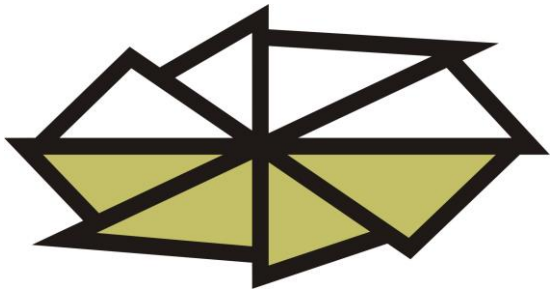
Technická univerzita vo Zvolene



Číslo 5/2014

Bezpečnostná smernica

Obsah

Prvá časť
Všeobecné ustanovenia

Čl. 1

Účel smernice

1) Smernica upravuje niektoré práva a povinnosti všetkých zamestnancov Technickej univerzity vo Zvolene (ďalej len univerzita), v oblasti ochrany a bezpečnosti majetku, informácií a ďalších hodnôt, ktoré univerzita vlastní.
2) Smernica upravuje práva a povinnosti oprávnených osôb v oblasti ochrany, získavania, manipulácie a likvidácie osobných údajov podľa zákona 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (Príloha č.1).
3) Súčasťou smernice sú ustanovenia upravujúce bežné vzťahy zamestnancov, činnosť zamestnancov, povinnosti a práva v dobe ohrozenia univerzity, v dobe útoku na chránené hodnoty a záujmy univerzity a v dobe po odstránení hrozby alebo odvrátení útoku.

Čl. 2

Základné pojmy

1) Aktíva – sú všetky hmotné i nehmotné hodnoty, ktoré univerzita vlastní, alebo využíva a slúžia najmä na plnenie ich služieb obyvateľstvu. Medzi hmotné aktíva patria najmä administratívne priestory, počítače, počítačové siete, komunikačné zariadenia a ďalšie hmotné predmety vo vlastníctve univerzity. Medzi nehmotné aktíva patria pracovné postupy, know-how, údaje o zamestnancoch a študentoch, ekonomické, finančné a obchodné údaje, majetkové práva a ďalší nehmotný majetok. Medzi aktíva patria tiež osoby, ktoré sú v zamestnaneckom, obchodnom a majetkovom vzťahu k univerzite.
2) 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.
3) Bezpečnostné opatrenie – je súbor činností, zariadení a postupov, ktoré vykonáva univerzita na ochranu aktíva pred hrozbou. Rozlišujú sa proaktívne a reaktívne bezpečnostné opatrenia.
4) Proaktívne bezpečnostné opatrenie – je bezpečnostným opatrením, ktoré je vykonávané v dobe, kedy sa hrozba voči aktívu neuplatňuje (preventívne opatrenie) a jeho cieľom je hrozbu úplne odvrátiť (znemožniť jej na aktívum pôsobiť) alebo znížiť jej účinnosť tak, aby dopady na univerzitu boli čo najnižšie.
5) Reaktívne bezpečnostné opatrenie – je opatrenie, ktoré sa vykonáva v dobe, keď sa hrozba realizuje a vplýva na konkrétne aktívum. Jeho cieľom je účinne zabrániť ďalšiemu pôsobeniu hrozby a tak minimalizovať jej účinky a zároveň vytvoriť predpoklady pre efektívne a skoré obnovenie aktíva a návrat do stavu pred pôsobením hrozby.
6) Bezpečnostný incident – je pôsobenie hrozby na aktívum a jej uplatnenie tak, že univerzite vznikajú škody bez ohľadu na ich rozsah a povahu.
7) Riziko – je odhad pravdepodobnosti možného pôsobenia konkrétnej hrozby na konkrétne aktívum (incidentu) vo vzťahu k predpokladanému dopadu na univerzitu.
8) Riadenie rizika – je súbor organizačných a ekonomických rozhodnutí a opatrení, ktorých účelom je nájsť optimálny pomer medzi ekonomickou náročnosťou vynaloženého úsilia na proaktívne opatrenie a jeho odhadovaným efektom.
9) Prevádzkový záznam – je záznam o chode a činnosti technického prostriedku, organizačnej súčasti a pod., a to najmä ak sú považované za aktíva.
10) Externá organizácia – organizácia alebo univerzita vstupujúca do informačného systému za účelom jeho údržby alebo obnovy.

11) Mobilné zariadenia – považujú sa prostriedky spracovania ako sú notebooky, palmtopy, laptopy, smart karty a mobilné telefóny.
12) Cloudové dátové úložisko (cloud) – zálohovanie dát na vzdialených serveroch.

Čl. 3

Bezpečnostný správca

1) Za organizáciu bezpečnosti a ochrany všetkých aktív univerzity, za poznávanie hrozieb a rizík zodpovedá „Bezpečnostný správca".
2) Bezpečnostného správcu menuje do funkcie rektor univerzity.
3) Bezpečnostný správca zodpovedá za:
   a) Vypracovanie a pravidelnú aktualizáciu „Bezpečnostného projektu". Prehodnotenie odhadov rizík vykonáva najmenej jedenkrát za rok.
   b) Bezpečnú, plynulú a spoľahlivú prevádzku informačných systémov univerzity z pohľadu informačnej bezpečnosti.
   c) Pridelenie aktív do správy Správcom aktív, ktorí potom zodpovedajú za ich ochranu a bezpečnosť. O pridelení aktív je povinný viesť si inventár, v ktorom je vymedzený účel používania aktíva.
   d) Zabezpečenie a organizáciu pravidelných školení zamestnancov ohľadom informačnej bezpečnosti.
   e) Poučenie zamestnancov univerzity a tretích strán o svojich právach a povinnostiach predtým, ako získajú prístup k informačným systémom univerzity.

Čl. 4

Správa aktív univerzity

1) Aktíva univerzity sa na účely tejto smernice členia do nasledujúcich skupín:
   a) aktíva s vysokou ochranou - sú to tie aktíva, ktorých poškodenie alebo strata by ohrozila záujmy univerzity v plnom rozsahu,
   b) aktíva so zvýšenou ochranou – sú tie aktíva, ktorých poškodenie alebo strata by čiastočne ohrozili záujmy univerzity,
   c) aktíva obvyklej ochrany – sú to aktíva, ktorých individuálne poškodenie alebo strata spôsobia ľahko odstrániteľnú škodu alebo neohrozia záujmy univerzity.
2) Zaradenie predmetu alebo skutočnosti medzi aktíva vykonáva Bezpečnostný správca.
3) Zamestnanci používajúci aktívum so zvýšenou a vysokou ochranou sú povinní oznámiť správcovi tohto aktíva akúkoľvek skutočnosť, o ktorej sa domnievajú, že by mohla byť hrozbou pre dané aktívum.
4) Za ochranu a správu aktív obvyklej ochrany sú zodpovední zamestnanci, ktorí za tieto aktíva prevzali hmotnú zodpovednosť alebo im boli zverené do používania.
5) Aktívum sa môže používať len na ten účel, ktorý je deklarovaný v inventári aktív. Iné dočasné použitie je možné len so súhlasom bezpečnostného správcu.
6) Bezpečnostný správca pravidelne, najmenej jedenkrát za rok, zvoláva poradu Správcov aktív.

Čl. 5

Hrozby

1) Každý zamestnanec je povinný ohlásiť skutočnosti, ktoré by mohli indikovať zvýšenú pravdepodobnosť hrozby alebo jej pôsobenie, Bezpečnostnému správcovi, ktorémukoľvek Správcovi aktíva alebo svojmu nadriadenému.

