BEZPEČNOSTNÉ SMERNICE

Prevádzkovateľ: Základná škola s materskou školou

Adresa: Makov 264

Mesto: Makov

PSČ: 023 56

IČO: 42 388 104

OBSAH

Bezpečnostná smernica č. 1 3

Úlohy a povinnosti pracovníkov prevádzkovateľa pri ochrane osobných údajov 3

Bezpečnostná smernica č. 2 5

Postupy pri zakladaní nových záznamov, aktualizácii údajov a používaní záznamov 5

Bezpečnostná smernica č. 3 6

Podmienky úschovy a likvidácie písomností obsahujúcich osobné údaje 6

Bezpečnostná smernica č. 4 7

Podmienky poskytnutia, vypožičiavania, prenášania a prepravy písomností obsahujúcich osobné údaje 7

Bezpečnostná smernica č. 5 8

Rozmnožovanie písomností obsahujúcich osobné údaje 8

Bezpečnostná smernica č. 6 9

Kľúčový režim objektu prevádzkovateľa a povinnosti držiteľov kľúčov 9

Bezpečnostná smernica č. 7 10

Úlohy a povinnosti prevádzkovateľa pri práci s automatizovanou časťou IS 10

Bezpečnostná smernica č. 8 12

Postup pri bezpečnostných incidentoch a preventívne opatrenia 12

Bezpečnostná smernica č. 9 13

Zálohovanie údajov v počítačovom systéme 13

Príloha č. 1 15

O právach dotknutej osoby 15

Na základe § 2 ods. 2 vyhlášky č. 164/2013 Z. z. o rozsahu a dokumentácii bezpečnostných opatrení nahradzujeme dokumentáciu „závery vyplývajúce z bezpečnostného zámeru a analýzy bezpečnosti informačného systému na konkrétne podmienky prevádzkovaného IS" týmito bezpečnostnými smernicami.

Bezpečnostná smernica č. 1

Úlohy a povinnosti pracovníkov prevádzkovateľa pri ochrane osobných údajov

1. Osoby zodpovedné za bezpečnosť osobných údajov:

a) Za bezpečnosť osobných údajov u prevádzkovateľa zodpovedá prevádzkovateľ, ktorý môže výkonom dohľadu písomne poveriť, oznámiť a na úrade dať vyškoliť zodpovednú osobu alebo viaceré osoby, ktoré musia byť bezúhonné a mať platné potvrdenie úradu o absolvovaní skúšky podľa § 24 zákona č. 122/2013 Z. z.
b) Prevádzkovateľ spracúva osobné údaje prostredníctvom poučených pracovníkov - oprávnených osôb, ktoré musia svojím podpisom potvrdiť rozsah oprávnení, povolených činností a podmienok spracúvania osobných údajov.

2. Osoby oprávnené na prácu s osobnými údajmi:

a) Pracovať s osobnými údajmi u prevádzkovateľa je oprávnený personál zariadenia, vrátane zastupujúceho personálu, a to v rozsahu stanovenom písomným záznamom o poučení oprávnenej osoby.
b) Iné osoby pracujúce v zariadení nie sú oprávnené vykonávať akékoľvek operácie s osobnými údajmi.

3. Povinnosťou zodpovedných osôb/prevádzkovateľa je:

a) Poznať a dodržiavať ustanovenia zákona č.122/2013 Z. z. 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 pracovníkom.
d) Zabezpečiť aktualizáciu bezpečnostnej dokumentácie.
e) Najmenej jedenkrát ročne overiť dodržiavanie skutočností uvedených v písomných záznamoch o poučení oprávnených osôb a ďalšej bezpečnostnej dokumentácie.
f) Pri výbere pracovníkov posúdiť a prihliadať na ich bezúhonnosť, spoľahlivosť, dôveryhodnosť a schopnosť zachovávať mlčanlivosť o chránených údajoch.
g) Zriadiť kontaktné miesto na nahlasovanie výskytu incidentov.
h) Viesť evidenciu bezpečnostných incidentov, evidenciu kľúčov a kontrolných činností.
i) Upovedomiť zamestnancov, zmluvných partnerov a používateľov v pozícií tretích strán o povinnosti ohlásiť výskyt udalostí informačnej bezpečnosti a spozorovaných, a potenciálnych bezpečnostných slabín v IS.
j) Zabezpečiť pravidelné monitorovanie a preskúmavanie spracúvania osobných údajov tretími stranami.

