Katolícka univerzita v Ružomberku

Vnútorný predpis č. 1/2017

Bezpečnostná smernica

CZ 96/2017 RE

Platnosť od: 11.1.2017 Účinnosť od: 11.1.2017

V Ružomberku dňa: 10.1.2017

KATOLÍCKA UNIVERZITA V RUŽOMBERKU
formujúca myseľ i srdce

REKTOR
Hrabovská cesta 1A, 034 01 Ružomberok
www.ku.sk, tel.: +421 44 43 04 693, fax: +421 44 43 04 694, e-mail: rektor@ku.sk

CZ 96/2017 RE

Bezpečnostná smernica

Obsah:

Hlava I. Všeobecné ustanovenia 2
Čl. 1 Účel smernice 2
Čl. 2 Základné pojmy 2
Hlava II. Zodpovednosť za ochranu osobných údajov 3
Čl. 3 Zodpovedná osoba 3
Čl. 4 Kontrolná činnosť 4
Hlava III. Osobné údaje v správe univerzity 4
Čl. 5 Manipulácia s osobnými údajmi 4
Čl. 6 Manipulácia s médiami 6
Hlava IV. Prostriedky informačných technológií 6
Čl. 7 Správca informačných technológií 6
Čl. 8 Zálohovanie a archivovanie údajov 6
Čl. 9 Prístupové práva 7
Čl. 10 Pracovné stanice na ktorých sa pracuje s osobnými údajmi 7
Čl. 11 Zamestnanci externej organizácie 8
Čl. 12 Prístup do siete internet a mailová komunikácia 8
Čl. 13 Antivírová ochrana 8
Čl. 14 Bezpečnostné incidenty 8
Čl. 15 Havarijné plánovanie 9
Čl. 16 Záverečné ustanovenia 9

Hlava I.
Všeobecné ustanovenia

Čl. 1
Účel smernice

a) Smernica upravuje niektoré práva a povinnosti všetkých zamestnancov Katolíckej univerzity v Ružomberku (ďalej len univerzita) a iných oprávnených osôb predovšetkým v oblasti ochrany osobných údajov.
b) Smernica upresňuje a aplikuje závery vyplývajúce z analýzy bezpečnosti informačných systémov a vymedzuje rozsah bezpečnostných opatrení z hľadiska ochrany osobných údajov.
c) Smernica stanovuje pravidlá pre ochranu osobných údajov. Tieto pravidlá sú povinní dodržiavať všetci zamestnanci univerzity a iné oprávnené osoby.
d) S touto smernicou musia byť oboznámení všetci zamestnanci univerzity a iné oprávnené osoby, ktoré sa podieľajú na spracovávaní osobných údajov v mene univerzity.

Čl. 2
Základné pojmy

a) **Zákon** – zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

b) **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.

c) **Zodpovedná osoba** – fyzická osoba poverená výkonom dohľadu nad ochranou osobných údajov v zmysle § 23 Zákona.

d) **Oprávnená osoba** - každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovnoprávneho vzťahu, 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.

e) **Dotknutá osoba** - je každá fyzická osoba, ktorej sa osobné údaje týkajú.

f) **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.

g) **Sprístupňovanie osobných údajov** – sprístupňovaním osobných údajov je oznámenie osobných údajov, alebo umožnenie prístupu k nim príjemcovi, ktorý ich ďalej nespracúva.

h) **Poskytovanie osobných údajov** – poskytovaním osobných údajov je odovzdávanie osobných údajov tretej strane, ktorá ich ďalej spracúva.

i) **Súhlas dotknutej osoby** – je akýkoľvek slobodne daný výslovný a zrozumiteľný prejav vôle, ktorým dotknutá osoba na základe poskytnutých informácií vyjadruje súhlas so spracúvaním svojich osobných údajov.

j) **Likvidácia osobných údajov** – rušenie osobných údajov rozložením, vymazaním, alebo fyzickým zničením hmotných nosičov tak, aby sa z nich osobné údaje nedali reprodukovať.