2) Bezpečnostný správca posúdi na základe indikovanej zmeny stavu hrozieb a na základe poslednej platnej verzie rizikovej analýzy, ktoré aktíva môžu byť hrozbou dotknuté a upozorní o tejto skutočnosti Správcov aktív, ktoré hrozba môže ohroziť. Bezpečnostný správca, ak je to potrebné, rozhodne o zmene bezpečnostného režimu. Správcovia aktív sú povinní prijať okamžité opatrenia na odvrátenie alebo elimináciu hrozby. V nevyhnutných prípadoch môže opatrenie prijať Bezpečnostný správca. Bezpečnostný správca o prijatých opatreniach bezodkladne informuje Správcov dotknutých aktív.
3) Prijatie opatrení na odvrátenie alebo elimináciu hrozby oznámia Správcovia dotknutých aktív Bezpečnostnému správcovi a poskytnú mu všetky podklady potrebné k vypracovaniu Záznamu o bezpečnostnom incidente.

Čl. 6

Prevádzkové záznamy

1) Ak je vedený prevádzkový záznam o činnosti a chode technického prostriedku, ktorý je aktívom s vysokou ochranou, je povinnosťou Správcu tohto aktíva, v prípade bezpečnostného incidentu, vyhodnotiť tento záznam.
2) 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.

Čl. 7

Bezpečnostné incidenty

1) Detekcia incidentov je súbor činností a opatrení, vedúci k včasnému zisteniu bezpečnostného incidentu, resp. k včasnému zisteniu, že hrozba pôsobí na niektoré aktívum univerzity.
2) Detekcia sa vykonáva nasledovným spôsobmi:
   a) automatizovanými technickými prostriedkami – sú to napr. prostriedky hlásiace výskyt požiaru, senzory zisťujúce pohyb a pod.,
   b) automatickými informatickými (programovými) prostriedkami - sú to špecializované programy, ktoré vyhodnocujú prevádzkové záznamy, indikujú potenciálny incident,
   c) sústavnou činnosťou zamestnancov – primeraná ostražitosť zamestnancov, najmä Správcov aktív a Bezpečnostného správcu a výkon kontrolnej činnosti.
3) Ak výstupy z automatizovaných prostriedkov umožňujú záznam týchto výstupov, manipuluje sa s nimi ako s prevádzkovými záznamami.
4) Pri zistení incidentu musí byť o tomto informovaný Bezpečnostný správca a všetci správcovia dotknutých aktív. Na základe povahy incidentu a zasiahnutých aktív rozhodne Bezpečnostný správca o zmene bezpečnostného režimu univerzity.
5) O každom bezpečnostnom incidente musí byť spracovaný záznam. Záznam spracúva Bezpečnostný správca. Každý zamestnanec je povinný poskytnúť Bezpečnostnému správcovi všetky podklady a údaje, ktoré potrebuje pre spracovanie záznamu o bezpečnostnom incidente.
6) Záznam o bezpečnostnom incidente musí obsahovať:
   a) Dátum a čas, kedy incident bol zistený, kedy skončil, a ak je to možné, zistiť aj kedy incident začal.
   b) Opis spôsobu, ako bol incident zistený – uvedie sa najmä meno zamestnanca, ktorý incident ohlásil.
   c) Dátum a čas, kedy bol zmenený bezpečnostný režim univerzity.
   d) Chronologický opis priebehu incidentu, opis hrozieb, ktoré sa realizovali, a spôsob, akým sa realizovali.

e) Zoznam dotknutých aktív, doklad o škodách a predpokladaná doba zotavenia.
f) Porovnanie s rizikovou analýzou Bezpečnostného projektu – doklad, či bolo možné incident očakávať, či boli správne odhadnuté rizikové indexy a pod..
g) Opis prijatých opatrení – doklad, kedy a kým boli prijaté, doklad o ich účinnosti a trvaní.
h) Návrh na prijatie opatrení pre zamedzenie recidívy incidentu, odhad pravdepodobnosti recidívy, záznam o úprave rizikovej analýzy Bezpečnostného projektu, ak takúto úpravu bolo potrebné vykonať.
i) Zoznam opatrení a nariadení, ktoré boli porušené a mohli spôsobiť že incident nastal, zoznam zamestnancov ktorí tieto nariadenia porušili.

7) Ak nastal bezpečnostný incident vedomou alebo nevedomou činnosťou zamestnanca, bude sankcionovaný podľa príslušných ustanovení Zákonníka práce a Pracovného poriadku.

Čl. 8

Kontrolná činnosť

1) Kontrolná činnosť je súbor činností, ktorých úlohou je zisťovanie stavu bezpečnosti a ochrany aktív, stavu pripravenosti a účinnosti opatrení a výkon dozoru nad plnením tejto smernice.
2) Kontrolnú činnosť vykonáva Bezpečnostný správca a správcovia príslušného aktíva.
3) Každý zamestnanec je povinný poskytnúť všetky informácie, ktoré si kontrola vyžiada a sú vo vzťahu ku kontrolným úlohám.
4) Správa o výsledkoch kontroly musí obsahovať:
   a) chronologický opis priebehu kontrolnej činnosti,
   b) zoznam zistených nedostatkov,
   c) odporúčané opatrenia.
5) Bezpečnostný správca na základe skutočností uvedených v správe o výsledkoch kontroly nariadi vykonanie opatrení na odstránenie nedostatkov zistených kontrolou. Nariadenie musí mať písomnú formu a dotknutí zamestnanci s ním musia byť preukázateľne oboznámení. Výkon kontrolnej činnosti dokumentuje Bezpečnostný správca.
6) Bezpečnostný správca je povinný zabezpečiť výkon kontrolnej činnosti, ktorej predmetom je ochrana a bezpečnosť aktív s vysokou ochranou, najmenej jedenkrát za rok. Táto kontrola musí byť ukončená najmenej 1 mesiac pred predložením Vyhodnotenia stavu bezpečnosti.
7) Bezpečnostný správca má právo oboznámiť sa s výsledkami inej kontroly, ktorá bola vykonaná a ktorej predmetom nebolo zisťovanie stavu ochrany a bezpečnosti. Ak vo výsledkoch a záveroch kontroly sú skutočnosti, ktoré signalizujú alebo informujú o narušení bezpečnosti a ochrany, je Bezpečnostný správca povinný uvedené informácie okamžite prešetriť formou ním samostatne vykonanej kontroly.

Čl. 9

Bezpečnostné režimy

1) Bezpečnostný režim je stav organizácie života univerzity alebo jeho časti, ktorý zodpovedá aktuálnemu ohrozeniu aktív univerzity.
2) Stupeň a rozsah bezpečnostného režimu určuje Bezpečnostný správca na základe poznania aktuálneho stavu bezpečnosti a úrovne ohrozenia aktív univerzity.
3) Rozoznávajú sa nasledovné režimy:

a) ZELENÝ – normálny stav bežného života a chodu univerzity, kedy nie je bezprostredne ohrozené žiadne aktívum univerzity. O tomto režime sa nevedie dokumentácia a neprijímajú sa žiadne osobitné opatrenia,
b) ORANŽOVÝ (ohrozenie)– činnosť a život univerzity nie je ničím zmenená alebo ovplyvnená, ale úroveň ohrozenia niektorých aktív je zvýšená (zvýšená je pravdepodobnosť realizácie niektorej hrozby), čo vyžaduje monitorovanie tohto stavu a prijatie ďalších proaktívnych opatrení.
c) ČERVENÝ (kríza)– činnosť a život univerzity je zmenený následkom účinku niektorých hrozieb na aktíva univerzity. Vyžaduje sa prijatie účinných reaktívnych opatrení na odvrátenie hrozby a minimalizáciu škôd.
d) MODRÝ (zotavenie) – špeciálny režim po ČERVENOM režime, kedy dochádza ku konsolidácii života univerzity, rekonštrukcii a náhrade poškodených aktív.

