Bezpečnostná smernica

Základná škola s materskou školou Breza

Vypracoval	Nový predpis	Ruší predpis
Meno a priezvisko: **PaedDr. Eva Rabčanová, štatutár** **Anna Škombárová, zodpovedná osoba**		
Organizačný útvar: **Základná škola s materskou školou Breza**	**Platnosť:** **28. 03. 2014**	**Účinnosť:** **01. 04. 2014**
Podpis:	**Dátum:** **28. 03. 2014**	**Počet strán:** 1/15

Obsah

Hlava I.
Všeobecné ustanovenia

Čl. 1
Účel smernice

a) Smernica upravuje niektoré práva a povinnosti všetkých zamestnancov Základnej školy s materskou školou Breza (ďalej len škola), v oblasti ochrany osobných údajov, ochrany a bezpečnosti majetku, informácií a ďalších hodnôt, ktoré škola vlastní.
b) Bezpečnostná smernica upresňuje a aplikuje závery vyplývajúce z analýzy bezpečnosti informačných systémov a vymedzuje rozsah bezpečnostných opatrení z hľadiska ochrany osobných údajov.
c) S touto smernicou musia byť oboznámení všetci zamestnanci školy a iné oprávnené osoby so vzťahom ku škole.
d) Zamestnanec nerešpektovaním uvedených pravidiel poruší svoje povinnosti, čím dôjde k porušeniu pracovnej disciplíny a následne sa vyvodia opatrenia v zmysle Pracovného poriadku.
e) V prípade nelegálneho chovania sa zamestnanec vystavuje nebezpečenstvu trestného postihu a zamestnávateľ si vyhradzuje právo upozorniť na takéto chovanie príslušné orgány. Od zamestnancov sa pri zisťovaní možného zneužitia výpočtovej techniky očakáva spolupráca s administrátorom IT.

Čl. 2
Základné pojmy

a) **Osobné údaje** – sú údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, pričom takou osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu.
b) **Zodpovedná osoba** – fyzická osoba poverená výkonom dohľadu nad ochranou osobných údajov po úspešnom absolvovaní skúšky.
c) **Oprávnená osoba –** každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovného pomeru, štátnozamestnaneckého pomeru, služobného pomeru, členského vzťahu, na základe poverenia, zvolenia alebo vymenovania, alebo v rámci výkonu verejnej funkcie a ktorá spracúva osobné údaje v rozsahu a spôsobom určeným v poučení podľa § 21 zákona 122/2013 Z. z. o ochrane osobných údajov.
d) **Dotknutá osoba –** je každá fyzická osoba, ktorej sa osobné údaje týkajú.
e) **Spracúvanie osobných údajov** – vykonávanie operácií alebo súboru operácií s osobnými údajmi, najmä ich získavanie, zhromažďovanie, šírenie, zaznamenávanie, usporadúvanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, premiestňovanie, využívanie, uchovávanie, blokovanie, likvidácia, ich cezhraničný prenos, poskytovanie, sprístupňovanie alebo zverejňovanie.
f) **Sprístupňovanie osobných údajov** – sprístupňovaním osobných údajov oznámenie osobných údajov alebo umožnenie prístupu k nim príjemcovi, ktorý ich ďalej nespracúva.
g) Poskytovanie osobných údajov – poskytovaním osobných údajov odovzdávanie osobných údajov tretej strane, ktorá ich ďalej spracúva.
h) **Súhlas dotknutej osoby** – akýkoľvek slobodne daný výslovný a zrozumiteľný prejav vôle, ktorým dotknutá osoba na základe poskytnutých informácií vyjadruje súhlas so spracúvaním svojich osobných údajov.

