Obec Stebnícka Huta
Stebnícka Huta 70, 086 33 Stebnícka Huta

BEZPEČNOSTNÉ SMERNICE NA OCHRANU OSOBNÝCH ÚDAJOV

v súlade s nariadením GDPR a zákonom č.18/2018 Z.z. o ochrane osobných údajov

Dokument na základe poskytnutých údajov pre prevádzkovateľa spracoval:
NAJ, s.r.o.
Nová Ľubovňa 1
065 11 Nová Ľubovňa
e-mail: jozef@jendro.sk tel.: 0911 794 174

Bezpečnostné smernice na ochranu osobných údajov schvaľuje starosta obce, ako štatutárny zástupca prevádzkovateľa Obec Stebnícka Huta.

V Stebníckej Hute, dňa 30.04.2019

.....
Gabriel Šiba
starosta obce

Obsah

Zoznam príloh Bezpečnostných smerníc

Príloha č.1 Zoznam informačných systémov podľa účelu
Príloha č.2 Zoznam informačných systémov podľa softvéru a aplikácií
Príloha č.3 Evidencia vypožičiavania a poskytovania dokumentov
Príloha č.4 Evidencia kľúčov a prístupových prvkov
Príloha č.5 Evidencia bezpečnostných incidentov
Príloha č.6 Hlásenie bezpečnostného incidentu
Príloha č.7 Záznam kontrolnej činnosti prevádzkovateľa

Bezpečnostné smernice tvoria súhrn bezpečnostných opatrení, slúžiacich na zvýšenie bezpečnosti spracúvania osobných údajov v informačných systémoch prevádzkovateľa. Vychádzajú z posúdenia vplyvu na ochranu osobných údajov.

Bezpečnostné smernice sú povinní dodržiavať všetci zamestnanci prevádzkovateľa **Obec Stebnícka Huta, Stebnícka Huta 70, 086 33 Stebnícka Huta** vrátane pracovníkov iných organizácii, sprostredkovateľov a ďalších osôb vykonávajúcich činnosti súvisiace s informačným systémom, ktorých k tomu viaže písomný právny akt.

Bezpečnostná smernica č. 1
Zodpovednosť za bezpečnosť osobných údajov

1. **Osoby zodpovedné za bezpečnosť osobných údajov:**
   a) Za bezpečnosť osobných údajov zodpovedá prevádzkovateľ. Prevádzkovateľ môže výkonom dohľadu nad dodržiavaním zákona o ochrane osobných údajov písomne poveriť zodpovednú osobu. Zodpovedná osoba má postavenie určené zákonom na ochranu osobných údajov.
   b) Prevádzkovateľ spracúva osobné údaje prostredníctvom poučených pracovníkov - oprávnených osôb, ktoré musia svojím podpisom potvrdiť poučenie, znalosti a rozsah poverení. Súčasťou poučenia je povinnosť mlčanlivosti v zmysle zákona o ochrane osobných údajov.

2. **Osoby oprávnené na prácu s osobnými údajmi:**
   a) Pracovať s osobnými údajmi je oprávnený personál, vrátane zastupujúceho personálu, a to v rozsahu stanovenom písomným poučením a oprávnením.
   b) Iné osoby pracujúce u prevádzkovateľa nie sú oprávnené prezerať alebo spracovávať osobné údaje.

3. **Povinnosťou prevádzkovateľa je:**
   a) Poznať a dodržiavať ustanovenia zákona o ochrane osobných údajov.
   b) Kontrolovať plnenie povinností oprávnených osôb a zabránenie prístupu nepovolaných osôb k osobným údajom.
   c) Priebežne hodnotiť riziko v ochrane osobných údajov, prijímať opatrenia a ukladať povinnosti oprávneným osobám.
   d) Zabezpečiť aktualizáciu dokumentácie k ochrane osobných údajov.
   e) Vykonávať kontrolu dodržiavania bezpečnostných opatrení a skutočností uvedených v písomných poučeniach a smerniciach.
   f) Pri výbere pracovníkov posúdiť a prihliadať na ich bezúhonnosť, spoľahlivosť, dôveryhodnosť a schopnosť zachovávať mlčanlivosť o chránených údajoch.

