov - nadbytočné a chybné dokumenty oprávnená osoba bez zbytočného odkladu zlikviduje skartovaním,
g) uzamyká priestory pri každom opustení v prípade, že v priestoroch už nie je iná oprávnená osoba prevádzkovateľa.

(12) Pri spracúvaní osobných údajov prostredníctvom úplne alebo čiastočne automatizovaných prostriedkov spracúvania oprávnená osoba najmä:

a) informačnú techniku (počítače, notebooky, USB kľúč, a pod.) umiestňuje iba v uzamykateľných priestoroch;
b) dbá na antivírusovú ochranu pracovných staníc sledovaním toho, či správne funguje primárne určený softvérový systém, ktorý je automaticky pravidelne aktualizovaný.

Čl. 35
Vlastník agendy

(1) Vlastník agendy je oprávnenou osobou podľa čl. 34, ktorá dohliada na dodržiavanie ustanovení Nariadenia pri spracúvaní osobných údajov v im zverenej pôsobnosti a poskytuje súčinnosť Zodpovednej osobe pri výkone jej povinností a právomocí.

(2) Vlastník agendy zodpovedá v rozsahu zverenej agendy najmä za:

a) posudzovanie a zabezpečovanie súladu spracúvania osobných údajov s Nariadením, ostatnými právnymi predpismi a touto smernicou,
b) poskytnutie súčinnosti Zodpovednej osobe pri vybavovaní žiadostí dotknutých osôb,
c) poskytnutie súčinnosti Zodpovednej osobe pri vypracovávaní a aktualizácii agend spracovania osobných údajov alebo inej bezpečnostnej dokumentácie,
d) plnenie bezpečnostných požiadaviek stanovených bezpečnostnou dokumentáciou,

e) kontrolu dodržiavania interných predpisov, ktoré upravujú spracúvanie osobných údajov,
f) posudzovanie adekvátnosti prostriedkov používaných pri spracúvaní osobných údajov v súčinnosti so Zodpovednou osobou,
g) navrhovanie spôsobov dosiahnutia súladu spracúvania osobných údajov s Nariadením a internými predpismi Úradu,
h) dohľad pri výbere Sprostredkovateľa alebo Subdodávateľa, za prípravu zmluvy o spracúvaní údajov a za jej obsah v súčinnosti so Zodpovednou osobou,
i) priebežné preverovanie (kontrola) dodržiavania podmienok dohodnutých so Sprostredkovateľom počas trvania zmluvného vzťahu,
j) preskúmavanie zmien procesu spracúvania osobných údajov najmenej raz ročne a bezodkladné hlásenie všetkých zmien spracúvania Zodpovednej osobe,
k) písomné upozornenie (aj elektronickou formou na emailovú adresu Zodpovednej osoby) adresované Zodpovednej osobe, na akékoľvek zistené porušenie ustanovení Nariadenia alebo iných právnych predpisov alebo interných predpisov pri spracúvaní osobných údajov.

(3) Vlastník agendy môže kedykoľvek kontrolovať dodržiavanie ustanovení týkajúcich sa Nariadenia a tejto smernice v rámci svojej pôsobnosti, a to i bez predchádzajúceho upozornenia.

(4) Vlastník agendy je oprávnený pri zabezpečovaní úloh uvedených v ods. 2 požadovať súčinnosť všetkých zamestnancov Úradu v rámci jemu zverenej agendy. Títo sú povinní poskytnúť mu bezodkladne potrebnú súčinnosť.

(5) Vlastník agendy je povinný na výzvu Zodpovednej osoby poskytnúť bezodkladne informácie o stave spracúvania osobných údajov v rámci jemu zverenej agendy.

(6) Vlastník agendy je povinný informovať Zodpovednú osobu o akýchkoľvek zmenách v rozsahu spracúvania osobných údajov v agendách, ktoré spadajú do jeho pôsobnosti (napr. vývoj nových informačných systémov a pod.).

(7) Vlastník agendy špecifikuje požiadavky na ochranu osobných údajov pre technologické systémy spracúvajúce jemu zverenú agendu. Tieto požiadavky sú pre zamestnanca zodpovedného za daný technologický systém záväzné.

(8) Vlastník agendy v spolupráci so Zodpovednou osobou zabezpečí písomné upozornenie pre Prevádzkovateľa, Sprostredkovateľa alebo Subdodávateľa v prípade, ak bol pri spracúvaní osobných údajov zistený nesúlad s Nariadením, prípadne nedodržanie dojednaných podmienok v písomnej Zmluve o spracúvaní osobných údajov.

