SLOVENSKÁ TECHNICKÁ UNIVERZITA
V BRATISLAVE

Prevádzková bezpečnostná smernica informačného systému STU

Verzia dokumentu:	**1.0**
Dátum:	**15.11.2013**
Abstrakt:	V dokumente je spracovaná Prevádzková bezpečnostná smernica informačného systému Slovenskej technickej univerzity v rámci splnenia povinností vyplývajúcich zo zákona č. 122/2013 Z.z. O ochrane osobných údajov a o zmene a doplnení niektorých zákonov. Smernica stanovuje rámcové pravidlá pre bezpečnú a spoľahlivú prevádzku a používanie informačného systému.
Číslo ex.	

Vypracovali : Centrum výpočtovej techniky STU
Fakulta informatiky a informačných technológií STU

SLOVENSKÁ TECHNICKÁ UNIVERZITA
V BRATISLAVE

Obsah :

1. Úvod

Slovenská technická univerzita v Bratislave (ďalej STU) v rámci splnenia povinností vyplývajúcich zo zákona č. 122/2013 Z.z. O ochrane osobných údajov a o zmene a doplnení niektorých zákonov spracovala Prevádzkovú bezpečnostnú smernicu informačného systému. Táto smernica odráža súčasný stav pri prevádzke informačného systému STU a vychádza z dobrej praxe bezpečnej a spoľahlivej prevádzky informačných systémov. V primeranej miere smernica ďalej vychádza z normy STN ISO/IEC 27002 Informačné technológie – Bezpečnostné techniky - Kódex praxe manažérstva informačnej bezpečnosti a v neposlednom rade aj z platnej právnej úpravy v SR.

Informačný systém predstavuje významný nástroj podporujúci efektívne fungovanie každej inštitúcie a to platí aj pre verejnú vysokú školu – Slovenskú technickú univerzitu v Bratislave. V niektorých činnostiach univerzity plní informačný systém nezastupiteľnú úlohu. Pod pojmom informačný systém sa rozumie hardvér, softvér, dáta, dátové elektronické komunikácie a pod. Neoddeliteľnou súčasťou správneho fungovania a využívania služieb informačného systému sú zamestnanci zabezpečujúci jeho prevádzku a používatelia využívajúci jeho funkcie pri plnení svojich pracovných povinností. Správne používanie a využívanie informačného systému na STU vedie k jej úspešnému fungovaniu a stáva sa pre jej zamestnancov pomocníkom pri zvyšovaní kvality a produktivity práce.

Táto prevádzková smernica stanovuje rámcové pravidlá pre bezpečnú a spoľahlivú prevádzku a používanie informačného systému. Smernica je vypracovaná tak, aby dodržiavanie jej jednotlivých častí, článkov a pravidiel zo strany zamestnancov STU viedlo k zabezpečeniu ochrany pred prienikom nepovolaných osôb do počítačovej siete STU-STUNET, do informačných systémov STU a do databáz, aplikácií a ďalších informácií STU, ktoré sa spracovávajú pomocou IT, ďalej v spolupráci s antivírusovou ochranou na zabezpečenie pri napadnutí lokálnej počítačovej siete, PC či systémov STU počítačovými vírusmi a možnej strate alebo modifikácii dát, ako aj na ochranu osobných údajov zamestnancov a študentov STU.

Smernica vymedzuje používanie a využívanie informačného systému, služieb Internetu, Intranetu, elektronickej pošty používateľmi IT.

Vzhľadom k tomu, že všetky prostriedky IT vrátane dát, aplikácií sú majetkom STU (nie zamestnancov a študentov STU), slúži táto smernica na ochranu STU pred ich prípadným možným zneužitím, poškodením, odcudzením zo strany používateľov IT.

Táto smernica neslúži ako návod na používanie samotného počítača, zariadenia alebo konkrétnej aplikácie, ale stanovuje rámcové pravidlá pri bezpečné a spoľahlivé používanie a prevádzku informačného systému a všetkých zariadení IT.

Prevádzková bezpečnostná smernica informačného systému STU je súčasťou Bezpečnostného projektu a nadväzuje na ďalšie dokumenty, ako sú najmä:
1. Bezpečnostný zámer informačného systému STU.
2. Havarijný plán informačného a počítačového systému STU.
3. Analýza bezpečnosti informačného systému STU.

4. Smernica na ochranu osobných údajov na STU.
5. Usmernenie na oznamovanie bezpečnostných incidentov na STU.
6. Pravidlá prevádzky dátovej siete – STUNET.
7. Pravidlá správy dátovej siete STUNET.
8. Klasifikácia aktív a informácií informačného systému STU. Smernica rektora č.1/2007-N

1.1 Základné pojmy

Aktívum – subjekt, ktorý má určitú hodnotu a je potrebné ho chrániť. Aktíva informačného systému sú softvér, hardvér, údaje, komunikačné prostriedky a zamestnanci, ktorých organizácia používa na zabezpečenie informatických služieb.
Analýza rizík – preskúmanie vzťahov medzi aktívami, hrozbami, bezpečnostnými slabinami a opatreniami s cieľom určiť aktuálnu úroveň rizík.
Asymetrický kryptosystém – je metóda šifrovania, pri ktorej sú použité dva rôzne kľúče, jeden šifrovací a druhý dešifrovací (šifrovaciemu kľúču sa hovorí privátny kľúč a dešifrovaciemu kľúču sa hovorí verejný kľúč).
Bezpečnostná brána (Firewall) – je zariadenie, ktoré realizuje bezpečné oddelenie chránenej vnútornej (privátnej) počítačovej siete od inej počítačovej siete alebo nechránenej (verejnej) siete, napríklad Internetu. Existuje viacero konfigurácií bezpečnostných brán. Najúčinnejšou konfiguráciou je konfigurácia tienenej podsiete (screened subnet). Táto konfigurácia obsahuje tienenú podsieť, ktorej sa hovorí demilitarizovaná zóna.
Bezpečnostná slabina – stav zraniteľnosti zapríčinený nedostatkom bezpečnostného opatrenia alebo jeho neprítomnosťou.
Bezpečnostné opatrenie – ľubovoľné zariadenie alebo akcia resp. predpis so schopnosťou/cieľom redukovania bezpečnostných slabín a hrozieb.
Bezpečnostný incident – je akákoľvek aktivita používateľa alebo iného subjektu porušujúca všeobecne bezpečnosť informačného systému, konkrétne niektorú zásadu bezpečnostnej politiky alebo niektoré bezpečnostné opatrenie.
Bezpečnostný manažér IT – je osoba zodpovedná za implementáciu celkovej bezpečnostnej politiky, jej presadzovanie a udržiavanie. Za výkon funkcie zodpovedá rektorovi STU (vedúcemu zamestnancovi súčasti STU)
Dostupnosť – údaje a služby informačného systému majú byť dostupné oprávneným osobám pri iniciovaní požiadavky na sprístupnenie údaja resp. použitie služby.
Dôsledok – straty ako výsledky naplnených hrozieb môžu byt' vyjadrené prostredníctvom jednej alebo viacerých oblasti dôsledkov. K základným oblastiam patrí zničenie, znemožnenie prístupu k službe, prezradenie a modifikácia.
Dôvernosť – údaj uložený v informačnom systéme resp. prenášaný sieťou má byť prístupný iba oprávneným osobám. Pod prístupom sa rozumie zobrazenie údaja, vytlačenie údaja i samotné zistenie faktu, že došlo k prenosu (uloženiu) údaja.
Hrozba – akcia alebo potenciálna akcia, ktorej výsledkom môže byt' degradácia: utajenia (kompromitácia), celistvosti (narušenie integrity) alebo dostupnosti (znemožnenie prístupu k službe) systému alebo siete.
Identifikácia a autentifikácia – zabezpečujú určenie a overenie identity používateľa. Identifikácia a autentifikácia umožňuje účtovateľnosť aktivít používateľov (napríklad spätnej kontroly prihlasovania sa a odhlasovania sa do systému) ako aj evidencie aktivít používateľov v systéme.