k) **Informačný systém osobných údajov (IS)** – je 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 tejto smernice rozumie aj súbor osobných údajov, ktoré sú spracúvané, alebo pripravené na spracúvanie čiastočne automatizovanými alebo inými ako automatizovanými prostriedkami spracúvania.

l) **Všeobecne použiteľný identifikátor** - všeobecne použiteľným identifikátorom je trvalý identifikačný osobný údaj dotknutej osoby, ktorý zabezpečuje jej jednoznačnosť v informačných systémoch (zvyčajne ide o rodné číslo).

m) **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.

n) **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.

o) **Aktíva** – sú všetky hmotné i nehmotné hodnoty, ktoré univerzita vlastní alebo využíva. Medzi hmotné aktíva patria najmä servery, počítače, počítačové siete, komunikačné zariadenia a ďalšie hmotné predmety vo vlastníctve univerzity. Medzi nehmotné aktíva patria najmä informačné systémy, pracovné postupy, know-how, údaje o zamestnancoch, ekonomické a finančné údaje a majetkové a obdobné práva.

p) **Hrozby** – sú vplyvy okolia, iných osôb, zariadení a prostriedkov, ktoré úmyselne, alebo neúmyselne vplývajú na aktíva univerzity tak, že ich univerzita nemôže využívať, alebo inak ohrozujú oprávnené záujmy univerzity.

q) **Externá organizácia** – organizácia 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, ako aj za dohľad nad ochranou osobných údajov, zodpovedá univerzita. Rektor univerzity poveruje organizáciou bezpečnosti a ochrany osobných údajov, ako aj dohľadom nad ochranou osobných údajov, zodpovednú osobu alebo niekoľko zodpovedných osôb.

b) Zodpovedná osoba je povinná zabezpečovať:
   1. vypracovanie a pravidelnú aktualizáciu „Bezpečnostného projektu“, pokiaľ je aktualizácia potrebná,
   2. vypracovanie a aktualizáciu evidenčných listov informačných systémov univerzity, v ktorých sú osobné údaje v elektronickej alebo papierovej forme,
   3. dodržiavanie Zákona pri získavaní osobných a citlivých údajov, ich poskytovaní, sprístupňovaní, prípadne zverejňovaní,
   4. kontrolu, či pri spracúvaní osobných údajov v informačnom systéme nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb,
   5. informovanie o zistení narušenia práv a slobôd dotknutých osôb pri spracúvaní osobných údajov, alebo porušení zákonných ustanovení v priebehu spracúvania osobných údajov rektora univerzity,

6. posúdenie, či osobné údaje svojím obsahom a rozsahom zodpovedajú účelu spracúvania, resp. či sú s daným účelom zlučiteľné,
7. kontrolu nad spracúvaním osobných údajov, či sú spracúvané aktuálne osobné údaje a či je vykonávaná likvidácia osobných údajov po splnení účelu ich spracovania,
8. posúdenie, či daným spracúvaním môže byť poverený sprostredkovateľ, ak je záujem na tom, aby spracúvanie vykonával,
9. určenie, ktoré podmienky ustanovené Zákonom je potrebné pri spracúvaní osobných údajov aplikovať,
10. posúdenie, či možno vykonávať cezhraničný tok osobných údajov, ak sa požaduje,
11. organizáciu školení zamestnancov ohľadom informačnej bezpečnosti minimálne raz za dva roky,
12. poučenie oprávnených osôb o ich právach a povinnostiach predtým, ako získajú prístup k osobným a citlivým údajom.