Čl. 36
Zodpovedná osoba

(1) Zodpovedná osoba zabezpečuje riadenie a koordináciu ochrany osobných údajov v rámci Úradu.

(2) Zodpovedná osoba zodpovedná najmä za:
a) posúdenie či spracúvaním osobných údajov nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb, a to ešte pred začatím spracúvania osobných údajov,
b) zabezpečenie poučenia oprávnených osôb, vrátane Vlastníkov agendy,
c) vybavovanie žiadostí dotknutých osôb,
d) dohľad nad plnením základných povinností Úradu ako Prevádzkovateľa,
e) zabezpečenie súladu činnosti Úradu pri spracúvaní osobných údajov s Nariadením,

f) vedenie záznamov o spracovateľských činnostiach (vrátane zoznamu tokov osobných údajov, zoznamu IS, prostredníctvom ktorých sú spracúvané osobné údaje, zoznamu Sprostredkovateľov),
g) navrhovanie Vlastníkov agend,
h) dohľad nad riešením neštandardných udalostí (incidentov) v oblasti spracúvania osobných údajov v súlade s platným rámcom a procesom pre riadenie bezpečnostných incidentov v podmienkach Úradu,
i) dohľad nad plnením povinností Sprostredkovateľmi a Subdodávateľmi,
j) včasné informovanie jednotlivých organizačných útvarov Úradu o zákonných alebo interných požiadavkách na ochranu informácií, ako aj o základných informáciách týkajúcich sa stratégie ochrany osobných údajov a súkromia v podmienkach Úradu,
k) reportovanie o stave ochrany osobných údajov a zaznamenaných incidentoch pri spracúvaní osobných údajov v rámci Úradu.

(3) Zodpovedná osoba môže písomne (e-mail) delegovať na určeného zamestnanca výkon jednej alebo viacerých právomocí uvedených v ods. 2; o delegovaní právomocí rozhoduje štatutár Úradu.

(4) Zodpovedná osoba zabezpečí potrebnú podporu pre Vlastníka agendy, ktorý upozorní na nesúlad so spracúvaním osobných údajov podľa čl. 35 bod 8.

(5) V prípade, ak nedôjde k náprave pri spracúvaní osobných údajov, Zodpovedná osoba zabezpečí upozornenie štatutára o neodstránení nesúladu pri spracúvaní osobných údajov Prevádzkovateľom, v prípade Sprostredkovateľa alebo Subdodávateľa aj upozornenie Dozorného orgánu.

(6) Zodpovednú osobu písomne určuje štatutár Úradu. Vzor písomného určenia tvorí prílohu 2 tejto smernice. Poverenie sa vyhotovuje najmenej v dvoch rovnopisoch. Vlastníci agendy sú menovaní štatutárom Úradu alebo ním písomne určenou osobou (napríklad Zodpovedná osoba) menovacím dekrétom, ktorý obsahuje náležitosti v rozsahu vzoru tvoriaceho prílohu č. 3 tejto smernice.

(7) Vlastníka agendy musí štatutár Úradu menovať pre každú agendu. Do času jeho vymenovania dohľad vykonáva Zodpovedná osoba.

(8) Zodpovedná osoba vedie zoznam Vlastníkov agend, spolu s kontaktnými údajmi. Zoznam Vlastníkov agend a kontaktné údaje Zodpovednej osoby sú dostupné všetkým zamestnancom Úradu.

(9) Štatutár, alebo ním poverený zamestnanec je povinný bezodkladne informovať Zodpovednú osobu o skončení pracovného pomeru zamestnanca menovaného za Vlastníka agendy.

(10) V prípade skončenia výkonu funkcie Zodpovednej osoby poverený pracovník (hlavný kontrolór obce) bezodkladne informuje štatutára Úradu (elektronicky) o potrebe nového určenia Zodpovednej osoby.

(11) Zodpovedná osoba musí byť odborne spôsobilá na plnenie úloh v oblasti ochrany osobných údajov v rozsahu ustanovenom Nariadením.

(12) Za zabezpečenie vzdelávania Vlastníkov agendy zodpovedá Zodpovedná osoba; Vlastník agendy je povinný sa takého školenia zúčastniť.

