S T U

Kolégium rektora
10.04.2019

Návrh smernice rektora
Prevádzková bezpečnostná smernica informačného systému Slovenskej technickej univerzity v Bratislave

Predkladá: **prof. Ing. Miroslav Fikar, DrSc**.
rektor STU

Vypracoval: **prof. Ing. Pavol Horváth, PhD**.
Centrum výpočtovej techniky STU
v spolupráci
s **JUDr. Marcelom Michaličkom**
Právny a organizačný útvar
a
s **doc. Ing. Ladislavom Hudecom, PhD.**
zodpovedná osoba STU

Zdôvodnenie: Zabezpečenie bezpečnosti správy a prevádzky informačného systému STU.

Návrh uznesenia: Kolégium rektora schvaľuje predložený materiál „Prevádzková bezpečnostná smernica informačného systému Slovenskej technickej univerzity v Bratislave “.

a) bez pripomienok,
b) s pripomienkami

Smernica rektora
číslo: xx/2019 – SR

Prevádzková bezpečnostná smernica informačného systému Slovenskej technickej univerzity v Bratislave

Dátum: DD.MM.2019

Slovenská technická univerzita v Bratislave, Vazovova 5, Bratislava

V Bratislave DD.MM. 2019
Číslo: xx/2019-SR

Rektor Slovenskej technickej univerzity v Bratislave v súlade s článkom 3 bod 1 písm. b) Smernice rektora číslo 4/2013 - SR „Pravidlá vydávania interných predpisov Slovenskej technickej univerzity v Bratislave“ zo dňa 03. 10. 2013

v y d á v a

nasledovnú smernicu rektora

Prevádzková bezpečnostná smernica informačného systému
Slovenskej technickej univerzity v Bratislave

Článok I.
Úvodné ustanovenia

1) Smernica rektora „Prevádzková bezpečnostná smernica informačného systému Slovenskej technickej univerzity v Bratislave“ (ďalej len „smernica“) je vnútorná organizačná a riadiaca norma Slovenskej technickej univerzity v Bratislave (ďalej len „STU“) vydaná rektorom, ktorá upravuje zabezpečenie bezpečnosti správy a prevádzky informačného systému STU.

2) Centrum výpočtovej techniky STU, (ďalej len „CVT STU“) ako pracovisko priamo riadené rektorom, zabezpečí plnenie povinností podľa tejto smernice v rozsahu uvedenom v článku II. tejto smernice na Rektoráte a centrálne financovaných súčastiach STU.

3) Dekani fakúlt STU zabezpečia plnenie povinností podľa tejto smernice v rozsahu uvedenom v článku II. tejto smernice prostredníctvom nimi priamo riadeného Výpočtového strediska.

4) Vedúci na všetkých stupňoch riadenia STU zabezpečia plnenie povinností podľa tejto smernice v rozsahu uvedenom v článku III. tejto smernice.

Článok II.

1) Špecifikácia povinností vedúcich zamestnancov STU v oblasti bezpečnosti správy a prevádzky IT:
    a) správa registra IP adries siete STUNET, pridelených fakulte STU alebo inej

súčasti STU,

b) autorizácia prístupu do lokálnej časti siete STUNET na fakulte (SW a personálne zabezpečenie), vrátane prideľovania adries elektronickej pošty,
c) prvotné prideľovanie prístupových hesiel do jednotlivých modulov informačného systému,
d) autorizácia prístupu do WIFI siete fakulty a do EDUROAM,
e) zabezpečenie inštalácie, prevádzky a údržby pracovných staníc, pripojených do lokálnej časti siete STUNET na fakulte,
f) zabezpečenie kontroly používania licencií SW produktov, inštalovaných v pracovných staniciach,
g) zabezpečenie bezpečnosti a ochrany prístupu do pracovných staníc, vrátane ochrany proti škodlivému SW,
h) identifikácia, riešenie a nahlasovanie sieťových incidentov, vrátane neoprávneného použitia hesiel.

2) Správcovia siete bez ohľadu na postavenie v hierarchii siete sú povinní zabezpečovať bezpečnosť prevádzky dátovej siete STUNET.
3) Správca siete STUNET je povinný upozorniť bezodkladne správcu lokálnej časti siete STUNET na fakulte na zistené bezpečnostné incidenty a tieto incidenty zdokumentovať.
4) Správca siete je povinný upozorniť ostatných správcov siete STUNET na zistené nedostatky v zabezpečení siete STUNET.
5) Správca má právo kontrolovať dáta používateľov a monitorovať ich činnosť v sieti a to buď náhodne, alebo cielene v prípadoch vzniku podozrenia na porušenie pravidiel prevádzky dátovej siete STUNET. Pri tejto činnosti je správca siete povinný zachovávať mlčanlivosť o informáciách ktoré získa, pokiaľ nezistí porušenie pravidiel prevádzky dátovej siete.

Článok III.

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 informačného systému 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, ktorý heslo vydal, 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 je zamestnanec povinný vyplniť požiadavkový list (vzor tlačiva je v prílohe metodického usmernenia), potvrdený priamym nadriadeným používateľa, vedúcim zamestnancom súčasti alebo pracoviska STU, ktorý ho predloží VS súčasti STU, alebo CVT STU. Pri akejkoľvek zmene (prístupové oprávnenia, zrušenie prístupu, skončenie pracovného pomeru a pod.) je povinný nadriadený používateľa IT predložiť nové tlačivo zo zmenou a odovzdať ho VS súčasti STU, alebo CVT STU.
6) V záujme zachovania bezpečnosti svojich počítačov, počítačových sietí a softvérového vybavenia má STU nainštalované rôzne programy (firewall, 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.
   Súbory, ktoré obsahujú dôverné údaje v zmysle smernice rektora Klasifikácia aktív a informácií informačného systému STU a Metodického usmernenie na vykonanie ustanovení tejto smernice, musia byť pri akomkoľvek prenose prostredníctvom Internetu zašifrované. V tomto smere bude používateľovi IT nápomocný zamestnanec VS súčasti STU, alebo CVT STU.
7) 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 VS súčasti STU, alebo CVT 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 pracovisko CVT STU.
8) 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.
9) 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 (pevné disky, dátové pásky, WORM média a pod.).
10) Ak je poškodený pevný disk, CD/DVD mechanika 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.
11) 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.

12) CVT STU zabezpečí inštaláciu, prevádzku a priebežnú aktualizáciu antivírusového systému, prístupného pomocou automatickej inštalácie a aktualizácie prostredníctvom siete STU – STUNET všetkým PC, inštalovaným na STU.
13) 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 a systémovému administrátorov.
14) Dokumentáciu o všetkých bezpečnostných incidentoch, ktoré sa vyskytli na STU vedie na to poverené pracovisko CVT 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.

Článok IV.
Záverečné ustanovenia

1) Podrobnosti o zabezpečení bezpečnosti správy a prevádzky informačného systému STU budú upravené v metodickom usmernení.
2) Na vydanie metodického usmernenia na vykonanie tejto smernice splnomocňuje rektor riaditeľa CVT STU.
3) Akékoľvek zmeny a doplnenia tejto smernice sú možné len na základe číslovaných, rektorom podpísaných, dodatkov k smernici.
4) Táto smernica nadobúda platnosť dňom jej podpisu a účinnosť dňom ..... 2019.

prof. Ing. Miroslav Fikar, DrSc.
rektor