Čl. 4
Kontrolná činnosť

a) Úlohou kontrolnej činnosti je zisťovanie stavu bezpečnosti a ochrany informačných systémov, v ktorých sa osobné údaje spracovávajú a výkon dozoru nad plnením tejto smernice. Kontrolnú činnosť vykonáva zodpovedná osoba.
b) Každý zamestnanec je povinný poskytnúť všetky informácie potrebné pre vykonanie kontroly.
c) Zodpovedná osoba je povinná zabezpečiť výkon kontrolnej činnosti priebežne.
d) Zodpovedná osoba má právo oboznámiť sa s výsledkami inej kontroly, ktorá bola vykonaná a ktorej predmetom nebolo zisťovanie stavu ochrany a bezpečnosti informačných systémov, v ktorých sa osobné údaje spracovávajú. Ak vo výsledkoch a záveroch kontroly sú skutočnosti, ktoré signalizujú, alebo informujú o narušení bezpečnosti a ochrany osobných údajov, je zodpovedná osoba povinná uvedené skutočnosti okamžite prešetriť.
e) Výsledky kontroly predkladá zodpovedná osoba rektorovi univerzity.

Hlava III.
Osobné údaje v správe univerzity

Čl. 5
Manipulácia s osobnými údajmi

a) Oprávnená osoba musí byť poučená v zmysle Zákona. Toto poučenie musí byť v súlade s jeho pracovnou náplňou. Poučenie zabezpečuje zodpovedná osoba.
b) Osobné údaje musia byť ukladané a prenášané len zabezpečeným spôsobom.
c) Zabezpečenie osobných údajov sa vykonáva nasledovnými opatreniami:
   1. Dokumenty na papieri a na pamäťových médiách, ktoré obsahujú osobné údaje, musia byť zabezpečené pred neoprávneným prístupom (napr.: ukladané v uzamykateľnej skrini, ktorá je umiestnená v uzamykateľnej miestnosti).
   2. Prenášanie papierových dokumentov s osobnými 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 alebo inak zabezpečené pred neoprávneným vniknutím. Dokumenty a obrazovky počítačov musia byť umiestnené tak, aby nepovolané osoby z nich nemohli prečítať osobné údaje. Pracoviská, kde nie je možné zabezpečiť uzamknutie priestorov, je potrebné inak zabezpečiť pred neoprávneným prístupom k osobným údajom.
   4. Zhotovovať (tlačiť) dokumenty s osobnými údajmi na zariadeniach, ktoré nie sú zabezpečené pred neoprávneným prístupom, napr. tlačiarne umiestnené na chodbách, kde majú prístup

študenti alebo verejnosť, sa povoľuje len za podmienky, že bude zamedzený prístup neoprávneným osobám k vytlačeným dokumentom obsahujúcim osobné údaje.

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. Zakazuje sa poskytovať a sprístupňovať osobné údaje cez telefón alebo inými nezabezpečenými komunikačnými nástrojmi.

d) Pri získavaní a spracúvaní osobných údajov sú oprávnené osoby povinné dodržiavať nasledovné záväzné pravidlá:
   1. Pri získavaní osobných údajov do jednotlivých IS v rámci prevádzkovateľa 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 náplne práce spracúva osobné údaje fyzických osôb a je oprávnená osoba podľa § 21 Zákona.
   3. Pri získavaní a spracúvaní osobných údajov je oprávnená osoba povinná zabezpečiť ochranu osobných údajov pred ich sprístupnením inej neoprávnenej osobe.
   4. Oprávnená osoba kontroluje a overuje správnosť a aktuálnosť osobných údajov po ich získaní a zaradení v IS.
   5. Spracúvať len správne, úplne a podľa potreby aktualizované osobné údaje vo vzťahu k účelu spracúvania.
   6. Ak je to možné, tak nesprávne a neúplné osobné údaje bez zbytočného odkladu opraviť alebo doplniť.
   7. Pred získavaním osobných údajov od dotknutej osoby túto osobu ústne alebo písomne oboznámiť s názvom a sídlom univerzity, s účelom spracúvania osobných údajov, s rozsahom spracúvania osobných údajov, o predpokladanom okruhu tretích strán pri poskytovaní osobných údajov, alebo príjemcov, o predpokladanom sprístupňovaní osobných údajov, o forme zverejnenia, ak sa osobné údaje zverejňujú, a o tretích krajinách, ak sa predpokladá, alebo je zrejmé, že sa do týchto krajín uskutoční cezhraničný prenos osobných údajov.
   8. Poučiť dotknutú osobu o dobrovoľnosti, alebo povinnosti poskytnutia osobných údajov a o existencii jej práv podľa § 28 Zákona.
   9. Zabezpečiť preukázateľný súhlas na spracúvanie osobných údajov dotknutej osoby v informačnom systéme osobných údajov univerzity, ak sa osobné údaje spracúvajú na základe súhlasu dotknutej osoby, alebo ak to vyžaduje Zákon.
   10. Preukázať príslušnosť oprávnenej osoby k univerzite hodnoverným dokladom (napr. služobným preukazom).
   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 a poškodením a 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) okrem osobných údajov, ktoré sú súčasťou obsahu registratúrnych záznamov univerzity.

