

**Metodické usmernenie na vykonanie ustanovení Prevádzkovej
bezpečnostnej smernice informačného systému STU**

Vypracoval: prof. Ing. Pavol Horváth, CSc.

SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE

Obsah :

| | |
|---|-----------|
| 1. ÚVOD | 4 |
| 1.1 ZÁKLADNÉ POJMY | 4 |
| 2. VYMEDZENIE ČINNOSTI ZAMESTNANCOV A ŠTUDENTOV STU PRE ÚČELY TEJTO SMERNICE | 7 |
| 2.1 SYSTÉMOVÝ ADMINISTRÁTOR IT | 7 |
| 2.2 SPRÁVCA SIETE IT | 7 |
| 2.3 DATABÁZOVÝ ADMINISTRÁTOR IT (PRIVILEGOVANÝ POUŽÍVATEL) | 7 |
| 2.4 TECHNIK IT | 8 |
| 2.5 POUŽÍVATEL IT | 8 |
| 3. POUŽÍVATEL INTERNETU | 9 |
| 4. POUŽÍVATEL INTRANETU | 9 |
| 4.1 POUŽÍVATEL ELEKTRONICKEJ POŠTY | 9 |
| 4.2 ZAMESTNANEC | 9 |
| 4.3 ŠTUDENT | 9 |
| 5. PRAVIDLÁ SPRÁVY A PREVÁDZKY DÁTOVEJ SIETE – | 9 |
| STUNET | 9 |
| 5.1 ZÁKLADNÉ USTANOVENIE | 9 |
| 5.2 PRÍSTUPOVÉ PRÁVA A IDENTIFIKÁCIA UŽÍVATEĽOV | 10 |
| 5.3 ORGANIZAČNÁ ŠTRUKTÚRA SPRÁVY DÁTOVEJ SIETE STUNET | 11 |
| 5.4 PRÁVA A POVINNOSTI SPRÁVCOV DÁTOVEJ SIETE STUNET | 11 |
| 5.5 POUŽÍVANIE DÁTOVEJ SIETE STUNET | 12 |
| 5.6 PRAVIDLÁ PRE PRIPOJENIE K DÁTOVEJ SIETI STUNET | 13 |
| 6. PRAVIDLÁ NA POUŽÍVANIE PROSTRIEDKOV IT | 14 |
| 6.1 POUŽÍVANIE HARDVÉRU | 14 |
| 6.2 POUŽÍVANIE SOFTVÉRU | 14 |
| 6.3 POUŽÍVANIE INTERNETU, INTRANETU A ELEKTRONICKEJ POŠTY | 15 |
| 6.4 POUŽÍVANIE HLASOVEJ, FAXOVEJ A OBRAZOVEJ KOMUNIKÁCIE | 16 |
| PRI POSIELANÍ OSOBNÝCH ÚDAJOV ALEBO INÝCH CITLIVÝCH INFORMÁCIÍ | 16 |
| 6.5 KAMEROVÉ SYSTÉMY | 17 |
| 7. PRAVIDLÁ NA TVORBU PRÍSTUPOVÝCH HESIEL | 17 |
| 7.1 HESLO ADMINISTRÁTORA | 17 |
| 7.2 HESLÁ POUŽÍVATEĽOV S PRIVILEGOVANÝM PRÍSTUPOM | 17 |
| 7.3 HESLÁ OSTATNÝCH POUŽÍVATEĽOV | 17 |
| 7.4 PRIDEĽOVANIE ADRESY ELEKTRONICKEJ POŠTY | 18 |
| 7.5 PRIDEĽOVANIE PRÍSTUPOVÝCH HESIEL DO INFORMAČNÉHO | 18 |
| SYSTÉMU | 18 |
| 7.6 PRIDEĽOVANIE HESIEL PRE VZDIALENÝ VPN PRÍSTUP DO | 19 |
| WIFI SIETE | 19 |
| 8. PRAVIDLÁ RIADENIA PRÍSTUPU K AKTÍVNYM PRVKOM | 19 |
| KOMUNIKAČNEJ INFRAŠTRUKTÚRY | 19 |
| 9. DISCIPLINÁRNY POSTIH ŠTUDENTOV ZA PORUŠENIE | 20 |
| PRAVIDIEL PREVÁDZKY DÁTOVEJ SIETE STUNET | 20 |
| 10. DISCIPLINÁRNY POSTIH ZAMESTNANCOV ZA PORUŠENIE | 20 |
| PRAVIDIEL PREVÁDZKY DÁTOVEJ SIETE STUNET | 20 |

SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE

| | |
|--|-----------|
| 11. OCHRANA SÚKROMIA A ZVEREJŇOVANIE INFORMÁCIÍ..... | 21 |
| 12. ÚČTOVATEĽNOSŤ A AUDITNÉ ZÁZNAMY | 22 |
| 13. ZÁLOHOVANIE ÚDAJOV SERVEROV INFORMAČNÉHO | 23 |
| SYSTÉMU | 23 |
| 13.1 BEZPEČNOSTNÁ ZÁLOHA..... | 24 |
| 13.2 LIKVIDÁCIA ARCHÍVNYCH MÉDIÍ | 24 |
| 13.3 PLÁN KONTINUITY ČINNOSTI INFORMAČNÉHO SYSTÉMU STU..... | 25 |
| 14. KLASIFIKÁCIA, OZNAČOVANIE A MANIPULÁCIA S | 25 |
| DOKUMENTAMI | 25 |
| 15. ZABEZPEČENIE OCHRANY OSOBNÝCH ÚDAJOV PRI DODÁVKE, | 25 |
| INŠTALÁCII A ÚDRŽBE TECHNICKÝCH A PROGRAMOVÝCH PROSTRIEDKOV | |
| INFORMAČNÉHO A KOMUNIKAČNÉHO SYSTÉMU STU | 25 |
| 16. PREVIERKA INFORMÁCIÍ A ZARIADENÍ INFORMAČNÉHO | 26 |
| A POČÍTAČOVÉHO SYSTÉMU STU..... | 26 |
| 17. KONTROLNÁ ČINNOSŤ | 26 |
| 18. PRÍLOHY | 26 |
| 18.1 ZOZNAM SPRÁVCOV MODULOV IS NA PRACOVISKU UIS CVT STU..... | 26 |
| 18.2 ZOZNAM INTEGRÁTOROV AIS NA FAKULTÁCH | 26 |
| 18.3 ZOZNAM SPRÁVCOV SIETE STUNET | 27 |
| 18.4 HELPDESK CVT STU..... | 27 |

1. Úvod

Informačný systém predstavuje významný nástroj podporujúci efektívne fungovanie každej inštitúcie a to platí aj pre verejnú vysokú školu – Slovenskú technickú univerzitu v Bratislave. 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.