Informačná technológia (IT) – IT predstavuje súbor technických (hardvérových), programových (softvérových), komunikačných, sieťových a iných podporných prostriedkov, pomocou ktorých sa spracovávajú a uchovávajú informácie a údaje poisťovne automatizovaným spôsobom. V tomto zmysle IT zahŕňa aj informačné systémy.
Informačný systém (IS) – IS predstavuje konkrétne použitie IT pre plnenie špecifických požadovaných funkcií. Informačný systém v zmysle zákona č. 428/2002 Z.z. je chápaný širšie a predstavuje ho napríklad aj papierová forma kartotéky.
Integrita – údaj uložený v informačnom systéme resp, prenášaný sieťou smie byť modifikovaný iba oprávnenými osobami a oprávneným spôsobom. Pod modifikáciou sa chápe zmena obsahu údaja, zmena statusu, opätovné vytvorenie údaja alebo jeho časti.
Metodik aplikácie – je zamestnanec celouniverzitného odborného útvaru IT STU, ktorý špecifikuje funkčné požiadavky modulu IS, zúčastňuje sa akceptačného testovania modulu a školenia používateľov.
Podporná technická infraštruktúra IT – predstavuje technické zariadenia, ktoré plnia podporné funkcie zabezpečujúce požadované prevádzkové podmienky IT (napr. záložné napájacie zdroje, klimatizácia a pod.).
Používateľ IT – je autorizovaná osoba, ktorej bolo zodpovedným zamestnancom STU priradené používateľské konto a prístupové práva k údajom a funkciám (zdrojom) STU
Prevádzkovateľ IS – prevádzkovateľom IS je STU, ktorá v zmysle Organizačného poriadku zodpovednosť za prevádzku IS delegovala na celouniverzitný odborný útvar IT.
Programové vybavenie (softvér) – je súhrn všetkého programového vybavenia oficiálne inštalovaného do technických prostriedkov. Pre účely tohoto materiálu sú zložky programového vybavenia nasledovné:

- **aplikačné programové vybavenie (APV),** ktoré vzniká pracovnou činnosťou riešiteľov (interných alebo externých) na základe požiadaviek používateľov – zamestnancov univerzity, slúži na podporu a zabezpečenie plnenia poslania a funkcií STU.
- **systémové programové vybavenie,** ktoré slúži na zabezpečenie riadneho spracovania automatizovaných úloh. Toto je neoddeliteľnou súčasťou technického vybavenia.
- **podporné programové nástroje,** ktoré slúžia na tvorbu jednoduchých automatizovaných úloh (textové, prezentačné a tabuľkové systémy apod.) alebo na elektronickú komunikáciu používateľov (elektronická pošta, Internetové prehliadače a pod.) v rámci spoločnosti alebo aj mimo nej.

Riadenie prístupu – umožňuje selektívne prideľovať prístup k zdrojom a údajom v informačnom systéme.
Riziko (bezpečnostné) – uskutočnenie nepriaznivej udalosti (hrozby) s určitou pravdepodobnosťou.
Rizikové elementy – hodnota aktíva, frekvencia hrozby, dôsledok hrozby, efektívnosť opatrení.
Rozbočovač (hub) – je aktívny prvok lokálnej počítačovej siete, ktorý zosiluje elektrický signál prenášajúci správy a umožňuje pripojiť viacero káblov do jedného miesta siete.
Optický prepínač – je aktívny prvok lokálnej počítačovej siete, slúžiaci na prepínanie pripojených optických trás, segmentov počítačovej siete.
Smerovač (router) – je aktívny prvok sieťovej infraštruktúry, ktorý rozhoduje o smerovaní správ (paketov) v počítačovej sieti tak, aby sa správa dostala od odosielateľa k adresátovi. Jeho funkcia sa nastavuje pomocou konfiguračného súboru.
Symetrický kryptosystém – je metóda šifrovania, pri ktorej je šifrovací aj dešifrovací kľúč rovnaký (kľúču sa hovorí tajný kľúč).

Technické prostriedky (hardvér) – predstavujú všetku výpočtovú techniku v spoločnosti, ako sú osobné počítače, terminály, pracovné stanice, prenosné počítače (notebooky), tlačiarne, servery, snímače dokumentov, záložné jednotky, záložné zdroje, sieťové komponenty, ktoré sú používané autonómne alebo spriahnuto – v rámci lokálnej (LAN) alebo rozsiahlej (WAN) počítačovej siete.
Vlastník aktíva – je organizačný útvar univerzity, ktorý špecifikuje funkčné vlastnosti aktíva, zodpovedá za jeho funkčnosť a ochranu a autorizuje prístupové práva používateľov k aktívu. K základným aktívam spoločnosti patria moduly IS (moduly APV) a príslušné údaje a technické prostriedky.

2. Vymedzenie činnosti zamestnancov a študentov STU pre účely tejto smernice

V tejto časti sú špecifikované činnosti súvisiace s bezpečnou a spoľahlivou prevádzkou a používaním informačného systému pre jednotlivé skupiny zamestnancov a študentov .

2.1 Systémový administrátor IT

1. Inštaluje systémové programy (predovšetkým operačné systémy).
2. Manipuluje s diskovými médiami a tlačiarňami.
3. Je zodpovedný za plnú prevádzkyschopnosť systémových prostriedkov a nástrojov.
4. Na základe povolení bezpečnostného manažéra IT zriaďuje nové používateľské kontá, prideľuje pre ne základné prístupové práva a preveruje oprávnenosť prístupových práv a používateľských kont. Rovnako na základe povolenia ruší používateľské kontá.
5. Zodpovedá za zálohovanie a archiváciu systémových a používateľských dát, za archív a vedenie evidencie záložných médií a ich bezpečné uloženie.
6. Denne náhodne monitoruje činnosť používateľov. Činnosti používateľov sa zaznamenávajú do auditných záznamov (logovacie súbory), ktoré sa vyhodnocujú a archivujú.
7. Pravidelne kontroluje stav technických súčastí informačného systému.
8. Raz týždenné nastavuje a kontroluje stav serverov.

2.2 Správca siete IT

1. Podľa požiadaviek bezpečnostnej politiky nastavuje prístupové práva na aktívnych sieťových prvkoch a komunikačných zariadeniach.
2. Pravidelne monitoruje stav siete pomocou programových nástrojov pre riadenie siete.
3. Udržuje v aktuálnom stave informácie o topológii siete, aktívnych a pasívnych prvkoch, o ich parametroch a nastaveniach.
4. Podrobný popis práv a povinností správcov chrbticovej siete a lokálnych sietí súčastí STU upravujú dokumenty : „Pravidlá prevádzky dátovej siete - STUNET“ a „ Pravidlá správy dátovej siete STUNET“, ktoré vydal rektor STU.