4. Povinnosťou oprávnených osôb je:

a) Poznať a uplatňovať zásady bezpečnostnej dokumentácie.
b) Poznať a uplatňovať bezpečnostné smernice a postupy upravujúce prácu s osobnými údajmi.
c) Používať a oboznamovať sa s osobnými údajmi výhradne na účely súvisiace s pracovnoprávnym vzťahom a plnením pracovných povinností, používanie údajov na iný účel alebo porušenie mlčanlivosti je vážnym porušením pracovnej disciplíny a ako také môže viesť k okamžitému zrušeniu pracovného pomeru.
d) Povinnosť mlčanlivosti neplatí, ak je to nevyhnutné na plnenie úloh orgánov činných v trestnom konaní a vo vzťahu k Úradu na ochranu osobných údajov.
e) Zabezpečenie spracovania predložených osobných údajov v informačnom systéme prevádzkovateľa, v predpísanej štruktúre a v závislosti od rozsahu svojich oprávnení.
f) 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.
g) Neponechávať osobné údaje voľne dostupné na chodbách a v iných neuzamknutých miestnostiach alebo na iných miestach, vo verejne prístupných miestach, opustených dopravných prostriedkoch a pod.

h) Uzamykať chránený priestor pri každom opustení v prípade, že v miestnosti už nie je iná oprávnená osoba prevádzkovateľa.
i) Pri odchode z objektu prevádzkovateľa uzatvárať a uzamykať okná a dvere, vypínať počítačovú techniku, osvetlenie, elektrické a plynové spotrebiče.
j) Uplatňovať politiku „čistého stola a čistej obrazovky" (vypínať počítačovú techniku, ukladať osobné alebo inak citlivé údaje do pridelených úschovných objektov).
k) Informovať zodpovednú osobu o zistení neoprávnenej manipulácie alebo nájdení chránenej písomnosti, s ktorou nie sú oprávnení pracovať.
l) Viesť evidenciu vypožičiavania a poskytnutia výpisu dokumentov.
m) Zachovávať mlčanlivosť o bezpečnostných opatreniach a chránených údajoch.
n) Neodnášať písomnosti, počítačové médiá alebo inak zaznamenané údaje z priestorov prevádzkovateľa bez vedomia alebo súhlasu osoby zodpovednej za ochranu osobných údajov.
o) Ak je to možné, pri práci s osobnými údajmi uplatňovať pravidlo komisionálnosti.
p) Pri skončení pracovného pomeru, obdobného vzťahu alebo výkonu funkcie je oprávnená osoba povinná odovzdať prevádzkovateľovi pracovnú agendu vrátane všetkých médií (listiny, USB, CD a pod.) obsahujúcich osobné údaje.

5. Osoba poverená získavaním osobných údajov je povinná:

a) Preukázať na požiadanie svoju totožnosť dotknutej osobe, ktorej osobné údaje požaduje.
b) V prípade ak je dotknutou osobou dieťa, žiak, tak všetky povinnosti vykonáva zákonný zástupca dieťaťa.
c) Bez vyzvania vopred oznámiť dotknutej osobe účel spracovania osobných údajov a zoznam osobných údajov (platí pre všetky IS). Podrobnosti stanovia formuláre evidencie IS.
d) Bez vyzvania vopred oznámiť zamestnancovi školy, že jeho osobné údaje potrebuje pre spracovanie mzdovej personálnej a odvodovej agendy.
e) Oznámiť zamestnancovi, že jeho osobné údaje budú poskytnuté okrem sprostredkovateľa, zdravotným poisťovňam /zákon č. 580/2004 Z. z./, sociálnej poisťovni /zákon č. 461/2003 Z. z./, daňovému úradu / zákon č. 595/2003 Z. z./ prípadne iným tretím osobám ak to ustanovuje osobitný zákon. Podrobnosti stanoví formulár evidencie IS.
f) Bez vyzvania vopred oznámiť žiakovi, dieťaťu zákonnému zástupcovi, že jeho osobné údaje potrebuje pre zabezpečenia výchovno-vzdelávacieho procesu a všetky účely s ním súvisiace podľa osobitného zákona (245/2008 Z. z.).
g) Oznámiť žiakovi, dieťaťu zákonnému zástupcovi, že jeho osobné údaje budú poskytnuté Národnému ústavu certifikovaných meraní vzdelávania /zákon č. 245/2008 Z. z./, obci Makov ako zriaďovateľovi školy /zákon č. 245/2008 Z. z./, prípadne iným tretím osobám ak to ustanovuje osobitný zákon.
h) Poučiť dotknutú osobu o dobrovoľnosti alebo povinnosti poskytnutia osobných údajov a o existencii jej práv podľa § 28 zákona č. 122/2013 Z. z. (pozri prílohu č. 1).
i) Zabezpečiť preukázateľný súhlas na spracúvanie osobných údajov dotknutej osoby v informačnom systéme osobných údajov prevádzkovateľa, ak sa osobné údaje spracúvajú na základe súhlasu dotknutej osoby alebo ak to vyžaduje zákon č. 122/ 2013 Z. z. alebo osobitný zákon.

6. Zodpovednosť :

a) Bezpečnostné smernice školy sú záväzné pre všetkých zamestnancov školy. Za oboznámenie sa zamestnancov školy s týmito smernicami zodpovedá riaditeľ školy alebo ním písomne poverený zástupca riaditeľa.
b) Porušenie týchto smerníc sa bude považovať za porušenie pracovnej disciplíny v súlade s príslušnými ustanoveniami Zákonníkom práce a Pracovným poriadkom Základnej školy s materskou školou Makov.