4. **Povinnosťou oprávnených osôb je:**
   a) poznať a uplatňovať zásady ochrany osobných údajov stanovené v dokumentácii na ochranu osobných údajov.
   b) poznať a uplatňovať bezpečnostné smernice upravujúce prácu s osobnými údajmi.
   c) používať osobné údaje výhradne na účely súvisiace s ich pracovným zaradením a plnením pracovných povinností; používanie údajov na iný účel je vážnym porušením pracovnej disciplíny.

d) pracovať s údajmi tak, aby sa zabránilo chybám, strate, odcudzeniu, poškodeniu alebo zničeniu údajov a po skončení práce s osobnými údajmi zabezpečiť úschovu písomností, uzamykanie priestorov a vypnutie počítačového systému.

e) informovať prevádzkovateľa, resp. zodpovednú osobu o zistení neoprávnenej manipulácie alebo nájdení chránenej písomnosti, s ktorou nie sú oprávnení pracovať.

f) viesť evidenciu vypožičiavania a poskytnutia výpisu dokumentov.

g) zachovávať mlčanlivosť o bezpečnostných opatreniach a chránených údajoch.

5. **Osoba poverená získavaním osobných údajov je povinná:**

a) preukázať na požiadanie svoju totožnosť a príslušnosť k prevádzkovateľovi osobe, od ktorej osobné údaje požaduje.

b) pri zisťovaní osobných údajov od dotknutej osoby bez vyzvania vopred oznámiť dotknutej osobe, že jej osobné údaje potrebuje pre svojho zamestnávateľa a oznámiť účel spracovania získaných osobných údajov v informačnom systéme prevádzkovateľa.

Bezpečnostná smernica č. 2

Zásady pri zakladaní, aktualizácii a používaní záznamov

1. Prevádzkovateľ vedie záznamy o dotknutých osobách v zmysle platných právnych predpisov.
2. Záznamy a zmeny v záznamoch majú právo vykonávať oprávnené osoby, písomne poverené a poučené.
3. Zisťovanie osobných údajov môžu vykonávať len oprávnené a poučené osoby. Postup a spôsob pri získavaní osobných údajov určuje Bezpečnostná smernica č.1 bod 5. Rozsah údajov zisťovaných od dotknutej osoby je daný osobitnými zákonmi a ich špecifikácia je uvedená v evidenčných listoch informačných systémov.
4. Oprávnená osoba zodpovedná za vedenie dokumentácie zakladá jednotlivé písomnosti v zázname tak, aby zabránila ich vypadávaniu pri bežnej práci so záznamom (lepením, zošívaním, vložením do obalov).
5. Osoba, ktorá používa záznamy a iné písomnosti obsahujúce osobné údaje je povinná zabezpečiť, aby sa s týmito dokumentmi pracovalo v diskrétnej vzdialenosti, mimo priestoru, ktorý je v bezprostrednej blízkosti osôb neoprávnených na styk s práve spracovávanými osobnými údajmi.

Bezpečnostná smernica č. 3

Zásady pre úschovu a likvidáciu písomností obsahujúcich osobné údaje

1. Písomnosti obsahujúce osobné údaje sa ukladajú do uzamykateľných skríň (kartoték) na to určených, uzamykateľných kontajnerov a zásuviek kancelárskeho stola, alebo do iných uzamykateľných zariadení. Požiadavka na uzamykateľnosť zariadení na úschovu písomností nie je záväzná v prípade dostatočnej fyzickej ochrany priestorov. napr. strážnou službou, alarmom alebo uzamknutím vstupných dverí zámkom s bezpečnostnou vložkou.
2. Za úschovu písomnosti obsahujúcej osobné údaje zodpovedá oprávnená osoba, ktorá písomnosť používa. Táto je povinná po skončení používania uložiť písomnosť na chránené miesto alebo ju odovzdať osobe, od ktorej písomnosť získala.
3. Za likvidáciu nepotrebných písomností obsahujúcich osobné údaje zodpovedá poverená osoba, ktorá písomnosť spracováva. Za odovzdanie alebo likvidáciu dokumentov po lehote uloženia zodpovedá osoba zodpovedná za registratúru, resp. štatutár prevádzkovateľa. Dokumenty obsahujúce osobné údaje a iné údaje podliehajúce ochrane musia byť zlikvidované skartovacím zariadením, spálením alebo inou metódou zamedzujúcou čitateľnosť.