2.3 Databázový administrátor IT (privilegovaný používateľ)

1. Zriaďuje a eviduje a ruší kontá používateľov a skupín, pravidelne preveruje oprávnenosť používateľských kont a prípadne prístupových práv.
2. Vykonáva pravidelný audit databáz a pravidelne ich vyhodnocuje a zálohuje.
3. Uskutočňuje pravidelnú údržbu databáz, monitorovanie ich priestorových nárokov, optimálne nastavovanie parametrov databáz v závislosti od stavu operačného systému a od aktuálnej situácie v databázach.

4. Rieši havarijné stavy podľa havarijného poriadku, pri haváriách obnovuje dáta, funkčnosť databáz a konzultuje neštandardné stavy s dodávateľskými firmami.
5. Testuje a nasadzuje nové databázové softvéry, prípadne ich update a upgrade.
6. Zálohuje databázy a kontroluje pravidelnosť a spoľahlivosť prevádzky z hľadiska obnovy databáz po poškodení dát a obnovy databáz k dátumu.
7. Archivuje systémové a používateľské dáta databáz a vedie evidenciu záložných médií a archívu.
8. Denne námatkovo monitoruje činnosť používateľov. Činnosti používateľov sa zaznamenávajú do auditných záznamov (logovacie súbory), ktoré sa vyhodnocujú a archivujú.
9. Kontroluje v logovacích súboroch oprávnenosť vstupu do databázy (ochrana pred neoprávneným vstupom), zisťuje či bola prekonaná bezpečnostná brána a ak bola tak preveruje postup jej prekonania.
10. Spolupracuje s ostatnými oddeleniami pri testovaní, výberovom konaní pre nový softvér.
11. Tvorí a spolupodieľa sa na tvorbe návrhov smerníc, upresnení a školení súvisiacich s bezpečnosťou informačných systémov.

2.4 Bezpečnostný manažér IT

1. Nastavuje bezpečnostné charakteristiky pre jednotlivé komponenty informačného systému vrátane komunikačných prvkov.
2. Vyhodnocuje a spravuje kontrolné záznamy.
3. Vykonáva bezpečnostné školenia používateľov.
4. Kontroluje fyzickú bezpečnosť počítačového vybavenia a hlavnej miestnosti (serverovne), archívnych médií a výstupných zariadení (tlačiarne, zapisovače, atď.).
5. Kontroluje prístup k zariadeniam systému.
6. Kontroluje bezpečné uloženia záložných médií a archív.
7. Povoľuje zavedenie nových používateľov.
8. Kontroluje a spravuje systém prihlasovania užívateľov a stanovuje maximálnu dobu životnosti hesiel podľa bezpečnostnej politiky.
9. Riadi a zabezpečuje päťročnú archiváciu súborov týkajúcich sa bezpečnostných záznamov operačného systému a dôležitých aplikácií.
10. Analyzuje prieniky do informačných systémov a vytvára, optimalizuje a spravuje bezpečnostnú politiku STU.

2.5 Technik IT

1. Odstraňuje technické poruchy a závady na zariadeniach IT a to buď svojpomocne, napr. výmenou súčiastky, časti dielu alebo celého dielu za nový v rámci záručných podmienok, alebo formou doručenia chybného zariadenia do príslušného servisného strediska alebo dohovoru o oprave cez dodávateľa daného zariadenia.
2. Realizuje technické prepojenia lokálnych počítačových sietí na súčastiach a pracoviskách STU.

3. Pripája zariadenia IT do elektrickej siete napájania a do počítačovej siete STU - STUNET.
4. Prepája jednotlivé zariadenia IT medzi sebou.
5. Na základe príkazov priameho nadriadeného, vedúceho útvaru IT súčasti STU, bezpečnostného manažéra IT vykonáva fyzickú kontrolu nainštalovaného softvéru na PC a o výsledku im podá písomnú správu.
6. Vykonáva previerku zariadení IT, ktoré podliehajú pravidelnému technickému auditu.

2.6 Používateľ IT

1. Používa PC, operačný systém na ňom nainštalovaný, ako aj všetky aplikácie, na ktoré dostal oprávnenie.
2. Prihlasuje sa do počítačovej siete a používa zdieľané súbory, databázy, aplikácie, tlačiarne, či iné zariadenia podľa práv, ktoré mu boli pridelené na základe požiadavkového listu, potvrdeného jeho priamym nadriadeným, vedúcim útvaru IT súčasti STU, resp. vedúcim zamestnancom riaditeľom Centrálneho útvaru informatiky STU.
3. Je preukázateľne poučený o povinnosti dodržiavať túto smernicu a riadiť sa ňou pri svojej práci.
4. Riadi sa pokynmi zamestnancov celouniverzitného odborného útvaru IT STU a obracia sa na nich v prípade závad, porúch a mimoriadnych situácií.
5. Dbá na ochranu spracovávaných dát.
6. PC a ostatné zariadenia IT používa výhradne na služobné účely vyplývajúce z jeho opisu pracovnej činnosti. Na iné účely použitia zariadení IT potrebuje písomný súhlas priameho nadriadeného.

2.7 Používateľ Internetu

Zamestnanec a študent STU, ktorému bolo pridelené používateľské konto a na základe toho umožnený prístup do celosvetovej počítačovej siete Internet.

2.8 Používateľ intranetu

Zamestnanec a študent STU, ktorému bolo pridelené používateľské konto a na základe toho umožnený prístup do Intranetu počítačovej siete STU.

2.9 Používateľ elektronickej pošty

Zamestnanec a študent STU, ktorému bolo pridelené používateľské konto a na základe toho umožnené používanie elektronickej pošty (e-mailu).

2.10 Zamestnanec

Pre účely tejto smernice sa za zamestnanca považujú všetci kmeňoví zamestnanci STU a aj externí zamestnanci, ktorí majú s STU pracovno-právny vzťah, prípadne iný zmluvný vzťah.

2.11 Študent

Pre účely tejto smernice sa za študenta považujú študenti všetkých stupňov - bakalárskeho, inžinierskeho a doktorandského a foriem a to tak dennej ako aj externej formy štúdia na Slovenskej technickej univerzite.

3. Pravidlá na používanie prostriedkov IT

3.1 Používanie hardvéru

1. Na pracoviskách STU sa používa iba taký hardvér, ktorý je schválený príslušnými vedúcimi zamestnancami súčastí STU a je evidovaný v evidencii majetku na oddelení správy majetku ekonomického odboru STU ako HIM alebo DIM.
2. Akýkoľvek iný hardvér sa zakazuje používať.
3. Zakazuje sa akýkoľvek zásah do hardvéru alebo jeho konfigurácie a jeho svojvoľné premiestňovanie či výmena. Touto činnosťou je poverený technik príslušného útvaru IT súčasti STU, ktorý túto činnosť vykoná na základe schváleného požiadavkového listu - vzor je v prílohe tejto smernice.
4. Pri presune, sťahovaní či výmene treba požiadať o prevedenie a zaregistrovanie zmeny v evidencii majetku ekonomický odbor , oddelenie správy majetku STU a to formou požiadavkového listu.
5. Používatelia IT, ktorým boli zverené či zapožičané prenosné notebooky, či akékoľvek zariadenie IT, sú povinní používať ich tak, aby nedošlo k ich strate, zneužitiu či krádeži a nesmú ich požičať, prenechať, odovzdať tretej osobe, či u tretej osoby takéto zariadenie založiť formou záložného práva. V prípade potreby požičania zvereného IT zariadenia inej osobe musí používateľ IT zariadenia požiadať o písomný súhlas príslušného vedúceho zamestnanca STU. Dôverné údaje uložené na disku notebooku musia byť zašifrované a šifrovací kľúč musí byť uložený mimo notebook (napríklad na USB dongle)
6. Poruchu hardvéru treba nahlásiť útvaru IT súčasti STU formou požiadavkového listu, ktorý tvorí prílohu tejto smernice, prípadne vnútornou poštou alebo e-mailom. Pracovníci oddelenia IT sa okamžite, prípadne podľa dohody postarajú o odstránenie, nápravu, opravu či výmenu.