Slovenská technická univerzita v Bratislave (ďalej STU) v rámci splnenia povinností vyplývajúcich z čl. 32 Nariadenia na ochranu osobných údajov 2016/679 General Data Protection Regulation (ďalej len GDPR), ako aj podľa § 39 zákona č. 18/2018 Z.z. o ochrane osobných údajov Z.z. **je povinná ako prevádzkovateľ vykonať také technické a organizačno-právne opatrenia aj v oblasti bezpečnosti a ochrany prístupu v technickej infraštruktúre, ako sú používanie aktuálnych verzií operačných, databázových a sieťových programov, programov proti škodlivému softvéru, sieťových zariadení pre zabezpečenie prevádzky dátovej siete STUNET a zariadení, vrátane softvéru pre zabránenie útokov na technické zariadenia (servery, PC stanice a iné) zapojené v sieti STUNET, ako aj mimo nej.**

Táto prevádzková bezpečnostná 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.

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 inforatických služieb.

Analýza rizík – preskúmanie vzťahov medzi aktívami, hrozbami, bezpečnostnými slabunami 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. Najúčinnjšou konfiguráciou je konfigurácia tienenej podsiete (screened subnet). Táto konfigurácia obsahuje tienenu 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, resp. vedúcemu zamestnancovi súčasti STU.

Centrálny útvar informatiky na STU – Centrum výpočtovej techniky STU – ďalej CVT STU.

Dostupnosť – údaje a služby informačného systému majú byť dostupné oprávneným osobám pri iniciovaní požiadavky na sprístupnenie údajov resp. použitie služby.

Dôsledok – straty ako výsledky naplnených hrozieb môžu byť vyjadrené prostredníctvom jednej alebo viacerých oblastí 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 údajov, vytlačenie údajov i samotné zistenie faktu, že došlo k prenosu (uloženiu) údajov.

Hrozba – akcia alebo potenciálna akcia, ktorej výsledkom môže byť 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 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 alebo geografickom základe.

Integrita – údaj uložený v informačnom systéme resp. prenášaný sieťou smie byť modifikovaný iba oprávnenými osobami a oprávneným spôsobom. Pod modifikáciou sa chápe zmena obsahu údajov, zmena statusu, opätovné vytvorenie údajov 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.

SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE

Perióda zálohovania – interval medzi časmi vytvárania dvoch po sebe nasledujúcich záloh dát z toho istého systému.

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, ktorým je centrum výpočtovej techniky STU.

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 pridelovať 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.

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 spriahnuté – v rámci lokálnej (LAN) alebo rozsiahlej (WAN) počítačovej siete.

Účel spracovania osobných údajov sa rozumie konkrétne vymedzený alebo ustanovený zámer, na základe ktorého bude prevádzkovateľ spracúvať osobné údaje viažuce sa na jeho činnosť. Tento účel by si mal prevádzkovateľ stanoviť vopred a mal by byť oprávnený.

Útvar IT súčasti STU – Výpočtové stredisko fakulty STU- ďalej len VS súčasti STU.

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.

Zodpovedná osoba – je osoba zodpovedná za implementáciu celkovej bezpečnostnej politiky, jej presadzovanie a udržiavanie, je ustanovená v zmysle §44 zákona č. 18/2018 Z.z, o ochrane osobných údajov. Za výkon funkcie zodpovedá rektorovi STU (vedúcemu zamestnancovi súčasti STU).

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. Zriaďuje nové používateľské kontá, prideluje pre ne základné prístupové práva a preveruje oprávnenosť prístupových práv a používateľských kont. Rovnako ruší používateľské kontá.
5. Zodpovedá za zálohovanie a archiváciu systémových a používateľských dát, za archív a vedenie evidencie záložných médií a ich bezpečné uloženie. Rieši havarijné stavy.
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. Udržiava v aktuálnom stave informácie o topológii siete, aktívnych a pasívnych prvkoch, o ich parametroch a nastaveniach. Rieši havarijné stavy.
4. Podrobný popis práv a povinností správcov chrbticovej siete a lokálnych sietí súčastí STU je uvedený v kapitole 3.

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. Zálohujie 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 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 súčiastiach 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 a 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 s tým, že pripravuje inováciu zariadení IT, tak, aby na nich bolo možné inštalovať najnovšie verzie operačných, systémových a aplikačných programových produktov.
7. Dôsledne aplikuje opravy (patche) odporúčané výrobcom pre operačné systémy a systémové programy na všetkých inštalovaných zariadeniach IT na STU v okruhu svojej pôsobnosti.

2.5 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 výpočtového strediska súčasťou STU, resp. vedúcim zamestnancom, alebo riaditeľom Centra výpočtovej techniky STU.

3. Je preukázateľne poučený o povinnosti dodržiavať túto smernicu a riadiť sa ňou pri svojej práci.
4. Riadi sa pokynmi zamestnancov Výpočtového strediska súčasťi STU a CVT 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.

3. Používateľ Internetu

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

4. Používateľ intranetu

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

4.1 Používateľ elektronickej pošty

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

4.2 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.

4.3 Študent

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

5. Pravidlá správy a prevádzky dátovej siete – STUNET

5.1 Základné ustanovenie

1. Dátová sieť Slovenskej technickej univerzity v Bratislave (ďalej len STUNET) je súčasťou metropolitnej dátovej siete v Bratislave. Je priamo pripojená na Slovenskú akademickú dátovú sieť pre vedu, výskum a vzdelávanie – SANET a jej prostredníctvom do európskej vysokorýchlostnej dátovej siete pre vedu výskum a vzdelávanie GEANT a medzinárodnej dátovej siete INTERNET.
2. Pod pojmom dátová sieť STUNET sa pre účely aplikácie týchto pravidiel považujú všetky technické a programové prostriedky, slúžiace k prepojeniu počítačov, ako aj prostriedky k využitiu tohto pripojenia. Poslaním dátovej siete STUNET je vzájomné

prepojenie objektov Slovenskej technickej univerzity v Bratislave a Trnave a ich pripojenie do metropolitnej siete v Bratislave pre zabezpečenie výučby, výskumu a prevádzky školy :

- Metropolitná chrbticová sieť je časť dátovej siete, ktorá prepája objekty STU v Bratislave a v Trnave s objektmi vysokých škôl v Bratislave, pracoviskami SAV a Ministerstvom školstva vedy výskumu a športu SR.
- Chrbticová sieť STU - STUNET je časť metropolitnej siete , ktorá prepája vstupné prípojné miesto areálu STU s prípojnými miestami lokálnych sietí fakúlt a súčastí (napr. študentský domov) STU
- Lokálna sieť fakulty alebo súčasti STU je časť dátovej siete STUNET , ktorá zahŕňa koncové zariadenia (používateľské pracovné stanice, servery, tlačiarne a ďalšie zariadenia) a ktorá prepája tieto zariadenia s prípojným miestom lokálnej siete v rámci areálu i medzi sebou navzájom.
- Server je obslužný počítač (resp. program), ktorý poskytuje presne stanovené služby alebo prostriedky (zdroje) používateľov.
- Sieťová aplikácia je program, ktorý pracuje pre užívateľa a ktorý používateľovi poskytuje vopred stanovené sieťové služby.
- Sieťová služba je služba na zabezpečenie stanovených požiadaviek alebo potrieb používateľov.