Svojím podpisom potvrdzujem preštudovanie a prijatie zásad tejto smernice:

V Makove, dňa..... .....
podpis

Bezpečnostná smernica č. 2

Postupy pri zakladaní nových záznamov, aktualizácii údajov a používaní záznamov

1. Prevádzkovateľ vedie záznamy o osobných údajoch dotknutých osôb spoločnosti v rozsahu nevyhnutnom na splnenie účelu spracovania osobných údajov.
2. Záznamy a zmeny v záznamoch majú právo vykonávať oprávnené osoby, ktoré sú písomne poverené a poučené.
3. Získavanie osobných údajov môžu vykonávať len oprávnené a poučené osoby. Postup a spôsob pri získavaní osobných údajov určuje Bezpečnostná smernica č.1 bod 5.
4. Získavať osobné údaje nevyhnutné na dosiahnutie účelu spracúvania kopírovaním, skenovaním alebo iným zaznamenávaním úradných dokladov (občiansky preukaz, pas, vysvedčenie a pod.) na nosič informácií možno len vtedy, ak s tým dotknutá osoba písomne súhlasí alebo ak to osobitný zákon výslovne umožňuje bez súhlasu dotknutej osoby. To neplatí, ak ide o získavanie osobných údajov na účely uzatvorenia pracovnoprávneho alebo obdobného vzťahu.
5. Oprávnená osoba zodpovedná za vedenie dokumentácie zakladá jednotlivé písomnosti tak, aby zabránila ich vypadávaniu pri bežnej práci so záznamom (lepením, zošívaním, vložením do obalov).
6. Osoba, ktorá používa záznamy a iné písomnosti obsahujúce osobné údaje je povinná zabezpečiť, aby sa s týmito dokumentmi pracovalo mimo priestorov, ktoré sú v bezprostrednej blízkosti osôb neoprávnených na styk s osobnými údajmi.
7. Oprávnená osoba 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).
8. Oprávnená osoba 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.
9. V prípade tlače dokumentov obsahujúcich osobné údaje zabezpečuje, aby sa počas tlačenia s nimi 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.
10. Zhromaždené osobné údaje musia byť spracúvané vo forme umožňujúcej identifikáciu dotknutých osôb počas doby nie dlhšej ako je nevyhnutné na dosiahnutie účelu spracúvania.
11. Prevádzkovateľ je povinný zabezpečiť správnosť a aktuálnosť osobných údajov vo vzťahu k účelu spracúvania.
12. Správnosť, úplnosť a aktuálnosť osobných údajov môže prevádzkovateľ zabezpečovať:
    - Zmluvným záväzkom dotknutých osôb, že mu povinne nahlásia akúkoľvek zmenu osobných údajov,
    - Na základe zákona, ktorý povinnosť nahlasovať zmeny údajov dotknutým osobám nariaďuje,
    - Oslovením dotknutých osôb v pravidelných intervaloch.

Svojím podpisom potvrdzujem preštudovanie a prijatie zásad tejto smernice:

V Makove, dňa 3. 8. 2015

.....
podpis

Bezpečnostná smernica č. 3

Podmienky úschovy a likvidácie písomností obsahujúcich osobné údaje

1. Písomnosti obsahujúce osobné údaje sa u prevádzkovateľa 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 fyzickej ochrany priestorov strážnou službou, alebo uzamknutím vstupných dverí zámkom s bezpečnostnou vložkou a bezpečnostným kovaním.
2. Všetky dokumenty súvisiace s pedagogickou dokumentáciou sú súčasťou registratúry podľa zákona č. 359/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov.
3. Pri archivácii ostatných dokumentov obsahujúcich osobné údaje prevádzkovateľ postupuje podľa ustanovení zákona č. 359/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov, prípadne aj podľa iných osobitných zákonov.
4. 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.
5. Prevádzkovateľ zabezpečí bezodkladnú likvidáciu osobných údajov po splnení účelu ich spracovania. Osobné údaje možno ďalej spracúvať len v nevyhnutnom rozsahu na historický výskum, vedecký výskum a vývoj alebo na účely štatistiky, čo sa nepovažuje za nezlučiteľné s pôvodným účelom spracúvania a zároveň je prevádzkovateľ povinný označiť ich, anonymizovať ich, ak tým možno dosiahnuť účel spracúvania a zlikvidovať ich ihneď ako sa stanú nepotrebnými.
6. V prípadoch, ak osobitný zákon ustanovuje lehotu, ktorá neumožňuje osobné údaje bezodkladne zlikvidovať zabezpečí bezodkladnú likvidáciu až po uplynutí lehoty ustanovenej osobitným zákonom.
7. Ak dotknutá osoba uplatní námietku podľa § 28 ods. 3 písm. a) zákona č. 122/2013, prevádzkovateľ je povinný bez zbytočného odkladu zlikvidovať osobné údaje okrem osobných údajov uvedených v § 10 ods. 3 písm. d) zákona č. 122/2013 v poštovom styku.
8. Likvidáciu nepotrebných citlivých dokumentov musí schváliť zodpovedná osoba. Dokumenty musia byť zlikvidované za prítomnosti minimálne 2 osôb skartovacím zariadením, spálením alebo inou metódou zamedzujúcou čitateľnosť.