3.2 Používanie softvéru

1. Pri práci s PC je zakázané pracovať s iným softvérom, než aký bol nainštalovaný, resp. schválený útvarom IT súčasti STU.
2. Používateľ IT používa len ten softvér, na ktorého používanie má podľa schválenej požiadavky formou požiadavkového listu, ktorého vzor je prílohou tejto smernice, právo.
3. Pri akejkoľvek zmene týkajúcej sa používateľa IT a majúcej vplyv na používanie softvéru je povinný jeho priamy nadriadený formou požiadavkového listu či príslušného formuláru požiadať o vykonanie tejto zmeny príslušné oddelenie IT.
4. Po zakúpení softvéru tento nový softvér inštalujú zamestnanci príslušného útvaru IT súčasti STU alebo zamestnanci dodávateľskej firmy za prítomnosti zamestnanca útvaru IT a ekonomický odbor, oddelenie správy majetku má povinnosť tento softvér zaevidovať.
5. Poruchu softvéru treba nahlásiť príslušnému útvaru IT súčasti STU formou požiadavkového listu, ktorý tvorí prílohu tejto smernice, prípadne vnútornou poštou

alebo e-mailom. Pracovníci útvaru IT súčasti STU sa okamžite, prípadne podľa dohody postarajú o odstránenie, nápravu, opravu či výmenu.

6. Zakazuje sa používať, uchovávať, distribuovať akýkoľvek pirátsky softvér a údaje na hardvérovom vybavení STU.

3.3 Používanie služieb Internetu, intranetu a elektronickej pošty

1. STU celouniverzitný útvar IT používa softvér a systémy, ktoré umožňujú monitorovať a zaznamenávať všetky použitia celosvetovej počítačovej siete Internet a elektronickej pošty. Systémy môžu zaznamenávať každý prístup na webové stránky, diskusné skupiny, použitie elektronickej pošty, prenos súborov do a z STU.
2. Používateľ Internetu či elektronickej pošty, musí vedieť, že STU má právo v súlade so zákonnou úpravou preverovať použitie týchto prístupov. Výpisy z prístupov predkladá vedeniu STU bezpečnostný manažér IT na požiadanie.
3. STU má právo prekontrolovať všetky dáta a akékoľvek súbory uložené na lokálnych diskoch PC používateľov IT, či v ich domovských adresároch na serveroch a to na základe nariadenia tejto kontroly vedením STU alebo bezpečnostným manažérom IT.
4. Zobrazenie, archivovanie, uchovávanie, rozširovanie, spracovávanie alebo zaznamenávanie akéhokoľvek obrázku, či dokumentu s jednoznačným sexuálnym obsahom v ktoromkoľvek počítačovom systéme STU sa zakazuje.
5. Prístup na Internet a elektronickú poštu sa nesmú vedome použiť na porušenie zákonov, predpisov a legislatívy SR, či iných štátov.
6. Akýkoľvek softvér alebo súbor získaný prostredníctvom Internetu a uložený na počítači lokálnej siete súčasti STU, či na lokálny disk používateľa, sa stáva majetkom STU. Všetky takéto súbory, dokumenty či softvér, sa môžu používať výhradne len spôsobom, ktorý je v súlade s ich licenciami, autorskými právami, po odsúhlasení útvarom IT a musia priamo súvisieť s pracovnými povinnosťami používateľa IT.
7. Zakazuje sa získavanie a následné ukladanie zábavného softvéru alebo hier, videí, obrázkov a zvukových súborov z Internetu alebo prostredníctvom elektronickej pošty, hranie hier na Internete a prostredníctvom neho. Takisto sa zakazuje rozširovanie akéhokoľvek softvéru či údajov, ktoré sú majetkom STU bez jej predchádzajúceho písomného súhlasu vedúceho zamestnanca centrálneho útvaru IT STU.
8. Používateľom Internetu a elektronickej pošty v STU sa zakazuje využívať svetovú počítačovú sieť Internet a elektronickú poštu na zámerné rozširovanie akýchkoľvek vírusov, červíkov, trójskych koňov alebo iného škodlivého softvéru. Takisto používateľ nesmie využiť či zneužiť prístup na Internet či elektronickú poštu na vyradenie, preťaženie alebo oklamanie akéhokoľvek počítačového systému alebo počítačovej siete a tým narušiť súkromie alebo bezpečnosť iného používateľa či spoločnosti.
9. Každý používateľ Internetu a elektronickej pošty sa bude identifikovať svojim menom, prípadne pracovným zaradením, alebo u študentov STU fakultou a katedrou, na ktorej študuje, ak sa to vyžaduje.
10. Hovoriť, písať a prispievať v mene STU, alebo jej súčasti do akýchkoľvek diskusných skupín môžu len zamestnanci STU, ktorí sú riadne poverení komunikáciou s médiami. Ostatní používatelia Internetu a elektronickej pošty sa môžu zúčastňovať na

diskusiách a fórach v priebehu pracovnej doby, ak sa to vzťahuje na ich odbornú činnosť, ale v tom prípade vystupujú ako jednotlivci vo vlastnom mene a sú povinní informovať ostatných zúčastnených, že nie sú oprávnení vystupovať v mene STU, alebo jej súčasti. Pri účasti v týchto diskusiách a fórach je používateľ Internetu a elektronickej pošty povinný zdržať sa akýchkoľvek politických, náboženských, rasových prejavov, prejavov neznášanlivosti a prejavov urážajúcich ľudskú dôstojnosť, či prejavov týkajúcich sa trestnej činnosti a zverejňovať údaje a dôverné informácie STU.

11. Používatelia Internetu a elektronickej pošty môžu využívať prístup na Internet a elektronickú poštu pre prieskum alebo prezeranie informačných zdrojov nesúvisiaci s pracovnou náplňou počas obedovej alebo inej prestávky, alebo po pracovnej dobe, ale za predpokladu, že budú dodržané všetky ustanovenia tejto smernice.
12. STU je povinná poskytnúť orgánom činným v trestnom konaní všetky dostupné záznamy, týkajúce sa prístupu na Internet a elektronickú poštu príslušného používateľa Internetu a elektronickej pošty podľa príslušných zákonných ustanovení.
13. Používateľ Internetu a elektronickej pošty musí porozumieť a riadiť sa právnymi predpismi, autorským právom, obchodnými značkami. V tomto je používateľom Internetu a elektronickej pošty nápomocné právne oddelenie STU.
14. Komerčné používanie Internetu na podporu vedľajšej podnikateľskej činnosti zamestnanca STU alebo jej súčasti mimo jeho pracovnej náplne je možné iba na základe podmienok stanovených v zmluve, uzavretej medzi STU a Združením používateľov slovenskej akademickej dátovej siete - SANET, prevádzkujúcim pripojenie siete STU do medzinárodnej siete Internet.