Pravidlá uvedené v tomto usmernení sú záväzné pre správcov dátovej siete STUNET. Tieto pravidlá sú rovnako záväzné pre používateľov, ktorí spravujú samostatne svoje výpočtové prostriedky napojené na dátovú sieť STUNET.

3. Správca dátovej siete STUNET je osoba zodpovedná za prevádzku konkrétnej dátovej siete, jej častí alebo sieťovej aplikácie.

5.2 Prístupové práva a identifikácia užívateľov

1. Dátovú sieť STUNET môžu využívať len oprávnení používatelia. Oprávnenými používateľmi (ďalej len používateľ) sú používatelia, ktorí boli preukázateľne oboznámení s týmto usmernením. Aktuálny zoznam používateľov dátovej siete s IP adresami zariadení a využívaní doménového priestoru udržiava správca dátovej siete, alebo jej časti.
2. Oprávnenie používať prostriedky dátovej STUNET majú zamestnanci a študenti STU. Používanie dátovej siete STUNET osobami iných organizácií, je možné len na základe písomného povolenia vydaného rektorom STU, dekanom, alebo vedúcim zamestnancom súčasti STU. Takéto povolenie sa vzťahuje len na používanie siete STUNET a neplatí automaticky aj na používanie Slovenskej akademickej dátovej siete SANET. (STU nemá právo predávať ani umožňovať prístup do siete SANET iným organizáciám. Toto právo prislúcha len Združeniu SANET prostredníctvom svojej správy uzlov).
3. Pokiaľ je pre prístup k dátovej siete STUNET požadovaná identifikácia používateľa, je používateľ povinný používať meno pridelené správcovi dátovej siete STUNET. Používateľ je povinný používať pre overenie identity heslo, vytvorené na základe pravidiel, udržiavať toto heslo v tajnosti, tak aby bolo zabránené jeho zneužitiu.
4. Používateľ nesmie poskytnúť pridelené meno a heslo inej osobe. Za hrubé porušenie pravidiel sa považuje poskytnutie mena a hesla osobe, ktorá nemá nárok na prístup do siete, alebo ktorej bol prístup odopretý alebo zablokovaný.

5. Používateľ nesmie zneužiť nedbanlivého správania iného používateľa, (napr. náhodné zistenie mena a hesla, zabudnuté odhlásenie a pod.) k tomu, aby pracoval pod iným – cudzím menom a heslom.
6. Prístupové práva používateľa sú pridelené správcovi dátovej siete. Používateľ sa nesmie žiadnymi prostriedkami pokúsiť získať prístupové práva, ktoré mu neboli pridelené. Pokiaľ používateľ získa prístupové práva neoprávnene bez vlastného pričinenia, napr. chybou systému, je povinný túto skutočnosť bezodkladne ohlásiť správcovi súčasti dátovej siete (na úrovni katedry, ústavu, objektu fakulty) na adresu **spravca.xxxxxx@stuba.sk** napr. **spravca.cvtstu@stuba.sk** a tieto práva nesmie použiť.
7. Používateľ sa dopustí hrubého porušenia disciplíny pokiaľ sa pokúsi zneužiť dátovú sieť STUNET k získaniu neautorizovaných prístupových práv k ľubovoľným informačným zdrojom dostupným prostredníctvom dátovej siete STUNET, pokiaľ podnikne cez sieť STUNET softvérové útoky na počítače a iné zariadenia kdekoľvek v sieti Internet.

5.3 Organizačná štruktúra správy dátovej siete STUNET

1. Dátová sieť má hierarchickú štruktúru. Člení sa na:
 - a) chrbticovú sieť
 - b) lokálnu sieť fakúlt a súčastí STU
 - c) sieťové aplikácie
2. Správu chrbticovej siete, vrátane prípojných miest do akademickej siete SANET, medzinárodných sietí GEANT (európskej vysokorychlostnej dátovej siete pre vedu výskum a vzdelávanie) a medzinárodnej siete Internet a celouniverzitných sieťových aplikácií zabezpečuje Centrum výpočtovej techniky na STU. Správu chrbticovej siete areálov STU, správu lokálnych sietí fakúlt a súčastí STU a správu lokálnych sieťových aplikácií, zabezpečujú príslušní správcovia siete, súčastí STU.
3. Prevádzku centrálnych informačných systémov a centralizovanej výpočtovej techniky zabezpečuje Centrum výpočtovej techniky STU. Jeho poslanie a pôsobnosť vymedzuje organizačný poriadok STU a Organizačný poriadok CVT STU.
4. Správcovia študentských dátových sietí na študentských domovoch a jedálňach sú podriadení správcovi chrbticovej siete STU a na vyššej úrovni riaditeľovi Centra výpočtovej techniky STU.
5. **Zoznam správcov jednotlivých súčastí siete STUNET musí byť verejne dostupný a aktuálny na www stránke CVT STU.**

5.4 Práva a povinnosti správcov dátovej siete STUNET

1. Správca lokálnej sieťovej aplikácie a lokálnych serverov:
 - a) zabezpečuje prevádzku sieťovej aplikácie (inštalácia, úpravy, konfigurácia,
 - b) zálohovanie dát a pod.)
 - c) vytvára používateľské kontá podľa zásad platných pre konkrétnu lokálnu sieťovú
 - d) aplikáciu a prideliť používateľom prístupové práva.
 - e) zodpovedá za bezpečné uloženie záložných dát, rieši havarijné stavy