12. ČASŤ
KONTROLNÁ ČINNOSŤ

Čl. 37
Kontrolná činnosť

(1) Predmetom kontrolnej činnosti v oblasti ochrany osobných údajov je skúmanie a vyhodnocovanie výkonu spracúvania osobných údajov a činností zameraných na dodržiavanie bezpečnosti informačných systémov, v ktorých Úrad spracúva osobné údaje.

(2) Kontrolná činnosť je zameraná najmä na:

a) dodržiavanie všeobecne záväzných právnych predpisov a interných predpisov upravujúcich ochranu osobných údajov ako chránených informácií,

b) činnosť oprávnenej osoby,

c) činnosť a dodržiavanie ochrany osobných údajov v prostredí Sprostredkovateľov,

d) preverenie a zistenie príčin neoprávnenej manipulácie s osobnými údajmi alebo pokusu narušenia ochrany osobných údajov a na vykonanie potrebných opatrení na zamedzenie nežiadúcich následkov a ich opakovania,

e) plnenie opatrení na nápravu zistených nedostatkov,

f) aktuálnosť záznamov o spracovateľských činnostiach (zoznam tokov údajov, zoznam informačných systémov spracúvajúcich osobné údaje, zoznam Sprostredkovateľov).

(3) Za výkon kontrolnej činnosti v oblasti dodržiavania jednotlivých ustanovení zmlúv s tretími stranami (externými spracovateľmi osobných údajov) zodpovedá vedúci organizačného útvaru, ktorý primárne zabezpečuje kontakt s treťou stranou.

(4) Vlastník agendy zodpovedá za kontrolu a posudzovanie efektívnosti implementácie, udržiavania a dodržiavania navrhnutých bezpečnostných mechanizmov a opatrení.

(5) Kontrolu dodržiavania ochrany osobných údajov v pôsobnosti Úradu v rozsahu ods. 2 tejto smernice vykonáva Zodpovedná osoba.

Čl. 38
Formy kontrolných činností

(1) Formy kontrolných činností sú najmä:

a) periodické kontroly,

b) následné kontroly,

a) náhodné kontroly.

Čl. 39
Periodické kontroly

(1) Periodické kontroly sa vykonávajú štvrťročne. Výkon kontroly sa vzťahuje najmä na:

a) kontrolu nastavenia bezpečnostných parametrov zariadení výpočtovej techniky a komunikačnej infraštruktúry podľa požadovanej konfigurácie (konfigurácia aktívnych sieťových prvkov, klientskych operačných systémov a serverov),

b) kontrolu stavu a zabezpečenia technických miestností s prostriedkami na spracovanie informácií, archívnych miestností, a kancelárií, kde sa spracúvajú osobné údaje,
c) kontrolu zálohovania a manipulácie s pamäťovými médiami a ich označovania,
d) kontrolu v rozsahu čl. 37 ods. 2 tejto smernice.

Čl. 40
Následné kontroly

(1) Následnú kontrolu je potrebné vykonať pri niektorých činnostiach, ktoré môžu mať dopad na stav zabezpečenia informačných systémov a stav zabezpečenia ochrany osobných údajov.

(2) O periodických, následných a náhodných kontrolách a ich výsledkoch je vypracovaný záznam z kontroly. Záznam z kontroly je uložený u Zodpovednej osoby.

Čl. 41
Náhodné kontroly

(1) Náhodná kontrola sa vykonáva najmä na overenie dodržiavania postupov určených smernicou, právnymi predpismi pre oblasť ochrany osobných údajov, ktorých dodržiavanie je závislé na ľudskom faktore.

(2) Náhodnou kontrolou sa overuje najmä dodržiavanie:
a) pravidiel pre používanie internetu,
b) pravidiel pre používanie elektronickej pošty,
c) využívania technických prostriedkov zamestnancami,
d) pravidiel pre bezpečné používanie prenosných počítačov a prenosných médií,
e) pravidiel čistého stola a čistej obrazovky,
f) pravidiel pre uzamykanie kancelárií a priestorov Úradu,
g) pravidiel pre vstup do priestorov Úradu a sprevádzanie osôb v priestoroch Úradu.

Čl. 42
Dokumentácia kontrolných činností

(1) V prípade zistenia nedostatkov v priebehu kontroly sa do Záznamu z kontroly zapíše aj spôsob a časový plán realizácie opatrení na ich odstránenie.