3.4 Používanie hlasovej, faxovej a obrazovej komunikácie pri posielaní osobných údajov alebo iných citlivých informácií

1. Používanie hlasovej, faxovej a obrazovej komunikácie na STU pri posielaní osobných údajov alebo iných citlivých informácií sa riadi smernicou rektora č. 1/2007-N **„Klasifikácia aktív informácií informačného systému STU“.**
2. Každý vlastník aktív informačného systému je povinný dodržiavať pri používaní hlasovej, faxovej a obrazovej komunikácie vyššie uvedenú smernicu s tým, že každé porušenie ustanovení tejto smernice bude chápané ako porušenie pracovnej disciplíny v zmysle pracovného poriadku.
3. Každý vlastník aktív informačného systému zabezpečí, aby posielanie osobných údajov a citlivých informácií mohli vykonávať len písomne poverené osoby na základe zaškolenia. O poverení a zaškolení vedie evidenciu vlastník aktív, resp. bezpečnostný manažér STU.
4. Všetky zariadenia slúžiace na zber, archivovanie a posielanie citlivých informácií informačného systému sa musia využívať v súlade s pridelenými oprávneniami na základe prevádzkovej bezpečnostnej smernice informačného systému STU a pravidiel prevádzky dátovej siete STUNET. Toto ustanovenie zahŕňa aj dodržiavanie povinností informovať administrátora IT a správcu lokálnej siete súčasti STU o prípadných zmenách o pôvodne zastavených funkcionalít zariadení IKT a bezpečnostného manažéra STU o bezpečnostných incidentoch.

5. Vedúci zamestnanci fakúlt a ostatných súčastí STU zabezpečia pri nástupe nového zamestnanca jeho vstupné zaškolenie na používanie informačného systému, vrátane ochrany a bezpečnosti prístupu. Absolvovanie vstupného zaškolenia musí byť dokumentované a archivované na príslušnom personálnom útvare fakulty alebo súčasti STU.
6. Vedúci zamestnanci fakúlt a ostatných súčastí STU zabezpečia preškolenie zamestnancov v zmysle tejto smernice ako súčasť preškolenia „Bezpečnosti pri práci“ s pravidelnou minimálne 3-ročnou periodicitou vrátane vyhotovenia príslušných protokolov o vykonaní preškolenia,

4. Všeobecné pravidlá bezpečnosti IT

1. Používateľ IT je oprávnený pracovať v súlade s pridelenými právami a oprávneniami iba s počítačom, softvérom a údajmi potrebnými pre výkon jeho činnosti.
2. Je zakázané poskytovať tretím osobám špecifické informácie o používateľoch IS STU, ktoré by mohli byť zneužité pre neoprávnený prístup k údajom a programom, najmä identifikácie a autentifikácie, rozsah oprávnení a práv a heslá používateľov IT.
3. Každý používateľ IT má pridelené svoje prihlasovacie meno a heslo, ktoré musí zachovať v tajnosti. Tieto mená a heslá pomáhajú stanoviť osobnú zodpovednosť. Zakazuje sa spoločné používanie prihlasovacích mien a hesiel viacerými používateľmi IT. V prípade nebezpečia prezradenia je potrebné tieto heslá okamžite zmeniť.
4. Používateľ IT je plne zodpovedný za svoje heslo, nesmie byť ľahko uhádnuteľné, alebo odvoditeľné. V prípade zabudnutia hesla používateľom IT, si používateľ IT v súčinnosti so zamestnancami útvaru IT nastaví nové heslo.
5. V prípade zamestnancov, ktorí majú prístup k zaheslovaným dátam, súborom či programom a nikto iný takýto prístup nemá, musí svoje heslo uložiť v zalepenej podpísanej obálke u svojho nadriadeného. Pre zriadenie prístupu do počítačovej siete, programov, či Internetu a elektronickej pošty sa musí vyplniť požiadavkový list, ktorého vzor je prílohou tejto smernice, a sú povolené priamym nadriadeným používateľa, vedúcim zamestnancom súčasti alebo pracoviska STU, ktorý sa predloží útvaru IT súčasti STU. Pri akejkoľvek zmene (právo, oprávnenie, zrušenie prístupu, skončenie pracovného pomeru) je povinný nadriadený používateľa IT predložiť nové tlačivo zo zmenou a odovzdať ho útvaru IT súčasti STU.
6. V záujme zaistenia bezpečnosti svojich počítačov, počítačových sietí a softvérového vybavenia má STU nainštalované rôzne programy (firewall, proxy server, antivírusové prostriedky), monitorovacie systémy pre Internet a elektronickú poštu a bezpečnostné systémy. Zamestnancom a študentom STU sa zakazuje vyraďovať z činnosti, narúšať, prekonávať alebo obchádzať ktorékoľvek bezpečnostné zariadenie alebo systém .
7. Súbory, ktoré obsahujú citlivé (dôverné) údaje v zmysle citovanej smernice rektora č. 1/2007-N, musia byť pri akomkoľvek prenose prostredníctvom Internetu zašifrované. V tomto smere bude používateľovi IT nápomocný útvar IT súčasti STU. O takomto prenose musí byť vopred informovaný bezpečnostný manažér IT.
8. Pri opustení pracoviska, aj krátkodobého, je potrebné vylúčiť akúkoľvek možnosť neoprávneného prístupu tretích osôb k dátam a manipuláciu s nimi. V prípade, že používateľ IT, či zamestnanec útvaru IT súčasti STU zistí pokus o narušenie bezpečnosti IT týkajúce sa ochrany dát, je povinný takémuto pokusu podľa svojich

schopností a možností zabrániť a okamžite o tom informovať svojho nadriadeného a bezpečnostného manažéra IT a centrálny útvar IT.

9. V prípade prítomnosti zástupcu alebo zástupcov servisnej alebo dodávateľskej firmy je povinný zodpovedný vedúci zamestnanec STU, alebo jej súčasti určiť zamestnanca STU, ktorý bude zodpovedný za dohľad nad dodržiavaním ustanovení tejto smernice zo strany zástupcu alebo zástupcov servisných alebo dodávateľských firiem.
10. V prípade poruchy zariadenia IT, ktoré by mohlo obsahovať dáta, musí technik IT pred odovzdaním tohto zariadenia do opravy odstrániť všetky možné médiá, na ktorých by sa dáta mohli nachádzať (diskety, pevné disky, dátové pásky, worm média a pod.).
11. Ak je poškodený pevný disk, alebo disketová mechanika so zablokovanou disketou, alebo iné podobné čítacie alebo zapisovacie zariadenie so zablokovaným médiom, tak je technik IT povinný dať zástupcovi servisnej firmy podpísať čestné prehlásenie o mlčanlivosti, ktoré bude súčasťou zmluvy, prípadne objednávky.
12. Je zakázané poskytovať v akejkoľvek forme akékoľvek údaje o informačných systémoch STU, dáta, databázy či prehľady iným osobám, organizáciám bez predchádzajúceho písomného súhlasu dekana, prorektora alebo rektora STU. a bezpečnostného manažéra IT.
13. Centrálny útvar IT STU zabezpečí inštaláciu, prevádzku a priebežnú aktualizáciu antivírusového systému, prístupného pomocou automatickej inštalácie a aktualizácie prostredníctvom siete STU – STUNET všetkým PC, inštalovaným na STU.
14. Každý bezpečnostný incident, ktorý sa vyskytne na hardvéri, softvéri, zariadeniach počítačovej siete STU musí byť okamžite ohlásený podľa jeho povahy správcovi siete, správcovi aplikácie, databázovému administrátorovi, systémovému administrátorovi a bezpečnostnému manažérovi IT STU. Dokumentáciu o všetkých bezpečnostných incidentoch, ktoré sa vyskytli na STU vedie bezpečnostný manažér IT STU v denníku incidentov. Dokumentácia obsahuje, dátum vzniku incidentu, meno ohlasovateľa, popis incidentu a spôsobom jeho riešenia. Podrobne tento postup upravuje dokument „Usmernenie oznamovania bezpečnostných incidentov na STU“, vydaný rektorom STU.