i) **Likvidácia osobných údajov** – zrušenie osobných údajov rozložením, vymazaním alebo fyzickým zničením hmotných nosičov tak, aby sa z nich osobné údaje nedali reprodukovať.
j) **Informačný systém** – v ktorom sa na vopred vymedzený alebo ustanovený účel systematicky spracúva alebo má spracúvať akýkoľvek usporiadaný súbor osobných údajov prístupných podľa určených kritérií bez ohľadu na to, či ide o informačný systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe (ďalej len „informačný systém“); informačným systémom sa na účely tohto zákona rozumie aj súbor osobných údajov, ktoré sú spracúvané alebo pripravené na spracúvanie čiastočne automatizovanými alebo inými ako automatizovanými prostriedkami spracúvania.
k) **Všeobecne použiteľný identifikátor** – všeobecne použiteľným identifikátorom sa rozumie trvalý identifikačný osobný údaj dotknutej osoby, ktorý zabezpečuje jej jednoznačnosť v informačných systémoch (zvyčajne ide o rodné číslo).
l) **Zverejňovanie osobných údajov** – publikovanie, uverejnenie alebo vystavenie osobných údajov na verejnosti prostredníctvom masovokomunikačných prostriedkov, verejne prístupných počítačových sietí, verejným vykonaním alebo vystavením diela, verejným vyhlásením, uvedením vo verejnom zozname, v registri alebo v operáte, ich umiestnením na úradnej tabuli alebo na inom verejne prístupnom mieste.
m) **Úrad** – v tomto dokumente ide o Úrad na ochranu osobných údajov, ktorý je orgánom štátnej správy s celoslovenskou pôsobnosťou so sídlom v Bratislave, vykonávajúci nezávislý dozor nad ochranou osobných údajov a podieľajúci sa na ochrane základných práv a slobôd fyzických osôb pri spracúvaní ich osobných údajov.
n) **Aktíva** – sú všetky hmotné i nehmotné hodnoty, ktoré škola vlastní alebo využíva a slúžia najmä na plnenie jej predmetu podnikania. Medzi hmotné aktíva patria najmä servery, počítače, počítačové siete, komunikačné zariadenia a ďalšie hmotné premety vo vlastníctve školy. Medzi nehmotné aktíva patria najmä informačné systémy, pracovné postupy, know-how, údaje o zamestnancoch, ekonomické, finančné a obchodné údaje, majetkové a obdobné práva a ďalší nehmotný majetok.
o) **Hrozby** – sú vplyvy okolia, iných osôb, zariadení a prostriedkov, ktoré úmyselne alebo neúmyselne vplývajú na aktíva školy tak, že ich škola nemôže využívať alebo inak ohrozujú oprávnené záujmy školy.
p) **Externá organizácia** – organizácia alebo spoločnosť vstupujúca do informačného systému za účelom jeho údržby alebo obnovy.

Hlava II.
Zodpovednosť za ochranu osobných údajov

Čl. 3
Zodpovedná osoba

a) Za organizáciu bezpečnosti a ochrany osobných údajov v škole je poverená zodpovedná osoba podľa §23 zákona 122/2013 Z. z. o ochrane osobných údajov. Zodpovednú osobu písomne poveruje riaditeľ školy na základe jej súhlasu. Súčasťou poverenia je aj výpis z registra trestov s dátumom rovnakým ako poverenie.
b) Zodpovedná osoba zodpovedá za:
   1. vypracovanie a pravidelnú aktualizáciu „Bezpečnostného projektu“, pokiaľ je aktualizácia potrebná,
   2. vypracovanie a aktualizáciu evidenčných listov informačných systémov školy, v ktorých sú osobné údaje v elektronickej alebo papierovej forme,
   3. proces získavania osobných údajov, ich poskytovanie, sprístupňovanie, prípadne zverejňovanie,
   4. posúdenie pred začatím spracúvania osobných údajov v informačnom systéme, či ich spracúvaním nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb,
   5. zistenie narušenia práv a slobôd dotknutých osôb pred začatím spracúvania alebo porušenia zákonných ustanovení v priebehu spracúvania osobných údajov, zodpovedná osoba to bezodkladne oznámi riaditeľovi školy,
   6. posúdenie, či osobné údaje svojím obsahom a rozsahom zodpovedajú účelu spracúvania, resp. či sú s daným účelom zlučiteľné,
   7. zabezpečovanie aktuálnosti spracúvaných osobných údajov a za ich likvidáciu (ak bol splnený účel spracúvania alebo sa nedajú opraviť alebo doplniť tak, aby boli správne a aktuálne),
   8. rozhodnutie, či daným spracúvaním môže byť poverený sprostredkovateľ, ak je záujem na tom, aby spracúvanie vykonával,
   9. určenie, ktoré podmienky, ustanovené zákonom 122/2002 Z. z. o ochrane osobných údajov, je potrebné pri spracúvaní osobných údajov aplikovať,
   10. preverenie, či možno vykonávať cezhraničný tok osobných údajov, ak sa požaduje,
   11. zabezpečenie a organizáciu pravidelných školení zamestnancov ohľadom informačnej bezpečnosti,
   12. poučenie zamestnancov školy a tretích strán o svojich právach a povinnostiach predtým, ako získajú prístup k osobným údajom.

Čl. 4
Kontrolná činnosť

a) Kontrolná činnosť je súbor činností, ktorých úlohou je zisťovanie stavu bezpečnosti a ochrany informačných technológií, stavu pripravenosti a účinnosti opatrení a výkon dozoru nad plnením tejto smernice.
b) Kontrolnú činnosť vykonáva zodpovedná osoba.
c) Každý zamestnanec je povinný poskytnúť všetky informácie, ktoré si kontrola vyžiada a sú vo vzťahu ku kontrolným úlohám.
d) Výkon kontrolnej činnosti dokumentuje zodpovedná osoba v knihe kontrol.
e) Zodpovedná osoba je povinná zabezpečiť výkon kontrolnej činnosti najmenej 1x za rok.
f) Zodpovedná osoba má právo oboznámiť sa s výsledkami inej kontroly, ktorá bola vykonaná a ktorej predmetom nebolo zisťovanie stavu ochrany a bezpečnosti

informačných technológií. Ak vo výsledkoch a záveroch kontroly sú skutočnosti, ktoré signalizujú alebo informujú o narušení bezpečnosti a ochrany osobných údajov, je zodpovedná osoba povinná uvedené informácie okamžite prešetriť formou ňou samostatne vykonanej kontroly.

g) Výsledky kontroly predkladá zodpovedná osoba vedeniu školy.