e) Zamestnanci sú povinní zachovávať mlčanlivosť o osobných údajoch, s ktorými prídu do styku. Tie nesmú využiť ani pre osobnú potrebu a bez súhlasu nadriadeného ich nesmú zverejniť, nikomu poskytnúť a ani sprístupniť. Túto mlčanlivosť sú povinní zachovať aj po skončení spracovávania osobných údajov, alebo po skončení pracovného pomeru.

Čl. 6
Manipulácia s médiami

a) Všetky médiá s osobnými údajmi musia byť uložené v bezpečnom a chránenom prostredí.
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 elektronických médiách je potrebné dbať na zabezpečenie neoprávneného prístupu k týmto údajom v prípade straty alebo odcudzenia média, napríklad zašifrovaním, použitím kódovateľných médií a podobne.
d) Osobné údaje uchované na médiách (elektronických alebo papierových), ktoré už splnili svoj účel musia byť bezpečne, spoľahlivo a neobnoviteľne zlikvidované.

Hlava IV.
Prostriedky informačných technológií

Čl. 7
Správca informačných technológií

a) Správca informačných technológií (ďalej IT) je osoba alebo osoby poverené dohľadom a správou výpočtovej techniky, počítačových aplikácií a počítačových sietí univerzity. Správcami IT sú napríklad správca helpdesk, správca siete, správca dátového centra a správca informačného systému.
b) Správa informačných technológií musí byť organizovaná tak, aby sa minimalizovala hrozba zneužitia postavenia administrátora, zamestnanca univerzity, ktorý má prístupové práva k administratívnemu rozhraniu informačného systému, v ktorom sa spracovávajú osobné údaje.
c) Za ochranu dát IS je zodpovedný správca IT, poverený dohľadom a správou tohto IS. K tomuto účelu vykonáva správca IT 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.
d) Správca IT je zodpovedný za to, že osobné údaje a prístup k nim budú chránené aktuálnou verziou zabezpečovacích softvérových a hardvérových prostriedkov (antivírusovej ochrany, firewallom a inými zabezpečovacími prostriedkami). Držitelia pracovných staníc, na ktorých sú osobné údaje, sú povinní informovať správcu IT o tom, že zabezpečovacie softvérové a hardvérové prostriedky na ich pracovnej stanici sú nefunkčné alebo vykazujú chybové hlásenia.
e) Správca IT je povinný dbať na to, aby IS bol v aktuálnej verzii. Ak je úroveň zabezpečenia novej verzie vyššia, ako tej predchádzajúcej, je správca IT povinný iniciovať aktualizáciu IS.
f) Pri konfigurácii softvérových a hardvérových prostriedkov, ktoré prichádzajú do styku s osobnými údajmi, správca IT dbá na to, aby sa používali len tie prostriedky, ktoré sú nevyhnutné pre plnenie pracovných úloh a potrieb univerzity a aby k dátam na týchto prostriedkoch, ak je to možné, mali prístup len oprávnené osoby na to určené.