4) Bezpečnostný správca pri zmene bezpečnostného režimu univerzity musí určiť aj rozsah, pre ktorú časť univerzity zmenený režim platí.
5) Pri vyhlasovaní zmeny bezpečnostného režimu je možné vykonávať len tieto prechody medzi režimami:
a) Z režimu ZELENÝ je možné prejsť do režimu ORANŽOVÝ a ČERVENÝ,
b) Z režimu ORANŽOVÝ je možné prejsť do režimov ZELENÝ a ČERVENÝ,
c) Z režimu ČERVENÝ je možné prejsť do režimu MODRÝ,
d) Z režimu MODRÝ je možné prejsť do režimu ZELENÝ a ORANŽOVÝ.
6) O zmene Bezpečnostného režimu musia byť ihneď vyrozumení všetci správcovia aktív a všetci zamestnanci a osoby zodpovedné za výkon ochrany univerzity.

Čl. 10

ORANŽOVÝ REŽIM - Ohrozenie

1) Stav ohrozenia vyhlasuje Bezpečnostný správca, ak sa zmenila pravdepodobnosť výskytu a realizácie niektorej hrozby na aspoň jedno aktívum s vysokou ochranou. Bezpečnostný správca zmení režim 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.
2) Bezpečnostný správca pri vyhlásení režimu ORANŽOVÝ vykoná nasledovné úkony:
a) V spolupráci so správcami aktív, ktorých ohrozenie sa predpokladá, identifikuje, ktoré hrozby sa môžu realizovať a aké typy incidentov je možné očakávať.
b) Menuje Skupinu riadenia režimu, ktorej členmi sú okrem neho správcovia ohrozených aktív, ktoré by mohli byť incidentom bezprostredne ohrozené.
c) Založí a následne vedie dokumentáciu riadenia režimu.
d) Určí, pre ktoré časti univerzity režim platí.
e) Určí čas, odkedy režim platí.
3) Vedúcim skupiny je Bezpečnostný správca, ktorý zodpovedá za jej činnosť a zvoláva jej pracovné stretnutia.
4) Skupina riadenia režimu je povinná navrhnúť a prijať opatrenia, ktoré znížia úroveň rizika, ktoré zmenou pravdepodobnosti výskytu hrozby vzniklo. Skupina zároveň určí, ktorí ďalší zamestnanci sú povinní byť dosiahnuteľní aj mimo pracovnej doby, prípadne zotrvať na pracovisku, ak si to situácia vyžiada.
5) Skupina riadenia režimu má právo dočasne uzatvoriť priestory univerzity, odpojiť časť univerzity alebo celú univerzitu od internetu, nariadiť vypnutie počítačov, alebo ich odpojenie od počítačovej siete, ukladať zamestnancom úlohy, ktorých splnenie môže mať za následok znižovanie rizika, zakázať vstup cudzích osôb do priestorov univerzity.

6) Ak právomoci členov skupiny neumožňujú prijať potrebné opatrenia bezodkladne o tejto skutočnosti, vedúci skupiny informuje rektora univerzity alebo vedúceho pracovníka, ktorý ho zastupuje.
7) Po prijatí opatrení skupina odhadne ich účinnosť. Znovu posúdi úroveň rizika a rozhodne o prijatí ďalších opatrení alebo o prechode do režimu ZELENÝ a určí, ktorí členovia skupiny spracujú „Správu o riadení bezpečnostného režimu".
8) Prechodom do režimu ZELENÝ činnosť Skupiny riadenia režimu skončí.
9) Ak Skupina riadenia režimu zistí, že aj napriek prijatým opatreniam došlo k realizácii hrozby a dochádza k poškodzovaniu alebo ničeniu aktív univerzity, odporučí Bezpečnostnému správcovi vyhlásiť režim ČERVENÝ, ktorý je povinný tento režim bezodkladne vyhlásiť.
10) Prechodom do režimu ČERVENÝ sa Skupina riadenia režimu stáva základom pre vytvorenie Skupiny krízového riadenia.

Čl. 11

ČERVENÝ REŽIM – Krízový stav

1) Krízový stav vyhlasuje Bezpečnostný správca samostatne alebo na návrh Skupiny riadenia režimu (Čl. 10), ak bol zistený výskyt realizujúcej sa niektorej hrozby na aspoň jedno aktívum s vysokou ochranou. 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 univerzity. Bezpečnostný správca zmení režim na základe aktuálneho poznania stavu hrozieb, ktorý je indikovaný najmä analýzou obsahu prevádzkových záznamov alebo výskytom bezpečnostných incidentov.
2) Bezpečnostný správca pri vyhlásení režimu ČERVENÝ vykoná nasledovné úkony:
   a) Informuje vedenie univerzity a všetkých správcov aktív o vyhlásení režimu a dôvodoch, ktoré viedli k vyhláseniu režimu.
   b) Navrhuje zloženie Skupiny krízového riadenia. Návrh predloží vedeniu k schváleniu.
   c) Založí a následne vedie dokumentáciu riadenia režimu.
   d) Určí, pre ktoré časti univerzity režim platí.
   e) Určí čas, odkedy režim platí.
3) Členmi Skupiny krízového riadenia sú:
   a) bezpečnostný správca, alebo jeho zástupca – vedúci skupiny krízového riadenia,
   b) správcovia aktív, voči ktorým sa hrozby realizujú,
   c) správcovia aktív, u ktorých sa predpokladá, že sa môžu realizovať rovnaké alebo súvisiace hrozby.
4) Prvé stretnutie zvoláva Bezpečnostný správca.
5) Skupina krízového riadenia je povinná navrhnúť a prijať opatrenia, ktoré zabránia ďalšej realizácii hrozieb a eliminujú rozširovanie účinkov hrozieb. Skupina je povinná najmä prijať také opatrenia, ktoré zabezpečia ochranu zdravia osôb, zachovanie schopnosti výučby a ochranu majetku univerzity.
6) Skupina riadenia režimu má právo najmä pozastaviť činnosť niektorých prevádzok, dočasne uzatvoriť priestory univerzity, odpojiť časť univerzity alebo celú univerzitu od internetu, nariadiť vypnutie počítačov alebo ich odpojenie od počítačovej siete, ukladať zamestnancom úlohy, zakázať vstup cudzích osôb do priestorov univerzity, evakuovať osoby z priestorov organizácie.
7) Skupina môže určiť, ktorí ďalší zamestnanci okrem členov skupiny sú povinní byť dosiahnuteľní aj mimo pracovnej doby, prípadne zotrvať na pracovisku, ak si to situácia vyžiada.
8) Skupina pravidelne vykonáva tieto kroky:
   a) identifikuje hrozbu – voči ktorému aktívu pôsobí a v akom rozsahu, odhaduje škody, ktoré sú alebo by mohli byť spôsobené,

b) prijíma opatrenia na izolovanie nepostihnutých aktív a častí univerzity,
c) prijíma opatrenia vedúce k zabráneniu ďalšieho rozširovania hrozby,
d) prijíma opatrenia na odvrátenie (elimináciu) hrozby,
e) vyhodnotí prijaté opatrenia, posúdi rozsah škôd a opätovne monitoruje dotknuté aktíva a hrozby, ktoré sa realizovali alebo majú zvýšenú pravdepodobnosť výskytu.
f) Pokračuje v činnosti podľa bodu 1. tohto odseku alebo navrhne zmenu režimu.