Hlava III.
Osobné údaje školy

Čl. 5
Manipulácia s osobnými údajmi

a) Každý zamestnanec, ktorý príde do styku s osobnými údajmi (oprávnená osoba), musí byť poučený podľa zákona 122/2013 Z. z. o ochrane osobných údajov. Toto poučenie musí byť v súlade s jeho pracovnou náplňou. Poučenie vykonáva zodpovedná osoba alebo ňou poverená osoba.
b) Osobné údaje a personálne údaje môžu byť ukladané a prenášané len zabezpečeným spôsobom.
c) Zabezpečenie osobných údajov sa vykonáva nasledovnými opatreniami:
   1. Dokumenty na papieri a na pamäťových médiách musia byť ukladané v uzamykateľnej skrini, ktorá je umiestnená v uzamykateľnej miestnosti. Vstup do tejto miestnosti je povolený len vedúcemu personálneho oddelenia a ním určeným zamestnancom.
   2. Prenášanie papierových dokumentov s personálnymi údajmi je možné len v uzavretých a nepriehľadných schránkach alebo obaloch.
   3. Miestnosti, v ktorých sa spracúvajú osobné údaje musia byť v neprítomnosti zamestnanca uzamknuté. Miestnosti musia byť vybavené zábranným opatrením (prepážkou), ktorá zamedzí neoprávneným osobám nahliadať do dokumentov a na obrazovky počítačov alebo odcudziť média a dokumenty. Obrazovky počítačov musia byť umiestnené tak, aby nepovolané osoby z nich nemohli prečítať osobné údaje.
   4. Zakazuje sa zhotovovať (tlačiť) dokumenty s osobnými údajmi na iných zariadeniach, než na zariadeniach, ktoré sú umiestnené v zabezpečených priestoroch v správe správcu personálnych údajov.
   5. Zakazuje sa zanechávanie dokumentov s osobnými údajmi v tlačových zariadeniach napr. kopírkach, tlačiarňach alebo faxoch bez dozoru.
   6. Zamestnanci sú povinní dodržiavať pravidlo čistého stola – nenechávať v neprítomnosti, najmä po skončení pracovnej doby, na stole dokumenty s osobnými údajmi.
   7. Poskytovať a sprístupňovať osobné údaje cez telefón je zakázané.
d) Pri získavaní a spracúvaní osobných údajov sú zamestnanci povinní dodržiavať nasledovné záväzné pravidlá:
   1. Pri získavaní osobných údajov do jednotlivých IS osobných údajov v rámci školy IS vyžadovať od fyzických osôb len tie osobné údaje, ktoré sú potrebné pre účel ich spracúvania.
   2. Získavať osobné údaje môže len ten zamestnanec, ktorý v rámci pracovnej zmluvy a náplni práce, spracúva osobné údaje fyzických osôb a je oprávnená osoba podľa §21 zákona 122/2013 Z. z. o ochrane osobných údajov.
   3. Pri získavaní a spracúvaní osobných údajov, je zamestnanec povinný zabezpečiť ochranu osobných údajov tak, že získavať a spracúvať osobné údaje môže len v prítomnosti oprávnených osôb. V prípade, ak v mieste získavania alebo spracúvania osobných údajov sa nachádza aj ďalšia neoprávnená osoba, je oprávnená osoba povinná prijať opatrenia k tomu, aby tieto údaje nemohli byť známe tejto neoprávnenej osobe a zabrániť tomu, aby táto neoprávnená osoby mohla do písomností obsahujúcich osobné údaje nahliadnuť a pod..
   4. Oprávnená osoba kontroluje a overuje správnosť a aktuálnosť osobných údajov po ich získaní a zaradení v informačnom systéme osobných údajov.

