Smernica rektora Trnavskej univerzity v Trnave č. 8/2015 o pravidlách spravovania a používania počítačov v univerzitnej sieti

Dátum: 22. september 2015

Schválil: Kolégium rektora TU v Trnave

Podpis: .....

Čl. 1 Účel a rozsah pôsobnosti smernice

1) Trnavská univerzita v Trnave (ďalej len „TU“ alebo „univerzita“) má v súlade s § 29 Výnosu MF SR č.55/2014 Z.z. o štandardoch pre informačné systémy verejnej správy (ďalej len „výnos MF“) schválený strategický dokument Politika informačnej bezpečnosti TU, ktorý stanovuje ciele, hlavné úlohy a postupy pri riadení informačnej bezpečnosti. Univerzita ako povinná osoba v zmysle výnosu MF prijíma vnútorné predpisy, ktoré stanovujú konkrétne povinnosti zamestnancov a študentov v procesoch súvisiacich s informačnou bezpečnosťou.
2) TU má vybudovanú a centrálne spravovanú dátovú sieť. V každej univerzitnej budove existuje štruktúrovaný kabelážny systém (ďalej Len „ŠKS“), prostredníctvom ktorého sa pripájajú k univerzitnej sieti pracovné stolové počítače (ďalej len „PC“) zamestnancov, PC v učebniach a voľne dostupných priestoroch univerzity (študovňa Univerzitnej knižnice, PC miestnosti a chodby fakúlt TU).
3) Každý PC pridelený zamestnancovi TU je určený na vykonávanie pracovných činností v súlade s pracovnou náplňou daného zamestnanca. PC umiestnený v niektorej voľne dostupnej miestnosti univerzity je určený na vzdelávanie a štúdium. Všetky PC sú majetkom univerzity, ktorá je v súlade s ustanoveniami výnosu MF povinná stanoviť pravidlá ich prevádzky.
4) Účelom tejto smernice je v súlade s Politikou informačnej bezpečnosti TU stanoviť pravidlá pridelenia, inštalácie, spravovania, používania a likvidácie PC, ktoré sú súčasťou univerzitnej dátovej siete prostredníctvom pevného pripojenia v zásuvkách ŠKS.
5) Táto smernica sa vzťahuje na všetkých zamestnancov všetkých súčastí TU, ktorí využívajú služby univerzitnej dátovej siete.

Čl. 2 Pravidlá pridelenia PC zamestnancovi

1) Zamestnancovi univerzity, ktorý má v stanovenej náplni práce používanie PC, schvaľuje pridelenie PC manažér 2.stupňa (prorektor, kvestor, dekan, riaditeľ pracoviska) alebo 3.stupňa riadenia (tajomník fakulty alebo vedúci katedry). Uvedený manažér rozhodne, či sa zamestnancovi pridelí nový PC alebo PC, ktorý predtým používal iný zamestnanec.
2) Manažér 2. alebo 3.stupňa riadenia v súlade s § 41 písm. c) výnosu MF požiada administrátora systému na správu identít o zabezpečenie prístupu a špecifikáciu rolí pre používateľa PC do všetkých univerzitných informačných systémov (ďalej len „UIS“), v ktorých bude vykonávať činnosti v súlade s jeho pracovnou náplňou. Vyplnenú žiadosť, ktorá tvorí Prílohu č.1 tejto smernice – *Žiadosť o prístup k UIS*, zašle na e-mail: idm@truni.sk.
3) V prípade, že zamestnanec dostáva PC, ktorý predtým používal iný zamestnanec, príslušný manažér 2. alebo 3.stupňa riadenia rozhodne, či elektronické dokumenty predchádzajúceho používateľa budú archivované alebo vymazané. V prípade, že na PC boli uložené osobné údaje, je manažér 2. alebo 3. stupňa riadenia povinný zabezpečiť ich ďalšie spracúvanie v súlade so zákonom č.122/2013 Z.z. o ochrane osobných údajov a s bezpečnostnou smernicou TU na ochranu osobných údajov.
4) Nový PC pre zamestnanca zabezpečuje príslušná súčasť univerzity v súlade s podmienkami platnými pre verejné obstarávanie výpočtovej techniky univerzitou.

5) Hardvérové parametre PC musia byť v súlade s technickou špecifikáciou uvedenou v rámcovej zmluve s dodávateľom(mi) výpočtovej techniky pre univerzitu. Prípadné požiadavky na iné parametre PC podliehajú schváleniu hardvérového špecialistu CIS TU. Platí zásada, že technické parametre PC musia byť zvolené tak, aby bolo možné PC pripojiť do univerzitnej domény a nainštalovať na ňom softvér v súlade s Prílohou č.2 tejto smernice - *Inštalácia PC zaradeného v doméne TU* .

