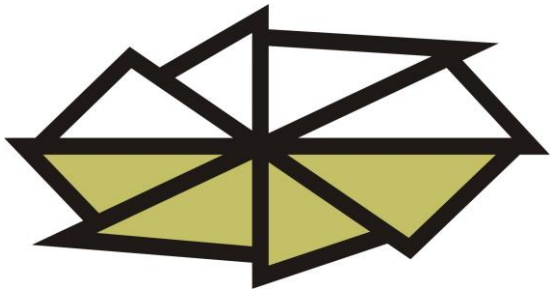
Technická univerzita vo Zvolene

R – 6878/2019



Bezpečnostná smernica
o ochrane osobných údajov
na TU vo Zvolene
č. 3/2019

Bezpečnostná smernica

o ochrane osobných údajov na TU vo Zvolene

č. 3/2019

OBSAH:

Prvá časť Všeobecné ustanovenia 4

Čl. 1 Účel smernice 4

Čl. 2 Skratky a základné pojmy 4

Čl. 3 Prístup oprávnených osôb do automatizovaného a neautomat. spracúvania OU 10

Čl. 4 Rektor 11

Čl. 5 Zodpovedná osoba 11

Čl. 6 Bezpečnostný správca 12

Čl. 7 Správca aktíva 12

Čl. 8 Správa aktív univerzity 13

Čl. 9 Rozsah zodpovednosti OO 14

Čl. 10 Hrozby 14

Čl. 11 Prevádzkové záznamy 14

Čl. 12 Bezpečnostné incidenty 15

Čl. 13 Spôsob identifikácie incidentov 15

Čl. 14 Organizačné opatrenia určujúce činnosti pri narušení objektu a chráneného priestoru a pri pokuse o narušenie objektu a chráneného priestoru 16

Čl. 15 Organizačné opatrenia pri narušení fungovania IS 19

Čl. 16 Organizačné opatrenia určujúce činnosti v prípade vzniku iných mimoriadnych udalostí 20

Čl. 17 Postup pri haváriách IT aktív 21

Čl. 18 Kontrolná činnosť 23

Čl. 19 Bezpečnostné režimy 24

Čl. 20 ORANŽOVÝ REŽIM - Ohrozenie 25

Čl. 21 ČERVENÝ REŽIM – Krízový stav 26

Čl. 22 MODRÝ REŽIM – Zotavenie 27

Druhá časť Osobitné ustanovenia o niektorých aktívach 28

Čl. 23 Aktíva informačných technológií 28

Čl. 24 Zálohovanie a archivovanie údajov 29

Čl. 25 Autentizácia 29

Čl. 26 Manažment hesiel 30

Čl. 27 Záväzné pravidlá pre spracúvanie osobných údajov na univerzite 31

Čl. 28 Zásady spracúvania OU 34

Čl. 29 Likvidácia OU 35

Čl. 30 Ekonomické údaje 36
Čl. 31 Fyzická ochrana 36
Čl. 32 Pracovné stanice 36
Čl. 33 Mobilné zariadenia 37
Čl. 34 Antivírová ochrana 37
Čl. 35 Prístup do siete internet a mailová komunikácia 38
Čl. 36 Kryptografické opatrenia a šifrovanie 39
Čl. 37 Manipulácia s médiami 39
Čl. 38 Zamestnanci externej organizácie 40
Čl. 39 Záverečné ustanovenia 40
Prílohy 41
Príloha č. 1 Kniha kontrol – vzor 41
Príloha č. 2 Vzor „Poverenia bezpečnostného správcu“ rektorom univerzity 42
Príloha č. 3 Zoznam správcov aktív pre jednotlivé druhy informačných aktív 43
Príloha č. 4 Záznam o porušení ochrany osobných údajov – vzor 44

Pôsobnosť: Technická univerzita vo Zvolene

Spracoval: Ing. Daniela Ukropová

Kontrolou dodržiavania poverení: kvestor TUZVO
prorektor pre rozvoj TUZVO

Účinnosť od: 01.10.2019

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 Nariadenia EU 2016/679 a zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.
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. 1
Skratky a základné pojmy

BP	bezpečnostný projekt
BS	bezpečnostná smernica
BA	bezpečnostná analýza
PV	posúdenie vplyvu na ochranu osobných údajov
GDPR	General Data Protection Regulation – Nariadenie EÚ 2016/679
OU	osobný údaj
AutIS alebo IS	automatizovaný informačný systém
OO	oprávnená osoba
DO	dotknutá osoba
ZO	zodpovedná osoba poverená dohľadom nad ochranou osobných údajov
FO	fyzická osoba
UOOU	Úrad na ochranu osobných údajov (dozorný orgán SR)
PC	pracovná stanica (počítač)
NTB	notebook, mobilná pracovná stanica (počítač)
LAN	lokálna počítačová sieť
UPS	zdroj neprerušovaného napájania (z angl. Uninterruptible Power Supply/Source/System)
DVR	digitálny videorekordér
HW	hardvér (hmotné technické zariadenie)
SW	softvér (programové vybavenie)
OS	operačný systém
AD	active directory

EPS	elektronická požiarna signalizácia
EZS	elektronický zabezpečovací systém
RIS	rezortný informačný systém MŠVVaŠ SR
RPaP	registratúrny plán a poriadok
TUZVO	Technická univerzita vo Zvolene (ďalej len univerzita)
CIT	Centrum informačných technológií
APV	aplikačné programové vybavenie
NPS	národné porovnávacie skúšky
UTV	Univerzita tretieho veku

Osobné údaje – sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej len dotknutá osoba), ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je napríklad meno, priezvisko, všeobecný identifikátor (ďalej len rodné číslo), identifikačné číslo, lokalizačné údaje, alebo on-line identifikátor, alebo odkazom na jeden alebo viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby. (článok 4, ods. 1 GDPR).

Osobitná kategória osobných údajov – sú osobné údaje, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, genetické údaje, biometrické údaje na individuálnu identifikáciu fyzickej osoby, údaje týkajúce sa zdravia alebo údaje týkajúce sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby (článok 9, ods. 1 GDPR).

Dotknutá osoba – každá fyzická osoba, ktorej osobné údaje sa spracúvajú (§ 5 písm. n) zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov).

Súhlas dotknutej osoby – je akýkoľvek slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby, ktorým formou vyhlásenia alebo jednoznačného potvrdzujúceho úkonu vyjadruje súhlas so spracúvaním osobných údajov, ktoré sa jej týka (článok 4, ods. 11 GDPR).

Genetické údaje – sú osobné údaje týkajúce sa zdedených alebo nadobudnutých genetických charakteristických znakov fyzickej osoby, ktoré poskytujú jedinečné informácie o fyziológii alebo zdraví tejto fyzickej osoby a ktoré vyplývajú najmä z analýzy biologickej vzorky danej fyzickej osoby (článok 4, ods. 13 GDPR).

Biometrické údaje – sú osobné údaje, ktoré sú výsledkom osobitného technického spracúvania, ktoré sa týka fyzických, fyziologických alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby, ako napríklad vyobrazenia tváre alebo daktyloskopické údaje (článok 4, ods. 14 GDPR).

Údaje týkajúce sa zdravia – sú osobné údaje týkajúce sa fyzického alebo duševného zdravia fyzickej osoby, vrátane údajov o poskytovaní zdravotnej starostlivosti, ktorými sa odhaľujú informácie o jej zdravotnom stave (článok 4, ods. 15 GDPR).

Spracúvanie osobných údajov - je operácia alebo súbor operácií s osobnými údajmi alebo so súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu

na to, či sa vykonáva automatizovanými prostriedkami alebo neautomatizovanými prostriedkami (článok 4, ods. 2 GDPR).

Obmedzenie spracúvania osobných údajov – je označenie uchovávaných osobných údajov s cieľom obmedziť ich spracúvanie v budúcnosti (článok 4, ods. 3 GDPR).

Porušenie ochrany osobných údajov – je porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim (článok 4, ods. 12 GDPR).

Poskytovanie osobných údajov – odovzdávanie osobných údajov tretej strane, ktorá ich ďalej spracúva.

Sprístupňovanie osobných údajov – oznámenie osobných údajov alebo umožnenie prístupu k nim príjemcovi, ktorý ich ďalej nespracúva.

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.

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

Účel spracúvania osobných údajov – vopred jednoznačne vymedzený alebo ustanovený zámer spracúvania osobných údajov, ktorý sa viaže na určitú činnosť.

Profilovanie – je akákoľvek forma automatizovaného spracúvania osobných údajov, ktoré pozostáva z použitia týchto osobných údajov na vyhodnotenie určitých osobných aspektov (znakov alebo charakteristík) týkajúcich sa fyzickej osoby, najmä na analýzu alebo predvídanie aspektov dotknutej fyzickej osoby súvisiacich s jej výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom (článok 4, ods. 4 GDPR).

Pseudonymizácia – je spracúvanie osobných údajov takým spôsobom, aby osobné údaje už nebolo možné priradiť ku konkrétnej dotknutej osobe bez použitia dodatočných informácií, ak sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia s cieľom zabezpečiť, aby osobné údaje neboli priradené identifikovanej alebo identifikovateľnej fyzickej osobe (článok 4, ods. 5 GDPR).

Log - záznam o priebehu činnosti používateľa v automatizovanom informačnom systéme (§ 5 písm. i) zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov).

Šifrovanie - transformácia osobných údajov spôsobom, ktorým opätovné spracúvanie je možné len po zadaní zvoleného parametra, ako je kľúč alebo heslo (§ 5 písm. j) zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov).

On-line identifikátor - identifikátor poskytnutý aplikáciou, nástrojom alebo protokolom, najmä IP adresa, cookies, prihlasovacie údaje do on-line služieb, rádiofrekvenčná identifikácia, ktoré môžu zanechávať stopy, ktoré sa najmä v kombinácii s jedinečnými identifikátormi alebo inými informáciami môžu použiť na vytvorenie profilu dotknutej osoby a na jej identifikáciu (§ 5 písm. k) zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov).

Informačný systém osobných údajov – je akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom základe alebo geografickom základe (článok 4, ods. 6 GDPR).

Prevádzkovateľ – je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene. Prevádzkovateľ alebo konkrétne požiadavky na jeho určenie môžu byť ustanovené v osobitnom predpise alebo medzinárodnej zmluve, ktorou je Slovenská republika viazaná, ak takýto predpis alebo táto zmluva ustanovuje účel a prostriedky spracúvania osobných údajov (článok 4, ods. 7 GDPR).

Sprostredkovateľ – je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa (článok 4, ods. 8 GDPR).

Príjemca – je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorému sa osobné údaje poskytnú bez ohľadu na to, či je treťou stranou. Za príjemcu sa nepovažuje orgán verejnej moci, ktorý spracúva osobné údaje na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, v súlade s pravidlami ochrany osobných údajov vzťahujúcimi sa na daný účel spracúvania osobných údajov (článok 4, ods. 9 GDPR).

Tretia strana – je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý nie je dotknutou osobou, prevádzkovateľ, sprostredkovateľ a osoby, ktoré sú na základe poverenia prevádzkovateľa alebo sprostredkovateľa poverené spracúvaním osobných údajov (článok 4, ods. 10 GDPR).

Zodpovedná osoba - osoba určená prevádzkovateľom alebo sprostredkovateľom, ktorá plní úlohy podľa tohto zákona (§ 5 písm. s) zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov).

Hlavná prevádzkareň - je (článok 4, ods. 16 GDPR):

1. miesto centrálnej správy prevádzkovateľa v Európskej únii, ak ide o prevádzkovateľa s prevádzkarňami vo viac než jednom členskom štáte, okrem prípadu, keď sa rozhodnutia o účeloch a prostriedkoch spracúvania osobných údajov prijímajú v inej prevádzkarni prevádzkovateľa v Európskej únii a táto iná prevádzkareň má právomoc presadiť vykonanie takýchto rozhodnutí, pričom v takom prípade sa za hlavnú prevádzkareň považuje prevádzkareň, ktorá takéto rozhodnutia prijala,
2. miesto centrálnej správy sprostredkovateľa v Európskej únii, ak ide o sprostredkovateľa s prevádzkarňami vo viac než jednom členskom štáte alebo ak sprostredkovateľ nemá centrálnu správu v Európskej únii, prevádzkareň sprostredkovateľa v Európskej únii, v ktorej sa v kontexte činností prevádzkarne sprostredkovateľa uskutočňujú hlavné spracovateľské činnosti, a to v rozsahu, v akom sa na sprostredkovateľa vzťahujú osobitné povinnosti podľa Nariadenia EÚ.