5. Zakazuje sa, aby zamestnanci získavali osobné údaje fyzických osôb pod zámienkou iného účelu alebo inej činnosti, než účelu na, ktorý sú získavané.
6. Vykonávať povolené spracovateľské operácie podľa poučenia oprávnenej osoby len so správnymi, úplnými a podľa potreby aktualizovanými osobnými údajmi vo vzťahu k účelu spracúvania.
7. Nesprávne a neúplné osobné údaje je bez zbytočného odkladu povinné opraviť alebo doplniť; nesprávne a neúplné osobné údaje, ktoré nemožno opraviť alebo doplniť tak, aby boli správne a úplné je povinné blokovať, kým sa rozhodne o ich likvidácii.
8. Pred získavaním osobných údajov od dotknutej osoby ju oboznámiť s názvom a sídlom školy, účelom spracúvania osobných údajov, rozsahom spracúvania osobných údajov, predpokladanom okruhu tretích strán pri poskytovaní osobných údajov alebo príjemcov pri sprístupňovaní osobných údajov, forme zverejnenia, ak sa osobné údaje zverejňujú a tretie krajiny, ak sa predpokladá alebo je zrejmé, že sa do týchto krajín uskutoční cezhraničný prenos osobných údajov.
9. Poučiť dotknutú osobu o dobrovoľnosti alebo povinnosti poskytnutia osobných údajov a o existencii jej práv podľa § 28 zákona č. 122/2013 Z. z..
10. Zabezpečiť preukázateľný súhlas na spracúvanie osobných údajov dotknutej osoby v informačnom systéme osobných údajov školy, ak sa osobné údaje spracúvajú na základe súhlasu dotknutej osoby alebo ak to vyžaduje zákon č. 122/2013 Z. z., alebo osobitný zákon.
11. Získavať osobné údaje nevyhnutné na dosiahnutie účelu spracúvania kopírovaním, skenovaním alebo iným zaznamenávaním úradných dokladov na nosič informácií len vtedy, ak to osobitný zákon výslovne umožňuje bez súhlasu dotknutej osoby alebo na základe písomného súhlasu dotknutej osoby, ak je to nevyhnutné na dosiahnutie účelu spracúvania.
12. Chrániť prijaté dokumenty a súbory pred stratou, poškodením, zneužitím, odcudzením, neoprávneným sprístupnením, poskytnutím alebo inými neprípustnými formami spracúvania.
13. Vykonať likvidáciu osobných údajov, ktoré sú súčasťou už nepotrebných pracovných dokumentov (napr. rôzne pracovné súbory, pracovné verzie dokumentov v listinnej podobe) rozložením, vymazaním alebo fyzickým zničením hmotných nosičov tak, aby sa z nich osobné údaje nedali reprodukovať; to neplatí vo vzťahu k osobným údajom, ktoré sú súčasťou obsahu registratúrnych záznamov školy.

e) Zamestnanci sú povinní zachovávať mlčanlivosť o osobných údajoch, s ktorými prídu do styku. Tie nesmú využiť ani pre osobnú potrebu a bez súhlasu riaditeľa školy ich nesmú zverejniť, nikomu poskytnúť a ani sprístupniť. Túto mlčanlivosť sú povinní zachovať aj po skončení spracovávania osobných údajov alebo po skončení pracovného pomeru.
f) Každý zamestnanec je zodpovedný za fyzickú bezpečnosť svojho pracoviska a zverených mu pracovných prostriedkov. Pri odchode z pracoviska je povinný uzamknúť pracovisko, uzavrieť okná a prekontrolovať zariadenia, či nemôžu spôsobiť požiar alebo inú haváriu. Ak zamestnanec nemôže túto povinnosť splniť, oznámi to ihneď svojmu nadriadenému alebo zodpovednej osobe.

Čl. 6
Manipulácia s médiami

a) Všetky média s osobnými a citlivými údajmi musia byť uložené v bezpečnom, chránenom prostredí, podľa špecifikácie výrobcu.

b) Informácie, ktoré majú byť uchované po dobu dlhšiu, ako je doba životnosti média, na ktorom sú uložené (na základe špecifikácie výrobcu), musia byť uložené aj na inom mieste, aby sa tak predišlo strate spôsobenej nečitateľnosťou média.
c) Pri prenášaní osobných údajov na médiách mimo priestory školy je potrebné tieto údaje zašifrovať. O forme šifrovania rozhoduje Správca IT.
d) Obsahy akýchkoľvek opakovateľne použiteľných médií, ktoré majú byť odnesené zo školy, musia byť zmazané, ak už nie sú ďalej potrebné.
e) Média, ktoré nie sú už potrebné, sa musia bezpečne a spoľahlivo zlikvidovať.

