Smernica riaditeľky CPPPaP

číslo 12 /2014

INFORMAČNÁ BEZPEČNOSŤ

SMERNICA NADOBÚDA ÚČINNOSŤ DŇOM JEJ VYDANIA

SCHVÁLILA: **MGR. DGMAR KÚTNA, RIAD. CPPPAP**

Obsah

1. ÚČEL VYDANIA SMERNICE

Cieľom Smernice riaditeľky Centra pedagogicko-psychologického poradenstva a prevencie v Dubnici nad Váhom č. 06/2014 *Informačná bezpečnosť* je upraviť pravidlá a podmienky bezpečného používania a bezpečnej správy informačného systému; vymedzuje bezpečnosť pracovných staníc, počítačovej siete a upraviť povinnosti používateľov informačných systémov a ďalšie práva a povinnosti súvisiace so zabezpečením informačnej bezpečnosti v Centre pedagogicko-psychologického poradenstva a prevencie Dubnica nad Váhom(ďalej len CPPPaP) v súlade so zákonom č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

2. ROZSAH PLATNOSTI

Smernica č. 06/2014 *Informačná bezpečnosť* je záväzná pre všetkých zamestnancov CPPPaP, na ktorých sa vzťahuje zákon NR SR č. 552/2003 Z. z. o výkone práce vo verejnom záujme (ďalej len zákon o výkone práce).

3. SÚVISIACA LEGISLATÍVA

- Zákon NR SR č. 552/2003 Z.z. o výkone prác vo verejnom záujme v znení neskorších predpisov
- Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
- Zákon č. 618/2003 Z. z. o autorskom práve a o právach súvisiacich s autorským právom (autorský zákon) v znení neskorších predpisov
- Zákon č. 610/2003 Z. z. o elektronických komunikáciách v znení neskorších predpisov
- Zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov
- Nariadenie vlády č. 216/2004 Z. z. ktorým sa ustanovujú oblasti utajovaných skutočností
- Zákon č 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
- Zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ochrane osobných údajov“)

4. POJMY A SKRATKY

- **Autorizácia** – oprávnenie na prístup k aktívu, alebo na vykonávanie činnosti. Proces overovania, zisťovania prístupových práv.
- **Bezpečnosť** – vlastnosť objektu alebo subjektu, ktorá určuje mieru jeho ochrany proti možným škodám. Taktiež stav, pri ktorom je riziko poškodenia aktív obmedzené na prijateľnú úroveň.
- **Bezpečnostný incident** – udalosť ktorá bezprostredne ohrozila aktívum alebo činnosť univerzity v rozpore s platnou bezpečnostnou politikou.

- **Chránené údaje/informácie** – najmä databázy osobných údajov a ďalšie informácie, ktoré správca označí za chránené.
- **Dôvernosť** – zabezpečenie toho, že k informáciám majú prístup len tí, ktorí majú na to autorizáciu.
- **Hrozba** – čokoľvek, čo môže spôsobiť škodu. Akcia alebo udalosť, ktorá môže ohroziť bezpečnosť aktíva.
- **Informačná bezpečnosť** – bezpečnosť informácií a všetkých ostatných aktív informačných technológií a informačných systémov. Informačná bezpečnosť je súčasťou celkovej bezpečnosti.
- **Informačný systém** – súbor technických a programových prostriedkov, záznamových médií, dát a personálu, ktoré sa používajú na spracovanie informácií v určitej oblasti pôsobenia.
- **Integrita** – neporušenosť, celistvosť, presnosť, kompletnosť.
- **Opatrenia, bezpečnostné opatrenia, ochranné opatrenia** – prax, postupy, alebo mechanizmy, ktoré znižujú bezpečnostné riziká.
- **Osobné údaje** – osobné údaje v znení zákona o ochrane osobných údajov.
- **Pracovná stanica** – počítač určený na priame fyzické používanie používateľom.
- **Riziko** – potenciálna možnosť, že daná hrozba využije zraniteľnosť aktív a spôsobí tak stratu alebo zničenie aktív.
- **Správca** – osoba, ktorá má na starosti správu, prevádzku, údržbu aktíva.
- **Spracovanie informácií** – manipulácia, uchovávanie, prezentácia, respektíve ochrana informácií.
- **Zamestnanec** – osoba, ktorá má pracovnoprávny vzťah s CPPPaP Dubnica nad Váhom (tiež **používateľ**).