Čl. 3 Pravidlá inštalácie a spravovania PC

1) Pripojenie PC do univerzitnej siete, inštaláciu operačného systému a všetkých softvérových komponentov na PC potrebných pre vykonávanie pracovných činností používateľa PC vykoná odborný zamestnanec univerzity, ktorým je na fakulte informatik fakulty a na pracovisku univerzity poverený zamestnanec CIS TU.
2) Na PC zamestnanca, ktorý bude pripojený do dátovej siete TU, odborný zamestnanec nainštaluje iba taký softvér, ktorý:
    a) je uvedený v Prílohe č.2 tejto smernice, a ktorý využíva univerzita na základe platných licencií,
    b) je v súlade s licenčnými ustanoveniami zmluvy uzatvorenej medzi MŠVVaŠ SR a spoločnosťou Microsoft Slovakia s názvom *Campus and School – Enrollment for Education Solutions*,
    c) je v súlade s platnými licenciami udelenými pre danú súčasť univerzity,
    d) je v súlade s platnými licenciami udelenými pre daný PC alebo daného používateľa,
    e) je dostupný na voľné používanie a šírenie (Freeware),
    f) patrí do kategórie Open Source a je pokrytý GNU GPL (general public license) licenciou.
3) Odborný zamestnanec je povinný každý PC, ktorého používateľom je pedagóg alebo zamestnanec univerzity, alebo je určený pre študentov v učebniach alebo voľne dostupných priestoroch univerzity, zaradiť do univerzitnej domény a nastaviť na ňom jednotnú politiku pre správu a aktualizáciu PC v súlade s postupom schváleným GIB, ktorý je súčasťou Prílohy č.2 k tejto smernici.
4) V univerzitnej doméne je nastavená jednotná politika pre správu a aktualizáciu PC. Výnimky z jednotnej politiky pre používateľa PC môže odborný zamestnanec realizovať iba na základe žiadosti manažéra 2. alebo 3.stupňa riadenia, ktorej technická možnosť realizácie musí byť schválená hardvérovým špecialistom. O nezaradení PC používateľa do univerzitnej domény môže rozhodnúť iba GIB.
5) Ak je používateľ PC študent alebo zamestnanec pracujúci s UIS, ktorých centrálnu správu zabezpečujú správcovia CIS TU, odborný zamestnanec povolí na PC funkcionalitu zdieľania obrazovky. Túto funkcionalitu môžu použiť iba správcovia UIS pri servisných činnostiach, pričom na každé zdieľanie obrazovky musí dať súhlas používateľ PC.
6) Odborný zamestnanec je povinný zabezpečovať administrátorskú správu a aktualizáciu všetkých PC danej súčasti, ktoré sú zaradené v univerzitnej doméne a majú nastavenú jednotnú politiku pre správu a aktualizáciu PC, v súlade s predpismi vydanými GIB a pokynmi hardvérového špecialistu CIS TU.

7) Odborný zamestnanec je povinný zabezpečiť, aby na každom PC bol nainštalovaný antivírový softvér vykonávajúci pravidelné kontroly, ktorý je automatizovane aktualizovaný v súlade s pokynmi hardvérového špecialistu CIS TU.

8) Odborný zamestnanec odovzdá nainštalovaný PC používateľovi, ktorý prevzatie PC potvrdí na preberacom protokole. Preberací protokol archivuje oddelenie pre evidenciu a správu majetku rektorátu TU.

9) Pri odovzdaní nainštalovaného PC je odborný zamestnanec povinný poučiť používateľa PC o zásadách bezpečnej práce s PC v prostredí univerzitnej siete a v prostredí internetu. Zamestnanec preberajúci PC podpíše *Záznam z poučenia o zásadách bezpečnej práce s PC v prostredí univerzitnej siete a v prostredí internetu*, ktorý je súčasťou Prílohy č.3 k tejto smernici.

10) V prípade, ak používateľ PC nemá schválenú výnimku z pravidiel jednotnej politiky pre správu a aktualizáciu PC uvedenú v ods.4) tohto článku a napriek tomu nedodržuje uvedené pravidlá, odborný zamestnanec oznámi túto skutočnosť manažérovi GIB. GIB bude uvedený prípad posudzovať ako bezpečnostný incident a navrhne manažérovi 2. alebo 3.stupňa riadenia danej súčasti spôsob jeho vyriešenia.