2. Správca lokálnej siete fakulty a súčasti STU:
 - a) zabezpečuje prevádzku lokálnej siete od prípojného miesta chrbticovej siete areálu až ku koncovým používateľským pracovným staniciam
 - b) zabezpečuje správnu funkciu lokálnych serverov
 - c) vytvára a spravuje používateľské kontá podľa zásad platných pre prevádzku lokálnej dátovej siete a prideliťuje používateľom prístupové práva
 - d) udržiava konfiguráciu systémov pre počítače, ktorých systém je spúšťaný zo servera
 - e) prideliťuje IP adresy zariadeniam z rozsahu IP adries, ktoré má v správe
 - f) udržiava aktuálny zoznam MAC a IP adries všetkých pripojených zariadení a všetky zmeny hlási správcovi lokálnej siete fakulty
 - g) spravuje príslušný doménový priestor fakulty, alebo súčasti
 - h) informuje používateľov o pravidlách práce v sieti
 - i) zodpovedá za bezpečné uloženie záložných dát, rieši havarijné stavy

3. Správca chrbticovej siete STU:
 - a) zabezpečuje prevádzku chrbticovej siete
 - b) zabezpečuje pre STUNET konektivitu pripojených dátových sietí
 - c) uskutočňuje pravidelné monitorovanie chrbticovej siete
 - d) zabezpečuje prevádzku centrálnych serverov
 - e) poskytuje odborné konzultácie vedeniu školy
 - f) sleduje vývojové trendy v oblasti dátových sietí a navrhuje spôsob ich implementácie do siete STUNET
 - g) organizuje zavádzanie nových sieťových služieb
 - h) poskytuje odborné konzultácie správcom podriadených sietí
 - i) riadi a správu doménového priestoru stuba.sk
 - j) usmerňuje a konzultuje podmienky registrácie domén prvej úrovne **xxx.sk** pre prevádzku v sieti STUNET.

4. Správca siete na všetkých úrovniach najmä:
 - a) zabezpečuje prevádzku siete, servera alebo sieťovej aplikácie
 - b) kontroluje dodržiavanie pravidiel prevádzky siete
 - c) monitoruje prevádzku siete a rieši prípadné kolízie
 - d) zálohuje a archivuje dáta na spravovaných zariadeniach

5.5 Používanie dátovej siete STUNET

1. Používateľ môže používať výpočtové prostriedky a dátovú sieť STUNET výlučne pre vedecké, výskumné, vzdelávacie, vývojové a umelecké účely, alebo úlohy súvisiace s prevádzkou, riadením a správou STU. Za porušenie pravidiel sa považuje najmä použitie siete pre komerčnú činnosť nesúvisiacu s činnosťou STU, ďalšie šírenie obchodných a reklamných informácií, politickú, náboženskú alebo rasovú agitáciu, propagáciu násilia, drog a šírenia takých materiálov, ktoré sú v rozpore so zákonom.
2. Používateľ má právo používať výlučne legálne nadobudnuté programové vybavenie. Kopírovať programy je možné pri dodržaní platných autorských zákonov. Voľne dostupné programové produkty a informačné materiály, získané s pomocou dátovej siete STUNET smie používateľ používať výlučne pre účely uvedené v odst. 1. Za

hrubé porušenie pravidiel je považované použitie dátovej siete STUNET na ponuku nelegálne získaného programového vybavenia, informačných materiálov, umeleckých alebo literárnych diel a dát.

3. Používateľ nesmie zasahovať do žiadnych programových produktov, dát, systémového a technického prostredia dátovej siete STUNET bez výlučného súhlasu správcu siete. Zvlášť prísne zakázané sú neautorizované zmeny konfigurácie počítačov alebo iných prostriedkov, ktoré by mohli mať vplyv na správnu prevádzku dátovej siete STUNET. Študenti ako používatelia dátovej siete nie sú oprávnení inštalovať akékoľvek programy v dátovej sieti bez výslovného súhlasu správcu siete.
4. Používateľ má právo používať vyčlenený diskový priestor, výpočtové prostriedky a dátovú sieť STUNET len pri zohľadnení jej celkového zaťaženia. Používateľ nesmie vedome narušiť činnosť výpočtových prostriedkov, obmedziť prácu ďalších používateľov, ani chod a výkonnosť siete. Musí bezodkladne vykonať pokyny správcu dátovej siete na zníženie záťaže, ktorú generuje do siete.
5. Veľkosť posielanej elektronickej pošty a konferencií môže byť v dátovej sieti STUNET obmedzená. Konkrétny limit veľkosti elektronickej pošty je stanovený technickým vybavením siete a určuje ho správca siete STUNET. Pri prekročení používateľského limitu využívaného diskového priestoru môže dôjsť k automatickému zablokovaniu príjmu pošty pre konkrétneho používateľa.
6. STU nezodpovedá za stratu používateľských dát a obsahu informácií, ktorá vznikla akýmkoľvek spôsobom v sieti STUNET. Za vytváranie záložných kópií používateľských programov a informačných dát zodpovedajú používatelia sami.
7. Používateľ nesmie ďalej používať počítač, ktorý je napadnutý vírusom a informoval ho o tom antivírusový program alebo iný používateľ. Je povinný okamžite vykonať kroky na jeho odvírenie, resp. zničenie škodlivých programov alebo odpojenie zo siete do príchodu správcu siete alebo ním povereného technika siete STUNET.
8. Slovenská technická univerzita je členom Združenia slovenskej akademickej dátovej siete SANET a sieť STUNET je priamo pripojená do tejto siete, preto všetci používatelia siete STUNET sú povinní dodržiavať a „Všeobecné pravidlá používanie siete SANET“.

5.6 Pravidlá pre pripojenie k dátovej sieti STUNET

1. Používateľ dátovej siete STUNET je povinný požiadať o súhlas správcu lokálnej siete fakulty a súčasti STU siete:
 - a) pred pripojením každého nového zariadenia na dátovú sieť
 - b) pred zmenou konfigurácie zariadenia, ktorá by mohla mať vplyv na bezporuchovú prevádzku siete
 - c) pred trvalým odpojením zariadenia od dátovej siete
2. Správca siete STUNET zaregistruje prípojné zariadenia podľa pravidiel správy dátovej siete STUNET v Bratislave a prideli pripojenému zariadeniu IP adresu.
3. Za správnu inštaláciu operačného systému a sieťového programového vybavenia počítačov, pripojených k dátovej sieti STUNET zodpovedá poverený zamestnanec, určený správcom siete alebo používateľ pokiaľ mu správca siete povolil inštalovať operačný systém samostatne.
4. Pri samostatnej správe operačného systému a sieťového programového vybavenia počítača pripojeného do dátovej siete musí používateľ dodržiavať príslušné pokyny správcu siete na príslušnej úrovni.