Hlava IV.
Prostriedky informačných technológií

Čl. 7
Správca informačných technológií

a) Správa informačných technológií musí byť organizovaná tak, aby sa minimalizovala hrozba zneužitia postavenia administrátora.
b) Za ochranu údajov je zodpovedný Správca informačných technológií (ďalej IT), ktorého poveril riaditeľ školy. K tomuto účelu vykonáva nasledovné činnosti:
   1. Vykonáva kopírovanie údajov na záložné médiá (zálohovanie údajov).
   2. Vykonáva kopírovanie údajov na archívne médiá (archivovanie údajov).
   3. Vykonáva nastavenia prístupových práv k údajom tak, aby k nim mohli pristupovať len oprávnení používatelia.
   4. Inštaluje, spravuje a zabezpečuje také služby (aplikácie), ktoré umožnia zvýšenú ochranu údajov.
c) Správca IT je zodpovedný za pravidelnú a včasnú aktualizáciu všetkých programových prostriedkov tak, aby boli včas odstraňované chyby v týchto softvérových prostriedkoch, ktorými sú najmä operačné systémy a ich súčasti, databázové systémy, používané aplikácie (najmä ak komunikujú po sieti), systém antivírusovej ochrany a firewally.
d) Správca IT je povinný priebežne nainštalovať všetky dostupné nové opravy softvérového vybavenia, pokiaľ sa tým nenaruší bezproblémový chod a činnosť. Raz za 6 mesiacov je Správca IT povinný overiť, či neboli vydané nové verzie softvéru.
e) Zakazuje sa používanie neovereného kódu. Pod pojmom neoverený kód sa rozumie taký program, ktorý nemá garanciu výrobcu o jeho spoľahlivosti alebo nebol overený Správcom IT v izolovanom prostredí, či neobsahuje nežiaduce funkcie a chyby. Overenie sa vykonáva tak, aby nemohlo dôjsť k ohrozeniu osobných údajov školy a musí sa preveriť najmä správanie programu v sieťovom prostredí a vo vzťahu k údajom uloženým na pamäťovom médiu počítača.
f) Pri konfigurácii prostriedkov, programov a služieb Správca IT dbá na to, aby sa používali len tie prostriedky, programy a služby, ktoré sú nevyhnutné pre plnenie pracovných úloh a potrieb školy. Zakazuje sa používanie programov, sieťových služieb a IT prostriedkov, ktoré nie sú potrebné pre výkon práce zamestnancov a plnenie ich úloh. Používané programy, služby a prostriedky musia byť konfigurované tak, aby k nim mali prístup len tí zamestnanci, ktorí tieto programy, služby a prostriedky potrebujú k svojej práci.

Čl. 8
Zálohovanie a archivovanie údajov

a) Správca IT je povinný vykonávať zálohovanie minimálne raz za deň.
b) Médiá so záložnými údajmi musia byť uložené v inej miestnosti, než sa nachádza počítač, z ktorého boli záložné údaje vyhotovené.
c) Správca IT musí minimálne raz za rok vykonať test funkcionality dátového nosiča zálohy.

Čl. 9
Prístupové práva

a) Správca IT nesmie povoliť heslá kratšie ako 6 znakov. Správca nesmie ako heslo použiť takú kombináciu znakov, ktorú by bolo možné priradiť k jeho osobe, akými sú napríklad meno používateľa a jeho rodinných príslušníkov napísané spredu či odzadu, telefónne číslo domov alebo na pracovisko a podobne. Heslo musí obsahovať minimálne jedno veľké písmeno, jedno číslo alebo špeciálny znak.

b) Zamestnancom sa zakazuje zverejňovať alebo vyzradiť prihlasovacie údaje (heslá) inej osobe. Taktiež sa zakazuje držanie záznamu hesiel (napr. na papieri, v softvérovom súbore alebo prenosnom zariadení), ak takýto záznam nemôže byť bezpečne uložený.
c) Prístupové oprávnenia prideľuje používateľovi Správca IT na základe požiadavky vedúceho základného organizačného útvaru alebo osobitného útvaru. Tvoria ich prístupové meno, prístupové heslo a súbor nastavení, ktoré definujú povolené aktivity používateľa.
d) Používateľ sa nesmie žiadnymi prostriedkami pokúšať získať prístupové práva alebo privilegovaný stav, ktorý mu nebol pridelený Správcom IT.
e) Pokiaľ používateľ v dôsledku chyby programových alebo technických prostriedkov získa privilegovaný stav, ktorý mu nebol udelený alebo mu prístupové práva neboli pridelené, je povinný túto skutočnosť neodkladne oznámiť Správcovi IT.
f) Po skončení pracovného pomeru je Správca IT povinný odobrať odchádzajúcemu zamestnancovi jeho prihlasovacie údaje a zmeniť ich tak, aby sa mu znemožnil ďalší prístup.
g) Prístupové oprávnenia sú prideľované podľa typu používateľa:
   1. administrátor – prístup k správe a údržbe IT, mal by to byť Správca IT,
   2. používateľ – prístup len k tým modulom aplikácie, s ktorými bezprostredne pracuje,
   3. externý používateľ – zamestnanec externej firmy, ktorá spravuje a udržiava danú aplikáciu.