(2) Výsledkom kontroly môže byť aj revízia a/alebo prepracovanie bezpečnostnej politiky na ochranu osobných údajov, súvisiacich smerníc a dokumentov určených na preukazovanie súladu s Nariadením.

(3) Záznam z kontroly bezpečnosti informačného systému obsahuje nasledovné údaje:
a) kontrolujúca osoba,
b) druh (periodicita) kontroly,
c) dátum vykonania kontroly,
d) predmet kontroly,
e) uvedenie predchádzajúcej kontroly ak ide o náhodnú kontrolu,
f) opatrenia na odstránenie nedostatkov zistených kontrolou,
g) dátum vypracovania záznamu,
h) podpis kontrolujúcej osoby a Zodpovednej osoby.

Čl. 43
Kontrolná činnosť Dozorného orgánu

(1) Každý zamestnanec Úradu je povinný informovať Zodpovednú osobu najneskôr do 24 hodín od doručenia oznámenia o kontrole. V prípade, ak oznámenie o kontrole bolo doručené Dozorným orgánom v čase výkonu kontroly (kontrola, ktorá sa neoznamuje vopred), osoba, ktorej bolo oznámenie doručené (spravidla štatutár Úradu alebo osoba poverená konať v mene štatutára Úradu), bezodkladne informuje Zodpovednú osobu.

(2) Zodpovedná osoba musí byť prítomná pri výkone kontroly.

(3) Všetka dokumentácia, súčinnosť, všetky vyjadrenia smerujúce k Dozornému orgánu musia byť predložené Zodpovednej osobe na vyjadrenie.

(4) Zodpovedná osoba zodpovedá za komunikáciu s Dozorným orgánom (v zmysle čl. 39 Nariadenia) pri výkone kontroly a za jeho sprevádzanie počas kontroly. V prípade neprítomnosti Zodpovednej osoby, štatutár Úradu určí zamestnanca (spravidla Vlastníka agendy), na plnenie úloh Zodpovednej osoby pri výkone kontroly v Úrade.

(5) Všetci zamestnanci Úradu sú povinní riadiť sa pokynmi, usmerneniami Zodpovednej osoby a poskytovať jej všetku požadovanú súčinnosť.

(6) Poskytnúť kópie dokladov, dokumentov, pamäťových médií a iných materiálov je možné len na základe písomného potvrdenia o ich prevzatí.

13. ČASŤ
ZÁSADY SPRACÚVANIA OSOBNÝCH ÚDAJOV

Čl. 44
Vzdelávanie zamestnancov

(1) Za výkon všeobecného preškolenia o ochrane osobných údajov novoprijatých zamestnancov Úradu zodpovedá Zodpovedná osoba.

(2) Preškolenie novoprijatých zamestnancov musí byť vykonané v preukázateľnej forme a po podpise príslušným preškoleným zamestnancom a osobou, ktorá vykonala preškolenie, je záznam z preškolenia doručený na založenie do osobného spisu každého zamestnanca.

(3) Preškolenie novoprijatých zamestnancov je vykonané najneskôr do 1 mesiaca od nástupu zamestnanca. Najneskôr v deň nástupu je novoprijatý zamestnanec povinný oboznámiť sa so smernicami a usmerneniami upravujúcimi pravidlá pri spracúvaní osobných údajov.

(4) Za pravidelné vzdelávanie zamestnancov o ochrane osobných údajov, spravidla v intervale jedného roka, zodpovedá Zodpovedná osoba. Zodpovedná osoba môže delegovať realizáciu školenia na Vlastníkov agendy.

Čl. 45
Spracúvanie osobných údajov

(1) Úrad preferuje v maximálne možnej miere získavanie a/alebo poskytovanie osobných údajov formou štandardizovaných zmlúv alebo formulárov.

(2) Pri získavaní osobných údajov je Vlastník agendy povinný dbať na dodržiavanie princípov transparentného informovania dotknutých osôb o spracúvaní osobných údajov v zmysle čl. 13 a 14 Nariadenia.

(3) Vlastník agendy v spolupráci so Zodpovednou osobou navrhne spôsob informovania dotknutých osôb v rozsahu zverenej agendy. Zodpovedná osoba schvaľuje podmienky a spôsob poskytovania informácií dotknutým osobám.

(4) Osobné údaje môžu byť poskytnuté alebo zverejnené na návrh Vlastníka agendy. Návrh musí byť schválený Zodpovednou osobou. Postup pri poskytovaní osobných údajov alebo ich zverejňovaní je upravený v smerniciach alebo iných interných predpisoch.