9) Skupina má právomoc vydávať akékoľvek nariadenia, ktorých účelom je odvrátenie hrozieb. Každý zamestnanec univerzity je povinný nariadenie skupiny vykonať a rešpektovať. Nevykonanie či nerešpektovanie nariadenia sa považuje za hrubé porušenie pracovnej disciplíny, ktorého následkom môže byť skončenie pracovného pomeru a vymáhanie náhrady škody, ktorá bude univerzite spôsobená.
10) Skupina krízového riadenia pravidelne informuje rektora univerzity o stave krízy, prijatých opatreniach a prognóze.
11) Prechod z režimu ČERVENÝ je možný len do režimu MODRÝ. Prechod písomne schvaľuje vedúci skupiny krízového riadenia. Návrh na prechod do režimu MODRÝ musí obsahovať:
a) čas, kedy režim ČERVENÝ skončí,
b) odôvodnenie, prečo sa navrhuje ukončiť režim,
c) prehľad o škodách,
d) návrh na zloženie Skupiny zotavenia (skupiny riadenia režimu MODRÝ).
12) Prechodom do režimu MODRÝ skupina krízového riadenia skončí svoju činnosť.

Čl. 12

MODRÝ REŽIM – Zotavenie

1) Režim MODRÝ je vyhlásený skončením režimu ČERVENÝ, súhlasom rektora univerzity so skončením tohto režimu.
2) Režim je riadený a organizovaný Skupinou zotavenia menovanou rektorom pri skončení režimu ČERVENÝ. Zloženie skupiny odráža rozsah škôd spôsobených počas krízového stavu. Skupina zotavenia musí byť schopná plniť všetky úlohy ako v režime ORANŽOVÝ. Členmi skupiny musia byť najmä:
a) Bezpečnostný správca alebo jeho zástupca,
b) Správcovia aktív, ktoré boli dotknuté v krízovom stave.
3) Povinnosťou skupiny je:
a) Detailne identifikovať všetky škody
b) Navrhnúť vedeniu univerzity postup pri odstraňovaní škôd. Postup musí obsahovať stanovenie priorít, časovú postupnosť, technickú špecifikáciu opatrení na odstránenie škôd a odhad ekonomickej náročnosti.
c) Dôkladne vyšetriť dôvody, príčiny, prečo došlo k realizácii hrozieb a škodám.
d) Vypracovať správu, v ktorej uvedie doklad o zvládnutí krízového stavu, doklad o škodách a výsledky vyšetrovania vrátane návrhov na opatrenia, ktoré zamedzia ďalšiemu opakovaniu podobnej krízovej situácie.
4) Skupina okrem úloh režimu MODRÝ plní aj úlohy režimu ORANŽOVÝ, aby boli neustále overované potenciálne hrozby a predišlo sa recidíve.
5) Prechod do režimu ZELENÝ je možný len ak pominuli dôvody na plnenie úloh režimu ORANŽOVÝ, ak skupina splnila úlohy stanovené týmto odsekom, ak bol schválený postup odstránenia škôd a ak je možné považovať stav ako celku z bezpečnostného hľadiska za konsolidovaný.
6) Prechod do režimu ZELENÝ schvaľuje rektor univerzity.

Druhá časť
Osobitné ustanovenia o niektorých aktívach

Čl. 13
Aktíva informačných technológií

1) Aktívami informačných technológií (IT aktíva) sa rozumejú všetky technické a softvérové prostriedky, ktoré slúžia na ukladanie, prenos a spracovanie informácií v digitálnej podobe bez ohľadu na účel tohto spracovania.
2) Správa IT aktív musí byť organizovaná tak, aby sa minimalizovala hrozba zneužitia postavenia administrátora. Bezpečnostný správca nesmie byť správcom žiadneho IT aktíva.
3) Za ochranu údajov je zodpovedný ten správca IT aktíva, na ktorého technických prostriedkoch (pamäťových médiách) sú tieto údaje uložené. K tomuto účelu vykonáva nasledovné činnosti - úkony:
   a) Vykonáva alebo v spolupráci s iným správcom zabezpečuje kopírovanie údajov na záložné médiá (zálohovanie údajov).
   b) Vykonáva alebo v spolupráci s iným správcom zabezpečuje kopírovanie údajov na archívne médiá (archivovanie údajov).
   c) Vykonáva nastavenia prístupových práv k údajom tak, aby k nim mohli pristupovať len oprávnení používatelia. Ak sú údaje aktívom, rešpektuje pokyny správcu tohto aktíva.
   d) Inštaluje, spravuje a zabezpečuje také služby (aplikácie), ktoré umožnia zvýšenú ochranu údajov šifrovaním alebo elektronickým podpisom.
4) Správca IT aktíva 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.
5) Správca aktíva je povinný raz priebežne nainštalovať všetky dostupné nové opravy softvérového aktíva, pokiaľ sa tým nenaruší bezproblémový chod činnosť aktíva. Raz za 12 mesiacov je správca aktíva povinný overiť, či neboli vydané nové verzie softvéru.
6) 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 aktíva v izolovanom prostredí či, neobsahuje nežiaduce funkcie a chyby. Overenie sa vykonáva tak, aby nemohlo dôjsť k ohrozeniu aktív univerzity a musí sa preveriť najmä správanie programu v sieťovom prostredí a vo vzťahu k údajom uloženým na pamäťovom médiu počítača.
7) Pri konfigurácii prostriedkov, programov a služieb správca IT aktíva dbá na to, aby sa používali len tie prostriedky, programy a služby, ktoré sú nevyhnutné pre plnenie pracovných úloh a potrieb univerzity. 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 svoje práci.
8) Správca IT aktíva vedie dokumentáciu o spravovanom aktíve, ktorá obsahuje základné konfiguračné údaje, údaje o inštalovaných programoch, údaje o IP adresách a doménových menách a údaje o užívateľoch.

Čl. 14

Zálohovanie a archivovanie údajov

1) Správca IT aktíva je povinný vykonávať zálohovanie a archiváciu podľa metodiky zálohovania a archivácie.
2) Médiá s archívnymi údajmi musia byť uložené v inej miestnosti, než sa nachádza počítač, z ktorého boli záložné údaje vyhotovené.
3) Záložné a archivačné médiá sa považujú za médiá obsahujúce digitálne bezpečnostné dokumenty.
4) Zamestnanci sú povinní na zálohovanie obsahu svojich počítačov, notebookov a tabletov používať primárne centrálne dátové úložisko zriadené na univerzite. Prístupové práva a nastavenia zálohovania zamestnancom vyšpecifikuje príslušný správca IT aktíva.
5) Zakazuje sa na centrálne dátové úložisko univerzity ukladať dáta osobného charakteru ako sú napríklad súkromné fotky, súkromné videozáznamy a podobne.
6) Zakazuje sa používanie externých dátových úložísk (cloud) na ukladanie personálnych a ekonomických údajov, nepublikovaných výsledkov vedeckej činnosti a iných dát, ktorých únikom by mohla byť univerzita vystavená porušeniu zákona č.122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov alebo iných zákonov Slovenskej republiky.