5. Používateľ nesmie používať pre pripojenie k dátovej sieti inú sieťovú adresu než mu bola pridelená (automatické alebo statické pridelenie adresy).

6. Pravidlá na používanie prostriedkov IT

6.1 Používanie hardvéru

1. Na pracoviskách STU sa používa iba taký hardvér, ktorý je schválený príslušnými vedúcimi VS súčasti STU, riaditeľom CVT STU a je evidovaný v evidencii majetku na oddelení správy majetku súčasti 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 VS súčasti STU alebo CVT 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, oddelenie správy majetku súčasti STU a to formou požiadavkového listu.
5. Používatelia IT, ktorým boli zverené či zapožičané prenosné notebooky, či akékoľvek iné 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 kľúči)
6. Poruchu hardvéru treba nahlásiť príslušnému VS súčasti STU, alebo CVT STU formou požiadavkového listu, ktorý tvorí prílohu tejto smernice, prípadne vnútornou poštou alebo e-mailom. Zamestnanci VS súčasti STU sa okamžite, prípadne podľa dohody postarajú o odstránenie, nápravu, opravu či výmenu.

6.2 Používanie softvéru

1. Pri práci s PC je zakázané pracovať s iným softvérom, než aký bol nainštalovaný, resp. schválený VS 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 VS súčasti STU alebo zamestnanci dodávateľskej firmy za prítomnosti zamestnanca príslušného VS súčasti STU a oddelenie správy majetku má povinnosť tento softvér zaevidovať.
5. Poruchu softvéru treba nahlásiť príslušnému VS súčasti STU formou požiadavkového listu, ktorý tvorí prílohu tejto smernice, prípadne vnútornou poštou alebo e-mailom.

Pracovníci VS súčasť 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.
7. Na inštalovanom hardvérovom vybavení STU je nevyhnutné dôsledne pravidelne kontrolovať aktuálnosť a platnosť inštalovaných opráv (patch) odporúčaných výrobcom a v prípade ich neaktuálnosti požadovať ich aktualizáciu.

6.3 Používanie Internetu, intranetu a elektronickej pošty

1. Pre zaistenie bezpečnosti a kontinuity prevádzky IS a siete STUNET, ako aj v prípade požiadavky na súčinnosť orgánom činným v trestnom konaní, má STU právo na prístup k záznamom elektronickej pošty a právo preveriť oprávnenosť prístupu zamestnanca a študenta do IS a do siete STUNET .
2. Zobrazenie, archivovanie, uchovávanie, rozširovanie, spracovávanie alebo zaznamenávanie akéhokoľvek obrázku, či dokumentu s jednoznačným sexuálnym obsahom v ktoromkoľvek počítačovom systéme STU sa zakazuje.
3. Prístup na Internet a elektronickejšť poštu sa nesmú vedome použiť na porušenie zákonov, predpisov a legislatívy SR, či iných štátov.
4. Akýkoľvek softvér alebo súbory, dokumenty, získané prostredníctvom Internetu a uložené na počítači lokálnej siete súčasť STU, sa môžu používať výhradne len spôsobom, ktorý je v súlade s ich licenciami, autorskými právami, po odsúhlasení zamestnancami VS súčasť STU a musia priamo súvisieť s pracovnými povinnosťami používateľa IT.
5. 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.
6. Používateľom Internetu a elektronickej pošty v STU sa zakazuje využívať svetovú počítačovú sieť Internet a elektronickejšť poštu na zámerné rozširovanie akýchkoľvek vírusov, červíkov, trójskych koňov alebo iného škodlivého softvéru. Takisto používateľ nesmie využiť či zneužiť prístup na Internet či elektronickejšť poštu na vyradenie, preťaženie alebo oklamanie akéhokoľvek počítačového systému alebo počítačovej siete a tým narušiť súkromie alebo bezpečnosť iného používateľa či spoločnosti.
7. 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.
8. Hovoriť, písať a prispievať v mene STU, alebo jej súčasť 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 súčasť. 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.

9. Používatelia Internetu a elektronickej pošty môžu využívať prístup na Internet a elektronickejšiu 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.
10. STU je povinná poskytnúť orgánom činným v trestnom konaní všetky dostupné záznamy, týkajúce sa prístupu na Internet a elektronickejšiu poštu príslušného používateľa Internetu a elektronickej pošty podľa príslušných zákonných ustanovení.
11. 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.
12. Komerčné používanie Internetu na podporu vedľajšej podnikateľskej činnosti zamestnanca STU alebo jej súčasť 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.

6.4 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 „**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.
4. Všetky zariadenia slúžiace na zber, archivovanie a posielanie citlivých informácií informačného systému sa musia využívať v súlade s pridelenými oprávneniami na základe tejto **Prevádzkovej bezpečnostnej smernice informačného systému STU**. Toto ustanovenie zahŕňa aj dodržiavanie povinností informovať administrátora IT a správcu lokálnej siete súčasť STU o prípadných zmenách o pôvodne zastavených funkcionalít zariadení IKT o bezpečnostných incidentoch.
5. Rektor, dekaní fakúlt, a ostatní vedúci zamestnanci súčasť 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 súčasť STU.
6. Vedúci zamestnanci fakúlt a ostatných súčasť 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,

6.5 Kamerané systémy

1. STU má právo používať na monitorovanie svojich vnútorných priestorov a na prístupových komunikáciách kamerové systémy, z dôvodov zabezpečenia ochrany majetku a osôb.
2. Na všetkých priestoroch, ktoré sú monitorované kamerovým systémom musí byť označenie na viditeľnom mieste „Priestor je monitorovaný kamerovým systémom“.
3. Záznamy sa aktuálne zapisujú na pamäťové médium a v lehote 15 dní musia byť z archívu priebežne mazané.
4. Prístup k archívnym záznamom a tiež k on-line monitoru majú len poverené osoby s osobitným zreteľom.
5. Kamerové systémy nesmú byť použité na monitorovanie osôb pri pracovnej činnosti, príchodu a odchodu do práce ako aj pri ostatných bežných činnostiach na pracovisku.

7. Pravidlá na tvorbu prístupových hesiel

7.1 Heslo administrátora

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 CVT STU.

7.2 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.

7.3 Heslá ostatných používateľov

VS súčasť STU a CVT 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.