Čl. 8
Zálohovanie a archivovanie údajov

a) Zálohovanie údajov sa vykonáva na zálohovacie zariadenia, médiá tak, aby bola možná obnova dát s osobnými údajmi v prípade zlyhania IS. Zálohovacie zariadenia, média, musia byť uskladnené tak, aby stratou dát na produkčných systémoch nedošlo zároveň k strate

zálohovaných dát (napr. z dôvodu živelnej udalosti). Dáta zo zálohovacích zariadení, médií, musia byť zabezpečené pred skopírovaním, odcudzením či zneužitím, neoprávneným prístupom.

b) Archivovanie údajov sa vykonáva na archivačné zariadenia, médiá, registratúrne hárky tak, aby bol možný prístup k osobným údajom spätne v zmysle Zákonom a univerzitou stanovených pravidiel uchovávania osobných údajov. Archivované údaje nesmú byť uskladnené v miestnosti, kde je prevádzkovaný IS, ktorého dáta sa zálohujú alebo kde je uskladnená záloha IS. Archivované údaje musia byť zabezpečené pred skopírovaním, odcudzením či zneužitím, neoprávneným prístupom.

Čl. 9
Prístupové práva

a) Zamestnanci, pre zabezpečenie prístupu k osobným údajom, nesmú mať heslá kratšie ako 8 znakov. Zamestnanec 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 a jedno číslo alebo špeciálny znak.
b) Zamestnancom sa zakazuje zverejňovať alebo vyzradiť prihlasovacie údaje (heslá) inej osobe. Taktiež sa zakazuje držanie zoznamu hesiel (napr. na papieri, v softvérovom súbore, alebo prenosnom zariadení), ak takýto zoznam nemôže byť bezpečne uložený.
c) Používateľ sa nesmie žiadnymi prostriedkami pokúšať získať prístupové práva alebo privilegovaný stav, ktorý mu nebol pridelený.
d) Správca IT, ktorý spravuje prístup k IS je povinný bez odkladu odobrať prístupové práva zamestnancovi, s ktorým bol rozviazaný pracovný pomer a to na podnet z personálneho oddelenia.

Čl. 10
Pracovné stanice, na ktorých sa pracuje s osobnými údajmi

Pracovnou stanicou sa pre účely tejto smernice rozumie personálny počítač, notebook, tenký klient alebo iné hardvérové zariadenie v majetku univerzity, na ktorom sa spracovávajú, uchovávajú alebo likvidujú osobné údaje.

a) Zamestnanec môže na pracovných staniciach používať výlučne len programové vybavenie nainštalované správcom IT, resp. nainštalované s ich preukázateľným súhlasom. Inštalovanie softvéru na pracovné stanice zamestnancom, za účelom napríklad výučbového procesu, je na plnej zodpovednosti zamestnanca vzhľadom k porušeniu Zákona.
b) 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.
c) Zamestnanec je pred opustením pracoviska povinný ukončiť prácu s aplikačným programovým vybavením a odhlásiť sa zo svojho prístupu k IS.
d) Pri krátkodobej neprítomnosti môže zamestnanec nahradiť odhlásenie sa z IS spustením šetriča obrazovky s heslom, resp. jej uzamknutím.
e) 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. Prípadné odchýlky od požadovaného stavu je povinný čo najúplnejšie zdokumentovať a bezodkladne ohlásiť správcovi IT.
f) Zakazuje sa používať na prenos či archiváciu osobných dát USB zariadenia, ktoré nie sú zabezpečené pred neoprávneným prístupom, napríklad heslom.

Čl. 11
Zamestnanci externej organizácie

a) Prístup zamestnancov externej organizácie do informačných systémov zriaďuje ten správca IT, ktorý má v správe príslušný IS.
b) Správca IT vydá zamestnancovi externej organizácie prístupové práva a heslo podľa článku 9 tejto smernice.
c) Správca IT je povinný zabezpečiť bezpečný šifrovaný prístup.
d) Správca IT je povinný bez odkladu po ukončení dôvodu, pre ktorý bol zriadený prístup, tento prístup zrušiť.
e) Zodpovedná osoba je povinná poučiť zamestnancov externej organizácie o ochrane osobných údajov a o mlčanlivosti ohľadom osobných a citlivých údajov. Táto skutočnosť musí byť zakomponovaná do zmluvy s externou organizáciou.