Svojím podpisom potvrdzujem preštudovanie a prijatie zásad tejto smernice:

V Makove, dňa 3. 9. 2015 ....
podpis

Bezpečnostná smernica č. 4

Podmienky poskytnutia, vypožičiavania, prenášania a prepravy písomností obsahujúcich osobné údaje

1. Záznamy a ďalšie chránené písomnosti je možné zapožičať iba so súhlasom oprávnenej osoby.
2. Záznamy a originály písomností obsahujúcich osobné údaje je možné poskytnúť, zapožičať alebo sprístupniť okrem sprostredkovateľa, len osobám, organizáciám a inštitúciám v súlade so zákonom č. 580/2004 Z. z., zákonom č. 461/2003 Z. z., zákonom č. 595/2003 Z. z. a iné. Presná špecifikácia je súčasťou evidenčných listov IS.
3. Vypožičanie dokumentov obsahujúcich chránené písomnosti odovzdávajúca oprávnená osoba zapíše do evidencie vypožičiavania a poskytnutia výpisu dokumentov.
4. Záznamy a ďalšie chránené písomnosti sa zapožičiavajú spravidla na 1 pracovný deň. Iba v odôvodnených prípadoch sa zapožičiavajú na dlhšiu dobu. To neplatí pre tretie strany v pozícii sprostredkovateľa, ktorým sa osobné údaje poskytujú na dobu nevyhnutnú pre splnenie účelu spracovania.
5. Záznamy je možné prenášať výhradne v zalepenej obálke alebo uzavretom obale, s otvorom prelepeným lepiacou páskou.
6. Písomnosti alebo záznamy prenášajú dotknuté osoby alebo na túto činnosť poverený personál prevádzkovateľa.
7. Písomnosti obsahujúce osobné údaje sa prepravujú výhradne doporučenou poštovou zásielkou alebo kuriérom.
8. V prípade, že zariadenie dostane zásielku v poškodenom obale, preverí dôvod poškodenia u doručujúcej osoby a odsúhlasí obsah zásielky s odosielateľom.
9. Odovzdanie písomnosti na prenos alebo prepravu musí oprávnená osoba, ktorá odovzdáva písomnosti na prenos, zaznamenať v evidencii vypožičiavania a poskytnutia výpisu dokumentov. Oprávnená osoba, ktorá pripravuje a balí písomnosti na prenos alebo prepravu, je povinná obsah obálky pred zalepením skontrolovať, či nedošlo k zámene odosielaných písomností.
10. Písomnosti v záznamoch určených na prenos alebo prepravu musia byť pevne spojené s obalom tak, aby sa zabránilo nekontrolovanej manipulácii s nimi alebo strate.
11. Po vrátení vypožičaných písomností je oprávnená osoba povinná skontrolovať úplnosť písomností a či nedošlo k zámene písomností.

Svojím podpisom potvrdzujem preštudovanie a prijatie zásad tejto smernice:

V Makove, dňa 3. 8. 2015

.....
podpis

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 automatizovanej časti informačného systému, odpisu, fotokópie alebo inej písomnosti právnickej alebo fyzickej osobe, ktorá nie je dotknutou osobou, sa eviduje v evidencii vypožičiavania a poskytnutia výpisu dokumentov.

Svojím podpisom potvrdzujem preštudovanie a prijatie zásad tejto smernice:

V Makove, dňa 3. 8. 2015 .....

.....
podpis

Bezpečnostná smernica č. 6

Kľúčový režim objektu prevádzkovateľa 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 zodpovednosťou za ochranu osobných údajov. Náhradné kľúče od dverí a zariadení pre prípad mimoriadnych udalostí sú uložené u prevádzkovateľa.

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

1. Zodpovedná osoba vedie o evidovaných kľúčoch evidenciu, 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;
f) dátum vrátenia.

Osoba, ktorá nie je oprávnená na prácu s osobnými údajmi môže mať pridelené a samostatne používať evidované kľúče od priestorov prevádzkovateľa iba s podmienkou, že pamäťové média, písomnosti a iné dokumenty obsahujúce osobné údaje sú uzamykané v zariadeniach na úschovu prístupných iba držiteľom evidovaných kľúčov.

2. Držiteľ evidovaných kľúčov je povinný:

a) zaobchádzať s kľúčmi tak, aby nedošlo k ich strate alebo krádeži;
b) zamedziť vstupu nepovolaných osôb do objektu;
c) osobne dohliadať na prácu 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;
d) uzamykať okná, dvere a zariadenia, od ktorých má pridelené evidované kľúče vždy, keď sa vzďaľuje z pracoviska;
e) pred uzamknutím a opustením pracoviska uschovať všetky pamäťové médiá a písomnosti obsahujúce osobné údaje, ktoré sú voľne položené v priestoroch pracoviska;
f) bez omeškania oznámiť zodpovednej osobe stratu alebo krádež evidovaných kľúčov;
g) na výzvu zodpovednej osoby v stanovenom termíne odovzdať evidované kľúče.