5. POPIS ČINNOSTI

5.1 Kategorizácia a klasifikácia informácií a pracovných staníc

1. Údaje CPPPaP sú klasifikované podľa ich citlivosti a potrebnej úrovne ochrany. CPPPaP pre svoje potreby klasifikuje údaje na tri základné úrovne:
    a. Verejné - údaje verejne prístupné komukoľvek (napríklad údaje na webovej stránke).
    b. Interné - údaje určené iba na interné použitie v rámci organizácie, odhalenie týchto dát verejnosti, alebo osobe mimo organizácie by mohlo spôsobiť žiadne, alebo iba malé škody. Interné pracovné stanice slúžia ako učebné pomôcky. Tieto zariadenia musia byť technicky zabezpečené tak, aby nemohli ohroziť bezpečnosť ostatných aktív CPPPaP. Nesmú byť používané na prístup k osobným údajom.
    c. Chránené - údaje určené iba pre oprávnené osoby v rámci organizácie alebo mimo nej. Odhalenie týchto dát neoprávnenej osobe by mohlo spôsobiť stredné alebo vážne škody.
2. Pracovné stanice, na ktorých prebieha spracovanie osobných údajov sú klasifikované ako chránené. Klasifikáciu ostatných pracovných staníc určuje ich správca.
3. Správca zmení klasifikáciu pracovnej stanice používateľa na internú na základe žiadosti používateľa, ak sú splnené všetky nasledovné podmienky:
    a. používateľ má dostatočné bezpečnostné povedomie, dokáže zaistiť bezpečnosť pracovnej stanice a dokáže zabrániť tomu, aby sa pracovná stanica stala zdrojom útoku,
    b. na pracovnej stanici nebudú spracúvané osobné údaje.

4. Osobná pracovná stanica je zariadenie v osobnom majetku zamestnanca. Za bezpečnosť osobnej pracovnej stanice zodpovedá jej používateľ. Používateľ osobnej pracovnej stanice stráca nárok na technickú podporu poskytovanú správcom. Na osobnej pracovnej stanici sa nesmú spracovávať chránené údaje.

5.2 Spracovanie osobných údajov

1. Používatelia môžu na spracúvanie databáz osobných údajov používať len chránené pracovné stanice.
2. Každý export osobných údajov mimo CPPPaP, s výnimkou zákonom požadovaných exportov, musí byť schválený riaditeľom CPPPaP, pričom musia byť dodržané ustanovenia zákona o ochrane osobných údajov.

5.3 Zálohovanie dát

1. Ak nie je uvedené inak, pre všetky informačné systémy platí stratégia zálohovania dát.
2. Smernica riaditeľky Centra pedagogicko-psychologického poradenstva a prevencie Dubnica nad Váhom č. *Zálohovanie údajov* konkretizuje podmienky, spôsob a postup, akým sa budú údaje zálohovať v CPPPaP.

5.4 Bezpečnosť pracovných staníc

1. Softvér môže na počítač inštalovať len jeho správca.
2. Pracovné stanice klasifikované ako chránené musia mať aplikované nasledovné bezpečnostné opatrenia a nastavenia:
    a. Nastavenie automatickej inštalácie bezpečnostných záplat operačného systému s minimálnou periódou jeden deň.
    b. Záznam aktivít počítača (logovanie) vzdialene minimálne na úrovni záznamov o prihlásení a odhlásení používateľa.
    c. Vypnuté automatické zapamätávanie hesiel vo webovom prehliadači.
    d. Používateľ nesmie mať práva:
        - administrátora,
        - odmietnuť aktualizáciu operačného systému,
        - meniť nastavenia antivírusu,
        - zapisovať do iných ako správcom špecifikovaných adresárov a jeho domovského adresára,
        - meniť systémové nastavenia rozhraní (okrem prenosných počítačov).
    e. Nastavenia špecifické pre OS Windows:
        - nastavenie automatickej aktualizácie antivírusu s minimálnou periódou jeden deň,
        - zapnutá on-line kontrola všetkých súborov minimálne pri spúšťaní, alebo kontrola lokálnych diskov počítača aspoň raz týždenne.
    f. Automatické spúšťanie programov z externých dátových médií (autorun) musí byť vypnuté.
    g. Zakázané automatické načítavanie komponentov správy elektronickej pošty (najmä obrázkov) z internetových zdrojov pri prehliadaní správy elektronickej pošty.
    h. Zákaz bootovania z iných médií ako je primárny pevný disk.
    i. Zmeny v BIOS-e chránené heslom.
    j. Používateľ nesmie mať práva odmietnuť reštart, ak je potrebný pre účely aplikácie bezpečnostných záplat. Používateľ môže pozastaviť reštart najdlhšie však do konca pracovnej doby daného dňa.
    k. Používateľ nesmie mať práva používať iné ako správcom nainštalované programy.