Čl. 12
Prístup do siete internet a mailová komunikácia

Každý zamestnanec, ktorému bol umožnený prístup do siete internet, je povinný rešpektovať nasledovné zásady:

1. prístup do siete internet využívať len v súlade so svojou pracovnou náplňou,
2. dodržiavať etické zásady a zdržiavať sa činností, ktoré by mohli viesť k poškodeniu dobrého mena univerzity, alebo k iným škodám,
3. v prípade potreby prenosu osobných údajov cez internet je nevyhnutné tieto údaje pred prenosom zabezpečiť šifrovaním,
4. je zakázané zo siete internet preberať nelegálny obsah (softvér, súbory chránené autorskými právami a pod.),
5. obsah dát odosielaných v rámci siete univerzity a cez internet nesmie byť v rozpore s dobrými mravmi,
6. rešpektovať zákaz posielať reťazové a hromadné e-maily, reklamné správy a pod., pokiaľ tieto nie sú nevyhnutnou súčasťou vedeckej práce alebo výučbového procesu alebo neboli prikázané nadriadeným.

Čl. 13
Antivírová ochrana

a) Správcovia IT sú zodpovední za zabezpečenie antivírovej ochrany a za inštaláciu a pravidelnú aktualizáciu softvéru potrebného na zabezpečenie tejto ochrany. Držitelia pracovných staníc sú povinní informovať správcu IT o tom, že antivírová ochrana na ich pracovnej stanici je nefunkčná alebo že uvádza chybové hlásenia.
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 príslušnému 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 univerzity).

Čl. 14
Bezpečnostné incidenty

a) Bezpečnostným incidentom je každé ohrozenie IS, ktorého následkom by mohlo dôjsť k neoprávnenému prístupu k osobným údajom, k ich strate, zmene či zneužitiu.

b) Detekcia incidentov je súbor činností a opatrení vedúcich k včasnému zisteniu bezpečnostného incidentu, resp. k včasnému zisteniu, že incident môže spôsobiť narušenie spracovania osobných údajov.
c) 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 prostriedkami – sú to napríklad špecializované programy, ktoré vyhodnocujú prevádzkové záznamy a indikujú potenciálny incident.
   3. Sústavnou činnosťou zamestnancov – primeraná ostražitosť zamestnancov.
   4. Vykonávaním kontrol na pracoviskách.
d) Pri zistení incidentu musí byť o tomto informovaná zodpovedná osoba.

Čl. 15
Havarijné plánovanie

a) Havarijné 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 pracovnej stanice,
   2. náhradnú pracovnú stanicu,
   3. reinštaláciu alebo inštaláciu OS a konfiguráciu,
   4. inštaláciu aplikácií a antivírovej ochrany,
   5. nastavenie prístupových práv,
   6. v prípade neodkladnosti prístup k IS z inej funkčnej pracovnej stanice.
c) V prípade výpadku servera je správca IT povinný po identifikácií 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,
   4. obnovenie systémových a konfiguračných súborov zo záložných kópií,
   5. inštaláciu antivírovej ochrany, ak je to potrebné,
   6. inštaláciu IS a obnovenie dát zo záložných médií.
d) V prípade výpadku sieťového prepojenia je správca IT povinný po identifikácií problému zabezpečiť:
   1. opravu alebo výmenu chybného aktívneho, alebo pasívneho prvku počítačovej siete,
   2. obnoviť konfiguračné nastavenia zariadenia,
   3. otestovať jednotlivé sieťové prepojenia.
e) S postupmi pri haváriách, poruchách a mimoriadnych situáciách, ktoré sledujú efektívnu obnovu systému, je potrebné oboznámiť všetkých vedúcich zamestnancov.

Čl. 16

Záverečné ustanovenia

a) Vnútorný predpis nadobúda platnosť a účinnosť dňom podpisu.
b) Dňom nadobudnutia platnosti Vnútorného predpisu č. 1/2017 (CZ 96/2017), sa ruší Vnútorný predpis č. 9/2016 Bezpečnostná smernica (CZ 391/2016 RE).

V Ružomberku dňa 10.1.2017

prof. ThDr. Jozef Jarab, PhD.,
rektor KU