Čl. 15

Autentizácia

1) Správca IT aktíva, ktoré vyžaduje autentizáciu, stanoví autentizačné postupy a mechanizmy.
2) Pre autentizačné mechanizmy správca IT aktíva stanoví parametre, a to najmä vlastnosti hesiel. Stanoví dĺžku, štruktúru a expiračnú dobu hesiel.
3) Správca nesmie povoliť heslá kratšie ako 6 znakov, heslá musia obsahovať aspoň jeden neabecedný znak a ich expiračná doba nesmie byť dlhšia ako 12 mesiacov. Zakazuje sa zverejňovať, alebo inej osobe vyzradiť neverejné autentizačné údaje (heslá). Taktiež sa zakazuje držanie záznamu hesiel (napr. na papieri, v nešifrovanom softvérovom súbore) ak takýto záznam nemôže byť bezpečne uložený. Zamestnanec je povinný chrániť autentizačný prostriedok v jeho vlastníctve (multifunkčný školský preukaz alebo obdobný prostriedok) pred odcudzením a zničením a nesmie ho prenechať inej osobe.
4) Správca IT aktíva môže prideliť autentizačné údaje a prostriedky len zamestnancom univerzity alebo zamestnancom firmy, ktorá robí údržbu daného aktíva.
5) Prístupové oprávnenia prideľuje používateľovi správca IT aktíva na základe požiadavky vedúceho základného organizačného útvaru alebo osobitného útvaru. Tvoria ich prístupové meno, prístupové heslo a súbor nastavení, ktoré definujú povolené aktivity používateľa.
6) Prístupové oprávnenia sú prideľované podľa typu používateľa :
   a) administrátor – prístup k správe a údržbe aktíva, mal by to byť správca aktíva,
   b) používateľ – prístup len k tým modulom aplikácie (aktíva), s ktorými bezprostredne pracuje,
   c) externý používateľ – zamestnanec externej firmy, ktorá spravuje a udržiava danú aplikáciu (aktívum), prístup je kontrolovaný správcom aktíva alebo administrátorom, ak ho tým poveril správca aktíva.
7) Správca aktíva je povinný preveriť používateľské prístupové práva minimálne raz za 12 mesiacov.
8) Oddelenie riadenia ľudských zdrojov je povinné oznámiť skončenie pracovného pomeru zamestnanca všetkým správcov IT aktív, ktorým vydal oprávnenie prideľovať

autentizačné údaje a prostriedky. Správcovia sú potom povinní zabezpečiť včasné odobratie autentizačných prostriedkov a znemožnenie prístupu k aktívam.

9) Ak viacero aktív vyžaduje autentizáciu, Bezpečnostný správca koordinuje činnosť správcov týchto aktív pri používaní autentizačných postupov, metód a prostriedkov.
10) Nedodržanie zásad používania hesla a autentizácie zamestnancom sa považuje za bezpečnostný incident.

Čl. 16

Osobné údaje univerzity

1) Správcom aktíva „osobné údaje univerzity“ je osoba zodpovedná za dohľad nad ochranou osobných údajov univerzity.
2) Osobné údaje a údaje týkajúce sa oddelenia riadenia ľudských zdrojov môžu byť ukladané a prenášané len zabezpečeným spôsobom.
3) Zabezpečenie personálnych údajov sa vykonáva nasledovnými opatreniami:
   a) 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 oddelenia riadenia ľudských zdrojov a ním určeným zamestnancom.
   b) Prenášanie papierových dokumentov s údajmi týkajúcich sa oddelenia riadenia ľudských zdrojov je možné len v uzavretých a nepriehľadných schránkach alebo obaloch.
   c) Prenášanie digitálnych dokumentov sieťou, emailom alebo na médiách, je možné vykonávať len v zašifrovanej podobe.
   d) Miestnosti, v ktorých sa spracúvajú osobné údaje, musia byť v neprítomnosti zamestnanca uzamknuté. Okná miestností musia byť opatrené žalúziami, ktoré znemožnia odpozeranie údajov. Ak sa miestnosť nachádza na prízemí, musia byť okná opatrené mrežami. Miestnosti musia byť vybavené zábranným opatrením (prepážkou), ktorá zamedzí neoprávneným osobám nahliadať do dokumentov a na obrazovky počítačov alebo zamedziť odcudzeniu médií a dokumentov. Obrazovky počítačov musia byť umiestnené tak, aby nepovolané osoby z nich nemohli prečítať osobné údaje.
   e) 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.
   f) Zakazuje sa zanechávanie dokumentov s osobnými údajmi v tlačových zariadeniach napr. kopírkach, tlačiarňach alebo faxoch bez dozoru.

Čl. 17

Ekonomické údaje

1) Ekonomickými údajmi sú všetky údaje o ekonomike a financiách univerzity, údaje o obchode, marketingu a obchodných partneroch. Do skupiny ekonomických údajov sa zaraďujú aj údaje o know-how a technologické informácie.
2) Ochrana ekonomických údajov sa vykonáva rovnakým spôsobom ako ochrana osobných údajov, okrem šifrovania.
3) O potrebe zašifrovania ekonomických údajov rozhoduje ich správca.

Čl. 18

Fyzická ochrana

1) Každý zamestnanec je zodpovedný za fyzickú bezpečnosť svojho pracoviska a jemu zverených 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 bezpečnostnému správcovi.
2) Umiestnenie aktív s vysokou ochranou musí byť vykonané tak, aby sa účinne zabránilo ich odcudzeniu alebo fyzickému poškodeniu.
3) Bezpečnostný správca na návrh Správcov aktív môže rozdeliť univerzitu na bezpečnostné zóny a určiť, ktoré osoby môžu do týchto zón vstupovať. Pre zamedzenie vstupu nepovolaných osôb do bezpečnostných zón prijme účinné opatrenia. Pre vytvorenú a zabezpečenú zónu určí správcu, ktorý má postavenie Správcu aktíva.

Čl. 19

Pracovné stanice

1) Zamestnanec je povinný používať zverené pracovné stanice len na pracovné účely. Porušenie tohto ustanovenia sa považuje za bezpečnostný incident.
2) Zamestnanec môže na pracovných staniciach používať výlučne len programové vybavenie nainštalované správcom aktíva počítačov, resp. nainštalované s ich 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.
3) Zamestnanec nemôže vytvárať a distribuovať kópie programového vybavenia inštalovaného na pracovnej stanici.
4) Zamestnanec pred opustením pracoviska je povinný ukončiť prácu s aplikačným programovým vybavením, odhlásiť sa zo siete a operačného systému a dohliadnuť na vypnutie pracovnej stanice.
5) Pri krátkodobej neprítomnosti môže zamestnanec nahradiť odhlásenie sa zo systému a vypnutie pracovnej stanice spustením šetriča obrazovky s heslom resp. jej uzamknutím.
6) Zamestnanci sú povinní vykonávať základnú údržbu pracovnej stanice (čistenie povrchu obrazovky, klávesnice, myši..). Odstraňovanie nepotrebných súborov dátových adresárov a pomocných adresárov operačného systému (Kôš, Temp, Temporary Internet Files...) prípadne spustenie programov určených na údržbu (scandisk, defragmentácia...) vykonávajú zamestnanci v spolupráci so správcom aktíva počítačov.
7) Zamestnanci sú povinní 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 sú povinní čo najúplnejšie zdokumentovať a bezodkladne ohlásiť správcovi aktíva počítačov.
8) Zakazuje sa pripájať do siete univerzity neschválené zariadenia (napr. notebooky, PDA, tlačiarne, sieťové prvky a pod.) a taktiež povoliť pripojenie cudzej osoby do siete univerzity bez vedomia bezpečnostného správcu.
9) Zamestnanec je povinný mať zaheslovaný počítač a dodržiavať ustanovenia článku 15 tejto smernice.