Čl. 10
Pracovné stanice

a) Zamestnanec je povinný používať zverené pracovné stanice len na pracovné účely. Porušenie tohto ustanovenia sa považuje za bezpečnostný incident.
b) Zamestnanec môže na pracovných staniciach používať výlučne len programové vybavenie nainštalované Správcom IT, resp. nainštalované s jeho preukázateľným súhlasom. Zamestnanec nemôže na pracovnej stanici meniť žiadne programové vybavenie, a tiež nemôže meniť konfiguráciu programového vybavenia s výnimkou zmien, s ktorými sa mení vzhľad pracovného prostredia.
c) Zamestnanec je zodpovedný za dodržiavanie autorských práv a licenčných podmienok, ktoré sa vzťahujú k programom, súborom, grafike, dokumentom, správam a ostatným materiálom, ktoré má v úmysle inštalovať, sťahovať, zverejňovať alebo kopírovať.
d) Zamestnanec nemôže vytvárať a distribuovať kópie programového vybavenia inštalovaného na pracovnej stanici.
e) Zamestnanec je pred opustením pracoviska povinný ukončiť prácu s aplikačným programovým vybavením, odhlásiť sa zo siete a operačného systému a dohliadnuť na vypnutie pracovnej stanice.
f) Pri krátkodobej neprítomnosti môže zamestnanec nahradiť odhlásenie sa zo systému a vypnutie pracovnej stanice spustením šetriča obrazovky s heslom, resp. jej uzamknutím.
g) Zamestnanec je povinný po inštalácii novej verzie programového vybavenia po dobu minimálne jedného týždňa venovať zvýšenú pozornosť činnosti systému a kontrolovať správnosť výsledkov jeho práce. Prípadne odchýlky od požadovaného stavu je povinný čo najúplnejšie zdokumentovať a bezodkladne ohlásiť Správcovi IT.
h) Zakazuje sa pripájať do siete školy vlastné zariadenia (napr. notebooky, PDA, tlačiarne a pod.), a taktiež povoliť pripojenie cudzej osoby do siete školy bez vedomia Správcu IT. Taktiež sa zamestnancom zakazuje používať vlastné USB kľúče. Porušenie tohto bodu sa považuje za bezpečnostný incident.

Čl. 11
Zamestnanci externej organizácie

a) Prístup zamestnancov externej organizácie do informačných systémov zriaďuje Správca IT.
b) Správca IT vydá zamestnancovi externej organizácie prístupové heslo a práva podľa článku 9 tejto smernice.
c) Správca IT je povinný zabezpečiť bezpečný šifrovaný prístup zamestnanca tretej strany k jeho aktívu.
d) Zamestnanci externej organizácie sú povinní pred prihlásením sa do informačného systému školy o tejto skutočnosti oboznámiť Správcu IT, a to buď prostredníctvom mailu alebo telefónom. Na základe tohto oznámenia im Správca IT povolí pripojenie. Po skončení údržby alebo inej činnosti zamestnancov externej organizácie, Správca IT zruší možnosť pripojenia.
e) Zodpovedná osoba je povinná poučiť zamestnancov externej organizácie o ochrane a mlčanlivosti ohľadom osobných a citlivých údajov. Táto skutočnosť by mala byť zakomponovaná do zmluvy s externou organizáciou.

Čl. 12
Prístup do siete internet a mailová komunikácia

a) Každý zamestnanec, ktorému bol umožnený prístup do siete internet, je povinný rešpektovať nasledovné zásady:
   1. prístup do siete internet využívať predovšetkým v súlade so svojou pracovnou náplňou,
   2. dodržiavať etické zásady a zdržiavať sa činností, ktoré by mohli viesť k poškodeniu dobrého mena pracoviska alebo k iným škodám,
   3. komunikácia v internete spravidla nie je chránená pred "odpočúvaním"; v prípade potreby prenosu osobných údajov je nevyhnutné ich pred prenosom zabezpečiť šifrovaním; ak nie je zamestnanec schopný prenos takto zabezpečiť, nie je prípustné ho uskutočniť,
   4. je zakázané zo siete internet preberať nelegálny obsah (softvér, súbory chránené autorskými právami a pod.); preberanie spustiteľných programov je povolené len po konzultácii so Správcom IT.
b) Výber blokovaných stránok bude v kompetencii Správcu IT na základe webovej analýzy. V prípade veľkého prenosu objemu dát nesúvisiacich s pracovnou činnosťou zamestnanca vyplývajúceho z výsledkov webovej analýzy, má právo Správca IT zakázať a znemožniť užívateľovi prístup do internetu.
c) Zamestnanec je povinný zabezpečiť správne adresovanie príjemcu mailovej správy a na prenos správ používať všeobecne dané dátové štandardy.
d) V prípade posielania citlivých a osobných údajov je povinný použiť kryptovanú komunikáciu za použitia kryptovacieho kľúča, ktorý mu bol na požiadanie vydaný Správcom IT.
e) Používať elektronickú poštu len na legálne účely. Obsah dát odosielaných v rámci siete školy a cez internet nesmie byť v rozpore s dobrými mravmi.
f) Je zakázané používanie elektronickej pošty na súkromné účely.
g) Rešpektovať zákaz posielať reťazové a hromadné e-maily, reklamné správy a pod..