Bezpečnostná smernica č. 4

Vypožičiavanie, prenášanie a preprava písomností obsahujúcich osobné údaje

1. Písomnosti, ktoré obsahujú osobné údaje možno zapožičať iba so súhlasom oprávnenej osoby.
2. Písomností obsahujúce osobné údaje je možné zapožičať alebo sprístupniť len osobám a inštitúciám v súlade s presnou špecifikáciou, ktorá je súčasťou evidenčného listu IS.
3. Vypožičanie písomnosti obsahujúcich osobné údaje odovzdávajúca oprávnená osoba zapíše do evidencie vypožičiavania a poskytnutia výpisu dokumentov.
4. Písomnosti s osobnými údajmi je možné prenášať výhradne v zalepenej obálke alebo uzavretom obale, s otvorom prelepeným lepiacou páskou.
5. Písomnosti prenášajú dotknuté osoby alebo na túto činnosť poverený personál prevádzkovateľa.
6. Písomnosti obsahujúce osobné údaje, ktoré je potrebné zaslať sa prepravujú výhradne doporučenou poštovou zásielkou alebo kuriérom.
7. V prípade, že prevádzkovateľ dostane zásielku v poškodenom obale, preverí dôvod poškodenia u doručujúcej osoby a odsúhlasí obsah zásielky s odosielateľom.
8. Odovzdanie písomnosti na prenos alebo prepravu musí oprávnená osoba, ktorá odovzdáva písomnosti na prenos, zaznamenať v ***Evidencii vypožičiavania a poskytovania dokumentov*** (Príloha č.3). Oprávnená osoba, ktorá pripravuje a balí písomnosti na prenos alebo prepravu, je povinná obsah obálky pred zalepením skontrolovať, či nedošlo k zámene odosielaných písomností.
9. Písomnosti určené na prenos alebo prepravu musia byť pevne spojené s obalom tak, aby sa zabránilo nekontrolovanej manipulácii s nimi alebo strate.
10. Po vrátení vypožičaných písomnosti je oprávnená osoba povinná skontrolovať úplnosť písomností a či nedošlo k zámene písomností.

Bezpečnostná smernica č. 5

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 oprávnená osoba.
3. Vydanie tlačeného výstupu z počítačového informačného systému, odpisu, fotokópie alebo inej písomnosti právnickej alebo fyzickej osobe, sa eviduje v ***Evidencii vypožičiavania a poskytovania dokumentov*** (Príloha č.3).

Bezpečnostná smernica č. 6

Prideľovanie kľúčov a povinnosti držiteľov kľúčov

Kľúče používané na vstup do priestorov prevádzkovateľa a otváranie zariadení v ktorých sa uschovávajú počítače, počítačové média a písomnosti obsahujúce osobné údaje (ďalej „evidované kľúče“) sa prideľujú osobám, ktoré určí prevádzkovateľ. Evidované kľúče prideľuje prevádzkovateľ, alebo osoba ním poverená.

Každý evidovaný kľúč musí byť označený jedinečným kódom (znakom), pod ktorým je zapísaný v evidencii.

1. **Prevádzkovateľ vedie Evidenciu kľúčov a prístupových prvkov, ktorá obsahuje:**
   a) identifikačný kód kľúča;
   b) označenie dverí, zariadenia alebo zámku, ktorý sa kľúčom otvára;
   c) dátum zaradenia kľúča do evidencie;
   d) identifikačné údaje osoby, ktorej bol kľúč pridelený;
   e) dátum pridelenia (vrátenia) kľúča a podpis osoby, ktorá preberá (vracia) kľúč.

Osoba, ktorá nie je oprávnená na prácu s osobnými údajmi môže mať pridelené a samostatne používať evidované kľúče od priestorov s IS iba s podmienkou, že pamäťové média AIS, písomnosti DIS a iné dokumenty obsahujúce osobné údaje sú dostatočne zabezpečené proti neoprávnenému prístupu iných ako oprávnených osôb.

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

Bezpečnostná smernica č. 7

Zásady bezpečnosti pri prevádzke informačných a komunikačných technológii

1. **Zodpovedné osoby za bezpečnosť osobných údajov a automatizovaný informačný systém:**
   a) Za bezpečnosť osobných údajov zodpovedá prevádzkovateľ. Ak má prevádzkovateľ určenú zodpovednú osobu, zodpovedná osoba je pri plnení úloh priamo zodpovedná štatutárnemu orgánu prevádzkovateľa. Zodpovedná osoba má postavenie oprávnenej osoby s právom prístupu do informačných systémov prevádzkovateľa v rozsahu potrebnom na plnenie úloh zodpovednej osoby.
   b) Za chod automatizovaného informačného systému zodpovedá prevádzkovateľ. Prevádzkovateľ môže mať určeného správcu automatizovaného informačného systému (ďalej len správca AIS) Správcom AIS, môže byť aj externá osoba, ktorej to vyplýva z uzavretej zmluvy s prevádzkovateľom. V takom prípade musí byť osoba poučená o mlčanlivosti.