Zástupca – je fyzická alebo právnická osoba so sídlom, miestom podnikania, organizačnou zložkou, prevádzkarňou alebo trvalým pobytom v členskom štáte, ktorú prevádzkovateľ alebo sprostredkovateľ písomne poveril podľa článku 27 Nariadenia EÚ a ktorá ho zastupuje, pokiaľ ide o jeho povinnosti podľa Nariadenia EÚ (článok 4, ods. 17 GDPR).

Podnik – je fyzická (podnikateľ) alebo právnická osoba vykonávajúca hospodársku činnosť bez ohľadu na jej právnu formu vrátane partnerstiev alebo združení, ktoré pravidelne vykonávajú hospodársku činnosť (článok 4, ods. 18 GDPR).

Skupina podnikov – je riadiaci podnik a ním riadené podniky (článok 4, ods. 19 GDPR).

Záväzné vnútropodnikové pravidlá – je politika ochrany osobných údajov, ktorú dodržiava prevádzkovateľ alebo sprostredkovateľ so sídlom, miestom podnikania, organizačnou zložkou, prevádzkarňou alebo trvalým pobytom na území členského štátu na účely prenosu alebo súborov prenosov osobných údajov prevádzkovateľovi alebo sprostredkovateľovi v jednej alebo viacerých tretích krajinách v rámci skupiny podnikov alebo podnikov zapojených do spoločnej hospodárskej činnosti (článok 4, ods. 20 GDPR).

Kódex správania - súbor pravidiel ochrany osobných údajov dotknutej osoby, ktorý sa prevádzkovateľ alebo sprostredkovateľ zaviazal dodržiavať (§ 5 písm. y) zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov).

Členský štát - štát, ktorý je členským štátom Európskej únie alebo zmluvnou stranou Dohody o Európskom hospodárskom priestore (§ 5 písm. aa) zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov)**.**

Tretia krajina - krajina, ktorá nie je členským štátom (§ 5 písm. ab) zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov)**.**

Cezhraničné spracúvanie – je buď (článok 4, ods. 23 GDPR):

a) spracúvanie osobných údajov, ktoré sa uskutočňuje v Európskej únii v kontexte činností prevádzkarní prevádzkovateľa alebo sprostredkovateľa vo viac ako jednom členskom štáte, pričom prevádzkovateľ alebo sprostredkovateľ sú usadení vo viac ako jednom členskom štáte, alebo

b) spracúvanie osobných údajov, ktoré sa uskutočňuje v Európskej únii v kontexte činností jedinej prevádzkarne prevádzkovateľa alebo sprostredkovateľa v Európskej únii, ale ktoré podstatne ovplyvňuje alebo pravdepodobne podstatne ovplyvní dotknuté osoby vo viac ako jednom členskom štáte.

Medzinárodná organizácia – je organizácia a jej podriadené subjekty, ktoré sa riadia medzinárodným právom verejným, alebo akýkoľvek iný subjekt, ktorý bol zriadený dohodou medzi dvoma alebo viacerými krajinami alebo na základe takejto dohody (článok 4, ods. 26 GDPR).

Dozorný orgán – je nezávislý orgán verejnej moci zriadený členským štátom podľa článku 51 (článok 4, ods. 21 GDPR). Na Slovensku je ním Úrad na ochranu osobných údajov sídliaci v Bratislave.

Dotknutý dozorný orgán – je dozorný orgán, ktorého sa spracúvanie osobných údajov týka, pretože (článok 4, ods. 22 GDPR):

a) prevádzkovateľ alebo sprostredkovateľ je usadený na území členského štátu tohto dozorného orgánu, alebo

b) dotknuté osoby s pobytom v členskom štáte tohto dozorného orgánu sú podstatne ovplyvnené alebo budú pravdepodobne podstatne ovplyvnené spracúvaním, alebo

c) sťažnosť sa podala na tento dozorný orgán.

Zamestnanec úradu - zamestnanec v pracovnom pomere alebo v obdobnom pracovnom vzťahu podľa osobitného predpisu alebo štátny zamestnanec, ktorý vykonáva štátnu službu v štátnozamestnaneckom pomere podľa osobitného predpisu (§ 5 písm. ac) zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov)**.**

Relevantná a odôvodnená námietka - je námietka voči návrhu rozhodnutia, či došlo k porušeniu Nariadenia EÚ, alebo či je plánované opatrenie vo vzťahu k prevádzkovateľovi alebo sprostredkovateľovi v súlade s Nariadením EÚ, ktoré musí jasne preukázať závažnosť rizík, ktoré predstavuje návrh rozhodnutia, pokiaľ ide o základné práva a slobody dotknutých osôb a prípadne voľný pohyb osobných údajov v rámci Európskej únie (článok 4, ods. 24 GDPR).

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.

Aktíva IS – OU umiestnené v IS, ktoré podľa zákona musia byť dostatočne zabezpečené. Aktíva sú obsiahnuté v používaných výpočtových alebo nevýpočtových prostriedkoch, na bezpečnosť ktorých majú vplyv ďalšie prvky nachádzajúce sa v oblasti fyzickej, objektovej, organizačnej a personálnej bezpečnosti. Všetky prostriedky, ktoré sa podieľajú aktívne alebo pasívne na spracúvaní osobných údajov.

Služba informačnej spoločnosti – služba poskytovaná informačnou spoločnosťou, to jest každá služba, ktorá sa bežne poskytuje za odmenu, na diaľku, elektronickým spôsobom a na základe individuálnej žiadosti príjemcu služieb (článok 4, ods. 25 GDPR).

Na diaľku - znamená, že služba sa poskytuje bez toho, aby pri tom boli obe strany súčasne prítomné.

Elektronickým spôsobom - znamená, že služba sa z miesta pôvodu odošle a na mieste určenia prijíma prostredníctvom elektronického zariadenia, určeného na spracovávanie (vrátane digitálneho komprimovania) a uskladňovanie údajov a je úplne vysielaná, prenášaná a prijímaná po drôte, prostredníctvom rádiových vĺn, optickým spôsobom, alebo inými elektromagnetickými prostriedkami.

Na základe individuálnej žiadosti príjemcu služieb - znamená, že služba sa poskytuje prostredníctvom prenosu údajov na individuálnu žiadosť.

Automatizovaný informačný systém – súhrn technických prostriedkov výpočtovej techniky, programové a aplikačné vybavenie, údajová základňa, pamäťové médiá s údajmi, inštalačné médiá, dokumentácia súvisiaca s technickým a programovým vybavením určeným na automatizované spracúvanie údajov.

Prevádzkový záznam – je záznam o činnosti a chode technického prostriedku počas doby životného cyklu zariadenia. Záznam môže byť vyhotovovaný manuálne alebo automatizovane (logovacie súbory).

Autorizovaný program – je programové vybavenie, inštalované na technické zariadenie alebo PC, ktorého inštaláciu schválila autorizovaná osoba (osoba s vedomosťami a oprávnením posúdiť používanie programového vybavenia). Neautorizovaným programom môže byť 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. Autorizovaným programom môže byť aj open source software, inštalovaný len s vedomím správcu systému.

Bezpečnostné riziko – potenciálna možnosť narušenia dôvernosti, integrity a dostupnosti spracúvaných osobných údajov.

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.

Zraniteľné miesto – slabina systému využiteľná na spôsobenie škôd. Zahrňuje slabé miesta aktíva IS alebo skupiny aktív IS, ktoré môžu byť využité hrozbou.

Hrozba – potenciálna možnosť využitia zraniteľného miesta - 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.

Bezpečnostné opatrenie – je súbor činností, zariadení a postupov, ktoré vykonáva univerzita na ochranu aktíva pred hrozbou. Rozlišujú sa proaktívne a reaktívne bezpečnostné opatrenia.

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 a jej aktíva boli čo najnižšie.

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.

Bezpečnostný incident – využitie zraniteľného miesta na spôsobenie škôd, strata na aktívach, prípadne ich poškodenie alebo zničenie.

Zvyškové riziko – riziko, ktoré zostáva po implementácii bezpečnostných opatrení.

Server – technický, alebo programový prostriedok, ktorý prostredníctvom sieťového pripojenia poskytuje služby viacerým používateľom (napr. dátový, faxový, tlačový).

Počítačová sieť – technické a programové prostriedky, ktoré umožňujú klientom využívať na základe pridelených oprávnení služby serverov, komunikáciu medzi klientmi.

Lokálna počítačová sieť – počítačová sieť pracujúca v rámci jedného obmedzeného priestoru (oddelenia, odboru, celej firmy), obvykle fungujúca celkom samostatne. Môže byť prípadne prepojená na iné počítačové siete.

Lokálna stanica – samostatne (mimo sieť) stojace, resp. pracujúce počítačové pracovisko. Tento pojem tiež môže vyjadrovať koncové pracovisko spracovávajúce dáta neposkytované v počítačovej sieti.

Koncové pracovisko – technický a programový prostriedok, ktorý umožňuje používateľovi IS prostredníctvom sieťového pripojenia využívať služby serverov, alebo poskytovať autonómne služby bez väzby na sieť. Ide spravidla o koncové PC či terminály. Používateľom koncového pracoviska (klientom) je každý kto na základe korektného prihlásenia získa možnosť využívať služby, ktoré toto pracovisko poskytuje.

Počítačový vírus – špeciálny program vytvorený za účelom narušiť programové vybavenie, poškodiť dáta, resp. znepríjemniť právu užívateľa. Vyznačuje sa schopnosťou prenášať svoje kópie do iných programov a tak sa šíriť.

Archivácia dát – činnosť, pri ktorej je vytvorená bezpečnostná kópia dát (záloha dát). Takto archivované dáta môžu byť použité v krízových situáciách, kedy bežne používané dáta sa stanú nepoužiteľnými (strata dát, narušenie dát a pod.).

Prevádzkový záznam – je záznam o chode a činnosti technického prostriedku, organizačnej súčasti a pod., a to najmä ak sú považované za aktíva.

Externá organizácia – organizácia alebo univerzita vstupujúca do informačného systému za účelom jeho údržby alebo obnovy.

Mobilné zariadenia – považujú sa prostriedky spracovania ako sú notebooky, palmtopy, laptopy, smart karty a mobilné telefóny.

Cloudové dátové úložisko (cloud) – zálohovanie dát na vzdialených serveroch.

Čl. 2
Prístup oprávnených osôb do automatizovaného a neautomatizovaného spracúvania OU

1) Schvaľovaciu právomoc k udeľovaniu prístupu do IS v automatizovanej a neautomatizovanej (manuálnej) forme spracúvania má priamy nadriadený oprávnenej osoby.
2) Vytvorením prístupu k OU v manuálnej forme sa rozumie poskytnutie kľúčov od úložných priestorov, určených na ich uchovávanie.
3) Prístup k OU automatizovane aj neautomatizovane spracúvaným má každá oprávnená osoba uvedený vo svojej náplni práce a dodatkoch k nej a vo svojom Poverení OO.
4) Univerzita má tieto oprávnené osoby:
   - štatutár t. j. rektor univerzity,

- ZO,
- bezpečnostný správca,
- správcovia jednotlivých aktív,
- samotní spracovatelia OU.

5) Za plnenie povinností prevádzkovateľa v zmysle zákona zodpovedá rektor. Rektor zabezpečuje organizáciu bezpečnosti, poznávanie hrozieb a rizík a ochranu aktív v zmysle tejto smernice prenesením právomocí na Bezpečnostného správcu.

Čl. 4
Rektor

1) Rektor zodpovedá za:
   a) zabezpečenie bezpečnej, plynulej a spoľahlivej prevádzky informačných systémov univerzity a za plnenie povinností prevádzkovateľa v zmysle zákona,
   b) zabezpečenie vypracovania a pravidelnú aktualizáciu Bezpečnostnej analýzy a súvisiacich dokumentov univerzity,
   c) písomné menovanie Bezpečnostného správcu,
   d) písomné menovanie ZO univerzity,
   e) zabezpečenie písomného/on-line informovania UOOU o určení ZO na univerzite alebo o jej odvolaní a zmenách,
   f) vytvorenie podmienok a poskytnutie zdrojov pre ZO tak, aby ZO mohla plne vykonávať úlohy definované Nariadením EÚ v čl. 39 a kontinuálne si rozširovala odborné znalosti v oblasti ochrany OU,
   g) zabezpečenie, aby ZO bola riadnym spôsobom a včas zapojená do všetkých záležitostí, ktoré súvisia s ochranou OU,
   h) zabezpečenie primeraných podmienok na výkon kontroly kontrolnému orgánu Úradu a poskytnutie primeranej súčinnosti v súlade s výkonom tejto kontroly,
   i) schvaľovanie pravidiel v oblasti ochrany OU pri prenose OU do tretích krajín, ak sa takýto prenos uskutočňuje,
   j) zabezpečenie pravidelných školení zamestnancov ohľadom informačnej bezpečnosti,
   k) zabezpečenie poučenia oprávnených osôb a vyhotovenia záznamu o tomto poučení,
   l) pravidelné zvolávanie porady s Bezpečnostným správcom a ZO, obvykle jedenkrát za rok, za účelom prerokovania aktuálneho stavu v oblasti bezpečnostnej situácie, bezpečnostných incidentov a výsledkov kontrolnej činnosti vykonanej na jednotlivých súčastiach za obdobie od predchádzajúcej porady. Bezpečnostný správca a ZO mu predkladajú návrhy na opatrenia a zlepšenie bezpečnostnej situácie. O priebehu porady a najmä o navrhovaných opatreniach sa vykoná zápis, ktorý je bezpečnostným dokumentom.