(5) Osobné údaje môžu byť poskytnuté tretej strane len na základe osobitného predpisu alebo na základe písomnej zmluvy o sprostredkovaní alebo ak dotknutá osoba dala písomný súhlas, ktorý schválila Zodpovedná osoba v každom individuálnom prípade poskytovania alebo zverejňovania osobných údajov.

(6) Vlastník agendy spracuje zoznam osobných údajov pre jednotlivé úkony (procesy), ktoré sa môžu poskytnúť alebo zverejniť. Zoznam schvaľuje Zodpovedná osoba. Vlastník agendy zodpovedá za informovanie zamestnancov o schválenom postupe.

(7) Ak poskytnutie osobných údajov tretej strane prebieha na základe súhlasu dotknutej osoby, Úrad spolu s osobnými údajmi poskytne tretej strane kópiu súhlasu dotknutej osoby.

Čl. 46
Správnosť a aktuálnosť osobných údajov

(1) Za správnosť a aktuálnosť osobných údajov zodpovedá Vlastník agendy. Osobný údaj považuje Úrad za správny, kým sa nepreukáže opak.

(2) V zmluvnom vzťahu s dotknutou osobou sa odporúča stanoviť povinnosť dotknutej osobe nahlasovať akúkoľvek zmenu svojich osobných údajov.

(3) Zamestnanec je povinný v prípade zistenia nesprávnych alebo neaktuálnych osobných údajov bezodkladne informovať príslušného Vlastníka agendy.

(4) Vlastník agendy zodpovedá za bezodkladnú opravu a doplnenie osobných údajov, ktoré sa v priebehu spracúvania stanú neaktuálnymi alebo sa preukáže, že sú nesprávne. O vykonaní opravy alebo likvidácii osobných údajov oboznamuje Vlastník agendy dotknutú osobu a tretie strany, ktorým boli osobné údaje poskytnuté, v lehote do 30 dní od zistenia tohto stavu. Od oznámenia možno upustiť, ak tým nebudú porušené práva dotknutej osoby. O postupe Vlastník agendy informuje Zodpovednú osobu.

(5) Opravu alebo likvidáciu osobných údajov Úrad nevykoná, ak takéto obmedzenie vyplýva zo všeobecne záväzného osobitného zákona, resp. nebol naplnený účel spracúvania osobných údajov.

Čl. 47
Likvidácia osobných údajov

(1) Doba uchovávania jednotlivých kategórií osobných údajov musí byť v súlade s ich účelom spracúvania. Po splnení účelu spracúvania, resp. uplynutí stanovenej doby uchovávania, musí byť zabezpečená bezodkladná likvidácia osobných údajov. Postup pri likvidácii osobných údajov prebieha v súlade s Registratúrnym poriadkom a Registratúrnym plánom Úradu.

(2) Každý zamestnanec je povinný zabezpečiť bezodkladnú likvidáciu osobných údajov, ktorých účel spracúvania pominul (napr. odpisy a kópie dokumentov s osobnými údajmi, osobné údaje nachádzajúce sa na pracovných staniciach, v domovských adresároch, v elektronickej pošte, atď.).

(3) Osobné údaje sa nezlikvidujú iba v nasledovných prípadoch:
a) ak osobitný zákon ustanovuje lehotu spracúvania, ktorá neumožňuje osobné údaje zlikvidovať,
b) ak sú osobné údaje v predarchívnej starostlivosti alebo sú súčasťou archívnych dokumentov.

14. ČASŤ
HAVARIJNÝ PLÁN A PLÁN OBNOVY

Čl. 48
Havarijný plán a plán obnovy činnosti

(1) Cieľom havarijného plánu a plánu obnovy činnosti je zabezpečenie plynulých činností prevádzkovateľa v prípade rozsiahlych bezpečnostných incidentov alebo živelných udalostí. Cieľom havarijného plánu je aj predchádzanie ohrozenia životov alebo zdravia ľudí.

(2) Havarijný plán a plán obnovy činnosti je podrobne upravený v interných predpisoch upravujúcich pravidlá pre informačnú bezpečnosť a kybernetickú bezpečnosť úradu a je platný pre pravidlá a princípy ochrany osobných údajov.

(3) V tejto smernici sú upravené základné princípy a postupy pre havarijný plán a plán obnovy činnosti.