7.4 Pridelovanie adries elektronickej pošty

1. Adresy elektronickej pošty v tvare meno.priezvisko@stuba.sk a prístupové heslá zamestnancov pridáva pri nástupe do zamestnania pracovník personálneho oddelenia súčasť STU.
2. Pri ukončení pracovného pomeru sa adresa elektronickej pošty a prístupové heslo zamestnanca zablokuje po uplynutí 180 dní.
3. Študentom I. ročníka pri zápise odovzdá automaticky vygenerovanú adresu **xxxxxx@stuba.sk** elektronickej pošty a prístupové heslo zamestnanec študijného oddelenia dekanátu príslušnej fakulty.
4. Pri prerušení alebo ukončení štúdia sa adresa elektronickej pošty a prístupové heslo zablokuje po uplynutí 180 dní.
5. Pri novom nástupe po prerušení štúdia študent požiada o znovu pridelenie adresy elektronickej pošty a prístupového hesla študijné oddelenie príslušnej fakulty.
6. Pri strate prístupového hesla môže študent požiadať o jeho vydanie zamestnanca študijného oddelenia fakulty.

7.5 Pridelovanie prístupových hesiel do Informačného systému

1. Prístupové heslá do EIS Magion pridávajú správcovia jednotlivých modulov na základe písomnej žiadosti príslušného nadriadeného vedúceho zamestnanca rektorátu, fakúlt a súčastí STU, zamestnanca pre ktorého sa vytvára prístup do EIS. Zoznam správcov EIS je v prílohe tejto smernice.
2. Pridelené heslo slúži na prvotné prihlásenie a po aktivovaní prístupu je používateľ na výzvu systému povinný si heslo zmeniť na základe previdiel uvedených v čl. 6.2.
3. Po ukončení pracovného pomeru sa heslo automaticky zmaže.
4. Prístup k jednotlivým modulom EIS Magion je možný len zo siete STUNET, alebo cez VPN STUNET.

5. Prístupové heslá do AIS pridelujú integrátori systému, personálne, a pedagogické oddelenie na fakultách a správca systému CVT STU. Pridelené heslo súži aj na prístup do elektronickej pošty, stravovacieho systému KREDIT, do knižničného systému ARL. Platnosť hesla overujú tieto systémy prostredníctvom služby LDAP. Zoznam integrátorov AIS je v prílohe tejto smernice.
6. Po ukončení pracovného pomeru alebo štúdia je prístup do informačného systému AIS možný cez ID použítľa nepretržite s obmedzenými funkcionalitami.
7. Pre zaručenie vyššej úrovne bezpečnosti prístupu a ochrany dát v AIS majú učitelia a doktoranti prístup k „Zápisníku učiteľa a výskumníka“ cez ďalší stupeň autentifikácie a to prostredníctvom „Preukazu zamestnanca“ s čipom, ku ktorému je pridelené heslo certifikačnou autoritou STU (pozri [Smernica rektora č. 3/2016-SR Zvýšenie bezpečnosti AIS STU](#) a [Certifikačný poriadok IS STU Bratislava CA 1.0.](#))
8. Prístup do dochádzkového systému (EDS) prideluje správca systému. Prihlasovacím menom je osobné číslo zamestnanca, prvotné heslo je rovnaké, systém po prihlásení žiada heslo zmeniť. Systém umožňuje nastaviť aj vyššiu úroveň prístupu umožňujúcu prezerat' a prípadne aj editovat' dochádzku podriadených zamestnancov. Toto právo prideluje na základe žiadosti nadriadeného zamestnanca správca EDS. Zoznam správcov je v prílohe tejto smernice.

7.6 Pridelovanie hesiel pre vzdialený VPN prístup do WIFI siete

1. Heslá sú vytvárané aplikačne v príslušnej používateľskej sekcii v informačnom systéme AIS.
2. Heslá nie sú zhodné s heslami na prístup do informačných systémov.
3. Po ukončení pracovného pomeru alebo štúdia sa heslo automaticky zablokuje.

8. 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 prostredníctvom priameho pripojenia nastavovacieho zariadenia (terminálu) na komunikačné rozhranie (port) aktívneho prvku vyhradeného výhradne pre tento účel, alebo vzdialene cez zabezpečenú managovaciu sieť do ktorej je možný prístup z internetu len prostredníctvom VPN tunela.
3. Každá zmena v nastavení aktívneho prvku chrbticovej siete STU a fakúlt musí byť evidovaná.
4. Zoznam oprávnených osôb pre prístup k aktívnym prvkom komunikačnej Infraštruktúry je v prílohe tejto smernice.

9. Disciplinárny postih študentov za porušenie pravidiel prevádzky dátovej siete STUNET

1. Porušenie pravidiel prevádzky dátovej siete STUNET je považované za porušenie vnútorných predpisov STU a rieši sa disciplinárnym konaním v zmysle čl. 2 Disciplinárneho poriadku STU.
2. Podľa čl. 3 citovaného Disciplinárneho poriadku je možné študentovi uložiť trest podmieneného vylúčenia zo štúdia a za zvlášť vážne porušenie pravidiel môže byť študent až vylúčený zo štúdia.
3. Pri závažnejších porušeníach alebo opakovanom menej závažnom opakovanom porušení pravidiel môže správca alebo ním poverená osoba vziať študentovi na vopred stanovenú dobu (max. 2 mesiace) oprávnenie voľného používania služieb dátovej siete okrem organizovanej výučby. Študent má v takomto prípade právo odvolať sa k dekanovi alebo vedúcemu zamestnancovi súčasti STU. Toto odvolanie nemá odkladný účinok.
4. Pri opakovanom alebo zvlášť závažnom porušení pravidiel sa bude postupovať takto:
 - a/ dňom zistenia porušenia pravidiel prevádzky dátovej siete stráca študent právo používať služby dátovej siete.
 - b/ celý prípad porušenia pravidiel spolu s dokumentáciou je odovzdaný disciplinárnej komisii príslušnej fakulty STU.
 - c/ Na základe rokovania disciplinárnej komisie dekan príslušnej fakulty rozhodne o uložení trestu. Trestom môže byť tiež znemožnenie služieb dátovej siete STUNET na stanovenú dobu alebo finančná pokuta. Prípadná trestno-právna zodpovednosť pri porušení pravidiel nie je týmto postupom obmedzená ani vylúčená.
5. Pri závažnom porušení pravidiel napr. nedovoleným získavaním alebo poskytovaním informačných zdrojov z Internetu má správca právo odpojiť celú sieť alebo jej časť na 24 hodín na vykonanie opatrení. Pri opakovanom takomto porušení pravidiel sa celý prípad rieši disciplinárnym postihom.