Čl. 13
Antivírová ochrana

a) Správca IT je zodpovedný za zabezpečenie antivírovej ochrany v škole a za inštaláciu a pravidelnú aktualizáciu softvéru potrebného na zabezpečenie tejto ochrany.
b) V prípade, že sa na pracovnej stanici zamestnanca zobrazí varovanie, že sa na disku alebo prenosnom médiu nachádza vírus alebo iný škodlivý kód, zamestnanec nesmie toto varovanie ignorovať. V prípade, že zavírené prenosné médium patrí inému subjektu, zamestnanec ho označí ako zavírené a vráti majiteľovi. V prípade zavírenia vlastného pevného disku alebo prenosného média, zamestnanec túto skutočnosť bezodkladne oznámi Správcovi IT.
c) V prípade objavenia vírusu v prijatej elektronickej pošte zamestnanec bezodkladne o tejto udalosti upovedomí Správcu IT. V žiadnom prípade zavírenú elektronickú poštu neposiela inému adresátovi a na svojej pracovnej stanici ju uschová len dočasne a len na žiadosť Správcu IT (na účely ďalšej analýzy prieniku vírusu do systémov pracoviska.).

Čl. 14
Bezpečnostné incidenty

a) Detekcia incidentov je súbor činností a opatrení vedúcich k včasnému zisteniu bezpečnostného incidentu, resp. k včasnému zisteniu, že hrozba môže spôsobiť narušenie spracovania osobných údajov.
b) Detekcia sa vykonáva nasledovnými spôsobmi:
   1. automatizovanými technickými prostriedkami – sú to napr. prostriedky hlásiace výskyt požiaru, senzory zisťujúce pohyb a pod.,
   2. automatickými a informatickými (programovými) prostriedkami – sú to špecializované programy, ktoré vyhodnocujú prevádzkové záznamy a indikujú potenciálny incident,
   3. sústavnou činnosťou zamestnancov – primeraná ostražitosť zamestnancov.
c) Ak výstupy z automatizovaných prostriedkov umožňujú záznam týchto výstupov, manipuluje sa s nimi ako s prevádzkovými záznamami.
d) Pri zistení incidentu musí byť o tomto informovaný Správca IT a vedúci organizačnej jednotky, kde incident nastal.
e) O každom bezpečnostnom incidente musí byť spracovaný záznam. Záznam spracúva Správca IT. Každý zamestnanec je povinný poskytnúť Bezpečnostnému správcovi všetky podklady a údaje, ktoré potrebuje pre spracovanie záznamu o bezpečnostnom incidente.
f) Záznam o bezpečnostnom incidente musí obsahovať:
   1. dátum a čas, kedy bol incident zistený, kedy skončil a ak je to možné zistiť, aj kedy incident začal,
   2. opis spôsobu, ako bol incident zistený – uvedie sa najmä meno zamestnanca, ktorý incident ohlásil,
   3. dátum a čas, kedy bol zmenený bezpečnostný režim školy,
   4. chronologický opis priebehu incidentu, opis hrozieb, ktoré sa realizovali a spôsob, akým sa realizovali,
   5. zoznam dotknutých aktív, doklad o škodách a predpokladaná doba zotavenia,
   6. porovnanie s rizikovou analýzou Bezpečnostného projektu – doklad, či bolo možné incident očakávať, či boli správne odhadnuté rizikové indexy a pod.,
   7. opis prijatých opatrení – doklad, kedy a kým boli prijaté, doklad o ich účinnosti a trvaní,

8. návrh na prijatie opatrení pre zamedzenie recidívy incidentu, odhad pravdepodobnosti recidívy, záznam o úprave rizikovej analýzy Bezpečnostného projektu, ak takúto úpravu bolo potrebné vykonať,
9. zoznam opatrení a nariadení, ktoré boli porušené a mohli spôsobiť, že incident nastal a zoznam zamestnancov, ktorí tieto nariadenia porušili.

g) Ak nastal bezpečnostný incident vedomou alebo nevedomou činnosťou zamestnanca, bude sankcionovaný podľa príslušných ustanovení zákonníka práce a pracovného poriadku.

Čl. 15
Prevádzkové záznamy

a) Ak je vedený prevádzkový záznam o činnosti a chode technického prostriedku, je povinnosťou Správcu IT pravidelne vyhodnocovať tento záznam.
b) Prostriedky, ktoré zaznamenávajú zápisy do prevádzkového záznamu musia byť nastavené tak, aby boli zaznamenané všetky dôležité skutočnosti, ktoré môžu byť dôležité pre ochranu aktív, ktorých sa týkajú.
c) Prevádzkovými záznamami sú najmä:
   1. prevádzkové záznamy o chode počítačov všetkých typov v OS MS Windows.