Svojím podpisom potvrdzujem preštudovanie a prijatie zásad tejto smernice:

V Makove, dňa 3.8.2015

.....
podpis

Bezpečnostná smernica č. 7

Úlohy a povinnosti prevádzkovateľa pri práci s automatizovanou časťou IS

1. Zodpovedné osoby za bezpečnosť osobných údajov a chod automatizovanej časti informačného systému:

a) Za bezpečnosť osobných údajov v automatizovanej časti IS zodpovedá prevádzkovateľ, ktorý môže výkonom dohľadu písomne poveriť, oznámiť a na úrade dať vyškoliť zodpovednú osobu alebo viaceré osoby, ktoré musia byť bezúhonné a mať platné potvrdenie úradu o absolvovaní skúšky podľa § 24 zákona č. 122/2013 Z. z.
b) Za chod automatizovanej časti informačného systému zodpovedá prevádzkovateľ, alebo na to určený pracovník (správca), ktorý musí svojím podpisom potvrdiť rozsah oprávnení, povolených činností a podmienok spracúvania osobných údajov.

2. Povinnosťou zodpovedných osôb (prevádzkovateľ, správca alebo ním poverená a úradom vyškolená osoba) je:

a) Mať neobmedzený prístup k celému informačnému systému.
b) Vykonávať registrácie a deregistrácie používateľov pre udeľovanie a odoberanie prístupových práv ku všetkým multipoužívateľským informačným systémom a službám.
c) V súvislosti s možnosťou prieniku do počítačového systému sa každá oprávnená osoba prezentuje vlastným prístupovým heslom, ktoré určí, alebo schváli zodpovedná osoba (dĺžka hesla je minimálne 6 znakov, musí obsahovať čísla, písmená a špeciálne znaky napr. @#$%*). Bezpečné heslo nesmie byť ako celok všeobecne známe (tzv. slovníkové) slovo a malo by sa meniť aspoň 2 x ročne. Heslo by sa pri zadávaní nemali zobrazovať na obrazovke. Zodpovedná osoba je zodpovedná aj za rušenie prístupových hesiel.
d) Stanovuje zodpovednosť a postupy riadenia vzdialených prostriedkov, vrátane prostriedkov v používateľských oblastiach.
e) Vedie evidenciu pracovných staníc.
f) Vedie zoznamy povolených a zakázaných softvérov, prípadne webových sídiel.

3. Zodpovedná, alebo oprávnená osoba zabezpečí nasledovné opatrenia:

3.1. Technické opatrenia

a) Priebežne počas práce s IS sleduje jeho činnosť a prípadné nekorektné správanie konzultuje s jeho dodávateľom.
b) Zabezpečí správne nastavenie brány FireWall.
c) Zabezpečí správne nastavenie antivírusového programu, hlavne vo vzťahu k dodávateľskej firme.
d) Zakáže použitie cudzích pamäťových nosičov a prezeranie a inštaláciu akýchkoľvek programov z internetu.
e) Zabezpečí zmazanie opakovateľne použiteľných médií, ktoré majú byť odnesené z organizácie, ak už ďalej nie sú potrebné.
f) Vedie záznam o vynesených médií z organizácie.
g) Zabezpečí riadne uloženie médií v bezpečnom, chránenom prostredí, podľa špecifikácií výrobcu.
h) Zabezpečí vypnutie automatického spúšťania programov z externých dátových médií.
i) Zabezpečí postupy na ochranu vymieňaných informácií pred odpočúvaním, kopírovaním, modifikáciou, nesprávnym smerovaním a zničením.
j) Zabezpečí aby zmeny v BIOS-e boli chránené heslom.
k) Zakáže bootovanie z iných médií ako je primárny pevný disk.
l) Zabezpečí využívania šifrovania pri posielaní a prijímaní elektronickej pošty.
m) Zabezpečí oddelenie súborov hesiel od dát aplikačných systémov.
n) Zabezpečí prenášanie hesiel v chránenej (zašifrovanej alebo hashovanej) podobe.
o) Zabezpečí vypnutie automatického zapamätávanie hesiel na webovom prehliadači.
p) Zabezpečí vytváranie auditných log záznamov, ktoré zaznamenávajú aktivity používateľov.
q) Zabezpečí používanie jedinečnej identifikácie (ID) používateľa.

r) Označí počítačové výstupy a nosiče osobných údajov.
s) Stanoví časový interval pre odpojenie terminálu z dôvodu jeho nečinnosti.
t) Podľa smernice pre zálohovanie zabezpečí bezchybný stav zálohovacích mechaník a nosičov.

3.2. Organizačné opatrenia

a) Počas pracovnej doby zamedzí prístup nepovolaným osobám k počítaču a iným aktívam IS.
b) Pomocný obslužný personál nesmie mať prístup k informačnému systému. V neprítomnosti prevádzkovateľa, alebo oprávnených osôb musí byť priestor s IS uzamknutý a prístup do počítača musí byť chránený heslom.
c) Pri krátkodobom odchode z priestorov uvedie počítač do stavu, kedy je na pokračovanie v programe potrebné zadať heslo.
d) Pri odchode z priestorov na záver pracovnej doby vykonaná zálohy databáz na prenosný nosič a pevný disk, vypne počítač a uzamkne priestory.