Čl. 49
Havarijné situácie

(1) Havarijné situácie sú mimoriadne udalosti, v dôsledku ktorých nemôže informačný systém a tým aj prevádzkovateľ pracovať v normálnom režime. Havarijné situácie sú vážne bezpečnostné incidenty, ktoré spôsobia prerušenie prevádzky informačného systému s finančným dopadom.

(2) Riadené a kontrolované zastavenie prevádzky IS v každej z možných mimoriadnych udalostí umožňuje
a) minimalizovanie ďalších škodlivých vplyvov,
b) stabilizovanie situácie bezprostredne po havárii,
c) ochranu databáz a informačných systémov,
d) uľahčenie obnovy databáz a informačných systémov.

(3) Havarijné situácie, podľa toho či sú ohrození ľudia a ich zdravie, rozdeľujeme na:
a) situácie, pri ktorých nie sú bezprostredne ohrozené životy alebo zdravie ľudí, napr.
   1. výpadok elektrickej energie na čas dlhší ako 24 hodín,
   2. výpadok komunikačného spojenia na čas dlhší ako 24 hodín,
   3. hardvérové chyby spôsobujúce výpadok kritických služieb na čas dlhší ako 24 hodín,
   4. vírusové infiltrácie spôsobujúce modifikáciu, vymazanie alebo iné formy kompromitácie kritických informácií a dát,
b) situácie, pri ktorých sú bezprostredne ohrozené životy alebo zdravie ľudí, napr.
   1. živelné pohromy (požiar, povodeň, zemetrasenie),

2. individuálny alebo organizovaný zločin (bombové atentáty, sabotáže),
3. priemyselné nehody (chemické znečistenie).

Čl. 50
Havarijný plán

(1) Všeobecné ohrozenie v priestoroch budovy (ďalej len „havarijný stav v budove“), v ktorej sídli prevádzkovateľ a všeobecné ohrozenie prevádzkovateľa (ďalej len „havarijný stav prevádzkovateľa“) vyhlasuje obvyklým spôsobom štatutár Úradu alebo ním poverená osoba.

(2) Stav ohrozenia informačných systémov prevádzkovateľa (ďalej len „havarijný stav IS prevádzkovateľa“) vyhlasuje zodpovedný správca IT.

(3) Pri vyhlásení havarijného stavu v budove nastáva havarijný stav prevádzkovateľa. Pri vyhlásení havarijného stavu prevádzkovateľa nastáva havarijný stav informačných systémov prevádzkovateľa.

(4) Havarijný stav informačných systémov prevádzkovateľa sa vyhlasuje rôznymi formami v závislosti na časových a technických možnostiach, a to ústne, telefonicky, elektronickou poštou, písomne. Konkrétna forma je v kompetencii vyhlasovateľa a zodpovedá havarijnému stavu.

(5) Havarijný stav musí byť oznámený všetkým zamestnancom, ktorí sú v čase vyhlasovania prítomní v priestoroch prevádzkovateľa. Ak sa havarijný stav týka aj iných zamestnancov, oznámi sa bez zbytočného odkladu.

Čl. 51
Rušenie havarijného stavu

(1) Rušiť havarijný stav môže iba ten kto ho vyhlásil. Zrušenie havarijného stavu sa oznamuje všetkým zamestnancom.

(2) V prípade predchádzajúceho vyhlásenia havarijného stavu v budove alebo havarijného stavu prevádzkovateľa, zrušenie havarijného stavu informačného systému prevádzkovateľa môže nastať až po zrušení havarijného stavu prevádzkovateľa, ktoré môže nastať až po zrušení havarijného stavu v budove.

Čl. 52
Plán obnovy činnosti

(1) Po stabilizácii situácie súvisiacej s vyhlásením havarijného stavu IS vedúci škodovej komisie zvolá škodovú komisiu, ak to umožňuje situácia a nebude tým obmedzená činnosť prevádzkovateľa.

(2) Škodová komisia musí mať k dispozícii presný zoznam informačných aktív (hardvéru a softvéru), ktorý jej poskytne správca IT.

(3) V súlade s Nariadením škodová komisia prerokúva aj možné finančné dopady v súvislosti s uplatnením práv fyzických osôb, ktoré boli havarijným stavom dotknuté na svojich právach pri spracúvaní ich osobných údajov.