5. Pravidlá na tvorbu prístupových hesiel

5.1 Heslo administrátora

Používateľ „**root**“, resp. administrátor serverov/pracovných staníc MS Windows:

1. Heslo musí byť menené pravidelne, v intervaloch medzi jednotlivými zmenami max. 90 dní.
2. Heslo musí mať najmenej 12 znakov, pričom v hesle môžu byť použité písmená anglickej abecedy, číslice a špeciálne znaky *,?.:-_!/|\=+[(]).* V hesle musí byť použitý najmenej jeden znak z intervalu *A ... Z*, aspoň jeden znak z intervalu *a ... z* a aspoň jedna číslica.
3. Posledných 5 použitých hesiel musí byť vzájomne rôznych.
4. Bezpečnostná kópia aktuálneho hesla administrátora musí byť zapísaná a uložená v zalepenej zapečatenej obálke u riaditeľa centrálneho útvaru IT STU.

5.2 Heslá používateľov s privilegovaným prístupom

Používatelia „správca DBS ORACLE, DBS Windows SQL“, „ správca OS Unix, OS MS Windows“ a pod. :

1. Heslo musí byť menené pravidelne, v intervaloch medzi jednotlivými zmenami max. 90 dní.
2. Heslo musí mať najmenej 12 znakov, pričom v hesle môžu byť použité písmená anglickej abecedy, číslice a špeciálne znaky *,?.:-_!/|\=+[()*. V hesle musí byť použitý najmenej jeden znak z intervalu *A ... Z*, aspoň jeden znak z intervalu *a ... z* a aspoň jedna číslica.
3. Posledných 5 použitých hesiel musí byť vzájomne rôznych.
4. Po piatom zadaní nesprávneho hesla musí systém zamknúť daný používateľský účet.

5.3 Heslá ostatných používateľov

Útvar IT súčasti STU a centrálny útvar IT STU musí evidovať v písomnej forme a archivovať údaje o zriadených používateľských účtoch, napríklad v Denníku používateľských účtov a prístupových práv. Oprávnenosť existencie používateľského účtu musí byť v pravidelných intervaloch (2×ročne) preverovaná.

1. Heslo musí byť menené pravidelne, v intervaloch medzi jednotlivými zmenami max. 180 dní.
2. Heslo musí mať najmenej 8 znakov, pričom v hesle môžu byť použité písmená anglickej abecedy, číslice a špeciálne znaky *,?.:-_!/|\=+[()*. V hesle musí byť použitý najmenej jeden znak z intervalu *A ... Z*, aspoň jeden znak z intervalu *a ... z* a aspoň jedna číslica.
3. Ako heslá sa nesmú používať slová a čísla, ktoré sú spojené s používateľom (jeho meno, dátum narodenia, tel. číslo a pod.).
4. Ak je heslo priradené administrátorom (pri vytvorení účtu, resp. pri zabudnutí hesla používateľom), po prvom prihlásení používateľa musí systém vynútiť zadanie nového používateľského hesla.
5. Posledných 5 použitých hesiel musí byť vzájomne rôznych.
6. Po piatom zadaní nesprávneho hesla musí systém zamknúť daný používateľský účet.

6. Pravidlá riadenia prístupu k aktívnym prvkom komunikačnej infraštruktúry

1. Aktívne prvky komunikačnej infraštruktúry – smerovače, prepínač, dátové brány (gateways), bezpečnostné brány (firewalls) a pod. – môžu byť prístupné iba autorizovaným oprávneným osobám, správcom chrbticovej siete STU a správcom lokálnych sietí súčastí STU.

2. Nastavovanie alebo zmena parametrov aktívnych prvkov komunikačnej infraštruktúry môže byť vykonávaná iba prostredníctvom priameho pripojenia nastavovacieho zariadenia (terminálu) na komunikačné rozhranie (port) aktívneho prvku vyhradeného výhradne pre tento účel. Uvedený vyhradený port nesmie byť prístupný cez dátovú sieť WAN alebo prostredníctvom diaľkového pripojenia.
3. NIE JE prípustné vzdialené (t.j. prostredníctvom dátovej siete WAN, resp. prostredníctvom diaľkového pripojenia) nastavovanie alebo zmena parametrov aktívnych prvkov komunikačnej infraštruktúry.
4. Autorizovaná oprávnená osoba (zamestnanec) o každom nastavení alebo zmene parametrov aktívneho prvku komunikačnej infraštruktúry vykoná zápis do Prevádzkovej knihy príslušného aktívneho prvku. Do Prevádzkovej knihy príslušného aktívneho prvku komunikačnej infraštruktúry sa tiež zapisuje každý výskyt bezpečnostne významnej udalosti v nasledovnej štruktúre:
   - meno zamestnanca, ktorý vykonáva zápis
   - popis problému
   - riešenie problému
   - zoznam osôb, ktorí boli zainteresovaní na riešení
   - stav, v akom zostalo riešenie problému
   - dátum, čas a podpis zamestnanca, ktorý vykonal zápis.
5. Pokyny na zaistenie bezpečnej prevádzky chrbticovej siete STU a lokálnych sietí súčastí STU a jej štruktúra je spracovaná v dokumentoch „Pravidlá prevádzky dátovej siete - STUNET“ a „ Pravidlá správy dátovej siete STUNET“, vydaných rektorom STU.

7. Účtovateľnosť a auditné záznamy

1. Cieľom účtovateľnosti a vytvárania auditných záznamov je záznam činností používateľov a zmien dôležitých údajov, detekcia, prevencia a potláčanie neregulárnych javov pri vstupe, výstupe a spracovaní údajov.
2. Všetky aplikácie IS a operačné systémy musia produkovať auditné záznamy. Tieto záznamy musia poskytovať informácie, ktoré umožnia neskoršie vyšetrovanie straty alebo neautorizovaných zásahov. Musia obsahovať minimálne záznam o významných zmenách údajov, čas a meno autorizovaného používateľa - pôvodcu zmeny.
3. Všetky súbory s auditnými záznamami musia byť chránené pred neautorizovaným prístupom a zásahom. Musia byť archivované v primeraných intervaloch. Auditné záznamy môžu byť vymazané iba s dvojnásobným autorizovaným súhlasom: bezpečnostného manažéra IS, riaditeľa centrálneho útvaru IT STU zodpovedného za bezpečnosť IS alebo inej k tomu oprávnenej osoby. Proces musí byť vykonaný pod dohľadom administrátora IS.
4. Auditné záznamy obsahujú tieto položky:
   - neúspešné pokusy používateľa o autentifikáciu,
   - prístup a aktivita privilegovaných používateľov,
   - neúspešné pokusy o prístup k údajom a funkciám,
   - zmeny v bezpečnostnom systéme a pridružených riadiacich informáciách,
   - všetky prihlásenia a odhlásenia používateľov so zápisom dátumu a času.