Čl. 5
Zodpovedná osoba

1) Univerzita, ako prevádzkovateľ má určenú ZO, ktorá má postavenie a úlohy v zmysle článkov 38 a 39 Nariadenia EÚ.
2) ZO je povinná zabezpečovať:
   a) poskytovanie informácií a poradenstva vedeniu univerzity a jej zamestnancom, ktorí vykonávajú spracúvanie OU, o ich povinnostiach podľa Nariadenia EÚ a ostatných právnych predpisov týkajúcich sa ochrany OU,
   b) monitorovanie súladu s Nariadením EÚ, s ostatnými právnymi predpismi týkajúcimi sa ochrany OU a s pravidlami univerzity v súvislosti s ochranou OU vrátane

rozdelenia povinností, zvyšovania povedomia a odbornej prípravy personálu, ktorý je zapojený do spracovateľských operácií a súvisiacich auditov,
c) poskytovanie poradenstva na požiadanie, pokiaľ ide o posúdenie vplyvu na ochranu údajov a monitorovanie jeho vykonávania podľa článku 35 Nariadenia EÚ,
d) spolupráca s UOOU ako dozorným orgánom,
e) plnenie úlohy kontaktného miesta pre UOOU v súvislosti s otázkami týkajúcimi sa spracúvania vrátane predchádzajúcej konzultácie uvedenej v článku 36 Nariadenia EÚ a podľa potreby aj konzultácie v akýchkoľvek iných veciach,
f) informovanie rektora o aktuálnej situácii v oblasti bezpečnosti OU, bezpečnostných incidentov a výsledkov kontrolnej činnosti vykonanej na jednotlivých súčastiach.

Čl. 6
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 „Bezpečnostnej analýzy". Prehodnotenie odhadov rizík vykonáva najmenej jedenkrát za rok.
   b) Bezpečnú, plynulú a spoľahlivú prevádzku informačných systémov univerzity z pohľadu informačnej bezpečnosti.
   c) Evidovať Správcov 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 uzatvorenia písomnej zmluvy so sprostredkovateľmi v zmysle požiadaviek zákona, pričom pri výbere sprostredkovateľa musí dbať na jeho odbornú, organizačnú a personálnu spôsobilosť a jeho schopnosť zaručiť bezpečnosť spracúvaných OU.
   e) Zabezpečenie a organizáciu pravidelných školení zamestnancov ohľadom informačnej bezpečnosti.
   f) Poučenie zamestnancov univerzity a tretích strán o svojich právach a povinnostiach predtým, ako získajú prístup k informačným systémom univerzity.
   g) Zabezpečenie realizácie opatrení v zmysle dokumentu Bezpečnostná analýza a riadenie rizík vrátane návrhu oparení.
4) Na Bezpečnostného správcu sa písomným poverením rektora prenášajú povinnosti a právomoci rektora ako štatutára vyplývajúce univerzite ako prevádzkovateľovi z Nariadenia EU a zákona č. 18/2018 Z. z. o ochrane OU.

Čl. 7
Správca aktíva

1) Správca aktíva je pri správe prideleného aktíva povinný postupovať v súlade so zákonnými predpismi, Nariadením EU, zákonom o ochrane OU a Bezpečnostnou smernicou tak, aby bola zabezpečená čo najlepšia a primeraná ochrana tohto aktíva. Prevádzkovateľ má pridelenie aktív do správy, s uvedením typu aktíva podľa citlivosti, spracované v interných predpisoch o rozdelení aktív jednotlivých súčastí univerzity a ich pridelení správcom aktív. Pridelenie aktíva do správy príslušnému správcovi platí po dobu platnosti príslušného interného predpisu. Ukončenie správy zaniká ukončením pracovného pomeru alebo pridelenie správy aktíva môže zaniknúť aj pridelením správy aktíva inému správcovi.
2) Správca prideleného aktíva zabezpečuje najmä:

a) spracovanie OU na príslušnom referáte/oddelení/katedre/útvare v rozsahu a spôsobom v rozsahu Záznamu o spracovateľských činnostiach,
b) dodržiavanie primeranej ochrany aktíva, zákonných a interných predpisov pri získavaní, spracovaní, uchovávaní a likvidácii OU aktíva v papierovej a/alebo elektronickej forme,
c) dodržiavanie pravidiel bezpečného spracovania údajov v elektronických systémoch,
d) prijímanie oznámení od podriadených zamestnancov a ostatných zamestnancov univerzity o možných hrozbách pre dané aktívum a prijímanie okamžitých opatrení na odvrátenie hrozby,
e) vyhotovenie písomného záznamu pri vzniku bezpečnostného incidentu na pracovisku v zmysle tejto smernice a informovanie ZO a svojho priameho nadriadeného,
f) informovanie ZO a svojho nadriadeného o skutočnostiach, o ktorých sa domnieva, že by mohli byť hrozbou pre dané aktívum alebo porušením predpisov,
g) navrhovanie opatrení na zvýšenie bezpečnosti daného aktíva,
h) spoluprácu so ZO pri vykonávaní kontrolnej činnosti v zmysle tejto smernice,
i) informovanie ZO dohliadajúcej na ochranu OU o pripravovaných dôležitých zmenách súvisiacich s rozsahom a spôsobom spracovania OU a to v dostatočnom časovom predstihu,
j) informovanie ZO o požiadavke na aktualizáciu informácií uvedených v „Záznamoch o spracovateľských činnostiach“ pre jednotlivé účely spracovania najmä o zmenách v zozname spracúvaných OU, v kategóriách príjemcov, o zmene pri uvedených osobitných právnych predpisoch alebo tretích krajinách do ktorých sa vykonáva prenos OU.

Čl. 8
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) Konflikty a spory medzi správcami aktív rozhoduje Bezpečnostný správca.
7) Pravidelná kontrola aktív pridelených do používania (hmotný a nehmotný majetok) sa vykonáva v rámci inventarizácie majetku. Bez vedomia správcu majetku nesmie byť pridelené aktívum zverené do používania inému zamestnancovi a ani nesmie byť zmenené umiestnenie tohto aktíva do inej kancelárie, budovy alebo súčasti univerzity.

Čl. 9
Rozsah zodpovednosti OO

1) OO sú povinné zachovávať mlčanlivosť o OU, s ktorými sa pri výkone svojej činnosti alebo aj náhodne oboznámia. Tie nesmú využiť pre osobnú potrebu a bez súhlasu prevádzkovateľa ich nesmú zverejniť a nikomu poskytnúť ani sprístupniť. Povinnosť mlčanlivosti trvá aj po zániku funkcie OO, alebo po skončení pracovného pomeru zamestnanca, alebo obdobného pracovného vzťahu. Povinnosť mlčanlivosti neplatí vo vzťahu k orgánom činných v trestnom konaní a vo vzťahu k UOOU, pri plnení jeho úloh.
2) OO prevádzkovateľa zodpovedajú za ochranu spracúvaných OU a za dodržiavanie mlčanlivosti o OU, s ktorými pracujú v rámci svojej náplne práce, alebo s ktorými sa pri výkone práce oboznámia. Ich oprávnenia a povinnosti definujú interné predpisy univerzity.
3) Porušenie povinností vyplývajúcich z tejto smernice zo strany zamestnanca je porušením ustanovení platného Pracovného poriadku univerzity. Zistenia nelegálnej inštalácie SW na počítačoch zamestnávateľa, použitie počítačového a programového vybavenia zamestnávateľa na komerčné účely, neoprávnené zverejnenie, sprístupnenie alebo poskytnutie OU iným právnickým alebo fyzickým osobám je závažným porušením pracovnej disciplíny.
4) Uplatnením postupu uvedeného v odseku 2) tohto článku, nie sú dotknuté práva a nároky prevádzkovateľa na prípadnú náhradu škody v zmysle príslušných zákonných ustanovení.
5) Podrobne spracované pravidlá spracúvania OU sú uvedené v článku 27 tohto dokumentu.

Čl. 10
Hrozby

1) Každý zamestnanec je povinný ohlásiť skutočnosti, ktoré by mohli indikovať zvýšenú pravdepodobnosť hrozby alebo jej pôsobenie Zodpovednej osobe, Bezpečnostnému správcovi, ktorémukoľvek Správcovi aktíva z CITu 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 Zodpovednej osobe všetky podklady potrebné k vypracovaniu Záznamu o bezpečnostnom incidente.

Čl. 11
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. 12
Bezpečnostné incidenty

1) Bezpečnostný incident je každá udalosť, pri ktorej dochádza k narušeniu (evidentnému alebo skrytému) bezpečnostnej politiky ochrany OU, čoho dôsledkom je spôsobenie škôd na OU, strata OU, prípadne ich poškodenie alebo zničenie OU.
2) Činnosti, ktoré charakterizujú narušenie bezpečnosti zahŕňajú:
   a) pokusy (úspešné i neúspešné) získať neautorizovaný prístup do systému alebo k jeho dátam,
   b) nežiadané prerušenie (rozvrátenie) alebo odmietnutie služby,
   c) neautorizované používanie systému pre spracúvanie alebo ukladanie údajov,
   d) zmeny systémového HW a SW bez súhlasu, vedomia prevádzkovateľa.
3) Pre spoľahlivé a včasné riešenie bezpečnostných incidentov je potrebné:
   a) definovať a klasifikovať čo najúplnejšiu množinu možných incidentov,
   b) vymedziť spôsoby identifikácie každého incidentu prichádzajúceho do úvahy,
   c) určiť povinnosti a kompetencie jednotlivých zamestnancov pre riešenie incidentov,
   d) vypracovať časový harmonogram jednotlivých činností pri riešení incidentu a prípadného odstraňovania jeho následkov,
   e) definovať spôsob minimalizácie rizika opakovaného výskytu incidentu,
   f) vypracovať najneskôr do 48 hodín Záznam o porušení ochrany OU (o vzniku a priebehu riešenia každého incidentu, pri ktorom je pravdepodobné, že porušenie povedie k riziku pre práva a slobody fyzických osôb) a záznam odovzdať ZO. Vzor záznamu je prílohou č. 4 tejto BS.
4) Množina možných incidentov:
   a) Incidenty vzniknuté prostredníctvom útokov zo siete Internet:
      i. pokusy o prienik do systému a používanie systému po napadnutí útočníkom,
      ii. preťaženie komunikačných liniek nevyžiadanými správami, počítačovými červami.
   b) Incidenty vzniknuté prostredníctvom útokov z vnútorného prostredia IS:
      i. pokusy o prekonanie zabezpečenia logického prístupu do chránených prostriedkov LAN,
      ii. pokusy o prekonanie zabezpečenia logického prístupu do chránených aplikácií, adresárov, databáz serverov a klientov obsahujúcich OU,
      iii. neoprávnené využívanie výpočtových prostriedkov.
   c) Neoprávnený fyzický prístup do priestorov s chránenými údajmi alebo fyzická likvidácia nosičov dát (papierových aj elektronických).
   d) Neoprávnená modifikácia dát a programov.
5) Ďalšie činnosti, ktoré charakterizujú narušenie bezpečnosti ako aj množinu možných incidentov upravuje usmerneniami UOOU.

Čl. 13
Spôsob identifikácie incidentov

1) Kontrolné mechanizmy pre zabránenie a minimalizáciu vzniku bezpečnostných incidentov sú monitoring a interný audit.
2) Rozsah monitorovania:
   a) sledovanie pripojenia systému k Internetu,
   b) sledovanie pripojenia pre vzdialený prístup,
   c) sledovanie prenosu po sieti LAN,
   d) sledovanie prístupu do chránených prostriedkov siete LAN,
   e) sledovanie prístupu do chránených aplikácií, adresárov, databáz s osobnými údajmi,
   f) kontrola pravidelného spúšťania testov integrity, antivírusových programov,

g) kontrola pohybu osôb v priestoroch IS.