2. **Prevádzkovateľ alebo správca AIS určí rozsah oprávnení podľa nasledujúcich pravidiel:**
   a) Získavať osobné údaje od dotknutých osôb môže len oprávnený pracovník, ktorému to vyplýva z pracovnej náplne a je poverenou osobou. Rozsah informačných systémov v ktorých je oprávnený spracovávať osobné údaje je stanovený v písomnom poverení oprávnenej osoby.

b) Osoby oprávnené pracovať s AIS musia prístup len do informačných systémov pre ktoré sú oprávnenými osobami. Prevádzkovateľ alebo správca AIS obmedzí prístup do ostatných informačných systémov.

c) V súvislosti s nastavením prístupov do informačných systémov musí byť každý prístup do operačného systému chránený heslom a prístup do databáz jednotlivých programov obmedzený pre jednotlivých používateľov najlepšie použitím mena a hesla na prístup k jednotlivým databázam programového vybavenia.

2.1. Prideľovanie a zmena hesiel

Novej oprávnenej osobe prideľuje prihlasovacie meno a prvé heslo správca AIS, ktorý ho odovzdá oprávnenej osobe spôsobom zamedzujúcim prezradenie hesla. Nový užívateľ si ihneď po prvom prihlásení do informačného systému zmení heslo podľa uvedených zásad.

V prípade podozrenia o prezradení hesla oprávnená osoba ihneď zmení prístupové heslá do informačného systému a vykoná záznam bezpečnostného incidentu na formulári ***Hlásenie bezpečnostného incidentu*** (Príloha č.6), ktorý prevádzkovateľ zaznamená do ***Evidencie bezpečnostných incidentov*** (Príloha č.5).

Heslá správcu AIS musia byť uložené pre prípad mimoriadnej udalosti v uzamknutej skrinke, najlepšie v zapečatenej obálke. Pri porušení pečate musia byť všetky heslá zmenené.

2.2. Zásady tvorby hesiel

Ako heslo neodporúčame používať z dôvodu veľkého rizika odhalenia slová súvisiace s oprávnenou osobou (meno, dátum narodenia), slová uvedené v slovníku, alebo jediné písmeno abecedy. Heslo má obsahovať kombináciu veľkých, malých písmen, číslic alebo špeciálnych znakov a jeho minimálna dĺžka je 6 znakov. Heslo sa musí pravidelne meniť podľa pravidiel určených prevádzkovateľom pre jednotlivé programové vybavenie.V prípade podozrenia o prezradení hesla oprávnená osoba ihneď zmení prístupové heslá

3. Manipulácia s technickými prostriedkami AIS

a) Pracovné stanice AIS 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 a v jej blízkosti.

b) Používateľ môže manipulovať s pracovnými stanicami AIS (zapínať, používať, vypínať) len v súlade s inštrukciami výrobcu, resp. dodávateľa zariadenia.

c) Používateľ nesmie znižovať životnosť pracovných staníc AIS hrubým zaobchádzaním a ich znečisťovaním.

d) V blízkosti technických zariadení AIS je zakázané jesť, piť a fajčiť, ale aj vykonávať iné činnosti hroziace znečistením technických zariadení (pestovanie kvetov v blízkosti technických zariadení), resp. znížením ich životnosti alebo spoľahlivosti (vibrácie atd.).

e) Používateľ nemôže:
- robiť zásahy do pracovných staníc AIS,
- pripájať k pracovným staniciam ďalšie technické zariadenia,
- odpájať technické zariadenia pracovnej stanice alebo ich premiestňovať,
- manipulovať s ovládacími prvkami pracovnej stanice okrem tých, ktoré sú umiestnené na vonkajšej strane skrinky pracovnej stanice, tlačiarne a krytu monitora (zapínanie, vypínanie a reštartovanie počítača a tlačiarne, vkladanie a vyberanie diskiet a CD z mechaník, výmena tonera, ovládanie nastavenia jasu, kontrastu, príp. ďalších prvkov regulujúcich obraz na monitore), a to za podmienok oboznámenia s ich ovládaním.

f) Opravy a úpravy pracovnej stanice môže vykonávať len prizvaný kvalifikovaný externý špecialista. Externý špecialista pritom môže zasahovať do pracovnej stanice iba so súhlasom štatutára prevádzkovateľa. Používateľ pracovnej stanice je povinný odmietnuť prístup k pracovnej stanici osobe, ktorá sa nepreukáže takýmto súhlasom.
g) 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 externý špecialista pri dodržaní podmienok bodu 6.
h) Odnímateľné pamäťové médiá používané na ukladanie údajov (diskety, CD, USB pamäťové moduly a podobne) musia byť skladované na bezpečnom mieste (uzamykateľný stôl, trezor, a podobne) tak, aby nedošlo k poškodeniu záznamu, predovšetkým nesmú byť vystavované teplotným extrémom, vlhkosti a prašnosti.
i) Do mechaník prenosných pamäťových médií (diskiet, pások, CD) nesmú byť vkladané znečistené alebo poškodené médiá.
j) Pri zapínaní a reštartovaní počítača nesmie byť v disketovej alebo CD mechanike založené pamäťové médium.