l. Blokovanie rizikových komponentov webových prehliadačov (napr. ActiveX) okrem správcom špecifikovaných dôveryhodných stránok.

5.5 Fyzická bezpečnosť

1. Pracovné stolíky v kancelárii musia byť uzamykateľné.
2. Sieťové uzly musia byť chránené proti vandalizmu a neoprávnenému fyzickému prístupu. Kabeláž v priestoroch musí byť fyzicky chránená tak, aby bez násilného vniknutia nebolo možné fyzické pripojenie sieťového zariadenia.
3. Káble, patch-panely a sieťové zásuvky musia byť označené tak, aby bolo možné zistiť, ktorý kábel vedie do ktorej zásuvky, respektíve miestnosti.

5.6 Povinnosti používateľov

1. Pri používaní informačných systémov CPPPaP sa musia používatelia riadiť:
   a. používateľskými predpismi daných informačných systémov,
   b. pokynmi správcu informačného systému,
2. Ak používateľ nevie posúdiť bezpečnostné riziko, môže sa obrátiť na správcu.

5.7 Chránené informácie

1. Každý používateľ, ktorý disponuje prístupovými právami na prístup k databázam osobných údajov, musí byť poučený o zásadách ochrany informácií v súlade so všeobecne záväznými právnymi predpismi a vnútornými predpismi CPPPaP.
2. Používatelia môžu spracúvať alebo uchovávať chránené informácie (napr. databázy osobných údajov, správy z vyšetrení) v nešifrovanej elektronickej forme len na chránených pracovných staniciach.
3. Dočasne vytvorené dokumenty obsahujúce chránené informácie musia byť po použití bezpečne zmazané, prípadne z nich musia byť odstránené chránené informácie.
4. Používateľ nesmie vystaviť riziku odcudzenia, prípadne poškodenia chránené informácie (napr. nesmie prenášať chránené informácie v nešifrovanej podobe na externých médiách mimo CPPPaP).

5.8 Heslá

1. Ak sa používateľ domnieva, že k jeho heslu získala prístup iná osoba, musí dané heslo okamžite zmeniť.
2. Ak je od používateľa požadovaná zmena hesla, nesmie si nastaviť také heslo, aké už používal v minulosti.
3. Používateľ:
   a. musí používať bezpečné heslo,
   b. môže zadávať heslo umožňujúce prístup k databázam osobných údajov len na chránených pracovných staniciach,
   c. nesmie v informačnom systéme CPPPaP používať rovnaké heslo ako v externých systémoch,
   d. nesmie umožniť iným osobám prístup ku svojim autorizačným prostriedkom (napr. heslu, USB Tokenu, ...),
   e. nesmie uchovávať heslo ani autorizačné prostriedky na miestach dostupných iným osobám (napr. na papieri v kancelárii, voľne uložené a pod.),
   f. nesmie zadávať svoje prístupové heslo do webových aplikácií, ktoré nie sú zabezpečené certifikátom dodávaným s webovým prehliadačom.