3) Prostriedky monitorovania:
   a) bezpečnostné prvky operačných systémov serverov a klientov LAN o prihlásení používateľov do výpočtových prostriedkov:
      i. prihlásenie používateľov do siete LAN,
      ii. správa používateľských účtov,
      iii. prístup k adresárovým službám,
      iv. monitorovanie systémových udalostí,
      v. monitorovanie prístupu k objektom,
      vi. monitorovanie používania oprávnení používateľov,
      vii. sledovanie vzdialeného prístupu na server,
   b) antivírusové programy:
      i. monitorovanie prítomnosti škodlivých programov rezidentným nastavením na serveroch, na ktoré môžu používatelia ukladať súbory a na pracovných staniciach,
      ii. monitorovanie integrity systémových a aplikačných súborov rezidentným nastavením na serveroch a pracovných staniciach.
4) Manuálne procesy:
   a) vyhodnocovanie auditných záznamov operačných systémov a aplikácií,
   b) vyhodnocovanie bezpečnostných incidentov,
   c) primeraná ostražitosť zamestnancov, najmä ZO, bezpečnostných správcov a vedúcich zamestnancov.
5) Aj napriek dobre nastaveným prevádzkovým mechanizmom monitoringu bezpečnosti treba uskutočňovať bezpečnostné kontroly hlavných prvkov bezpečnostných prostriedkov a opatrení pre uistenie, že nastavená bezpečnosť odpovedá miere rizík. Spôsob, forma a periodicita výkonu kontrolných činností pre zaistenie bezpečnosti je určená touto smernicou.

Čl. 14
Organizačné opatrenia určujúce činnosti pri narušení objektu a chráneného priestoru a pri pokuse o narušenie objektu a chráneného priestoru

1) Za narušenie objektu a chráneného priestoru a pokus o narušenie objektu a chráneného priestoru sa pre účely krízového plánu rozumie:
   a) krádež obyčajná,
   b) krádež vlámaním,
   c) pokus krádeže,
   d) teroristický útok,
   e) sabotáž, poškodzovanie cudzej veci, výtržnosť,
   f) hrozba uložením výbušného systému.
2) Krádežou sa rozumie trestný čin krádeže alebo jeho pokusu (§ 247 Trestného zákona č. 300/2005 Zb. v znení neskorších predpisov) a to aj v prípade, že došlo ku krádeži údajov bez rozdielu ich dôležitosti
   a) Pri pokuse o krádež/krádeži v objekte a chránenom priestore spôsobenej vlastným zamestnancom, zamestnancom iných servisných dodávateľských firiem, vlastným študentom alebo návštevou v pracovnej dobe, sa vykonajú tieto organizačné opatrenia:

Opatrenie	Kto vykoná	Spôsob
Zadržanie páchateľa/podozrivého za podmienky neohrozenia vlastnej bezpečnosti.	Každý pracovník objektu, ktorý krádež zistil a páchateľa prichytil.	Privolaním nadriadeného alebo pracovníka vedenia, ktorý je v dosahu, oznámením na vrátnicu a privolaním polície.

Opatrenie	Kto vykoná	Spôsob
		Zamedzením úniku páchateľa, ak je to možné, do príchodu polície.
Oznámenie narušenia chráneného objektu vlámaním.	Zamestnanec vrátnickej služby alebo vedúci pracovník.	Oznámením: - na č. 112 alebo Policajnému zboru na č.158 - zápisom do Knihy služieb.
Zabezpečenie miesta krádeže pred vniknutím neoprávnených a nepovolaných osôb.	Príslušná oprávnená osoba, u ktorej došlo v chránenom priestore k incidentu podľa pokynov svojho nadriadeného.	Uzamknutím priestoru, fyzickým strážením do príchodu polície.
Oznámenie zistenej krádeže dokumentov a nosičov s osobnými údajmi.	Štatutárny orgán a vedúci pracovník OO, u ktorej došlo k vlámaniu do chráneného priestoru.	Oznámením Policajnému zboru s vyhotovením písomného záznamu. Následne vypracovať Záznam o porušení ochrany OU a odovzdať ho ZO.
Vyhodnotenie príčin incidentu a prijatie opatrení.	Štatutárny orgán a vedúci pracovník OO.	Prijatím účinných opatrení a ich pís. oznámením ZO. Kontrolou prijatých opatrení.

b) Pri pokuse o krádež/krádeži vlámaním v objekte a chránenom priestore spôsobenej páchateľom v mimopracovnej dobe, sú na objekte prijaté tieto organizačné opatrenia:

Opatrenie	Kto vykoná	Spôsob
Preverenie miesta narušenia objektu.	Zamestnanec vrátnickej služby, alebo pracovník, ktorý sa prvý dostavil na pracovisko a zistil narušenie.	Obhliadkou miesta.
Zadržanie prítomného páchateľa za podmienky neohrozenia vlastnej bezpečnosti.	Zamestnanec vrátnickej služby, pričom je zakázané vystavovať sa neprimeranému nebezpečiu!	Urýchleným privolaním polície. Zamedzením úniku páchateľa, ak je to možné, do príchodu polície.
Oznámenie narušenia chráneného objektu vlámaním.	Zamestnanec vrátnickej služby.	Oznámením: - na č. 112 alebo Policajnému zboru na č.158 - vedúcemu pracovníkovi v dosahu a zápisom do Knihy služieb.
Zabezpečenie miesta krádeže do príchodu zamestnancov pred vniknutím nepovolaných osôb.	Zamestnanec vrátnickej služby.	Strážením (podľa prevádzkových možností).
Oznámenie zistenej krádeže vlámaním dokumentov a nosičov s osobnými údajmi.	Štatutárny orgán a príslušná oprávnená osoba, u ktorej došlo k vlámaniu do chráneného priestoru.	Oznámením Policajnému zboru s vyhotovením písomného záznamu. Následne vypracovať Záznam o porušení ochrany OU

Opatrenie	Kto vykoná	Spôsob
		a odovzdať ho ZO.
Vyhodnotenie príčin incidentu a prijatie opatrení.	Štatutárny orgán a vedúci pracovník OO.	Prijatím účinných opatrení a ich pís. oznámením ZO. Kontrolou prijatých opatrení.

3) Pri teroristickom útoku na objekt, sú na objekte prijaté tieto organizačné opatrenia:

Por.	Popis opatrenia	Kto vykoná	Spôsob
Zamestnanci a osoby zadržiavané v priestoroch organizácie a priamo ohrozované na životoch			
1.	Zabezpečenie bezpečnosti zadržiavaných osôb.	Každý zadržiavaný zamestnanec univerzity.	Primeranou spoluprácou s páchateľmi s cieľom navodiť kľud, neprovokovať k činom vedúcim k stratám na životoch.
2.	Únik z ohrozeného priestoru.	Každý zadržiavaný zamestnanec univerzity.	Únik realizovať len za asistencie privolanej ozbrojenej pomoci, účinne spolupracovať s tímom realizujúcim oslobodenie zadržiavaných osôb.
Zamestnanci priamo neohrozovaní teroristickým útokom			
1.	Oznámenie zistenej skutočnosti.	Každý zamestnanec univerzity, ktorý skutočnosť zistil.	Bezodkladne informovať orgány policajného zboru, potom nadriadeného zamestnanca a bezpečnostného správcu.
2.	Sledovanie a stráženie ohrozeného priestoru.	Do príchodu príslušníkov polície a vedenia univerzity každý zamestnanec univerzity.	Pozorovaním miesta teroristického útoku z bezpečnej vzdialenosti, sledovanie pohybu osôb a vozidiel.
3.	Zamedzenie vstupu ďalších osôb do ohrozeného priestoru.	Do príchodu príslušníkov polície a vedenia univerzity každý zamestnanec univerzity.	Podaním informácie vhodným spôsobom.
4.	Súčinnosť s policajným zborom.	Každý zamestnanec univerzity.	Podľa pokynov a požiadaviek poskytne každý zamestnanec policajnému zboru účinnú pomoc.
Cieľ zvládnutia každého teroristického útoku je najprv ochrana života a zdravia osôb a až následne majetku organizácie.			

4) Za poškodzovanie cudzej veci (majetku univerzity), sabotáž a výtržnosť sa všeobecne považujú činnosti, ktoré majú poškodiť majetok univerzity, alebo znemožniť jej ďalšie normálne fungovanie, pričom si páchateľ obvykle neprisvojuje majetok univerzity. Za majetok univerzity sa považuje hmotný, ale aj nehmotný majetok.
5) Pri zistení týchto činov sa postupuje rovnako ako pri krádežiach.
6) Pri hrozbe uloženia výbušného systému, sú na objekte prijaté tieto organizačné opatrenia:

Por.	Popis opatrenia	Kto vykoná	Spôsob
1.	Evakuácia zamestnancov univerzity a osôb nachádzajúcich sa v jej priestoroch.	Bezpečnostný správca alebo ním poverená osoba.	Hlasom, telefónom, osobne. Určiť miesto kam majú byť evakuované osoby.
2.	Informovať ostatné organizácie nachádzajúce sa v budove.	Bezpečnostný správca alebo ním poverená osoba.	Telefonickým vyrozumením, alebo vyslaním zamestnanca.
3.	Povinnosť oznámiť uloženie výbušného systému.	Bezpečnostný správca alebo ním poverená osoba.	Telefonicky policajnému zboru.
4.	Zabránenie vstupu osôb do priestorov univerzity.	Bezpečnostný správca alebo ním poverená osoba.	Po spoľahlivom zistení, že všetky osoby opustili priestory uzamknúť vstupné dvere.
5.	Spolupráca s policajným zborom.	Každý zamestnanec univerzity.	Podľa pokynov polície.

Čl. 15
Organizačné opatrenia pri narušení fungovania IS

1) Narušením fungovania IS univerzity sa rozumie akákoľvek situácia, ktorá má za následok poškodenie, zničenie, modifikáciu, alebo únik OU z počítačov. Narušením je takisto nežiadúce alebo nepredpokladané chovanie používaného softvéru, aj keď zdanlivo nevedie k narušeniu OU, programových prostriedkov a operačných systémov (jedná sa hlavne o činnosť vírusov alebo obdobných infiltrácií). Za narušenie sa považuje aj porucha počítača, ktorá môže spôsobiť stratu údajov.
2) Pre zvládnutie uvedených situácií sa stanovujú nasledujúce opatrenia:

Por.	Popis opatrenia	Kto vykoná	Spôsob
1.	Zamedzenie ďalších škôd.	Zamestnanec, ktorý skutočnosť zistil.	Bezodkladné bezpečné vypnutie počítača, odpojenie zdroja elektrickej energie, vrátane periférií. Odpojenie od komunikačných prostriedkov. Pri voľbe spôsobu vypnutia zvoliť malú stratu údajov (rozpracovanej práce) pred rozsiahlym poškodením zariadenia a údajov.
2.	Hlásenie potvrdeného úniku OU a jeho pravdepodobných dopadov pre práva a slobody fyzických osôb.	Zamestnanec, ktorý skutočnosť zistil. Správca aktíva CITu/súčasti univerzity	Informovať správcu dotknutého dátového aktíva. Informovať bezpečnostného správcu. Následne vypracovať Záznam o porušení ochrany OU a odovzdať ho ZO.
3.	Poskytnutie účinnej pomoci pri odstraňovaní škôd a vyšetrení incidentu.	Všetci zamestnanci univerzity.	Podľa pokynov bezpečnostného správcu a správcu aktíva.

3) Všetci zamestnanci univerzity a iné osoby využívajúce IS univerzity sú povinní riadiť sa ustanoveniami Organizačnej smernice č. 1/2010 O používaní prostriedkov informačných technológií na Technickej univerzite vo Zvolene.

Čl. 16
Organizačné opatrenia určujúce činnosti v prípade vzniku iných mimoriadnych udalostí

1) Mimoriadnymi udalosťami sa pre účely krízového plánu v súvislosti s ochranou IS organizácie rozumejú najmä:
   a) únos vedúcich zamestnancov a kľúčových zamestnancov s cieľom ohroziť univerzitu,
   b) vydieranie zamestnanca, nátlak na zamestnanca s cieľom prinútiť ho k spolupráci na poškodení univerzity, živelná pohroma, prírodná katastrofa, priemyselná a ekologická havária.
2) Únosom s cieľom ohroziť univerzitu sa rozumie najmä trestný čin brania rukojemníka (§ 234a trestného zákona), ktorého cieľom je prinútiť univerzitu, aby konala proti svojim vlastným záujmom, resp. aby inak porušovala zákony SR. V prípade únosu sa vykonajú tieto opatrenia:

Por.	Popis opatrenia	Kto vykoná	Spôsob
1.	Ohlásenie únosu policajnému zboru a nadriadenému zamestnancovi.	Zamestnanec, ktorý bol únoscami kontaktovaný, alebo sa o únose inak dozvedel.	Bezodkladne telefonicky informovať policajný zbor a vedenie univerzity.
2.	Spolupráca s únoscami.	Zamestnanec, ktorý je v kontakte s únoscami.	Uposlúchnuť pokyny únoscov (okrem podmienky neinformovať políciu), pokúsiť sa odložiť plnenie podmienok na prepustenie. S únoscami nevyjednávať, navodiť zdanie účinnej spolupráce.
3.	Súčinnosť s políciou.	Zamestnanec, ktorý je v kontakte s únoscami.	Postupovať podľa pokynov polície.