Čl. 53
Obnovenie prevádzky

(1) Plánovanie obnovy činnosti informačných systémov predstavuje koordináciu stratégie, procedúr a opatrení, ktoré umožnia po havárii obnovu informačných systémov prevádzkovateľa s cieľom minimálneho prerušenia kontinuity činnosti prevádzkovateľa.

(2) Plánovanie obnovy činnosti zahŕňa niekoľko postupov:
a) obnova činnosti informačných systémov v pôvodnom prostredí a na pôvodnom hardvéri,
b) obnova činnosti informačných systémov v náhradnej lokalite a na pôvodnom hardvéri,
c) obnova činnosti informačných systémov s použitím alternatívneho hardvéru v pôvodnom prostredí,
d) obnova činnosti informačných systémov s použitím alternatívneho hardvéru v náhradnom prostredí,
e) vykonávanie niektorých ovplyvnených procesov zabezpečovaných pôvodne informačným systémom prevádzkovateľa pomocou manuálnych prostriedkov.

(3) Prevádzkové zálohy sú umiestnené tak, aby bolo minimalizované riziko zničenia záloh v prípade ohrozenia technickej miestnosti v prípade závažného bezpečnostného incidentu.

Čl. 54
Testovanie plánov

(1) Prevádzkovateľ zabezpečí každoročne rozvrh testovania plánov, pričom zadáva ako a kedy by mal byť testovaný každý prvok plánu. Takéto testy zaisťujú, aby všetci členovia štábov (krízového štábu a štábu pre obnovu činnosti) a iní relevantní zamestnanci prevádzkovateľa tieto plány poznali a vedeli podľa nich konať.

(2) Testovanie plánov sa vykonáva aspoň raz za 6 mesiacov. Na poskytnutie záruky, že plán bude fungovať v reálnych podmienkach, sa používa škála viacerých techník. Tieto zahŕňajú
a) teoretické testovanie rôznych scenárov (diskusia o usporiadaní obnovy činnosti za použitia príkladov narušenia),
b) simulácie reálnych situácií,
c) technické testovanie obnovy zabezpečujúce, aby IS mohli byť obnovené efektívne,
d) testy dodávateľských prostriedkov a služieb,
e) kompletné nácviky (testujúce, či pracovníci, zariadenia, príslušenstvo a procesy dokážu zvládnuť prerušenia).

Čl. 55
Revízia a aktualizácie plánov

(1) Havarijný plán informačných systémov prevádzkovateľa a plán obnovy činnosti informačných systémov prevádzkovateľa musia byť udržiavané pravidelnými revíziami a aktualizáciami zaisťujúcimi ich kontinuálnu účinnosť. Do programu riadenia zmien musia byť včlenené procedúry zaisťujúce primeranú pozornosť venovanú otázkam nielen obnovy činnosti IS, ale aj kontinuity činnosti prevádzkovateľa.

(2) Zodpovednosť za pravidelné previerky plánu obnovy činnosti má určený zamestnanec.

(3) Medzi hlavné situácie, ktoré by mohli vynucovať aktualizáciu plánov sa zahŕňajú akvizícia nových zariadení, alebo aktualizovanie prevádzkových systémov a zmien

a) zamestnancov,
b) adries alebo telefónnych čísiel,
c) činnosti prevádzkovateľa,
d) umiestnenia zariadení,
e) legislatívy,
f) zmluvných partnerov a dodávateľov,
g) procesov.

Zoznam príloh

Príloha 1 Poverenie oprávnenej osoby
Príloha 2 Formulár na určenie Zodpovednej osoby
Príloha 3 Menovací dekrét pre vlastníka agendy
Príloha 4 Vybavovanie žiadostí dotknutých osôb
Príloha 5 Vyhlásenie o spracúvaní osobných údajov (zamestnanci)
Príloha 6 Príloha k Vyhláseniu o spracúvaní osobných údajov zamestnancov
Príloha 7 Vyhlásenie o spracúvaní osobných údajov (uchádzači o zamestnanie)
Príloha 8 Proces likvidácie
Príloha 9 Riadenie prístupov do IS
Príloha 10 Uplatnenie práv dotknutých osôb
Príloha 11 Hlásenie incidentu
Príloha 12 Nahlasovanie bezpečnostného incidentu
Príloha 13 Výkon kontrolných opatrení
Príloha 14 Rozsah oprávnení
Príloha 15 Rozsah zodpovednosti