Čl.20

Mobilné zariadenia

1) Pridelenie jednotlivých mobilných zariadení riadi správca mobilných aktív.

2) Pred odovzdaním zariadenia zamestnancovi je správca aktíva povinný nainštalovať na zariadenia softvér na antivírovú ochranu.
3) Zamestnanec je zodpovedný za fyzickú ochranu zariadenia pred krádežou alebo poškodením.
4) Krádež mobilného zariadenia v majetku univerzity sa považuje za bezpečnostný incident.

Čl. 21

Antivírová ochrana

1) Správca príslušného aktíva je povinný zabezpečiť inštaláciu a pravidelnú aktualizáciu antivírusových detekčných a nápravných softvérov na prehliadanie počítačov, serverov a médií na rutinnej báze. Vykonávané kontroly musia zahŕňať:
   a) Kontrolu všetkých súborov na elektronických alebo optických médiách, ako aj súborov prijatých prostredníctvom počítačovej siete, z hľadiska prítomnosti škodlivého kódu ešte pred používaním.
   b) Kontrolu príloh elektronickej pošty a stiahnutých súborov z hľadiska výskytu škodlivého kódu ešte pred spustením. Táto kontrola by sa mala vykonávať na rozličných miestach, napr. na elektronických poštových serveroch, pracovných staniciach a pri vstupe do siete prevádzkovanej univerzitou.
   c) Kontrolu pred nevyžiadanou poštou – Spamom.
   d) Kontrola webových stránok z hľadiska výskytu škodlivého kódu.
2) Správca príslušného aktíva je povinný venovať zvýšenú pozornosť tomu, aby škodlivý kód nebol zavedený počas výkonu pohotovostných procedúr alebo procedúr údržby.

Čl. 22

Prístup do siete internet a mailová komunikácia

1) Každý zamestnanec, ktorému bol umožnený prístup do siete internet, je povinný rešpektovať nasledovné zásady:
   a) prístup do siete internet využívať predovšetkým v súlade so svojou pracovnou náplňou
   b) dodržiavať etické zásady a zdržiavať sa činností, ktoré by mohli viesť k poškodeniu dobrého mena pracoviska alebo k iným škodám,
   c) komunikácia v internete spravidla nie je chránená pred "odpočúvaním". V prípade potreby prenosu osobných údajov je nevyhnutné tieto pred prenosom zabezpečiť šifrovaním. Ak nie je zamestnanec schopný prenos takto zabezpečiť, nie je prípustné ho uskutočniť,
   d) 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 aktíva počítačov a počítačovej siete.
2) Výber blokovaných stránok bude v kompetencii správcu aktív IT na základe webovej analýzy. V prípade veľkého prenosu objemu dát nesúvisiacich s pracovnou činnosťou zamestnanca, vyplývajúceho z výsledkov webovej analýzy, má pravo správca aktív IT zakázať a znemožniť užívateľovi prístup do internetu
3) Zamestnanec je povinný zabezpečiť správne adresovanie príjemcu mailovej správy a na prenos správ používať všeobecne dané dátové štandardy.
4) V prípade posielania citlivých a osobných údajov je povinný použiť kryptovanú komunikáciu za použitia kryptovacieho kľúča, ktorý mu bol na požiadanie vydaný bezpečnostným správcom
5) Používať elektronickú poštu len na legálne účely, 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.

7) Pravidelne vykonávať údržbu vlastnej elektronickej pošty (zálohovanie správ, mazanie, zhutňovanie a pod.).
8) Porušenie ustanovení tohto článku sa považuje za bezpečnostný incident.
9) Svoje identifikačne údaje je zakázané zadávať mimo sieť a doménu univerzity a tak isto aj do iných informačných systémov ako do systémov univerzity. Každý zamestnanec je povinný skontrolovať doménu stránky, kde zadáva svoje identifikačné údaje.

Čl.23

Kryptografické opatrenia a šifrovanie

1) Metódy šifrovania a prideľovanie kryptografických kľúčov riadi bezpečnostný správca v súčinnosti so správcami jednotlivých aktív a vedúcimi odborov.
2) Kryptografický kľúč generuje bezpečnostný správca na základe žiadosti schválenej vedúcim pracoviska. Túto skutočnosť zaznamená do zoznamu pridelených kryptografických kľúčov. Pričom zaznamená dátum expirácie kryptografického kľúča, ktorá nesmie byť dlhšia ako tri roky.
3) Bezpečnostný správca zabezpečuje:
   a) distribúciu určeným používateľom, vrátane toho, ako má byť kľúč aktivovaný,
   b) obnovu kľúčov, ktoré sa stratili alebo poškodili,
   c) zničenie kľúčov,
   d) zaznamenávanie a auditovanie aktivít, týkajúcich sa riadenia kľúčov,
   e) generovanie a získavanie certifikátov verejných kľúčov.
4) Zamestnanci, ktorí prenášajú citlivé dáta podľa článku 16 tejto smernice na USB kľúčoch a notebookoch, sú povinní tieto dáta šifrovať. Nedodržanie tohto nariadenia sa považuje za bezpečnostný incident.

Čl. 24

Manipulácia s médiami

1) Obsahy akýchkoľvek opakovateľne použiteľných médií, ktoré majú byť odnesené z organizácie, musia byť zmazané, ak už nie sú ďalej potrebné.
2) Pre všetky médiá s citlivými a osobnými údajmi, odnášané z organizácie, je potrebné urobiť autorizáciu.
3) Všetky médiá s osobnými a citlivými údajmi musia byť uložené v bezpečnom, chránenom prostredí, podľa špecifikácie výrobcu.
4) 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.
5) Médiá, ktoré nie sú už potrebné, sa musia bezpečne a spoľahlivo zlikvidovať.

Čl. 25

Zamestnanci externej organizácie

1) Prístup zamestnancov externej organizácie zriaďuje správca aktíva na základe schválenia bezpečnostným správcom. Bezpečnostný správca si vedie zoznam povolených prístupov k jednotlivým aktívam.
2) Správca vydá zamestnancovi externej organizácie prístupové heslo a práva podľa článku 15 tejto smernice.
3) Správca aktíva je povinný zabezpečiť bezpečný šifrovaný prístup zamestnanca tretej strany k jeho aktívu.

4) Poverení zamestnanci externej organizácie sú povinní pred prvým prihlásením k IT aktívu o tejto skutočnosti oboznámiť správcu aktíva buď prostredníctvom mailu alebo telefónom. Zároveň oznámia IP adresu, z ktorej budú k aktívu pristupovať.
5) Na základe tohto oznámenia im správca aktíva povolí pripojenie. Po skončení údržby alebo inej činnosti zamestnancom externej organizácie správca aktíva zruší možnosť pripojenia.
6) Bezpečnostný správca je povinný poučiť zamestnancov externej organizácie o ochrane a mlčanlivosti ohľadom osobných a citlivých údajov. Táto skutočnosť by mala byť zakomponovaná do zmluvy uzatvorenej s externou organizáciou.