3) Vydieranie a nátlak na zamestnanca sú hrozby iných osôb, alebo organizácií smerujúce k tomu aby vydieraný zamestnanec a zamestnanec na ktorého je vyvíjaný nátlak konal proti záujmom univerzity (najmä trestné činy podľa §§ 235 a 235a trestného zákona). Pre prípad vydierania a nátlaku sa stanovujú tieto organizačné opatrenia:

Por.	Popis opatrenia	Kto vykoná	Spôsob
1.	Ohlásenie vydierania a nátlaku.	Zamestnanec, ktorý je vydieraný, alebo zamestnanec, ktorý sa o takomto vydieraní dozvedel.	Bezodkladne telefonicky policajnému zboru a vedeniu univerzity.
2.	Spolupráca s vydieračmi.	Vydieraný zamestnanec.	Podľa pokynov polície spolupracovať, navodiť zdanie spolupráce a poskytnúť pomoc a informácie vedúce k odhaleniu vydierača.
3.	Izolovanie	Vedúci zamestnanec,	Vydieranému znemožniť

Por.	Popis opatrenia	Kto vykoná	Spôsob
	vydieraného.	bezpečnostný správca.	konanie proti záujmom univerzity – znemožnením používania telefónu, faxu, kopírovacích zariadení a PC, prípadne aj nevpustením do priestorov. Izoláciu konzultovať s policajným zborom.

4) Hrozby rozsiahlych živelných pohrôm, prírodných katastrof, alebo ekologických a priemyselných havárií sú nízke. Najpravdepodobnejšou živelnou pohromou je požiar. Pri ostatných pohromách a haváriách sa postupuje obdobne ako pri požiari. Pre zvládnutie požiaru je vypracovaný plán požiarnej ochrany, ktorý musí okrem iného stanoviť aj poradie evakuácie a záchrany majetku univerzity.

Čl. 17
Postup pri haváriách IT aktív

1) Pri spracúvaní OU v aktuálnych podmienkach univerzity týmto nehrozí bezprostredné riziko zničenia alebo nedostupnosti dát. Viacnásobne zálohované dáta zabezpečujú ochranu OU pred zničením pri technickej poruche, prípadne pri havárii väčšieho rozsahu a umožňujú ich obnovu v celom rozsahu.
2) Používané technické a programové vybavenie pre zálohovanie vyhovujú množstvu a rozsahu spracúvaných OU. Pri znefunkčnení PC alebo servera (požiar, fyzické poškodenie) správca aktíva nakopíruje uchovávané zálohy v celom rozsahu na nový PC, obnoví server a zaktualizuje antivírusovú ochranu.
3) Pripojenie do siete a ďalšie úkony potrebné k oživeniu celého systému realizuje podľa vlastného uváženia a technických možností univerzity.
4) Postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení na zníženie vzniku mimoriadnych situácií a možností efektívnej obnovy stavu IT zariadení a dát pred haváriou:

Popis havárie	Návrh preventívnych opatrení	Postupy na zabezpečenie stavu obnovy
1. Havárie IS spôsobené technickou chybou niektorého komponentu servera a siete.	- Monitorovať činnosť serverov, kontrolovať chybové hlásenia. - Podľa možnosti obmieňať HW/SW servera. - Zálohovať.	- Obnova zo zálohy.
2. Porucha servera spôsobená vírusom alebo neautorizovaným programom.	- Zabezpečiť antivírovú ochranu. - Inštalovať len autorizované programy oprávnenými zamestnancami. - Preverovať cudzie nosiče (FD – flash disky, CD ROM ...). - Nepripájať nepreverené PC bez vedomia správcu dotknutého aktíva do LAN.	- Odpojiť používateľov. - Spustiť antivírový program s aktuálnou DB vírusov. - Detegovať spôsob narušenia. - Odstrániť príčiny. - Opraviť narušenú funkčnosť.

Popis havárie	Návrh preventívnych opatrení	Postupy na zabezpečenie stavu obnovy
	- Nepoužívané rozvody odpojiť od aktívnych prvkov LAN. - Neotvárať nevyžiadané e-mailové prílohy, odoslané neznámou osobou. - Nespúšťať programy z prostredia internetu nepodpísane dôveryhodnou certifikačnou autoritou. - Nesťahovať neautorizované programy z prostredia internetu. - Sledovať aktuálne dianie na LAN a v sieti internet.	- Opätovne skontrolovať systém antivírovým programom. - Prekontrolovať všetky PC. - Nájsť zdroj infiltrácie a zabezpečiť jeho eliminovanie. - Znovu spustiť systém a pripojiť používateľov.
3. Porucha napájania, strata dodávky elektrickej energie.	Dôležité aktívne prvky siete, diskové polia a servery je nutné chrániť záložnými zdrojmi elektrickej energie so stabilizátorom sieťového napätia.	- V čase výpadku sa musí záložný zdroj automaticky aktivovať. - Pri dlhodobejšom výpadku sa server musí automaticky vypnúť (shutdown).
4. Havária aplikácie.	- Sledovať hlásenia aplikácie a zaznamenávať postrehy používateľov. - Sledovať prevádzkové záznamy – logy. - Monitorovať hlásenia a včas na ne reagovať.	- Preinštalovať aplikáciu - Nainštalovať novšiu verziu aplikácie. - Konzultovať chyby s dodávateľom.
5. Havária databáz.	- Sledovať súbory udalostí. - Monitorovať hlásenia programov a včas na ne reagovať. - Pravidelne kontrolovať chybové hlásenia aplikácie a databázy.	Po odstránení problému a kontrole obnoviť databázu zo záloh.
6. Porucha pracovných staníc.	- Používať len autorizované programy. - Inštalovať antivírové programy. - Inštalovať nové programy smie len poverený zamestnanec. - Používatelia nesmú zasahovať do konfiguračných súborov. - Chybové hlásenia sú povinní hlásiť správcovi aktíva z CITu. - Zálohovať dáta na určené	- Technická chyba – zabezpečiť opravu nefunkčnej časti. - Softvérové chyby – identifikovať príčinu, obnoviť súbory zo zálohy, preinštalovať OS, aktualizovať antivírovú ochranu.

Popis havárie	Návrh preventívnych opatrení	Postupy na zabezpečenie stavu obnovy
	média. - Za zálohy, prevádzku a bezpečnosť zodpovedá zamestnanec.	

Čl. 18
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 ZO, Bezpečnostný správca a správcovia príslušného aktíva o čom vyhotovujú zápis v knihe kontrol, ktorej vzor tvorí prílohu č. 1 tejto smernice. Záznamy z kontrol eviduje ZO.
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) dátum kontroly,
   b) predmet kontroly,
   c) chronologický opis priebehu kontrolnej činnosti,
   d) zistené výsledky kontroly,
   e) odporúčané opatrenia (pri zistených nedostatkoch).
5) Bezpečnostný správca na základe skutočností uvedených v knihe kontroly nariadi vykonanie opatrení na odstránenie nedostatkov zistených kontrolou. Nariadenie musí mať písomnú formu a dotknutí zamestnanci s ním musia byť preukázateľne oboznámení.
6) Bezpečnostný správca je povinný zabezpečiť výkon kontrolnej činnosti, ktorej predmetom je ochrana a bezpečnosť aktív s vysokou ochranou, najmenej jedenkrát za 2 roky. 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. V takomto prípade je Bezpečnostný správca povinný uvedené informácie okamžite prešetriť formou ním samostatne vykonanej kontroly.
8) Periodické kontroly je potrebné vykonávať podľa vlastného uváženia, nepravidelne, podľa možnosti minimálne 1x ročne, s ohľadom na rozsah spracúvaných OU.
9) Kontroly definované ako „periodické“ možno tiež vykonávať náhodne, podľa vlastného uváženia alebo pri podozrení na bezpečnostné riziko.
10) Stála kontrolná činnosť prebieha pri kontrole a evidencii jednorazového vstupu do budovy a pohybu externých osôb (návštev, stránok) v prostredí univerzity. Ohlásené návštevy by sa mali pohybovať v sprievode povereného zamestnanca. Študenti majú umožnený voľný pohyb v priestoroch fakúlt a študovní. Pri tejto kontrole sa predpokladá prirodzená aktivita a všímavosť všetkých zamestnancov univerzity.
11) Za stálu kontrolu považujeme aj monitorovanie verejných priestorov kamerovým monitorovacím systémom.
12) ZO podľa svojich možností vykonáva v priebehu roka, minimálne raz za dva roky kontrolu každého aktíva s vysokou a zvýšenou ochranou a OU spracúvaných v papierovej a elektronickej forme a realizáciu technických a organizačných opatrení na pracoviskách, na ktorých sa tieto OU spracúvajú. Kontroly vykonáva predovšetkým na pracoviskách:

a) personálnej a mzdovej činnosti,
b) študijnej/pedagogickej činnosti,
c) registratúrnych stredísk a archívu,
d) ďalšieho vzdelávania a UTV,
e) s agendou žiadateľov o sociálne štipendiá,
f) poskytujúcich služby e-shopu,
g) ďalšie pracoviská s aktívami vysokej a zvýšenej ochrany.

13) ZO vykonáva aj kontrolu bezpečnej likvidácie OU v spolupráci so správcom registratúrneho strediska. ZO raz ročne vykoná kontrolu plnenia opatrení prijatých počas kalendárneho roka.
14) Správcovia IT aktív z CITu vykonávajú v minimálne ročných intervaloch kontrolu v oblastiach:
    a) nastavenia prístupových práv používateľov IS (v zozname oprávnených používateľov so skutočným stavom),
    b) politika zložitosti hesla. Ak pri kontrole nájdu zápis hesla na dostupnom mieste (napr. rám monitora, nástenka), upozornia na nevhodnosť takéhoto konania,
    c) funkčnosť zámkových mechanizmov do serverovej miestnosti, miestností s uchovávanými zálohami dát a skriňových, trezorových zámkov,
    d) manipulácie s pamäťovými médiami (ich uchovávanie a zabezpečenie hlavne v mimopracovnej dobe proti prístupu neoprávnených osôb),
    e) kontroly auditných záznamov na severoch a pracovných staniciach (ak to umožňujú), sledujú sa hlavne pokusy o neoprávnený prístup.
15) Za periodickú kontrolnú činnosť považujeme aj:
    a) pravidelné obchôdzky a kontroly objektu v mimopracovnej dobe vrátnickou službou,
    b) pravidelné kontroly hasiacich prístrojov a ich revízie,
    c) pravidelný nácvik (jedenkrát ročne) evakuácie osôb z budovy,
    d) kontroly zápisov v Knihe služieb na vrátnici, prípadne v ďalších prevádzkových knihách, ktoré sa vedú,
    e) inventarizáciu majetku.
16) Následné kontroly je nevyhnutné vykonávať:
    a) po nainštalovaní nových verzií operačného systému, alebo aplikácií a databáz spracúvajúcich OU (v opätovnom nastavení bezpečnostných parametrov a komunikačnej infraštruktúry a tiež v novom nastavení prístupových práv klientov),
    b) pri odchode zamestnanca, alebo pri jeho preradení na inú prácu (či je zamestnanec odstránený zo zoznamu oprávnených užívateľov, či sú v doméne odstránené jeho prístupové práva).
17) Okrem kontroly internými zamestnancami univerzity je špeciálne bezpečnosť spracúvaných OU kontrolovaná zamestnancami UOOU. Inšpektori UOOU sú oprávnení vstupovať do priestorov univerzity, sú oprávnení požadovať poskytnutie písomností alebo záznamových médií, vrátane technických nosičov údajov. Sú oprávnení okrem iného požadovať od kontrolovanej osoby poskytnutie pravdivých a úplných ústnych alebo písomných informácií, vyjadrení a vysvetlení ku kontrolovaným skutočnostiam a k zisteným nedostatkom. Oprávnenia UOOU pri kontrole sú definované v § 93 Zákona č. 18/2018 Z. z. o ochrane OU a o zmene a doplnení niektorých zákonov.