10. Disciplinárny postih zamestnancov za porušenie pravidiel prevádzky dátovej siete STUNET

1. Porušenie ustanovení tohto usmernenia bude u zamestnancov STU považované za porušenie základných povinností zamestnanca v zmysle čl. 5 Pracovného poriadku STU v súlade s príslušnými ustanoveniami Zákonníka práce, a je možné z neho vyvodit' príslušné pracovno-právne dôsledky vrátane rozviazania pracovného pomeru.
2. Pri zistení porušenia pravidiel prevádzky dátovej siete STUNET, správca siete alebo ním poverená osoba upozorní zamestnanca, ktorý pravidlá porušil na túto skutočnosť. V prípade hrubého porušenia upozorní na porušenie pravidiel príslušného vedúceho zamestnanca súčasti STU.
3. Pri opakovanom porušení pravidiel sa bude postupovať takto:
 - a) Dňom zistenia porušenia pravidiel stráca zamestnanec právo používania služieb dátovej siete STUNET.
 - b) Celý prípad aj s dokumentáciou je odovzdaný dekanovi príslušnej fakulty STU alebo rektorovi STU v prípade ďalších súčastí STU a ten rozhodne o pracovno-

právnom opatrení alebo finančnej pokute. Prípadná trestno-právna zodpovednosť nie je týmto postupom obmedzená ani vylúčená.

11. Ochrana súkromia a zverejňovanie informácií

1. Pre používanie elektronickej pošty a elektronických konferencií platia rovnaké pravidlá, ako pre užívanie bežnej pošty, pričom elektronická poštová správa má charakter otvorenej listovej zásielky..
2. Používateľ je povinný dbať na to, aby jeho elektronická pošta bola presne adresovaná a nedochádzalo k nežiadúcemu obťažovaniu ostatných používateľov rozposielaním reťazových listov, alebo listov adresovaných na generátore adres, ktoré sú zhromaždené bez súhlasu adresáta.
3. Používateľ je povinný pri odoslaní elektronickej pošty používať pridelené používateľské meno (meno poštovej schránky). Za hrubé porušenie pravidiel je považované odosielanie listov s falošnou identitou s cieľom zavraždenia, získania neoprávnených informácií alebo podvodu.
4. Prijem elektronickej pošty z adres, ktoré porušujú vyššie uvedené tri ustanovenia 1. – 3. tohto článku môže byť zablokovaný.
5. Pri posielaní dokumentov s osobnými údajmi elektronickou poštou musí byť dokument pred odoslaním zašifrovaný („zaheslovaný“). Táto skutočnosť musí byť príjemcovi správy elektronickej pošty oznámená spolu s informáciou o získaní šifrovacieho kľúča („hesla“). Šifrovanie realizovať alebo natívnymi funkciami textových editorov (PDF alebo MS Office) alebo kompresným programom so šifrovaním (napr. 7-Zip). Ak sa na šifrovanie použije kompresný program so šifrovaním s voľbou šifrovacieho algoritmu, potom musí byť v správe pre príjemcu uvedený aj šifrovací algoritmus.
6. Pri posielaní správy študentom STU správu poslať na adresu elektronickej pošty, ktorú študentovi prideliť STU, a ako šifrovací kľúč („heslo“) použiť rodné číslo študenta bez lomky.
7. Pri posielaní správy iným osobám správu poslať na nimi uvedenú adresu elektronickej pošty, zvolený šifrovací kľúč („heslo“) poslať príjemcovi pošty iným kanálom (napr. správou SMS na mobil). Šifrovací kľúč („heslo“) musí mať aspoň desať znakov vrátane veľkého a malého písmena, špeciálny znak a číslicu. Nesmie obsahovať slová zo slovníka. Ak príjemca správy elektronickej pošty nedisponuje alternatívnym kanálom, potom sa za šifrovací kľúč („heslo“) zvolí dôverná informácia, ktorá je známa iba odosielateľovi a príjemcovi správy, napríklad číslo pasu, rodné číslo, atď. Krajným a bezpečnostne najhorším riešením je poslať šifrovací kľúč („heslo“) v následnej správe elektronickej pošty.
8. Používateľ nesie plnú právnu zodpovednosť za obsah vlastných verejne dostupných www stránok, iných informačných zdrojov, najmä však za prípadné porušenie autorského zákona pri kopírovaní a rozširovaní cudzích programov, informačných materiálov, umeleckých alebo literárnych diel a dát.
9. Súbor v používateľských adresároch a systémových stránkach elektronickej pošty sú súkromnými dátami ich vlastníkov. Používatelia majú nárok na ochranu súkromia, a to aj v prípade, keď svoje adresáre nechránia zvláštnou ochranou. Za hrubé porušenie pravidiel je považované vytváranie kópií cudzích dát, informačných materiálov a odposluch prevádzky na dátovej sieti STUNET s cieľom získania obsahu správ, alebo iných informácií.

10. Správca dátovej siete STUNET je oprávnený zamedziť prístup do súborov, ktoré by mohli byť využívané v rozpore s účelom uvedeným v čl. 4.2, prípadne ktoré ohrozujú bezpečnosť systému a dátovej siete (nebezpečné programy, vírusy, nástroje na odpočúvanie prevádzky, nástroje na odpočúvanie mena a hesla a pod.) a ich používateľ je povinný na vyzvanie správcu siete tieto programy bezodkladne odstrániť.
11. STU nezodpovedá za prípadné zneužitie dát pri prenose a uchovávaní informácií v dátovej sieti STUNET.
12. Správca dátovej siete STUNET má právo vykonávať všetky úkony nevyhnutné k výkonu svojej funkcie, vrátane prípadnej kontroly prenášaných dát a monitorovania činnosti používateľa v sieti. Pokiaľ používateľ používa pre utajenie informácií šifrovanie, je povinný v prípade pochybnosti o účele použitia v zmysle čl. III. odst 1 sprístupniť správcovi siete obsah dát.
13. Pre zabezpečenie ochrany súkromia v zmysle ustanovení Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a voľnom pohybe takýchto údajov (GDPR) a zákona č.18/2018 o ochrane osobných údajov platia „Podmienky ochrany súkromia“ zverejnené na www.stuba.sk. Tento dokument obsahuje a podrobný popis všetkých účelov spracovania a zverejňovania osobných údajov.
14. Pre zabezpečenia podmienky práva na prístup k osobným údajom podľa článku 15 GDPR je zriadené webové sídlo <https://is.stuba.sk/>. Z tohto sídla môžu študenti a doktorandi zistiť aké osobné údaje sa o nich spracovávajú a zverejňujú na základe oprávnených alebo verejných záujmov, podľa čl. 6 ods. 1 písm. e a f GDPR, vrátane tých, ku ktorým dali súhlas. Súhlas môžu kedykoľvek odvolať.
15. Na vyššie uvedenom webovom sídle <https://is.stuba.sk/> je odkaz na personálny portál zamestnanca, kde zamestnanec môže vidieť aké osobné údaje sa spracovávajú a zverejňujú, prípadne môže požiadať ich opravu podľa čl. 16 GDPR. Opravu je možné u študenta riešiť cez študijné oddelenie a u zamestnanca cez personálny útvar formou dodatkového vyhlásenia, alebo AIS si študent a zamestnanec môžu opraviť osobné údaje aj sami prostredníctvom svojho autorizovaného prístupu na portál AIS.