4. Manipulácia s programovým vybavením

a) Používateľ môže na pracovných staniciach používať výlučne len programové vybavenie nainštalované s preukázateľným súhlasom štatutára prevádzkovateľa, resp. správcu AIS. Používateľ nemôže na pracovnej stanici inštalovať ani odinštalovať žiadne programové vybavenie a tiež nemôže meniť konfiguráciu programového vybavenia s výnimkou zmien, s ktorými bol riadne oboznámený na školení o používaní príslušného programového vybavenia.
b) Používateľ nemôže vytvárať a distribuovať kópie programového vybavenia inštalovaného na pracovnej stanici.
c) Používateľ nemôže zasahovať do nastavení CMOS pracovnej stanice.
d) Používatelia pred opustením pracoviska sú povinní ukončiť prácu s aplikačným programovým vybavením a odhlásiť sa z operačného systému a nakoniec pracovnú stanicu vypnúť.
e) Pri krátkodobej neprítomnosti môže používateľ, pokiaľ mu to používané programové vybavenie umožňuje, nahradiť odhlásenie sa zo systému a vypnutie pracovnej stanice spustením šetriča obrazovky (ScreenSaver) s heslom.
f) Používatelia sú povinní vykonávať základnú údržbu pracovnej stanice: vyčistenie povrchu pracovnej stanice (obrazovka, klávesnica) aspoň raz mesačne čistenie (odstraňovanie nepotrebných súborov) svojich dátových adresárov a pomocných adresárov operačného systému (vrátane adresára Kôš, resp. Recycle Bin), príp. spustenie profylaktických programov (podľa použitého operačného systému - napr. scandisk, defragmentácia disku a pod.).
g) Používatelia sú povinní po inštalácii novej verzie programového vybavenia po dobu minimálne dvoch týždňov venovať zvýšenú pozornosť činnosti systému a kontrolovať správnosť výsledkov jeho práce. Prípadné odchýlky od požadovaného stavu sú povinní čo najúplnejšie zdokumentovať a bezodkladne ohlásiť správcovi AIS.

5. Pravidlá využívania internetu

Každý používateľ, ktorému bol umožnený prístup do siete Internet, je povinný 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 zamestnávateľa, ktorý mu prístup do siete umožnil. Je preto povinný rešpektovať etické zásady a zdržať sa činností, ktoré by viedli k poškodeniu dobrého mena zamestnávateľa alebo k iným škodám,

c) komunikácia v 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,
d) elektronická pošta sa dá sfalšovať. V prípade, že na základe údajov (obsahu) prijatej elektronickej pošty by mal používateľ realizovať závažné kroky, je povinný si overiť, či predmetnú elektronickú poštu naozaj poslal v nej uvedený odosielateľ,
e) Internet je bohatým zdrojom nielen informácií, ale aj rôznych programov. Pre získavanie programového vybavenia a jeho použitie na počítačových systémoch pracoviska platia rovnaké pravidlá, ako pre ostatné programové vybavenie.

6. Ochrana AIS pred infiltráciami z internetu

a) Prevádzkovateľ a správca AIS zodpovedajú za nainštalovanie a pravidelnú aktualizáciu antivírusového programu na počítačoch, ktoré sú pripojené k sieti Internet.
b) Používateľom je zakázaný akýkoľvek zásah do nastavenia rezidentnej antivírusovej ochrany pracovnej.
c) Používateľ je povinný mesačne alebo v prípade podozrenia na výskyt vírusu otestovať pracovnú stanicu.
d) V prípade, že sa na pracovnej ploche používateľa zobrazí varovanie, že sa na disku, vloženej diskete alebo CD nachádza vírus, používateľ nesmie toto varovanie ignorovať. V prípade, že zavírená disketa alebo CD patrí inému subjektu, používateľ ju viditeľne a výrazne označí ako zavírenú a vráti ju jej majiteľovi. V prípade zavírenia pevného disku, vlastnej diskety alebo CD používateľ túto skutočnosť bezodkladne oznámi správcovi AIS a disketu alebo CD viditeľne a výrazne označí ako zavírenú. V prípade zavírenia CD-R, používateľ je povinný médium viditeľne označiť ako zavírené a vyradiť z používania.
e) V prípade objavenia vírusu v prijatej elektronickej pošte používateľ bezodkladne o tejto udalosti upovedomí správcu AIS, ako aj odosielateľa predmetnej elektronickej pošty. V žiadnom prípade zavírenú elektronickú poštu neposiela inému adresátovi.
f) Je zakázané otvárať prílohy správ elektronickej pošty prijaté od nedôveryhodného odosielateľa alebo podozrivého obsahu správy od známeho odosielateľa (používateľ je povinný hodnovernosť obsahu správy overiť u odosielateľa).