Čl. 19
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. 20
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. 21
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. 22
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. 23
Aktíva informačných technológií

1) Aktívami informačných technológií (IT aktíva) sa rozumejú všetky technické, hardvérové prostriedky (hmotné IT aktíva) a softvérové, aplikačné prostriedky (nehmotné IT aktíva), 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.
3) IT aktívum má spravidla viacerých Správcov. Hmotné IT aktívum môže mať jedného Správcu a nehmotné IT aktívum môže mať ďalších dvoch Správcov (jedného na operačný systém a druhého na aplikáciu).
4) Za ochranu údajov, ak údaje nie sú samostatným aktívom, 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.
5) 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.
6) Správca aktíva je povinný priebežne nainštalovať všetky dostupné nové opravy softvérového aktíva, pokiaľ sa tým nenaruší bezproblémový chod a činnosť aktíva. Raz za 12 mesiacov je správca aktíva povinný overiť, či neboli vydané nové verzie softvéru.
7) Zakazuje sa používanie neautorizovaných programov.
8) 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.
9) Správca IT aktíva vedie dokumentáciu v písomnej alebo automatizovanej elektronickej forme o spravovanom aktíve, ktorá obsahuje základné konfiguračné údaje, údaje o inštalovaných programoch, údaje o IP adresách a doménových menách a údaje o užívateľoch. Túto dokumentáciu uchováva po celú dobu nainštalovania programov a v súlade s RPaP univerzity.

Čl. 24
Zálohovanie a archivovanie údajov

1) Správca IT aktíva je povinný vykonávať zálohovanie a archiváciu podľa metodiky zálohovania a archivácie, ktorú nastavuje a určuje správca aktíva. V rámci metodiky je minimálne určené predmet zálohovania, kto zálohovanie má vykonávať, v akých intervaloch a na akom médiu sa má záloha uchovávať.
2) Médiá so záložnými a 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 vrátane dokumentov obsahujúcich OU.
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) Je nevyhnutné, aby zamestnanci, ktorí spracúvajú a ukladajú OÚ na svojich pridelených lokálnych pracovných staniciach (ak nie je možné využívať centrálne úložisko), pravidelne zálohovali svoje súbory s dátami na externé médiá (napr. CD, DVD, prípadne ďalšie spôsoby podľa odporúčania správcov IT aktíva) pre prípad zničenia dát na disku ich počítača. Záložné médiá musia byť označené a uložené v uzamknutej zásuvke pracovného stola zamestnanca alebo v uzamknutej skrinke. Zakazuje sa vynášať tieto média z priestorov univerzity.
6) Zakazuje sa spracúvanie osobných údajov na lokálnych diskoch zamestnanca, ak na to nie je poverený.
7) Zakazuje sa na centrálne dátové úložisko univerzity ukladať dáta osobného charakteru ako sú napríklad súkromné fotky, súkromné videozáznamy a podobne.
8) Zakazuje sa používanie externých dátových úložísk (cloud) okrem oficiálne univerzitou poskytovaných externých dátových úložísk na ukladanie personálnych a ekonomických údajov, nepublikovaných výsledkov vedeckej činnosti a iných dát, ktorých únikom by mohla byť univerzita vystavená porušeniu Nariadenia EÚ a zákona č.18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov alebo iných zákonov Slovenskej republiky.

Čl. 25
Autentizácia

1) V oblasti elektronického spracovania dát sú OO univerzity autentifikované a identifikované použitím používateľského mena a použitím prístupových hesiel do operačného systému a následne do aplikácií IS. Neoprávnené osoby nemajú do prostredia uchovávaných OU v elektronickej a písomnej forme umožnený samostatný prístup.
2) Používateľské účty, ktoré sa na univerzite vytvárajú musia spĺňať nasledujúce požiadavky:
   a) každý používateľ musí byť jednoznačne identifikovateľný,
   b) používateľom môže byť len zamestnanec univerzity alebo zamestnanec sprostredkovateľa a študent univerzity,
   c) prístupové oprávnenia prideľuje používateľovi správca príslušného IT aktíva na základe požiadavky priameho nadriadeného používateľa, personálneho oddelenia alebo koordinátora príslušného IT systému na súčasti univerzity,
   d) prístupové oprávnenia sú prideľované podľa typu používateľa:
      i. administrátor – prístup k správe a údržbe aktíva,

ii. používateľ – prístup len k tým modulom a funkciám aplikácie, s ktorými bezprostredne pracuje,
iii. externý používateľ – prístup je kontrolovaný správcom aktíva alebo administrátorom, ak ho tým poveril správca aktíva,

e) meno používateľa (účtu) nesmie byť totožné s menom počítača,
f) heslo nesmie byť totožné s identifikátorom užívateľa (meno používateľa),
g) pri vytvorení účtu musí mať každý používateľ priradené odlišné heslo,
h) používateľ si musí pri prvom prihlásení zmeniť heslo, ktoré mu bolo pridelené administrátorom.

3) Oddelenie riadenia ľudských zdrojov je povinné oznámiť vznik pracovného pomeru, skončenie pracovného pomeru zamestnanca, prípadne zmeny oprávnení vyplývajúcich z podstatnej zmeny pracovnej náplne zamestnanca všetkým správcom IT aktív, ktorým vydal oprávnenie prideľovať autentizačné údaje a prostriedky a Zodpovednej osobe. Správcovia sú potom povinní zabezpečiť včasné odobratie autentizačných prostriedkov a znemožnenie prístupu k aktívam.
4) Ak viacero aktív vyžaduje autentizáciu, Bezpečnostný správca koordinuje činnosť správcov týchto aktív pri používaní autentizačných postupov, metód a prostriedkov.
5) Nedodržanie zásad používania hesla a autentizácie zamestnancom sa považuje za bezpečnostný incident.

Čl. 26
Manažment hesiel

1) Pre bezpečnú prácu je odporúčané nasledovné nastavenie politiky hesla a politiky konta:
   a) prístup po overení autentizačného procesu, ktorý overuje identitu užívateľa. Používajú sa na základe:
      i. použitia hesla alebo PINu,
      ii. technickým riešením (hardwarový kľúč, smart card,...),
      iii. použitím biometrických vlastností (otlačok prsta,...)
      iv. odpoveď na náhodne vygenerovaný kontrolný dotaz.
   b) ochrana heslom:
      i. vynútiť použitie histórie hesiel, napr. počet hesiel, ktoré si systém pamätá sú 3,
      ii. maximálna doba platnosti hesla, napr. počet dní 365,
      iii. minimálna dĺžka hesla, napr. počet znakov 8,
      iv. heslo musí spĺňať požiadavky na zložitosť,
   c) uzamknutie konta:
      i. hraničná hodnota uzamknutia konta, napr. počet povolených pokusov o prihlásenie sú 3,
      ii. automatické uzamknutie konta, napr. na 10 minút,
      iii. vynulovanie počítadla uzamknutia konta, napr. po čase 60 minút.
2) Bezpečnosť poskytovaná systémom hesla závisí od toho, či heslá zostanú utajené. Heslo je citlivé na jeho kompromitáciu vždy, keď je použité, uložené alebo inak poznané. Na zabezpečenie bezpečnosti musí byť starostlivo používané. Nasledujúce odporúčania pomáhajú ochrániť heslá:
   a) nikdy nezapisujte heslo,
   b) nikdy nezdieľajte heslo s nikým iným,
   c) použite rozdielne heslá pre prihlásenie sa do siete a pre účet Administrátor na počítači,
   d) meňte svoje heslo do siete aspoň každých 365 dní alebo podľa požiadaviek vynútených lokálnymi politikami zabezpečenia,
   e) zmeňte heslo okamžite, ak si myslíte, že mohlo byť kompromitované.
3) Aby heslo bolo silné, musí spĺňať nasledujúce požiadavky:
   a) musí byť najmenej 8 znakov dlhé,

b) musí obsahovať aspoň tri z nasledujúcich skupín znakov:
   i. veľké písmená bez diakritiky (A až Z),
   ii. malé písmená bez diakritiky (a až z),
   iii. číslice (0 až 9),
   iv. nie alfanumerické znaky (!, $,#,%),
c) musí byť odlišné od predchádzajúceho,
d) nesmie obsahovať meno alebo používateľské meno,
e) nesmie ho tvoriť bežné slovo alebo meno,
f) nesmie byť ľahko uhádnuteľné (napr. meno + rodné číslo,...),
g) nesmie byť slovníkový výraz.

Čl. 27
Záväzné pravidlá pre spracúvanie osobných údajov na univerzite

1) Správcom aktíva „osobné údaje univerzity“ je osoba zodpovedná za dohľad nad ochranou osobných údajov univerzity - ZO.
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 tohto článku bezpečnostnej smernice 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.
6) Oprávnená osoba je v súvislosti so spracúvaním osobných údajov povinná rešpektovať príslušné povinnosti formulované prevádzkovateľom, najmä v rámci:
   a) Bezpečnostnej smernice,
   b) Organizačného poriadku TU vo Zvolene,
   c) Pracovného poriadku TU vo Zvolene,
   d) Študijného poriadku TU vo Zvolene,
   e) Registratúrneho plánu a poriadku TU vo Zvolene
   f) v rámci dodržiavania pravidiel etiky.
7) Pri získavaní a spracúvaní OU sú OO povinné dodržiavať nasledovné záväzné pravidlá:
   a) Pri získavaní OU vyžadovať od fyzických osôb len tie údaje, ktoré sú nevyhnutné na dosiahnutie účelu ich spracúvania.
   b) Pri získavaní OU vytvoriť také podmienky, aby bola zachovaná dôvernosť získavaných údajov. Zabrániť odpozeraniu údajov z monitora počítača, nahliadnutiu do písomností alebo ich vypočutiu neoprávnenou osobou.
   c) Pri získavaní OU od DO je OO povinná DO oznámiť informácie podľa č. 13 Nariadenia EU, najmä:
      i. identifikačné údaje prevádzkovateľa, pre ktorého sú OU získavané,
      ii. kontaktné údaje ZO,
      iii. účel spracúvania OU a právny základ spracúvania OU,
      iv. ak sa spracúvanie zakladá oprávnenom záujme prevádzkovateľa podľa čl. 6 ods. 1 písm. f) Nariadenia EU, popis cieľa oprávnených záujmov, ktoré univerzita sleduje,
      v. príjemcov alebo kategórie príjemcov,
      vi. v relevantnom prípade informáciu o tom, že univerzita zamýšľa preniesť OU do tretej krajiny alebo medzinárodnej organizácii a informáciu o tom, či sa jedná o

krajinu s primeranými zárukami podľa rozhodnutia Komisie EU alebo sa prenos uskutočňuje na základe prijatia iných primeraných záruk (napr. podpísania štandardných doložiek) uvedených v čl. 46 alebo 47, či na základe výnimiek uvedených v čl. 49 ods. 1 Nariadenia EU (prenos na základe súhlasu DO/prenos je nevyhnutný na plnenie zmluvy medzi DO a univerzitou alebo je prenos nevyhnutný na uplatňovanie/obhajovanie právnych nárokov),

vii. doba uchovávania OU, alebo kritériá na jej určenie,

viii. existenciu práva požadovať prístup k svojim OU a práva na ich opravu alebo vymazanie alebo obmedzenie spracúvania, alebo práva namietať proti spracúvaniu, ako aj práva na prenosnosť údajov,

ix. ak sa OU získavajú na základe Súhlasu DO, existenciu práva kedykoľvek tento súhlas odvolať bez toho, aby to malo vplyv na zákonnosť spracúvania založeného na súhlase udelenom pred jeho odvolaním,

x. existenciu práva podať sťažnosť na UOOU,

xi. informáciu o tom, či je poskytovanie OU zákonnou alebo zmluvnou požiadavkou, alebo požiadavkou, ktorá je potrebná na uzavretie zmluvy, či je DO povinná poskytnúť OU, ako aj možné následky neposkytnutia takýchto OU.

d) Pri OU, ktoré neboli získané od DO je OO povinná DO oznámiť informácie podľa č. 14 Nariadenia EU, najmä:

i. identifikačné údaje prevádzkovateľa, pre ktorého sú OU získavané,

ii. kontaktné údaje ZO,

iii. účel spracúvania OU a právny základ spracúvania OU,

iv. kategórie dotknutých OU,

v. príjemcov alebo kategórie príjemcov,

vi. v relevantnom prípade informáciu o tom, že univerzita zamýšľa preniesť OU do tretej krajiny alebo medzinárodnej organizácii a informáciu o tom, či sa jedná o krajinu s primeranými zárukami podľa rozhodnutia Komisie EU alebo sa prenos uskutočňuje na základe prijatia iných primeraných záruk (napr. podpísania štandardných doložiek) uvedených v čl. 46 alebo 47, či na základe výnimiek uvedených v čl. 49 ods. 1 Nariadenia EU (prenos na základe súhlasu DO/prenos je nevyhnutný na plnenie zmluvy medzi DO a univerzitou alebo je prenos nevyhnutný na uplatňovanie/obhajovanie právnych nárokov),

vii. doba uchovávania OU, alebo kritériá na jej určenie,

viii. ak sa spracúvanie zakladá oprávnenom záujme prevádzkovateľa podľa čl. 6 ods. 1 písm. f) Nariadenia EU, popis cieľa oprávnených záujmov, ktoré univerzita sleduje,

ix. existenciu práva požadovať prístup k svojim OU a práva na ich opravu alebo vymazanie alebo obmedzenie spracúvania, alebo práva namietať proti spracúvaniu, ako aj práva na prenosnosť údajov,

x. ak sa OU získavajú na základe Súhlasu DO, existenciu práva kedykoľvek tento súhlas odvolať bez toho, aby to malo vplyv na zákonnosť spracúvania založeného na súhlase udelenom pred jeho odvolaním,

xi. existenciu práva podať sťažnosť na UOOU,

xii. informáciu o tom, z akého zdroja pochádzajú OU, prípadne informácie o tom, či údaje pochádzajú z verejne prístupných zdrojov.

e) Informácie podľa odsekov c) a d) nie je potrebné DO oznamovať, ak DO už dané informácie má,

f) Informácie podľa odseku d) nie je potrebné DO oznamovať, ak DO už dané informácie má, alebo sa poskytovanie takýchto informácií ukáže ako nemožné alebo by si vyžadovalo neprimerané úsilie, najmä v prípade spracúvania na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely, na ktoré sa vzťahujú podmienky a záruky podľa čl. 89 ods. 1 Nariadenia EÚ,

alebo pokiaľ je pravdepodobné, že povinnosť informovať znemožní alebo závažným spôsobom sťaží dosiahnutie cieľov takéhoto spracúvania.