3.3. Forma a periodicita kontrol

a) Minimálne jeden krát týždenne skontroluje náhodným výberom kompletnosť databázy v počítačovom systéme.
b) Jedenkrát za dva roky zabezpečí kontrolu počítačového systému špecializovaným servisným technikom. Tento zrealizuje overenie integrity pevného disku s verifikáciou povrchu, antivírusový scan a kontrolu technického stavu všetkých hardvérových komponentov.
c) V prípade pripájania PC na internet zabezpečí permanentnú antivírovú a antispamovú kontrolu.
d) Priebežne kontroluje či úroveň udeleného prístupu oprávnených pracovníkov je primeraná pracovnému účelu.
e) Minimálne jedenkrát za pol roka alebo po zmene (pracovný postup, degradácia, ukončenie pracovného/funkčného pomeru) preveruje prístupové práva.
f) Pri nekorektnom správaní systému skontroluje, alebo špecializovaným technikom zabezpečí kontrolu logových súborov v zobrazovači udalostí operačného systému /Event Viewer/.
g) V prípade použitia nosičov, ktoré sa vrátia od iných prevádzkovateľov, aplikuje pred použitím v systéme minimálne rýchle formátovanie. (Pri neznámych nosičoch platí zásada, že ich obsah sa neprezerá, nespúšťajú sa z nich žiadne aplikácie, iba sa prevedie ich formátovanie, ktoré odstráni prípadnú vírusovú nákazu.)
h) Minimálne jedenkrát týždenne, alebo po nekorektnom ukončení alebo výpadku energie vykoná systémovú kontrolu disku (scandisk), ak operačný systém takúto voľbu povoľuje.
i) Minimálne jedenkrát mesačne vykoná systémový scandisk a defragmentáciu disku, ak operačný systém takéto voľby povoľuje.
j) Pri údržbe a údržbových funkciách jednotlivých programov dodržiava zásady podľa návodu na použitie (tieto služby, ako napr. defragmentácia, kompresia a kontrola integrity databáz sa odporúča vykonať 1x mesačne).
k) Pri výzve na aktualizáciu systému zabezpečí spustenie stiahnutých aktualizácií v čo najkratšom termíne s dôrazom na bezpečnostné aktualizácie.
l) Podľa doporučení dodávateľa informačného systému vykonáva pravidelný servis databáz a operačného systému počítača.

Svojím podpisom potvrdzujem preštudovanie a prijatie zásad tejto smernice:

V Makove, dňa 3. 8. 2015 ..... podpis

Bezpečnostná smernica č. 8

Postup pri bezpečnostných incidentoch a preventívne opatrenia

Smernica vymedzuje základné pravidlá pre riešenie bezpečnostných incidentov. Definuje postup pri ohlasovaní bezpečnostných incidentov a slabých miest IS, postup pri riešení jednotlivých typov bezpečnostných incidentov a spôsob evidencie bezpečnostných incidentov a použitých riešení.

1. Zodpovedná, alebo oprávnená osoba zabezpečí nasledovné opatrenia:

a) Informuje všetkých používateľov o týchto postupoch a umiestnení kontaktného miesta pre ohlásenie bezpečnostných incidentov.
b) Každá osoba, ktorá má vedomosť o bezpečnostnom incidente (porucha, krádež, havária vírusová infiltrácia a pod.) okamžite po zistení takéhoto incidentu zabezpečí záchranu a ochranu IS ohlásením incidentu na kontaktnom mieste zodpovednej osobe prípadne ohlásením príslušným orgánom a organizáciám (polícia, požiarnici, SBS a pod.), resp. osobnou záchranou údajov (vynesením počítača, elektronických médií a papierovej dokumentácie a ich bezpečné uloženie na chránenom mieste) v prípade, že tým nie je ohrozené zdravie a bezpečnosť osôb.
c) Zodpovedná osoba poznačí incident do príslušnej evidencie vrátane podrobností (napr. miesta prieniku, vyskytujúcej sa poruche, správ na obrazovke, zvláštneho chodu systému a pod.) a ďalej postupujte podľa zoznamu identifikovaných incidentov a postupov.
d) Pri neautorizovanom prístupe do chránených priestorov, kompromitácií, krádeži alebo pokuse o krádež zváži a rozhodne, či kontaktovať špecializovanú firmu na fyzickú a objektovú bezpečnosť.
e) Pri havárii, nefunkčnosti alebo neštandardnom správaní v automatizovanej časti IS zváži a rozhodne, či kontaktovať počítačový servis, alebo softvérovú spoločnosť, ktorá počítačový systém dodala. Po konzultácii postupuje podľa inštrukcií dodávateľskej firmy.
f) V prípade nechceného vymazania databáz v žiadnom prípade nepokračuje v práci. Je bezpodmienečne nutné vypnúť počítač a kontaktovať dodávateľa informačného systému. (Ak po vymazaní súborov neuskutočňujete žiadne ďalšie inštalácie, obnovy, kopírovanie, atď., možno odborným prístupom tieto vymazané údaje obvykle obnoviť.)
g) Ak dôjde k vírusovej infiltrácií vykoná odvírenie počítača, kontrolu nastavenie antivírového programu a jeho aktuálnosti a vizuálnu kontrolu stavu databáz. Ak došlo k poškodeniu databáz vykoná reinštaláciu informačného systému a obnovu databáz zo záloh.
h) Ak je servis vykonávaný treťou osobou (počítačový technik, špecializovaná firma) oboznámi túto osobu s existenciou citlivých údajov v počítačových a dokumentových databázach a zabezpečí vyhotovenie písomného dokladu(súhlas servisného technika), že tieto skutočnosti berie na vedomie.
i) V prípade nutnosti odovzdať počítačový systém prostredníctvom nepoučených osôb (napr. preberanie reklamácií vo veľkých obchodných domoch) pred odovzdaním počítača, pokiaľ to jeho stav umožňuje, dáta zálohuje, potom všetky vymaže bezpečným spôsobom (odporúčame konzultáciu s odborníkom, nakoľko bežné zmazanie súborov je veľmi ľahko obnoviteľné a zneužiteľné).
j) Prevádzkovateľ zabezpečí pravidelné požiarne školenia oprávnených osôb a ostatných zamestnancov a v objekte na viditeľných miestach umiestni telefónne čísla pre nahlásenie bezpečnostného incidentu (požiarnici, vodárne, elektrárne, plynárne atď.)