Čl. 26

Záverečné ustanovenia

1) Bezpečnostná smernica č. 5/2014 má celouniverzitnú pôsobnosť.
2) Bezpečnostná smernica č. 5/2014 bola prerokovaná a schválená na zasadnutí Vedenia TU vo Zvolene dňa 20. 08. 2014.
3) Nadobudnutím účinnosti tejto Bezpečnostnej smernice ruší Smernicu č. 1/2005 k Bezpečnostnému projektu s účinnosťou od 01. 01. 2005.
4) Nadobudnutím účinnosti tejto Bezpečnostnej smernice ruší Bezpečnostnú smernicu č. R-14068/2012 s účinnosťou od 01. 01. 2013.
5) Poverenie bezpečnostného správcu a pridelenia správy aktív podľa Bezpečnostnej smernice č. R-14068/2012 sa považujú za poverenie bezpečnostného správcu a pridelenie správy aktív podľa tejto Bezpečnostnej smernice.
6) Bezpečnostná smernica nadobúda platnosť dňom jej podpisu rektorom TU s účinnosťou od 01. 09. 2014.

Vo Zvolene, dňa 27. 08. 2014

prof. Ing. Rudolf Kropil, CSc.
rektor

Zásady manipulácie s osobnými údajmi

Čl. 4

Účel predpisu

1) Zásady sú súčasťou poučení oprávnených osôb podľa §21 zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „zákon“).
2) So zásadami manipulácie s osobnými údajmi sú oboznámení všetci zamestnanci v rámci poučenia na oprávnenú osobu a sú povinní sa týmto predpisom riadiť a plne ho rešpektovať.
3) Zamestnanec nerešpektovaním Zásad manipulácie s osobnými údajmi poruší svoje povinnosti oprávnenej osoby, čím dôjde k porušeniu pracovnej disciplíny a následne k vyvodeniu opatrení v zmysle Pracovného poriadku a zákona.
4) Osobné údaje možno spracúvať len spôsobom ustanoveným zákonom a v jeho medziach tak, aby nedošlo k porušeniu základných práv a slobôd dotknutých osôb, najmä k porušeniu ich práva na zachovanie ľudskej dôstojnosti alebo k iným neoprávneným zásahom do ich práva na ochranu súkromia.
5) Osobné údaje môže spracúvať iba prevádzkovateľ alebo sprostredkovateľ.

Čl. 2

Práva oprávnenej osoby

1) Oprávnená osoba má právo najmä na:
   a) pridelenie prístupových práv do určených informačných systémov osobných údajov prevádzkovateľa v rozsahu nevyhnutnom na plnenie jej úloh; nevyhnutnosť priamo determinuje pracovné zaradenie oprávnenej osoby v rozsahu opisu činností jej pracovného miesta,
   b) opätovné poučenie, ak došlo k podstatnej zmene jej pracovného alebo funkčného zaradenia, a tým sa významne zmenil obsah náplne jej pracovných činností, alebo sa podstatne zmenili podmienky spracúvania osobných údajov alebo rozsah spracúvaných osobných údajov v rámci jej pracovného alebo funkčného zaradenia,
   c) porušenie povinnosti mlčanlivosti v zmysle § 22 ods. 2 zákona, ak je to nevyhnutné na plnenie úloh súdov a orgánov činných v trestnom konaní podľa osobitného zákona alebo vo vzťahu k Úradu na ochranu osobných údajov Slovenskej republiky (ďalej len „úrad“) pri plnení jeho úloh; ustanovenia o povinnosti mlčanlivosti podľa osobitných predpisov tým nie sú dotknuté,
   d) vykonávanie spracovateľských operácii s osobnými údajmi v mene prevádzkovateľa, vrátane osobitnej kategórie osobných údajov, v rozsahu nevyhnutnom na plnenie pracovných úloh určených opisom pracovného miesta oprávnenej osoby,
   e) odmietnutie vykonať pokyn k spracúvaniu osobných údajov, ktorý je v rozpore so všeobecne záväznými právnymi predpismi alebo dobrými mravmi,
   f) na vydanie dokladu (služobného preukazu), ktorým bude preukazovať svoju pracovnú príslušnosť k zamestnávateľovi.
2) Vo vzťahu ku kontrole vykonávanej podľa zákona, oprávnená osoba kontrolovanej osoby má právo najmä:
   a) na profesionálny prístup kontrolného orgánu pri výkone kontroly,

b) vyžadovať od kontrolného orgánu preukázať sa poverením na vykonanie kontroly a svojou príslušnosťou k úradu, ak je oprávnenou osobou štatutárny orgán, alebo osoba oprávnená konať v mene štatutárneho orgánu; to platí aj v prípade, ak sa na kontrole zúčastňuje aj prizvaná osoba,
c) oboznamovať sa s kontrolnými zisteniami a písomne sa k nim vyjadrovať, ak je oprávnenou osobou štatutárny orgán alebo osoba oprávnená konať v mene štatutárneho orgánu,
d) podávať písomné námietky po oboznámení sa s kontrolnými zisteniami, ak je oprávnenou osobou štatutárny orgán alebo osoba oprávnená konať v mene štatutárneho orgánu,
e) vyžadovať plnenie povinností kontrolného orgánu pri výkone kontroly podľa § 55 zákona, ak je oprávnenou osobou štatutárny orgán alebo osoba oprávnená konať v mene štatutárneho orgánu.

Čl. 3

Povinnosti oprávnenej osoby

1) Oprávnená osoba je v súvislosti so spracúvaním osobných údajov povinná rešpektovať príslušné povinnosti formulované prevádzkovateľom, najmä v rámci:
   a) Bezpečnostnej smernice, ktorej prílohou je tento interný predpis,
   b) Organizačného poriadku TU vo Zvolene,
   c) Pracovného poriadku TU vo Zvolene,
   d) Študijného poriadku TU vo Zvolene,
   e) Registratúrneho poriadku TU vo Zvolene
   f) v rámci dodržiavania pravidiel etiky.
2) Oprávnená osoba je ďalej povinná najmä:
   a) získavať na základe svojho pracovného zaradenia pre prevádzkovateľa len nevyhnutné osobné údaje výlučne na zákonom ustanovený alebo vymedzený účel; je neprípustné, aby oprávnená osoba získavala osobné údaje pod zámienkou iného účelu spracúvania alebo inej činnosti,
   b) vykonávať povolené spracovateľské operácie len so správnymi, úplnými a podľa potreby aktualizovanými osobnými údajmi vo vzťahu k účelu spracúvania,
   c) nesprávne a neúplné osobné údaje je bez zbytočného odkladu povinná opraviť alebo doplniť; nesprávne a neúplné osobné údaje, ktoré nemožno opraviť alebo doplniť tak, aby boli správne a úplné je povinná blokovať, kým sa rozhodne o ich likvidácii podľa Registratúrneho plánu TU vo Zvolene,
   d) pred získavaním osobných údajov od dotknutej osoby ju oboznámiť s názvom a sídlom prevádzkovateľa, 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,
   e) poučiť dotknutú osobu o dobrovoľnosti, alebo povinnosti poskytnutia osobných údajov a o existencii jej práv podľa § 28 zákona,
   f) 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 alebo osobitný zákon,
   g) preukázať príslušnosť oprávnenej osoby k prevádzkovateľovi hodnoverným dokladom (napr. služobným preukazom),
   h) 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,

i) postupovať výlučne v súlade s technickými, organizačnými a personálnymi opatreniami prijatými prevádzkovateľom podľa §§ 19 a 20 zákona,
j) 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 prevádzkovateľa,
k) v prípade nejasností pri spracúvaní osobných údajov sa obrátiť na prevádzkovateľa alebo zodpovednú osobu,
l) chrániť prijaté dokumenty a súbory pred stratou a poškodením a zneužitím, odcudzením, neoprávneným sprístupnením, poskytnutím alebo inými neprípustnými formami spracúvania,
m) dodržiavať mlčanlivosť o osobných údajoch podľa § 22 ods. 2 zákona, s ktorými oprávnená osoba v rámci svojho pracovného pomeru prichádza do styku, a to aj po zániku jej statusu, okrem zákonom priznaných výnimiek podľa § 22 ods. 5 zákona,
n) dodržiavať všetky povinnosti, o ktorých bola oprávnená osoba poučená.