12. Účtovateľnosť a auditné záznamy

1. Cieľom účtovateľnosti a vytvárania auditných záznamov je záznam činností používateľov a zmien dôležitých údajov, detekcia, prevencia a potlačanie 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 vyšetrenie 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, riaditeľa CVT STU a bezpečnostného manažéra STU 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.

13. 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:
 - a) Dátum, čas začiatku a ukončenia činnosti.
 - b) Označenie zodpovedajúceho záznamového média – napr. mg. pásky DAT, CD ROM, CD RW, DWD alebo adresy diskového poľa.
 - c) U pásek pre kontinuálne zálohovanie logických protokolov čísla protokolov uložených na páske.
 - d) U pásek s operatívnu a bezpečnostnou zálohou databázy číslo logického protokolu, ktoré patrí k danej páske.
 - e) U pásek s operatívnu a bezpečnostnou zálohou binárnych súborov operačného systému a vykonateľných súborov aplikácie označenie diskových priestorov zálohovaných na páske.
 - f) Miesto uloženia archívnej pásky.
 - g) Problémy, chyby a poznámky o priebehu zálohy.
 - h) Podpis zamestnanca.
3. 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).
4. Protipožiarny trezor musí byť umiestnený v dosahu zamestnanca vykonávajúceho zálohy, protipožiarny trezor musí byť umiestnený bezpečnom priestore chránenom elektronickým zabezpečovacím zariadením.
5. Operatívna záloha
Zálohovanie databáz databázového servera Oracle:
 - a) 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**.
 - b) 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.

- c) Takýmto spôsobom sú vykonávané aj zálohy databáz systému EIS MAGION, AIS (Akademický informačný systém), ARL (Knížničný informačný systém), Ubytovací systém študentov na ŠD, Stravovací systém Kredit pred a po uzávierke mesiaca, tie sú následne uložené na DVD médium alebo na diskové pole.
- d) 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.

13.1 Bezpečnostná záloha

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:
 - a) 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.
 - b) Po vykonaní zálohy je potrebné vykonať kontrolu záznamu o priebehu archivácie alebo spustiť kontrolu čitateľnosti archívnej pásky príkazom **dd**.
 - c) Pre bezpečnostné zálohy sú používané 4 sady archívnych pásek, ktoré sa cyklicky menia
3. Zálohovanie verzií aplikácií pri prechode na nové verzie aplikácie
 - a) Záloha verzií aplikácií pri prechode na novú verziu aplikácie sa vykoná na CD ROM, CD RW alebo DWD médiá spravidla na klientské rozhranie.

13.2 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 médiá (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).

13.3 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 záložného 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.

14. Klasifikácia, označovanie a manipulácia s dokumentami

1. Klasifikácia a označovanie dokumentov obsahujúcich citlivé informácie označované ako dôverné v papierovej aj v elektronickej forme a dokumentov s informáciami pre internú potrebu, ktoré sú zhromažďované, spracovávané a archivované na pracoviskách STU je určená vnútornými predpismi vydanými rektorom STU – **Smernicou rektora „Klasifikácia aktív a informácií informačného systému STU“**, **„Registratúrnym poriadkom STU a „Smernicou na ochranu osobných údajov STU“**.
2. Ostatné dokumenty, ktoré nespádajú do vyššie uvedených kategórií sú dokumenty verejne prístupné, ktoré nemajú charakter citlivých informácií a je možné ich ľubovoľne zverejňovať, kopírovať a šíriť.

15. 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 §79 zákona č. 15/2018 Z.z. O ochrane osobných údajov.

2. Rovnaká povinnosť sa týka aj dodávky technických a sieťových zariadení a komponentov. Pri pridelovaní 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“.

16. 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.

17. 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.

18. Prílohy

18.1 Zoznam správcov modulov IS na pracovisku UIS CVT STU

Kontakt: https://www.stuba.sk/sk/pracoviska/centrum-vypoctovej-techniky/cinnosti-a-sluzby/prevadzkovanie-informacneho-systemu.html?page_id=1598

18.2 Zoznam integrátorov AIS na fakultách

Kontakt: <https://is.stuba.sk/dok/integratori.pl>

18.3 Zoznam správcov siete STUNET

Aktuálny zoznam správcov siete STUNET je zverejnený na web stránke:

https://www.stuba.sk/sk/pracoviska/centrum-vypoctovej-techniky/cinnosti-a-sluzby/zoznam-spravcov-siete-stunet.html?page_id=12742

18.4 Helpdesk CVT STU

Helpdesk je centralizované kontaktné miesto Centra výpočtovej techniky STU, kde môžu koncoví používatelia získať technickú podporu, klásť otázky alebo nahlasovať požiadavky a problémy týkajúce sa výpočtovej techniky, informačných systémov, služieb alebo IKT infraštruktúry v správe CVT.

Cieľom helpdesku je poskytovať rýchlu a efektívnu pomoc používateľom, a súčasne centrálnu spravovať a dokumentovať požiadavky a ich riešenia.

Požiadavky alebo problémy sa zaznamenávajú ako tikety, ktoré obsahujú relevantné podrobnosti, ako opis problému, úroveň priority a aktuálny stav riešenia. Tiket (ďalej tiež ako Požiadavka) v sebe obsahuje vlákno správ medzi koncovým používateľom a špecialistom technickej podpory.

Helpdesk je dostupný ako webová aplikácia na adrese <https://helpdesk.stuba.sk>, cez ktorú môžete zadať novú požiadavku (tiket) aj bez prihlásenia sa.

Druhý spôsob práce s helpdeskom je jednoduché odoslanie e-mailu s požiadavkou na adresu helpdesk@stuba.sk, čo rovnako vytvorí tiket a používateľské konto, ak ešte neexistuje.

Manuál k Helpdesku nájdete na web stránke: https://www.stuba.sk/sk/pracoviska/centrum-vypoctovej-techniky/navody/helpdesk-stu-pouzivatelsky-manual.html?page_id=16454.

V Bratislave dňa : 1.2.2024



Ing. Marian Ďurkovič
riaditeľ CVT STU