8) Ak sú získavané OU pre uzavretie zmluvného vzťahu, kde je DO jednou zo zmluvných strán, nie je potrebný súhlas DO (podpis DO na zmluve vyjadruje zároveň jej súhlas so spracúvaním OU).
9) OO je pri získavaní OU povinná si overiť správnosť OU nahliadnutím do úradných dokladov.
10) Získavať OU kopírovaním, skenovaním alebo iným zaznamenávaním úradných dokladov na nosič informácií je možné len vtedy, ak je to nevyhnutné na účely spracúvania a ak s tým DO písomne súhlasí alebo to výslovne umožňuje osobitný zákon alebo je to v oprávnenom záujme univerzity, pričom tieto záujmy neprevažujú nad oprávnenými záujmami DO a sú uvedené v Záznamoch o spracovateľských činnostiach.
11) Možno poskytnúť len pravdivé OU. Za pravdivosť OU zodpovedá ten, kto ich poskytol.
12) OO zabezpečí likvidáciu tých OU, ktoré sa nedajú opraviť alebo doplniť tak, aby boli správne a úplné.
13) Poskytnúť informácie o OU môže OO len DO, sprostredkovateľovi alebo iným príjemcom uvedeným v Záznamoch o spracovateľských činnostiach, ak na to má OO oprávnenie uvedené v Poverení OO. Poskytovať OU telefonicky sa zakazuje. Telefonicky je možné iba potvrdiť alebo vyvrátiť spôsob a rozsah spracúvania OU.
14) Zverejňovanie OU je možné len na základe preukázateľného súhlasu DO, alebo ak to umožňuje osobitný zákon alebo zákonný predpis alebo ak je to v oprávnenom záujme univerzity, pričom tieto záujmy neprevažujú nad oprávnenými záujmami DO a sú uvedené v Záznamoch o spracovateľských činnostiach.
15) Zverejňovanie rodného čísla je zakázané.
16) Zverejňovanie obrazových záznamov dotknutej osoby musí byť v súlade s Ústavou SR a Občianskym zákonníkom (privolenie podľa § 12 ods. 1). Zverejňovanie individuálnych obrazových záznamov osôb na sociálnych sieťach mimo oficiálnych stránok univerzity alebo fakúlt a organizačných súčastí (zamestnanci, študenti a účastníci aktivít celoživotného vzdelávania,) za účelom vlastnej pozitívnej propagácie a informovania verejnosti o živote a dianí na univerzite, môže byť len na základe ich preukázateľného súhlasu.
17) DO si môže uplatňovať svoje práva v zmysle článkov 15 až 21 Nariadenia EU písomne, mailom alebo osobne a na základe písomnej Žiadosti o uplatnenie práva DO. Žiadosť je možné podať elektronickou poštou, faxom, poštou alebo osobne doručiť na adresu ZO.
18) Zakazuje sa, aby zamestnanci univerzity získavali OU fyzických osôb pod zámienkou iného účelu alebo inej činnosti než pre účel, pre ktorý sú získavané s výnimkou použitia OU na účel zlučiteľný s pôvodným účelom (napr. archivácia, štatistika).
19) Pri likvidácii nepotrebných dokumentov s OU v papierovej forme (okrem dokumentov, ktoré sú predmetom vyraďovacieho konania spisov) je zamestnanec povinný vždy použiť takú formu likvidácie, aby sa OU stali trvale nečitateľné (napr. dostupný skartačný stroj).
20) Prenášanie papierových dokumentov s osobnými údajmi je možné len v uzavretých a nepriehľadných schránkach alebo obaloch.
21) Zamestnanec oprávnený k vyžadovaniu OU od uchádzačov o zamestnanie je povinný vyžadovať len informácie s ohľadom na ustanovenia § 41 ods. 6 zákona č. 311/2001 Z.z. Zákonníka práce v znení neskorších predpisov, v nevyhnutnom rozsahu pre dosiahnutie účelu spracúvania a DO oboznámiť s podmienkami spracúvania. Materiály žiadosti o zamestnanie poskytnuté uchádzačom uchováva po dobu v zmysle RPaP univerzity.
22) Pri krátkodobom vzdialení alebo pri odchode z pracoviska je každý zamestnanec povinný zabezpečiť spracovávané dokumenty s OU a elektronické záznamové médiá (CD, DVD, pamäťové USB kľúče, externé disky) pred prístupom nepovolaných osôb uložením na určené miesto a uzamknúť pracovisko.

23) Odosielanie listových zásielok obsahujúcich OU realizovať formou doporučenej zásielky/úradnej zásielky (doporučene s doručenkou do vlastných rúk).
24) OU získané z verejne prístupných zdrojov spracúvať iba na základe súhlasu DO alebo na účel určený osobitným právnym predpisom pri výkone verejnej moci.
25) 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 alebo monitorovaním kamerovým systémom a pravidelnými obhliadkami pracovníkmi strážnej služby. 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.
26) Zakazuje sa zhotovovať (tlačiť) dokumenty s osobnými údajmi na iných zariadeniach než na zariadeniach, ktoré sú umiestnené v zabezpečených priestoroch a sú na to určené..
27) Zakazuje sa zanechávanie dokumentov s osobnými údajmi v tlačových zariadeniach napr. kopírkach, tlačiarňach alebo faxoch bez dozoru.
28) Porušenie povinností alebo zneužitie oprávnení pri spracúvaní OU bude považované za porušenie pracovnej disciplíny alebo za hrubé porušenie pracovnej disciplíny.
29) 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.

Čl. 28
Zásady spracúvania OU

1) OU musia byť:
   a) spracúvané zákonným spôsobom, spravodlivo a transparentne vo vzťahu k DO,
   b) získavané na konkrétne určené, výslovne uvedené a legitímne účely a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmito účelmi, pričom ďalšie spracúvanie na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či štatistické účely sa nepovažuje za nezlučiteľné s pôvodnými účelmi,
   c) primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú,
   d) správne a podľa potreby aktualizované; musia sa prijať všetky potrebné opatrenia, aby sa zabezpečilo, že sa OU, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bezodkladne vymažú alebo opravia,
   e) uchovávané vo forme, ktorá umožňuje identifikáciu DO najviac dovtedy, kým je to potrebné na účely, na ktoré sa OU spracúvajú; OU sa môžu uchovávať dlhšie, pokiaľ sa budú spracúvať výlučne na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely, za predpokladu prijatia primeraných technických a organizačných opatrení vyžadovaných GDPR,
   f) spracúvané spôsobom, ktorý zaručuje primeranú bezpečnosť OU, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením a to prostredníctvom primeraných technických alebo organizačných opatrení.
2) Zásada zákonnosti
   OU možno spracúvať len zákonným spôsobom a tak, aby nedošlo k porušeniu základných práv DO. Spracúvanie osobných údajov je zákonné, ak sa vykonáva na základe aspoň jedného z týchto právnych základov:
   a) DO vyjadrila súhlas so spracúvaním svojich OU aspoň na jeden konkrétny účel,

b) spracúvanie OU je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je DO, alebo na vykonanie opatrenia pred uzatvorením zmluvy na základe žiadosti DO,
c) spracúvanie OU je nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná,
d) spracúvanie OU je nevyhnutné na ochranu života, zdravia alebo majetku DO alebo inej FO,
e) spracúvanie OU je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej univerzite,
f) spracúvanie OU je nevyhnutné na účel oprávnených záujmov univerzity alebo tretej strany okrem prípadov, keď nad týmito záujmami prevažujú záujmy alebo práva DO vyžadujúce si ochranu OU, najmä ak je DO dieťa.

3) Zásada obmedzenia účelu
OU sa môžu získavať len na konkrétne určený, výslovne uvedený a oprávnený účel a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmto účelom. Ďalšie spracúvanie OU na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel, ak je v súlade s osobitným predpisom a ak sú dodržané primerané záruky ochrany práv DO t. j. sú zavedené primerané a účinné technické a organizačné opatrenia najmä na zabezpečenie dodržiavania zásady minimalizácie údajov a pseudonymizácie, sa nepovažuje za nezlučiteľné s pôvodným účelom.
4) Zásada minimalizácie osobných údajov
Spracúvané OU musia byť primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú.
5) Zásada správnosti
Spracúvané OU musia byť správne a podľa potreby aktualizované. Musia sa prijať primerané a účinné opatrenia na zabezpečenie toho, aby sa OU, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bez zbytočného odkladu vymazali alebo opravili.
6) Zásada minimalizácie uchovávania
OU musia byť uchovávané vo forme, ktorá umožňuje identifikáciu DO najneskôr dovtedy, kým je to potrebné na účel, na ktorý sa OU spracúvajú. OU sa môžu uchovávať dlhšie, ak sa majú spracúvať výlučne na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel na základe osobitného predpisu a ak sú dodržané primerané záruky ochrany práv DO.
7) Zásada integrity a dôvernosti
OU musia byť spracúvané spôsobom, ktorý prostredníctvom primeraných technických a organizačných opatrení zaručuje primeranú bezpečnosť OU vrátane ochrany pred neoprávneným spracúvaním OU, nezákonným spracúvaním OU, náhodnou stratou OU, výmazom alebo poškodením OU.
8) Zásada zodpovednosti
Univerzita je zodpovedná za dodržiavanie základných zásad spracúvania OU, za súlad spracúvania OU so zásadami spracúvania OU a je povinný tento súlad so zásadami spracúvania OU na požiadanie preukázať UOOU.

Čl. 29
Likvidácia OU

1) Univerzita zabezpečuje likvidáciu OU v zmysle platného RPaP.
2) Likvidáciu OU je potrebné vykonať tak, aby sa OU stali trvale nečitateľné.
3) Likvidáciu OU v papierovej forme vykonať fyzickým zničením dokumentov napr. skartáciou na pôde univerzity alebo prostredníctvom sprostredkovateľa. Likvidáciu údajov z kamerového systému je potrebné zabezpečiť nastavením cyklu časovej slučky záznamu na dobu nevyhnutnú na dosiahnutie účelu spracovania, najdlhšie však na dobu 15 dní.

4) Likvidáciu OU pri automatickom spracovaní vykonať ich trvalým vymazaním z dátových súborov IS.
5) Likvidáciu elektronických nosičov dát (USB kľúče, externé disky, pevné disky PC a serverov, CD DVD a pod.) je potrebné zabezpečiť fyzickým zničením alebo prostredníctvom SW, ktorý zaručí nenávratnú stratu dát (niekoľkonásobných prepisom nezmyselnými znakmi), ale zachová samotný nosič dát, alebo úplnou fyzickou likvidáciou – zlomením, rozbitím, použitím tlaku, teploty alebo vplyvom silného elektromagnetického poľa.
6) Likvidáciu OU alebo elektronických nosičov dát realizuje Správca IT aktíva.

Čl. 30
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. 31
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. 32
Pracovné stanice

1) Zamestnanec je povinný pri svojej práci na počítači a v počítačovej sieti univerzity dodržiavať platné interné predpisy univerzity.
2) Zamestnanec je povinný používať zverené pracovné stanice len na pracovné účely. Porušenie tohto ustanovenia sa považuje za bezpečnostný incident.
3) 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.
4) Zamestnanec nemôže vytvárať a distribuovať kópie programového vybavenia inštalovaného na pracovnej stanici.
5) 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. Pokiaľ sa pracovná stanica nevypína, je povinný opustiť pracovisko tak, aby iný pracovník nemohol pracovať na pracovnej stanici pod jeho prístupovými právami.