7. Zabezpečenie zálohovania a likvidácie produktov AIS

7.1. Záloha údajov na lokálnom disku pracovnej stanice

Používateľ zodpovedá za zálohovanie údajov na lokálnom disku pracovnej stanice, v prípade, že ich používateľ vytvára a používa pri svojej práci. Používateľ je v takom prípade zodpovedný aj za bezpečné uskladnenie pamäťových médií obsahujúcich záložné kópie údajov. Používateľ je povinný vykonať zálohu údajov na lokálnom disku minimálne **1x za mesiac**.

7.2. Záloha databáz programového vybavenia a údajov na zdieľaných diskoch

Štatutár prevádzkovateľa alebo určený správca AIS zodpovedá za zálohovanie údajov na serveroch, zdieľaných diskoch, externých pamäťových zariadeniach vrátane záloh databáz programového vybavenia.

Záloha údajov databáz informačných systémov prebieha v automatickom režime formou zálohy na pevný disk minimálne **1x za týždeň** a jej kópia je uchovávaná mimo priestorov prevádzkovateľa v zašifrovanom archívnom súbore cez vzdialenú správu, resp. na externom disku. Záloha ostatných dát a dokumentov vytvorených výpočtovou technikou sa vykonáva **1x za mesiac** na externý disk alebo USB kľúč, ktorý je uložený v trezore, resp. v bezpečnostnej skrini.

Ak prevádzkovateľ využíva server v sieti je povinný zabezpečiť zálohu kompletného systému servera tak, aby bolo možné v prípade potreby rýchlo obnoviť základné a aplikačné programové vybavenie, konfiguračné súbory, štruktúru súborového systému a všetky podstatné parametre systému potrebné pre rutinnú prevádzku, najlepšie zrkadlovou zálohou diskov.

V súvislosti s dlhodobým skladovaním databázových údajov je potrebné minimálne raz za rok zálohovať všetky databázy automatizovaného informačného systému na veľkokapacitný nosič DVD, ktorého výhodou je, že zápis je v podstate mechanický a tým aj odolný proti poškodeniu magnetickým poľom.

Správca AIS je povinný minimálne raz za rok overiť možnosť obnoviť informačný systém z vykonanej zálohy.

7.3. Likvidácia produktov IS

Všetky papierové záznamy a nosiče elektronických informácií obsahujúce osobné údaje (zoznamy, výpisy, diskiet, CD média pod.) sú po vylúčení z ďalšieho spracovania (ak nakladanie s nimi nepredpisuje iný zákon, napr. zákon č. 395/2002 Z.z. o archívoch a registratúrach) fyzicky zlikvidované. Tieto výstupy nesmú byť odovzdávané do zberu.

Prepisovateľné nosiče informácií (diskety, usb-kľúče a pod.) sa likvidujú vymazaním, alebo naformátovaním, neprepisovateľné nosiče informácií (CD a pod.) je potrebné fyzicky zlikvidovať napr. zlomením. Pevné disky po vyradení z informačného systému úplne vymazať nízko-úrovňovým formátovaním, prípadne zabezpečiť jeho fyzickú likvidáciu.

V prípade použitia **kamerového systému** so záznamom a monitorovaním priestoru prístupného verejnosti je povinná ho zlikvidovať najneskôr v lehote 15 dní odo dňa nasledujúceho po dni, v ktorom bol záznam vyhotovený, ak osobitný zákon neustanovuje inak, alebo ak nie je využitý na účely trestného konania alebo konania o priestupkoch.

8. Kontrola dodržiavania bezpečnostných opatrení

Kontrolu dodržiavania bezpečnostných smerníc vykonáva poverená osoba na základe poverenia. Pri kontrole sa zameria najmä na plnenie opatrení dôležitých pre zabezpečenie písomných a elektronických aktív pred poškodením alebo zneužitím.

O vykonaných kontrolách sa vedie ***Záznam kontrolnej činnosti*** (Príloha č.7), ktorý obsahuje o každej kontrole minimálne tieto údaje:

a) dátum a čas vykonanej kontroly,
b) rozsah kontroly,
c) zoznam odhalených nedostatkov pri spracovávaní osobných údajov,
d) návrh opatrení na riešenie zistených nedostatkov,
e) odporúčania zmien v organizačných a pracovných postupoch,
f) termín opakovanej kontroly zameranej na zistené nedostatky.