5.9 Pracovná stanica

1. Používateľ nesmie:
    a. robiť technické zásahy do počítača,
    b. neautorizovane meniť systémové nastavenia počítača,
    c. vynášať počítače z miestnosti bez povolenia správcu (s výnimkou prenosných počítačov),
    d. zapájať svoje alebo cudzie súkromné zariadenia do počítačovej siete CPPPaP,
    e. deaktivovať antivírus alebo iné bezpečnostné mechanizmy počítača,
    f. na počítačoch CPPPaP otvárať dátové nosiče, o ktorých sa domnieva, že obsahujú vírus,
    g. brániť kontrole počítača správcom,
    h. inštalovať softvér na chránenú pracovnú stanicu,
    i. ignorovať bezpečnostné varovné hlásenia počítača.
    j. získavanie neautorizovaného prístupu k systému CPPPaP alebo cudzím systémom,
    k. šírenie škodlivého kódu (tzv. malware, napr. počítačových vírusov) a nevyžiadanej elektronickej pošty,
    l. realizáciu sieťových útokov,
    m. narušovanie práce iných používateľov,
    n. znižovanie dostupnosti alebo kvality sieťových služieb,
    o. ďalšej škodlivej činnosti namierenej proti iným používateľom alebo systémom,
    p. činnosti v rozpore s platnou legislatívou SR.
2. Používateľ nesmie vykonávať činnosť za účelom získania prístupových práv alebo informácií, ktoré mu neprináležia. Ak takéto práva získa náhodne alebo vedome, nesmie ich použiť a musí o tom informovať príslušného správcu.
3. Zamestnanec nesmie umožniť prítomnosť cudzích osôb bez dozoru vo svojej kancelárii.
4. Ten, kto posledný opúšťa miestnosť, vypne pracovnú stanicu, miestnosť zamkne. Po skončení pracovnej doby musí aj zatvoriť všetky okná a zapnúť alarm. Podrobnejšie informácie určuje smernica riaditeľa CPPPaP č. *Ochrana majetku*.

5.10 Komunikácia

1. Pri vybavovaní žiadostí (napr. zadávanie informácií do informačného systému alebo poskytovanie informácií) si používateľ musí overiť, či žiadateľ má právo na požadovaný úkon a či je skutočne tou osobou, za ktorú sa vydáva.
2. Pri posielaní neverejných informácií prostredníctvom elektronickej pošty si musí používateľ overiť, či adresa, na ktorú správu posiela, skutočne patrí osobe, ktorej je správa určená.
3. Používateľ nesmie:
    a. posielať chránené informácie (napr. osobné údaje) mimo sieť CPPPaP (napr. na súkromné e-mailové adresy),
    b. poskytovať osobné údaje o klientoch alebo zamestnancoch CPPPaP tretím osobám,
    c. preposielať reťazové správy elektronickej pošty a iné podozrivé správy požadujúce, aby ich používateľ preposlal čo najväčšiemu množstvu ľudí (tzv. hoax),
    d. posielať nevyžiadané správy elektronickej pošty (tzv. spam),
    e. meniť hlavičky správ (napr. meniť meno alebo adresu odosielateľa).
4. Ak používateľ v e-mailovej komunikácii vystupuje ako zamestnanec CPPPaP, musí používať jemu správcom pridelenú oficiálnu e-mailovú adresu a to, ako adresu odosielateľa, tak aj ako tzv. reply-to adresu.
5. Pri odpovedaní alebo preposielaní správ elektronickej pošty musí používateľ skontrolovať zoznam adresátov a prípadnú predošlú komunikáciu, ktorá je obsahom

preposielanej správy.

6. E-mailová schránka a všetka elektronická komunikácia prechádzajúca cez počítačovú sieť CPPPaP je majetkom CPPPaP a správca ju môže kontrolovať.
7. Používateľ musí nahlásiť zistené bezpečnostné incidenty (napr. únik osobných údajov, únik hesiel iných používateľov, zneužitie informačných systémov) správcovi siete.

6. ZÁVEREČNÉ USTANOVENIA

1. Porušenie tejto smernice a súvisiacich predpisov sa považuje za porušenie pracovnej disciplíny.
2. CPPPaP môže pre vlastné potreby nakupovať len zariadenia schopné technicky spĺňať všetky touto smernicou na ne kladené bezpečnostné požiadavky.
3. Riaditeľka CPPPaP zabezpečí potrebnú súčinnosť aj prostriedky potrebné na splnenie bezpečnostných požiadaviek stanovených touto smernicou.