5. Administrátor aplikácie monitoruje a vyhodnocuje auditné záznamy aplikácie, systémový administrátor monitoruje a vyhodnocuje auditné záznamy operačného systému, bezpečnostný manažér IS monitoruje a vyhodnocuje všetky auditné záznamy.
6. Žiadna osoba nesmie mať prístupové práva umožňujúce neautorizovanú zmenu alebo vymazanie auditných záznamov.
7. Vyhodnocovanie auditných záznamov sa vykonáva nástrojom na to určeným (filtre s možnosťou nastavenia podozrivých operácií). Metodici aplikácií IS špecifikujú podozrivé operácie používateľov v aplikácii. Tieto operácie majú charakter nekorektných alebo nebezpečných operácií.

8. Zálohovanie údajov serverov informačného systému

1. Z pohľadu charakteru záloh sa zálohy delia na Operatívne a Bezpečnostné.
2. O vykonávaných činnostiach zálohovania vedie zamestnanec záznamy v Denníku záloh, ktoré obsahujú:
   1. Dátum, čas začiatku a ukončenia činnosti.
   2. Označenie zodpovedajúceho záznamového média – mg. pásky DAT, CD ROM, CD RW, DWD..
   3. U pások pre kontinuálne zálohovanie logických protokolov čísla protokolov uložených na páske.
   4. U pások s operatívnou a bezpečnostnou zálohou databázy číslo logického protokolu, ktoré patrí k danej páske.
   5. U pások s operatívnou a bezpečnostnou zálohou binárnych súborov operačného systému a vykonateľných súborov aplikácie označenie diskových priestorov zálohovaných na páske.
   6. Miesto uloženia archívnej pásky.
   7. Problémy, chyby a poznámky o priebehu zálohy.
   8. Podpis zamestnanca.
3. Pri použití čistiacej pásky musí byť o tom vykonaný záznam v Denníku záloh. Každá čistiaca páska má samostatný evidenčný list použitia.
4. Denník záloh, zálohovacie médiá s operatívnymi zálohami a zálohovacie médiá s bezpečnostnými zálohami záložnej sady A musia byť uložené v protipožiarnom trezore (požiarna odolnosť min. 60 minút a schopnosť ochrany obsahu trezoru voči striekajúcej vode).
5. Protipožiarny trezor musí byť umiestnený v dosahu zamestnanca vykonávajúceho zálohy, protipožiarny trezor musí byť umiestnený bezpečnom priestore chránenom elektronickým zabezpečovacím zariadením napojeným na strážnu službu objektu STU s definovanou samostatnou bezpečnostnou zónou alebo s bezpečnostnou zónou spoločnou pre miestnosť servera.
6. Zálohovacie médiá s bezpečnostnou zálohou záložnej sady B musia byť umiestnené v protipožiarnom trezore umiestnenom s samostatnej požiarnej zóne (iná budova, prenajatá bezpečnostná schránka v banke.

8.1 Operatívna záloha

1. Zálohovanie databáz databázového servera Oracle:
   1. Denne je automaticky vykonávaný logický backup databázy pomocou exportnej utility databázového servera **Oracle exp**, ktorá vykonáva logickú zálohu databázy, zálohovací skript shellu, ktorý túto utilitu využíva je volaný démonom operačného systému **unix cron**.
   2. Exportovaná je celá databáza (**full export**). Denne sú kontrolované log súbory z exportu databázy pre prípad výskytu chýb pri exporte. Výsledný súbor takto vytvorenej zálohy databázy, ktorý vo svojom názve obsahuje názov databázy a dátum vykonania jej zálohy je umiestnený na diskovom zariadení, na ktorom sa nenachádzajú žiadne súbory zálohovaných databáz. Raz za týždeň je takto vyexportovaná databáza uložená na zálohovacie páskové médium.
   3. Takýmto spôsobom sú vykonávané aj zálohy databáz systému EIS MAGION, AIS (Akademický informačný systém), KIS – OLIB (Knižničný informačný systém), Ubytovací systém študentov na ŠD, Stravovací systém Kredit pred a po uzávierke mesiaca, tie sú následne uložené na DVD médium.
   4. Dodatočne sa vykonáva záloha databázy pomocou fyzickej zálohy databázových súborov a automatickým archivovaním **online redo log súborov** (databáza pracuje v archive log móde pri ktorom sa odkladajú kópie generovaných redo log súborov), za využitia ktorých je možná obnova databázy z fyzickej zálohy databázových súborov. Databázové súbory sa ukladajú na pásku. Pravidelne sú na pásku zálohované archivované redo log súbory.

8.2 Bezpečnostná záloha

1. Zálohovanie súborov operačného systému a inštalácie databázového servera:

   1. Pravidelne sa vykonáva záloha operačného systému a súborov databázového servera pomocou nástroja **vdump** na pásku.

2. Zálohy vykonávané pri zmenách v rámci operačného systému a súborov databázového servera:
   1. Pri inštalovaní patchov pre databázový server, resp.operačný systém, nových verzií operačného systému a databázového servera, príp. iných zmien v rámci týchto systémov sa vykonáva fyzická záloha databázových súborov jednotlivých databáz, záloha operačného systému a súborov databázového servera.
   2. Po vykonaní zálohy je potrebné vykonať kontrolu záznamu o priebehu archivácie alebo spustiť kontrolu čitateľnosti archívnej pásky príkazom **dd.**
   3. Pre bezpečnostné zálohy sú používané 4 sady archívnych pások, ktoré sa cyklicky menia

3. Zálohovanie verzií aplikácií pri prechode ne nové verzie aplikácie
   1. Záloha verzií aplikácií pri prechode na novú verziu aplikácie sa vykoná na CD ROM, CD RW alebo DWD médiá spravidla na klientské rozhranie.

9. Likvidácia archívnych médií

1. Papierové médiá (tlačové výstupy informačného systému a pod.) musia byť likvidované v skartovacích strojoch umožňujúcich aspoň rozrezanie na prúžky so šírkou menšou ako 5 mm.
2. Skartovací stroj musí byť umiestnený v miestnosti (priestore) s inštalovanou veľkokapacitnou tlačiarňou alebo spoločnou sieťovou tlačiarňou.
3. Vyradené magnetické archívne média (diskety, pásky) a iné vyradené dátové médiá (CD-ROM, CD-RW) je potrebné skartovať (v skartovacom stroji, resp. pod dohľadom rozdrviť alebo fyzicky zlikvidovať v spaľovni odpadu).

10. Plán kontinuity činnosti informačného systému STU

1. Pre zabezpečenie kontinuity informačného systému je vypracovaný **„Havarijný plán informačného a počítačového systému STU“** ako súčasť zabezpečenia ochrany údajov a informačnej bezpečnosti informačného systému STU.
2. Súčasťou tohto havarijného plánu je aj plán obnovy činnosti informačného systému po jeho havárii.
3. Základnou podmienkou obnovy činnosti po havárii je zistiť dôvod havárie, alebo narušenia informačného a počítačového systému STU a zabrániť ďalším poškodeniam zariadení počítačového systému alebo dát.
4. Obnova činnosti havarovaného informačného systému STU podľa stupňa poškodenia je možná na pôvodnom (opravenom) HW alebo na dočasnom HW pôvodne slúžiacom pre iný účel. STU neplánuje prevádzkovať kompletnú zálohu HW a SW informačného systému, ani neplánuje vytvorenie a inštaláciu alternatívneho informačného počítačového systému v náhradnom prostredí. Rovnako tak STU neplánuje prevádzkovať plne záložný informačný a počítačový systém.
5. Pre zabezpečenie kontinuity informačného systému je nevyhnutné zabezpečiť zálohovanie všetkých relevantných dát informačného systému vrátane aktuálnych databáz.