So závermi a zisteniami vykonanej kontroly bezodkladne oboznámi prevádzkovateľa.

Podozrenie na porušenie zákona o ochrane osobných údajov alebo bezpečnostných smerníc oznámi štatutárovi resp. zodpovednej osobe.

Bezpečnostná smernica č. 8

Postupy pri haváriách, poruchách a iných mimoriadnych situáciách

Ak oprávnená osoba, alebo osoba, ktorá môže prísť do styku s osobnými údajmi zistí, alebo má podozrenie, že došlo k bezpečnostnej udalosti (zavírený počítač, neoprávnené používanie programového vybavenia, technická porucha výpočtovej techniky a pod.) je povinná bezodkladne upozorniť štatutára prevádzkovateľa alebo zodpovednú osobu prevádzkovateľa, ktorí rozhodnú o ďalšom postupe. O bezpečnostnom incidente sa vyhotoví ***hlásenie*** (Príloha č.6) a o incidentoch a ich riešení je prevádzkovateľ povinný viesť ***Evidenciu bezpečnostných incidentov*** (Príloha č.5).

Postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení na zníženie vzniku mimoriadnych situácií a možností efektívnej obnovy stavu pred haváriou.

Popis udalosti	**Návrh preventívnych opatrení**	**Postupy na zabezpečenie stavu obnovy**
1. Havárie IS spôsobené technickou chybou niektorého komponentu centrálneho počítača (server)	➢ Monitorovať činnosť serverov, kontrolovať chybové hlásenia ➢ Zabezpečiť dostatok finančných prostriedkov na obnovu IS ➢ Podľa možnosti obmieňať server každé tri roky ➢ Zálohovať	➢ Obnova zo zálohy
2. Porucha servera spôsobená vírusom neautorizovaným programom	➢ Zabezpečiť antivírovú ochranu ➢ Inštalovať len autorizované programy oprávnenými zamestnancami ➢ Preverovať cudzie nosiče (FD, CD ROM ...) ➢ Nepripájať nepreverené PC bez vedomia admin do LAN ➢ Nepoužívané pasívne rozvody odpojiť od aktívnych prvkov LAN ➢ Neotvárať nevyžiadané e-mailové prílohy ➢ Nespúšťať programy z prostredia internetu nepodpísane certifikačnou autoritou ➢ Nesťahovať neautorizované programy z prostredia internetu ➢ Sledovať aktuálne dianie na LAN a v sieti internet	➢ Odpojiť každého užívateľa ➢ Spustiť antivírový program s aktuálnou DB vírusov ➢ detekovať spôsob narušenia ➢ odstrániť príčiny ➢ opraviť narušenú funkčnosť ➢ opätovne skontrolovať systém antivírovým programom ➢ prekontrolovať všetky PC ➢ nájsť zdroj infiltrácie a zabezpečiť jeho eliminovanie ➢ znovu spustiť systém a pripojiť užívateľov
3. Porucha napájania, strata dodávky elektrickej energie	➢ Dôležité aktívne prvky siete je nutné chrániť záložnými zdrojmi elektrickej energie so stabilizátorom sieťového napätia	➢ V čase výpadku sa musí záložný zdroj automaticky aktivovať ➢ Pri dlhodobejšom výpadku sa server musí automaticky vypnúť (shutdown) ➢ Po nábehu el. energie je nutné server spustiť a skontrolovať