Čl. 16
Bezpečnostné režimy

a) Bezpečnostný režim je stav organizácie činnosti školy alebo jej časti, ktorý zodpovedá aktuálnemu ohrozeniu aktív školy.
b) Stupeň a rozsah bezpečnostného režimu určuje zodpovedná osoba alebo Správca IT na základe poznania aktuálneho stavu bezpečnosti a úrovne ohrozenia aktív školy.
c) Rozoznávajú sa nasledovné režimy:
   1. NORMÁLNY – normálny stav bežného chodu školy, kedy nie je bezprostredne ohrozené žiadne aktívum školy.
   2. OHROZENIE – činnosť školy nie je ničím zmenená alebo ovplyvnená, ale úroveň ohrozenia niektorého aktíva je zvýšená (zvýšená je pravdepodobnosť realizácie niektorej hrozby), čo vyžaduje monitorovanie tohto stavu a prijatie ďalších proaktívnych opatrení. Opatrenia sa prijímajú na základe aktuálneho poznania stavu hrozieb, ktorý je indikovaný najmä analýzou obsahu prevádzkových záznamov alebo výskytom bezpečnostných incidentov, ktoré síce bezprostredne nevyžadovali zmenu bezpečnostného režimu, ale dôsledky incidentu mohli spôsobiť zvýšenie pravdepodobnosti výskytu a realizácie niektorej z hrozieb. Po prijatí opatrení sa odhadne ich účinnosť, znovu sa posúdi úroveň rizika a rozhodne sa o prijatí ďalších opatrení alebo o prechode do režimu NORMÁLNY. Ak sa zistí, že aj napriek prijatým opatreniam došlo k realizácii hrozby a dochádza k poškodzovaniu alebo ničeniu aktív školy, vyhlási sa režim KRÍZA.
   3. KRÍZA – činnosť školy je zmenená následkom účinku niektorých hrozieb na aktíva školy. Vyžaduje sa prijatie účinných reaktívnych opatrení na odvrátenie hrozby a minimalizáciu škôd. Tento režim sa vyhlasuje, ak bol zistený výskyt realizujúcej sa niektorej hrozby na aspoň jedno IT aktívum (server alebo informačný systém), na ktorom sa spracovávajú osobné alebo citlivé údaje. Pod pojmom realizujúca sa hrozba sa rozumie taký stav, kedy je aktívum hrozbou poškodzované alebo ničené, čo má za následok znefunkčnenie aktíva alebo ohrozenie záujmov školy. Počas tohto režimu je možné odpojiť časť školy alebo celú škola od internetu, nariadiť vypnutie počítačov a serverov alebo ich odpojenie od počítačovej siete. Po odvrátení hrozby sa prechádza do režimu ZOTAVENIE.

4. ZOTAVENIE – špeciálny režim po KRÍZOVOM režime, kedy dochádza ku konsolidácii činnosti školy, rekonštrukcii a náhrade poškodených aktív. Navrhuje sa vedeniu školy postup pri odstraňovaní škôd. Postup musí obsahovať stanovenie priorít, časovú postupnosť, technickú špecifikáciu opatrení na odstránenie škôd a odhad ekonomickej náročnosti. Zodpovedná osoba v súčinnosti so Správcom IT je povinná dôkladne vyšetriť dôvody príčiny, a teda prečo došlo k realizácii hrozieb a škodám. Prechod do režimu NORMÁLNY je možný, ak bol schválený postup odstránenia škôd a ak je možné považovať stav školy ako celku z bezpečnostného hľadiska za konsolidovaný.

d) O zmene Bezpečnostného režimu musia byť ihneď vyrozumení všetci zamestnanci a osoby zodpovedné za výkon ochranu informačnej bezpečnosti v škole.

Čl. 17
Havarijné plánovanie

a) Havarijne plánovanie je súbor činností na zabezpečenie čo najvyššej dostupnosti údajov a ich ochrana pred zničením alebo poškodením.

b) V prípade výpadku pracovnej stanice je Správca IT povinný po identifikácií problému zabezpečiť:
   1. opravu alebo výmenu chybného dielu PC,
   2. náhradný PC,
   3. reinštaláciu alebo inštaláciu OS a konfiguráciu z inštalačných médií,
   4. inštaláciu klientskych aplikácií z inštalačných médií,
   5. inštaláciu antivírového programu,
   6. nastavenie prístupových práv,
   7. v prípade neodkladnosti prístup k informačným systémom z inej funkčnej pracovnej stanice.

c) V prípade výpadku servera je Správca IT povinný po identifikácii problému zabezpečiť:
   1. opravu servera v servisnej organizácii alebo náhradný server,
   2. inštaláciu hardware a jeho fyzické pripojenie do počítačovej siete,
   3. inštaláciu príslušného operačného systému servera,
   4. zo záložných kópií obnovenie systémových a konfiguračných súborov,
   5. inštaláciu antivírového programu a spustenie aktualizácie,
   6. inštaláciu IS a obnovenie dát z najmladších záložných médií.

d) V prípade výpadku sieťového prepojenia je Správca IT povinný po identifikácii problému zabezpečiť:
   1. opravu alebo výmenu chybného aktívneho alebo pasívneho prvku počítačovej siete,
   2. obnovenie konfiguračného nastavenia zariadenia,
   3. otestovanie jednotlivých sieťových prepojení.

e) S postupmi pri haváriách, poruchách a mimoriadnych situáciách, ktoré sledujú efektívnu obnovu systému, je potrebné oboznámiť všetkých vedúcich zamestnancov.

PaedDr. Eva Rabčanová
Riaditeľ školy