11. Klasifikácia, označovanie a manipulácia s dokumentami

1. Klasifikácia a označovanie dokumetov obsahujúcich citlivé informácie označované ako dôverné a dokumetov s informáciami pre internú potrebu, ktoré sú zhromažďované, spracovávané a archivované na pracoviskách STU je určená vnútornými predpismi vydanými rektorom STU – **Smernicou rektora č. 1/2007-N Klasifikácia aktív a informácií informačného systému STU, Registratúrnym poriadkom STU a Smernicou na ochranu osobných údajov STU.**

2. Ostatné dokumenty, ktoré nespadajú do vyššie uvedených kategórií sú dokumenty verejne prístupné, ktoré nemajú charakter citlivých informácií a je možné ich ľubovoľne zverejňovať, kopírovať a šíriť.

12. Zabezpečenie ochrany osobných údajov pri dodávke, inštalácii a údržbe technických a programových prostriedkov Informačného a komunikačného systému STU

1. Pri uzatváraní dodávateľských zmlúv na dodávku programových systémov, ich inštalácie, alebo na zabezpečenie ich pravidelnej údržby, je vedúci pracovník fakulty alebo súčasti STU povinný zabezpečiť, aby každá takáto zmluva obsahovala článok uvádzajúci povinnosť dodávateľa zachovávať mlčanlivosť pri styku s osobnými údajmi zamestnancov alebo študentov STU v súlade s ustanoveniami zákona č. 122/2013 Z.z. O ochrane osobných údajov a o zmene a doplnení niektorých zákonov.
2. Rovnaká povinnosť sa týka aj dodávky technických a sieťových zariadení a komponentov. Pri prideľovaní prístupových práv tretím osobám je potrebné postupovať podľa ustanovení tejto "Prevádzkovej bezpečnostnej smernice informačného systému STU".
3. Pri uzatváraní kooperačných zmlúv, dohôd o vykonaní práce alebo dohôd o pracovnej činnosti na činnosti vzťahujúce sa k informačnému a komunikačnému systému STU je potrebné postupovať podľa „Smernice na ochranu osobných údajov na STU".

13. Previerka informácií a zariadení informačného a počítačového systému STU

1. Pre zabezpečenie pravidiel pre bezpečnú a spoľahlivú prevádzku a používanie informačného systému STU v súlade s ustanoveniami tejto smernice je potrebné vykonávať priebežné kontroly jej plnenia:
    a. raz ročne vykonať previerku zariadení na zber a spracovanie informácií a dokumentov o používaní aktív informačného systému STU v zmysle zhody s bezpečnostným zámerom STU.
    b. raz za 3 roky realizovať externé audity prevádzkovaných informačných systémov. Pod externými auditmi sa rozumie, že audit prevádzkovaných informačných systémov vykoná dodávateľská firma, alebo komisia zložená z odborníkov z radov zamestnancov STU na informačné komunikačné technológie, ktorá nemá v pracovnej náplni zabezpečovať prevádzku informačných systémov.

14. Kontrolná činnosť

Kontrolnú činnosť dodržiavania tejto Smernice vykonávajú všetci vedúci zamestnanci a všetci vedúci útvarov STU, fakúlt STU a súčastí STU v rámci svojich právomocí a pôsobnosti.

15. Prílohy

15.1 Požiadavkový list na prístup k zdrojom informačného systému STU

<table>
<tr><td colspan="4">ŽIADANKA O PRÍSTUP K ZDROJOM IS STU</td></tr>
<tr><td colspan="2">FAKULTA, CUP STU</td><td colspan="2">Pracovisko:</td></tr>
<tr><td colspan="2">Meno :</td><td colspan="2" rowspan="2">Priamy nadriadený:</td></tr>
<tr><td>Miestnsť č.</td><td>Telefón:</td></tr>
<tr><td colspan="4">Žiadam o poskytnutie prístupových práv používateľa k zdrojom Informačnéhu systému STU: (špecifikácia zdrojov, napr. databáza časopisov a pod.)</td></tr>
<tr><td>Dátum:</td><td>Používateľ:</td><td>Priamy nadriadený:</td><td>Pracovník IKT:</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

15.2 Požiadavkový list na zmenu alebo premiestnenie hardvéru

<table>
<tr><td colspan="4">ŽIADANKA O ZMENU, PREMIESNENIE HARDVÉRU</td></tr>
<tr><td colspan="2">Fakulta, CUP STU</td><td colspan="2">Pracovisko:</td></tr>
<tr><td colspan="2" rowspan="2">Meno:</td><td colspan="2">Miestnosť:</td></tr>
<tr><td colspan="2">Č.telefónu:</td></tr>
<tr><td colspan="3">Druh výpočtovej techniky, zariadenie (vyznačiť):
1. monitor 2. klávesnica 3. myš
4. počítač 5. tlačiareň 6. notebook
7. scanner 8. iné</td><td>inventárne/evidenčné č.:</td></tr>
<tr><td colspan="4">Typové označenie (napr. tlačiareň HP LJ 1100):</td></tr>
<tr><td colspan="4">ŽIADAM O:</td></tr>
<tr><td>DÁTUM:</td><td>VYSTAVIL:</td><td colspan="2">PREVZAL:</td></tr>
<tr><td></td><td></td><td colspan="2"></td></tr>
</table>

15.3 Požiadavkový list na servisný zásah

<table>
<tr><th colspan="4">ŽIADANKA O SERVISNÝ ZÁSAH</th></tr>
<tr><td colspan="2">Fakulta, CUP STU</td><td colspan="2">Pracovisko:</td></tr>
<tr><td colspan="2" rowspan="2">Meno:</td><td colspan="2">Miestnosť:</td></tr>
<tr><td colspan="2">Č.telefónu:</td></tr>
<tr><td colspan="3">Druh výpočtovej techniky, zariadenie (vyznačiť):
1. monitor 2. klávesnica 3. myš
4. počítač 5. tlačiareň 6. notebook
7. scanner 8. iné</td><td>inventárne/evidenčné č.:</td></tr>
<tr><td colspan="4">Typové označenie (napr. tlačiareň HP LJ 1100):</td></tr>
<tr><td colspan="4">ŽIADAM O:</td></tr>
<tr><td>DÁTUM:</td><td>VYSTAVIL:</td><td colspan="2">PREVZAL:</td></tr>
<tr><td></td><td></td><td colspan="2"></td></tr>
</table>

15.4 Požiadavkový list na inštaláciu softvéru

<table>
<tr><td colspan="4">ŽIADANKA O INŠTALÁCIU SOFTVÉRU</td></tr>
<tr><td colspan="2">FAKULTA, CUP STU</td><td colspan="2">Pracovisko:</td></tr>
<tr><td colspan="2">Meno :</td><td colspan="2" rowspan="2">Priamy nadriadený:</td></tr>
<tr><td>Miestnosť:</td><td>Telefón:</td></tr>
<tr><td colspan="2">Názov softvéru :</td><td colspan="2">PC invent./eviden.č.:</td></tr>
<tr><td colspan="4">Žiadam o ištaláciu softvéru: (špecikácia inštalačného prostredia, OS, aplikačný SW))</td></tr>
<tr><td>Dátum:</td><td>Používateľ:</td><td>Priamy nadriadený:</td><td>Pracovník IKT:</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

V Bratislave dňa :

prof. Ing. Robert Redhammer, PhD.[1]
rektor

[1] Originál podpísanej Smernice rektora „Prevádzková bezpečnostná smernica informačného systému STU“ je uložený a k nahliadnutiu prístupný v kancelárii rektora a u bezpečnostného manažéra STU.