Popis havárie	**Návrh preventívnych opatrení**	**Postupy na zabezpečenie stavu obnovy**
4. Porucha prostriedkov demilitarizovanej zóny	➢ Monitorovať činnosť zariadení ➢ Monitorovať funkčnosť všetkých zariadení ➢ Zabezpečiť prístup len pre pracovníkov s oprávnením ➢ Periodicky meniť administrátorské a užívateľské prístupy s heslami ➢ Zabezpečiť antivírovú ochranu všetkých PC, ako aj e-mailového prístupu ➢ Zabezpečiť programovú aktuálnosť ➢ Zabezpečiť technickú aktuálnosť ➢ Kontrolovať súbory zaznamenávajúce činnosť systému ➢ Kontrolovať súbory	V prípade narušenia ➢ Odpojiť LAN od prostriedkov demilitarizovanej zóny ➢ Vyhľadať príčinu nefunkčnosti ➢ Odstrániť príčinu výmenou častí, inštalovaním aktualizácií, výmenou celku ➢ Poveriť prostriedky firewallu, prekladu adries (DNS) a proxy ➢ Po otestovaní funkčnosti pripojiť LAN
5. Porucha aktívnych prvkov siete	➢ Monitorovať činnosť ➢ Zabezpečiť dostatočnú kapacitu ➢ Pripájať ich prostredníctvom záložného zdroja ➢ Zabezpečiť dostatočnú ochranu pred nepovolaným prístupom	➢ Vymeniť nefunkčnú časť
6. Porucha pasívnej časti siete	➢ Premeranie kabeláže, zásuviek a konektorov	➢ Opraviť prípadne vymeniť vadnú časť
7. Havária databáz	➢ Sledovať konfiguračné súbory ➢ Monitorovať hlásenia programov a včas na ne reagovať ➢ Denne kontrolovať chybové hlásenia aplikácie a databázy	➢ Spustiť údržbu databáz ➢ Pri neodstránení nedostatkov obnoviť databázu zo zálohy
8. Havária 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	➢ Preinštalovať aplikáciu ➢ Nainštalovať novšiu verziu aplikácie ➢ Konzultovať chyby s dodávateľom
9. Porucha mail servera	➢ Sledovať konfiguračné súbory ➢ Monitorovať hlásenia a včas na ne reagovať ➢ Denne kontrolovať chybové hlásenia ➢ Nainštalovať antivírovú ochranu ➢ Zálohovať systém – obraz disku	➢ Vymeniť nefunkčnú časť ➢ Aktualizovať softvér ➢ V prípade výmeny disku previesť inštaláciu zo zálohy
10. Porucha pracovných staníc	➢ Používať len autorizované programy ➢ Inštalovať antivírové programy ➢ Inštalovať nové programy smie len poverený zamestnane	➢ Technická chyba – zabezpečiť opravu nefunkčnej časti, vymeniť nefunkčnú časť, zakúpiť novú pracovnú stanicu

Popis havárie	**Návrh preventívnych opatrení**	**Postupy na zabezpečenie stavu obnovy**
	➢ Užívatelia nesmú zasahovať do konfiguračných súborov ➢ Chybové hlásenia sú povinný hlásiť správcovi systému ➢ Zálohovať dáta na určené média ➢ Za zálohy, prevádzku a bezpečnosť zodpovedá zamestnanec	➢ Softvérova chyby – identifikovať príčinu, obnoviť súbory zo zálohy, preinštalovať OS, aktualizovať antivírovú ochranu
11. Chyba operačného systému PC	➢ Sledovať funkčnosť operačného systému ➢ Pravidelne spúšťať bezpečnostné aktualizácie operačného systému, ➢ Plánovať finančné prostriedky na obnovu výpočtovej techniky s novším a prepracovanejším operačným systémom. ➢ Zálohovať systém – obraz disku	➢ Obnoviť operačný systém z obnovovacieho bodu ➢ Preinštalovať operačný systém ➢ Nahradiť operačný systém, resp. zakúpiť novšiu výpočtovú techniku
11. Narušenie dverí, okien	➢ Pravidelne sledovať funkčnosť	➢ Neodkladne zabezpečiť opravu
12. Narušenie monitorovaného objektu	➢ Pravidelne sledovať funkčnosť poplašného zariadenia	➢ Hľadať a eliminovať príčinu narušenia
13.Mimoriadne udalosti spôsobené vplyvom zvyškových rizík: živelné pohromy, násilný vstup neoprávnenej osoby do objektu	➢ Vybudovať komplexný záložný systém mimo priestorov budovy v bezpečnej vzdialenosti ➢ Zabezpečiť niekoľkonásobné záložne kópie ➢ Vytvorenie chráneného komunikačného dátového kanálu na záložne pracovisko ➢ Zhotovenie havarijných plánov na zabezpečenie kontinuity činnosti ➢ Kontrolovať, čí sú splnené protipožiarne opatrenia ➢ Kontrolovať osoby pri vstupe do budovy ➢ Vo vytipovaných priestoroch inštalovať elektronický zabezpečovací systém, kamerový monitorovací systém, bezpečnostné mreže, dvere, zámky ➢ Zabezpečiť autentizáciu osôb pri vstupe do chránených priestorov	V prípade vyradenia IS z činnosti ➢ Zvolať krízový štáb ➢ Koordinovať činnosť podľa havarijných smerníc ➢ Aktivovať záložne pracovisko ➢ Skontrolovať úplnosť systému na záložnom pracovisku ➢ Spustenie záložnej prevádzky ➢ Odstránenie škôd na pôvodnom pracovisku ➢ Po obnovení funkčnosti vrátenie činnosti na pôvodné pracovisko V prípade napadnutia časti IS ➢ Presunúť aktíva do vyhovujúcich priestorov ➢ Inštalovať záložne databázy a pripojenia ak sú nutné ➢ Spustiť prevádzku ➢ Po odstránení dôsledkov vrátiť činnosť do stavu pred udalosťou