3) Vo vzťahu ku kontrole vykonávanej podľa zákona oprávnená osoba kontrolovanej osoby je povinná najmä:
   a) poskytnúť úradu potrebnú súčinnosť pri výkone jeho dozoru podľa zákona,
   b) strpieť overenie totožnosti a preukázanie príslušnosti ku kontrolovanej osobe kontrolným orgánom pri výkone kontroly podľa zákona,
   c) zdržať sa konania, ktoré by mohlo zmariť výkon kontroly,
   d) dostaviť sa na predvolanie úradu s cieľom podať vysvetlenia v určenom čase na určené miesto, ak je oprávnenou osobou štatutárny orgán, alebo osoba oprávnená konať v mene štatutárneho orgánu,
   e) umožniť kontrolnému orgánu výkon iných oprávnení kontrolného orgánu podľa § 56 zákona, ak je oprávnenou osobou štatutárny orgán, alebo osoba oprávnená konať v mene štatutárneho orgánu,
   f) oboznámiť sa s obsahom protokolu a na požiadanie kontrolného orgánu dostaviť sa na jeho prerokovanie, ak je oprávnenou osobou štatutárny orgán, alebo osoba oprávnená konať v mene štatutárneho orgánu.
4) Oprávnená osoba nesmie osobné údaje spracúvané prevádzkovateľom využiť pre osobnú potrebu, či potrebu inej osoby alebo na iné, než služobné účely podľa tohto záznamu.

Čl. 4

Zodpovednosť za porušenie práv a povinností

1) Oprávnená osoba je v zmysle § 22 zákona povinná zachovávať mlčanlivosť o osobných údajoch, ktoré spracúva a s ktorými príde do styku. Povinnosť mlčanlivosti trvá aj po ukončení spracúvania osobných údajov. Povinnosť mlčanlivosti neplatí, ak je to nevyhnutné na plnenie úloh súdu a orgánov činných v trestnom konaní podľa osobitného zákona, alebo vo vzťahu k úradu pri plnení jeho úloh podľa zákona; ustanovenia o povinnosti mlčanlivosti podľa osobitných predpisov tým nie sú dotknuté.
2) Porušením povinností alebo zneužitím oprávnení pri spracúvaní osobných údajov môže oprávnená osoba naplniť skutkovú podstatu správnych deliktov podľa §§ 67 a 68 zákona, a to nasledovným konaním:
   a) poskytnutím osobných údajov v rozpore s § 12 ods. 1 zákona,
   b) poskytnutím nepravdivých osobných údajov podľa § 16 ods. 1 zákona,

c) nepostupovaním v súlade s technickými, organizačnými alebo personálnymi opatreniami prijatými prevádzkovateľom alebo sprostredkovateľom podľa §§ 19 a 20 zákona,
d) porušením svojich povinností uložených v tomto zázname podľa § 21 zákona,
e) porušením povinnosti mlčanlivosti o osobných údajoch podľa § 22 zákona,
f) neposkytnutím úradu požadovanú súčinnosť pri výkone dozoru podľa zákona.

3) Oprávnená osoba môže v súvislosti s protiprávnym nakladaním s osobným údajmi čeliť aj trestnému stíhaniu za trestné činy podľa § 247 a § 374 zákona č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov alebo môže voči nej byť vedené disciplinárne konanie.

Príloha č.2: Vzor „Poverenia bezpečnostného správcu“ rektorom univerzity

Poverenie bezpečnostného správcu

Priezvisko, meno, titul : .....

Dátum a miesto narodenia: .....

Organizačné zaradenie: .....

Týmto poveruje vyššie uvedenú osobu v zmysle Bezpečnostnej smernice podľa čl.3, výkonom funkcie bezpečnostného správcu pre Technickú univerzitu vo Zvolene.

Bezpečnostný správca dozerá na dodržiavanie ustanovení Bezpečnostnej smernice č..... a zákonných ustanovení pri spracúvaní osobných a iných citlivých údajov.

Poverenie nadobúda účinnosť od

Vo Zvolene dňa

.....
rektor

Prevzal :

.....
Bezpečnostný správca

Príloha č.3: Zoznam správcov aktív pre jednotlivé druhy informačných aktív

Zoznam správcov aktív pre jednotlivé druhy informačných aktív

Por.č.:	Názov aktíva:	Typ aktíva:	Organizačné zaradenie správcu aktíva:
1.	Ekonomické údaje univerzity	aktívum s vysokou ochranou	Vedúci/a EO[1], OIS[2], RRP[3]
2.	Osobné údaje zamestnancov	aktívum s vysokou ochranou	Vedúci/a ORĽZ[4]
3.	Osobné údaje študentov	aktívum s vysokou ochranou	Študijný/á referent/ka na fakultách
4.	Univerzitný informačný systém	aktívum s vysokou ochranou	Univerzitný/á integrátor/ka UIS[5]
5.	Ostatné IS[6] univerzity	aktívum so zvýšenou ochranou	Administrátori jednotlivých IS
6.	Počítače a periférie	aktívum so zvýšenou ochranou	Vedúci/a odd. servisu užívateľom CIT[7]
7.	Antivírová ochrana	aktívum s vysokou ochranou	Vedúci/a odd. servisu užívateľom CIT
8.	Počítačová sieť a prístup do internetu	aktívum s vysokou ochranou	Správca siete TU
9.	Servery	aktívum s vysokou ochranou	Vedúci/a odd. komunikačných sietí CIT
10.	Fyzická ochrana objektu	aktívum so zvýšenou ochranou	Vedúci/a odd. investícií a prevádzky
11.	Archív univerzity	aktívum so zvýšenou ochranou	Poverený zamestnanec podateľne TU[8]

[1] Ekonomické oddelenie
[2] Oddelenie informačnej sústavy
[3] Referát riadenia projektov
[4] Oddelenie riadenia ľudských zdrojov
[5] Univerzitný informačný systém
[6] Informačné systémy
[7] Centrum informačných systémov
[8] Technická univerzita

Príloha č.4: Vzor „Pridelenia správy aktív“ správcom jednotlivých aktív univerzity

Pridelenia správy aktíva.

Priezvisko, meno, titul: .....

Organizačné zaradenie správcu: .....

Názov aktíva: Informačný systém .....

Typ aktíva: aktívum s vysokou ochranou

Prideľujem Vám do správy vyššie uvedené aktívum. Pri správe aktíva ste povinný postupovať tak, aby aktívum bolo čo najlepšie chránené. Ste povinný postupovať v súlade s Bezpečnostnou smernicou.

Dátum:

_____

Bezpečnostný správca

Aktívum prevzal dňa :

_____

Správca aktíva