Svojím podpisom potvrdzujem preštudovanie a prijatie zásad tejto smernice:

V Makove, dňa 3.8.2015 ..... podpis

Bezpečnostná smernica č. 9

Zálohovanie údajov v počítačovom systéme

Zálohovanie databáz počítačového systému je proces, pri ktorom sa vytvorí kópia všetkých databázových súborov programu, prípadne len jej časť, nevyhnutná na obnovu všetkých databáz v prípade poruchy alebo odcudzenia počítačového systému. Na vytvorenie zálohových súborov sa vo väčšine prípadov používajú štandardné komprimačné algoritmy (ZIP, CAB, ARJ, RAR atď.).

Táto smernica platí pre každý používaný program osobitne.

1. Typy zálohovania z hľadiska druhu a umiestnenia pamäťových nosičov:

a) Záloha na ten istý pevný disk PC, na ktorom je umiestnený program. Tento spôsob je najlacnejší a najrýchlejší. Princípom je vytvorenie kópie databáz do iného adresára, ako je nainštalovaný program. Zálohovanie rieši stratu integrity databáz, ako aj poškodenie údajových štruktúr vplyvom výpadku napájania. Nerieši stratu a poškodenie údajov spôsobenú neopraviteľnou poruchou pevného disku alebo odcudzením počítačového systému.
b) Záloha na iný pevný disk, alebo na iný počítač v sieti je bezpečnejší spôsob, ktorý eliminuje riziká technickej, alebo inej poruchy pevného disku. Nerieši problém odcudzenia počítačov. Na druhej strane je vyššie riziko narušenia údajov, nakoľko sú údaje uložené na viacerých PC.
c) Záloha na externé nosiče je bežný spôsob prenosu a uchovávania údajov. Treba uplatňovať zásadu nezálohovať stále na tie isté nosiče. Ideálne je na každý deň v týždni použiť iný súbor zálohovacích nosičov a tieto striedať (zálohovanie s cirkuláciou média).
d) Záloha na iný prenosný nosič (USB kľúč, CDR, CDRW, DVDR, Memory Card, prenosný pevný disk, magneto - pásková mechanika DAT). Z hľadiska ceny, kompatibility a spoľahlivosti je najvýhodnejšou metódou zálohovanie na USB kľúče. Cenovo výhodné a dostatočne spoľahlivé je aj napaľovanie na CD, DVD RW nosiče. Tento spôsob je však zložitejší, vyžaduje mať v PC príslušnú mechaniku a poznať niektorý z napaľovacích programov. Pri tomto spôsobe je nutné poznať lokalizáciu databázových súborov, prípadne lokalizáciu vykonaných záloh na pevnom disku. Tieto sa potom pomocou programu určeného pre napaľovanie CD/DVD kopírujú na zapisovateľný, alebo prepisovateľný CD/DVD disk.

2. Zásady, postupy a periodicita pri zálohovaní:

a) Každý deň vykonať bezpečnostnú zálohu na pevný disk vášho PC. Minimálne každý druhý deň (odporúčame každý deň) vykonať zálohu na prenosný nosič.
b) Podľa možností používať aspoň dva nezávislé nosiče.
c) Minimálne raz za mesiac vykonať úplné formátovanie pamäťových médií z dôvodu overenia ich funkčnosti.
d) Minimálne raz za mesiac overiť možnosť obnoviť informačný systém z vykonanej zálohy.
e) V žiadnom prípade nenechávať zálohové nosiče neuzamknuté v objekte. Treba si uvedomiť, že prípadný narušiteľ môže odcudziť nielen počítač, ale aj nosiče. V tomto prípade sú údaje nenávratne stratené.
f) Zálohy by mali byť uložené na vzdialenom mieste, v dostatočnej vzdialenosti, aby unikli akémukoľvek poškodeniu haváriou na hlavnom pracovisku.
g) Pri prenose údajov na iné miesto treba dodržiavať zásady bezpečnosti a ani v domácom prostredí ich nenechávať voľne prístupné.
h) V prípade, že dokumentáciu píšete najskôr do programu a potom každej dotknutej osobe vytvárate písaný dokument, nie je bezpodmienečne nutné každodenné zálohovanie na prenosné nosiče. Treba si však uvedomiť, že v prípade poškodenia disku, viete obnoviť len stav ku dňu vašej poslednej zálohy. Odporúčame minimálne každodenné zálohovanie údajov na pevný disk.
i) Nepotrebné údaje z nosiča treba vymazať formátovaním alebo fyzickou likvidáciou nosiča spálením, mechanickým rozbitím alebo použitím špecializovaného zariadenia na likvidáciu pamäťových nosičov.
j) V súvislosti s dlhodobým skladovaním databázových údajov, je potrebné minimálne 1x za rok zálohovať všetky databázy počítačového informačného systému a zálohy uložiť na "nový" zapisovateľný veľkokapacitný nosič (napr. CD, DVD, BlueRAY). Tieto zálohy je potrebné uložiť