6) Pri krátkodobej neprítomnosti môže zamestnanec nahradiť odhlásenie sa zo systému a vypnutie pracovnej stanice spustením šetriča obrazovky s heslom resp. jej uzamknutím (Ctrl+L). Zamestnanec je oprávnený zadávať a meniť heslá v počítači len na používateľskej úrovni.
7) 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.
8) 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 z CITu.
9) Bez vedomia Správcu IT aktíva z CITu sa zakazuje pripájať do siete univerzity vlastné neschválené zariadenia (napr. notebooky, tlačiarne, sieťové prvky a pod.) a taktiež povoliť pripojenie cudzej osoby do siete univerzity. Taktiež sa zakazuje používať na prenos OU nekryptované USB zariadenia alebo nepovolené cloudové služby, pokiaľ tieto zariadenia neboli zamestnancovi pridelené univerzitou alebo na to nemá súhlas Správcu aktíva z CITu.
10) Prenos OU mimo priestory univerzity prostredníctvom externých pamäťových médií je možný len v zašifrovanej podobe alebo médiami kryptovanými silným heslom. Porušenie tohto bodu sa považuje za bezpečnostný incident..
11) Zamestnanec je povinný mať zaheslovaný počítač a dodržiavať ustanovenia článkov 25 a 26 tejto smernice.

Čl.33
Mobilné zariadenia

1) Pridelenie jednotlivých mobilných zariadení riadi správca aktíva počítačov a mobilných zariadení z CITu.
2) Pred odovzdaním mobilného zariadenia (NTB, smartphone, tablet a pod.) zamestnancovi je Správca príslušného aktíva (IT referent zabezpečujúci podporu užívateľov) povinný nainštalovať na zariadenia softvér na antivírovú ochranu, kryptovanie a šifrovanie OU a softvér pre riadenie šifrovaného prístupu do lokálnej siete univerzity, ak to zamestnanec z titulu svojich pracovných povinností potrebuje.
3) Správca príslušného aktíva je povinný zabezpečiť na mobilných zariadeniach kryptované partície pevného disku alebo kryptované adresáre. Používateľ musí byť poučený o tom, že OU treba ukladať na mobilnom zariadení len na kryptovanú partíciu alebo do kryptovaného adresára.
4) Zamestnanec je zodpovedný za fyzickú ochranu zariadenia pred krádežou alebo poškodením.
5) Krádež mobilného zariadenia v majetku univerzity sa považuje za bezpečnostný incident.

Čl. 34
Antivírová ochrana

1) Správca príslušného aktíva je povinný zabezpečiť inštaláciu a pravidelnú aktualizáciu antivírusových detekčných a nápravných softvérov na prehliadanie počítačov, Windows 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.
3) V prípade, že sa na pracovnej stanici používateľa zobrazí varovanie, že sa na disku alebo prenosnom médiu nachádza vírus alebo iný škodlivý kód, používateľ nesmie toto varovanie ignorovať. V prípade, že zavírené prenosné médium patrí inému subjektu, používateľ ho označí ako zavírené a vráti majiteľovi. V prípade zavírenia vlastného pevného disku alebo prenosného média, používateľ túto skutočnosť bezodkladne oznámi Správcovi príslušného aktíva, prípadne po konzultácii s ním odstráni vírus z príslušného pamäťového média.
4) V prípade objavenia vírusu v prijatej elektronickej pošte používateľ bezodkladne o tejto udalosti upovedomí Správcu príslušného aktíva. V žiadnom prípade zavírenú elektronickú poštu neposiela inému adresátovi a na svojej pracovnej stanici ju uschová len dočasne a len na žiadosť Správcu príslušného aktíva.

Čl. 35
Prístup do siete internet a mailová komunikácia

1) Každý zamestnanec, ktorému bol umožnený prístup do siete internet, je povinný rešpektovať interné predpisy univerzity; minimálne tieto 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 IT aktív na základe webovej analýzy. V prípade veľkého prenosu objemu dát nesúvisiacich s pracovnou činnosťou zamestnanca, vyplývajúceho z výsledkov webovej analýzy, má právo správca aktív počítačovej siete 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 alebo zabezpečiť súbory obsahujúce OU silným heslom v zmysle heslovej politiky univerzity.
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, internými predpismi univerzity ani legislatívou stanovenými pravidlami.
6) Rešpektovať zákaz posielať reťazové a hromadné e-maily, reklamné správy a pod.

7) Rešpektovať zákaz používania nepovolených systémov pre zasielanie okamžitých správ obsahujúcich OU (instant messenger – Skype, Facebook, Hangouts, ...).
8) Pravidelne vykonávať údržbu vlastnej elektronickej pošty (zálohovanie správ, mazanie, zhutňovanie a pod.).
9) Porušenie ustanovení tohto článku sa považuje za bezpečnostný incident.
10) 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.36
Kryptografické opatrenia a šifrovanie

1) Metódy šifrovania a prideľovanie kryptografických kľúčov realizuje Správca aktíva „Počítače a periférie“, kde je šifrovanie nevyhnutné, v súčinnosti s vedúcimi pracovníkmi jednotlivých pracovísk.
2) Kryptografický kľúč generuje Správca aktíva „Počítače a periférie“. Túto skutočnosť zaznamená do zoznamu používaných kryptografických kľúčov, ktorý si vedie, pričom zaznamená dátum expirácie kryptografického kľúča, ktorá nesmie byť dlhšia ako tri roky.
3) Správca aktíva 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) Kryptografické opatrenia a šifrovanie je možné konzultovať s povereným zamestnancom Centra informačných technológií na univerzite
5) Zamestnanci, ktorí prenášajú osobné údaje a iné citlivé dáta na USB kľúčoch a notebookoch, sú povinní tieto dáta šifrovať. Nedodržanie tohto nariadenia sa považuje za bezpečnostné riziko.

Čl. 37
Manipulácia s médiami

1) Obsahy akýchkoľvek opakovateľne použiteľných médií, ktoré majú byť odnesené z organizácie, musia byť neobnoviteľne zmazané, ak už nie sú ďalej potrebné. Za zmazanie obsahu zodpovedá osoba, ktorá dala poverenie na odnos médií z univerzity (vedúci zamestnanec alebo Správca príslušného aktíva).
2) Pre všetky médiá s citlivými a osobnými údajmi odnášané z organizácie, je potrebné urobiť autorizáciu vykonaním záznamu o vynesení s uvedením mena a pracovnej pozície osoby, dátumu a času. Tento záznam musí obsahovať dátum, typ média, aké dáta sú uložené na médiu, dôvod vynesenia a kto médium vyniesol. Záznam vykonáva ten, kto médium autorizuje (vedúci zamestnanec alebo Správca príslušného aktíva).
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. Za riadne uchovanie informácií na médiách zodpovedá Správca príslušného aktíva.
5) Médiá, ktoré nie sú už potrebné, sa musia bezpečne a spoľahlivo zlikvidovať podľa pravidiel uvedených v tomto dokumente.

Čl. 38
Zamestnanci externej organizácie

1) Prístup zamestnancov externej organizácie zriaďuje správca príslušného 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 článkov 25 a 26 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 alebo ním poverená osoba je povinný poučiť zamestnancov externej organizácie o ochrane a mlčanlivosti ohľadom osobných a citlivých údajov. Táto skutočnosť musí byť zakomponovaná do zmluvy uzatvorenej s externou organizáciou.

Čl. 39
Záverečné ustanovenia

1) Bezpečnostná smernica o ochrane osobných údajov na TU vo Zvolene č. 3/2019 má celouniverzitnú pôsobnosť.
2) Bezpečnostná smernica o ochrane osobných údajov na TU vo Zvolene č. 3/2019 bola prerokovaná a schválená na zasadnutí vedenia TU vo Zvolene dňa 12.09.2019.
3) Nadobudnutím účinnosti tejto Bezpečnostnej smernice o ochrane osobných údajov na TU vo Zvolene č. 3/2019 sa ruší doterajšia Bezpečnostná smernica č. 5/2014, ktorá bola schválená na zasadnutí vedenia TU vo Zvolene dňa 20.08.2014.
4) Poverenie bezpečnostného správcu a pridelenia správy aktív podľa Bezpečnostnej smernice č. 5/2014 sa považujú za poverenie bezpečnostného správcu a pridelenie správy aktív podľa tejto Bezpečnostnej smernice o ochrane osobných údajov na TU vo Zvolene č. 3/2019.
5) Bezpečnostná smernica o ochrane osobných údajov na TU vo Zvolene č. 3/2019 nadobúda platnosť dňom jej podpisu rektorom TU vo Zvolene a účinnosť od 01.10.2019.

Vo Zvolene, 12.09.2019

_____

Dr. h. c. prof. Ing. Rudolf Kropil, PhD.
rektor

Príloha č. 1

Kniha kontrol – vzor (záznam o výkone kontroly nevyhnutných opatrení k ochrane OU v zmysle bezpečnostnej smernice)

Dátum kontroly	Predmet kontroly a zistené výsledky	Odporúčané opatrenia
	Kontrola opatrení na úseku ochrany OU na personálnom oddelení. NEDOSTATKY: a)... b)... VYKONAL: (meno a podpis)	1. .... 2. ....
	Kontrola vyhodnocovania prevádzkových záznamov serverov. NEDOSTATKY: a)... b)... VYKONAL: (meno a podpis)	1. .... 2. ....
	Kontrola opatrení pri prevádzkovaní kamerového monitorovacieho systému. NEDOSTATKY: a)... b)... VYKONAL: (meno a podpis)	Bez opatrení.
	atď.	atď.

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

P.č.	Názov aktíva	Organizačné zaradenie správcu aktíva
1	Antivírová ochrana	vedúci Oddelenia servisu užívateľom CIT
2	Ekonomické údaje univerzity	vedúca Ekonomického oddelenia
		vedúca Oddelenia riadenia projektov
3	Fyzická ochrana objektov	vedúci Oddelenia investícií a prevádzky
4	Osobné údaje študentov	referentka pre administratívno-správnu činnosť dekanátu
		študijná referentka dekanátu
5	Osobné údaje zamestnancov	vedúca Oddelenia riadenia ľudských zdrojov
6	Počítače a periférie vrátane mobilných zariadení pridelené konkrétnemu zamestnancovi univerzity	vlastník technického zariadenia
7	Počítače a periférie vrátane mobilných zariadení nepridelené konkrétnemu zamestnancovi univerzity	administrátor IS AuditPro
8	Počítačová sieť a prístupy do internetu	správca siete
9	Registratúrne stredisko univerzity	zamestnanec podateľne
10	Servery	vedúci Oddelenia komunikačných sietí CIT
11	Univerzitný IS a ostatné IS (AuditPro, CardPerson, Infos, Sofia atď.)	administrátor UIS a administrátori jednotlivých IS

Príloha č. 4

Záznam o porušení ochrany osobných údajov – vzor

Záznam o porušení ochrany osobných údajov

Prevádzkovateľ a sprostredkovateľ (čl. 33 Nariadenia EÚ 2016/679) sú povinní bez zbytočného odkladu a podľa možností najneskôr do 72 hodín po tom, ako sa o tom dozvedeli, oznámiť Úradu na ochranu osobných údajov SR porušenie ochrany osobných údajov, ktoré povedenie k riziku pre práva fyzických osôb. V prípade, že toto porušenie povedie k vysokému riziku pre práva a slobody fyzických osôb, je prevádzkovateľ povinný (čl. 34 Nariadenia EÚ 2016/679) bez odkladu oznámiť porušenie ochrany aj dotknutej osobe.

Prostredníctvom tohto záznamu oznamujem porušenie ochrany osobných údajov.

Meno, priezvisko oprávnenej osoby, ktorá porušenie zistila: .....

Dátum a čas zistenia porušenia ochrany OÚ: .....

Dátum a čas začiatku porušenia ochrany OÚ: .....

Dátum a čas konca porušenia ochrany OÚ: .....

Popis povahy porušenia ochrany OÚ: .....

.....

Popis kategórií dotknutých osôb, ktorých sa porušenie týka: .....

.....

Približný počet dotknutých osôb, ktorých sa porušenie týka: .....

Popis kategórií záznamov, ktorých sa porušenie týka: .....

.....

Približný počet záznamov, ktorých sa porušenie týka: .....

Popis pravdepodobných následkov porušenia: .....

.....

.....

Popis prijatých opatrení na nápravu porušenia ochrany OÚ ako aj opatrení na zmiernenie dopadu porušenia ochrany OÚ: .....

.....

.....

.....

Dátum a podpis osoby, ktorá oznamuje

Dátum prevzatia záznamu zodpovednou osobou a potvrdenie prevzatia: .....