na bezpečné miesto. Výhodou CD, DVD nosičov je, že zápis je v podstate mechanický, a tým aj odolný proti poškodeniu magnetickým poľom.

Svojím podpisom potvrdzujem preštudovanie a prijatie zásad tejto smernice:

V Makove, dňa 3.8.2015 .....

.....
podpis

Príloha č. 1

Práva dotknutej osoby

- právo vyžadovať od prevádzkovateľa na základe písomnej žiadosti:

  a) potvrdenie, či sú alebo nie sú osobné údaje o dotknutej osobe spracúvané,
  b) vo všeobecne zrozumiteľnej forme informácie o spracúvaní osobných údajov v informačnom systéme v rozsahu podľa zákona; pri vydaní rozhodnutia v zmysle § 28 ods. 5 zákona je dotknutá osoba oprávnená oboznámiť sa s postupom spracúvania a vyhodnocovania operácií,
  c) vo všeobecne zrozumiteľnej forme presné informácie o zdroji, z ktorého získal prevádzkovateľ osobné údaje dotknutej osoby na spracúvanie,
  d) vo všeobecne zrozumiteľnej forme zoznam osobných údajov dotknutej osoby, ktoré sú predmetom spracúvania,
  e) opravu alebo likvidáciu nesprávnych, neúplných alebo neaktuálnych osobných údajov, ktoré sú predmetom spracúvania,
  f) likvidáciu osobných údajov, ktorých účel spracúvania sa skončil; ak sú predmetom spracúvania úradné doklady obsahujúce osobné údaje, môže dotknutá osoba požiadať o ich vrátenie,
  g) likvidáciu osobných údajov, ktoré sú predmetom spracúvania, ak došlo k porušeniu zákona,
  h) blokovanie osobných údajov z dôvodu odvolania súhlasu pred uplynutím času jeho platnosti, ak prevádzkovateľ spracúva údaje na základe súhlasu dotknutej osoby,

- právo na základe písomnej žiadosti namietať voči:

  a) spracúvaniu osobných údajov, o ktorých sa predpokladá, že sú alebo budú spracúvané na účely priameho marketingu bez jej súhlasu a žiadať ich likvidáciu,
  b) využívaniu osobných údajov v rozsahu meno, priezvisko, titul, adresa na účely priameho marketingu v poštovom styku,
  c) poskytovaniu osobných údajov v rovnakom rozsahu na účely priameho marketingu,

- právo na základe písomnej žiadosti alebo osobne, ak vec neznesie odklad, namietať voči spracúvaniu osobných údajov v prípadoch uvedených v § 10 ods. 3 písm. a), e), f) alebo g) zákona vyslovením oprávnených dôvodov alebo predložením dôkazov o neoprávnenom zasahovaní do jej práv a právom chránených záujmov, ktoré sú alebo môžu byť v konkrétnom prípade takýmto spracúvaním osobných údajov poškodené; ak tomu nebránia zákonné dôvody a preukáže sa, že námietka dotknutej osoby je oprávnená, prevádzkovateľ je povinný osobné údaje, ktorých spracúvanie dotknutá osoba namietala, bez zbytočného odkladu blokovať a zlikvidovať ihneď, ako to okolnosti dovolia,
- právo na základe písomnej žiadosti alebo osobne, ak vec neznesie odklad, kedykoľvek namietať, nepodrobiť sa rozhodnutiu prevádzkovateľa, ktoré by malo pre ňu právne účinky alebo významný dosah, ak sa také rozhodnutie vydá výlučne na základe úkonov automatizovaného spracúvania jej osobných údajov. Dotknutá osoba má právo žiadať prevádzkovateľa o preskúmanie vydaného rozhodnutia metódou odlišnou od automatizovanej formy spracúvania, pričom prevádzkovateľ je povinný žiadosti dotknutej osoby vyhovieť, a to tak, že rozhodujúcu úlohu pri preskúmaní rozhodnutia bude mať oprávnená osoba; o spôsobe preskúmania a výsledku zistenia prevádzkovateľ informuje dotknutú osobu v lehote najneskôr 30 dní odo dňa doručenia žiadosti,
- právo pri podozrení, že sa jej osobné údaje neoprávnene spracúvajú, podať Úradu na ochranu osobných údajov SR návrh na začatie konania o ochrane osobných údajov.
- Ak dotknutá osoba nemá spôsobilosť na právne úkony v plnom rozsahu, jej práva v zmysle zákona môže uplatniť zákonný zástupca.
- Práva dotknutej osoby v zmysle zákona, ktorá nežije, môže uplatniť blízka osoba.