11) Ak používateľ na svojom PC nerešpektuje, resp. porušuje pravidlá jednotnej politiky a správy PC, prípadne ak nie je jeho PC zaradený v univerzitnej doméne, odborný zamestnanec a správca informačného systému nie sú povinní riešiť problémy na PC používateľa a problémy pri používaní informačného systému, ktoré vznikli v dôsledku nerešpektovania pravidiel jednotnej politiky a správy PC.

12) Ak používateľ na svojom PC aj po upozornení odborného zamestnanca preukazateľne porušuje pravidlá jednotnej politiky a správy PC, alebo porušuje ustanovenia uvedené v § 4 ods.1,2, 4 až 6 Smernice rektora č. 13/2012 Pravidlá používania a správy počítačovej a hlasovej siete Trnavskej univerzity v Trnave, je takéto konanie považované za porušenie pracovnej disciplíny.

Čl. 4 Zásady používania PC a povinnosti používateľa PC

1) Používateľ PC je povinný prihlasovať sa k PC výhradne svojimi prihlasovacími údajmi, ktorými sú používateľské meno a heslo. Používateľským menom je identifikačné číslo TUID alebo alias používaný v LDAP. Na vytvorenie hesla slúži samoobslužný internetový portál na správu používateľského účtu (https://idmportal.truni.sk/). Všetky potrebné informácie o systéme na správu identít sú uvedené na webovom sídle TU v sekcii Návody k UIS (http://www.truni.sk/sk/sprava-identit-identity-management-idm).

2) Z prideleného PC používateľ pristupuje iba k tým UIS a univerzitným sieťovým službám, ku ktorým má vygenerované prístupové údaje a príslušným správcom informačného systému vytvorené oprávnenia (používateľské roly) v súlade s čl.2 ods.2).

3) Z prideleného PC používateľ pristupuje iba k tým UIS a univerzitným sieťovým službám, ku ktorým má právo a povinnosť pristupovať na základe jeho pracovnej zmluvy a náplne.

4) Používateľ PC je povinný uchovávať svoje prihlasovacie údaje k PC a k UIS v tajnosti a nesmie ich odovzdať osobne alebo elektronicky (e-mailom, cez webový formulár)

inej osobe. Administrátori UIS a sieťových služieb nikdy nevyžadujú od používateľa PC poskytnutie jeho prihlasovacích údajov.

5) Používateľovi PC sa neodporúča využiť funkcionalitu na automatické zapamätanie hesla, najmä ak ide o heslo k zvlášť dôležitým informačným systémom.

6) V prípade, ak používateľ PC zistí, že iná osoba získala neoprávnený prístup k jeho PC, iný ako zdieľanie obrazovky správcom informačného systému uvedený v čl.3 ods.5), alebo sa iná osoba dokázala prihlásiť k UIS pomocou prihlasovacích údajov používateľa PC, ten je okamžite povinný nahlásiť túto skutočnosť odbornému zamestnancovi danej súčasti a odborný zamestnanec je povinný bezodkladne daný bezpečnostný incident (ďalej len BI) vyriešiť alebo do doby vyriešenia BI odstaviť PC a konto používateľa zablokovať.

7) Používateľ PC nie je oprávnený meniť svoj nastavený profil na PC bez vedomia odborného zamestnanca. V prípade, že tak urobí, preberá plnú zodpovednosť za výskyt chybových stavov na PC, za nesprávne vykonávanie aktualizácií softvéru a nesprávnu funkčnosť UIS. V tomto prípade platí zásada uvedená v čl.3 ods.11).

8) Používateľ PC samostatne nesťahuje a neinštaluje na pevný disk PC žiadny softvér bez vedomia odborného zamestnanca.

9) Používateľ PC pri práci na internete nenavštevuje stránky, ktoré predstavujú značné riziko kompromitovania bezpečnosti PC. Ide najmä o stránky s nelegálnym softvérom, erotické stránky, stránky na zdieľanie súborov, stránky určené na diskusné a zábavné fóra.

10) Používateľ PC nikdy nespúšťa programy alebo odkazy ponúkané neznámou webovou stránkou, nevypĺňa na nich žiadne formuláre a nevyhovuje žiadostiam o rôzne potvrdenia.

11) Používateľ PC nikdy neotvára prílohu v klientovi elektronickej pošty (napr. MS Outlook, Mozzila Thunderbird, ...), ale ju vždy uloží na lokálny disk a otvára pomocou aplikácie určenej na otváranie danej prílohy.

12) Používateľ PC ukladá do používateľských adresárov pevného disku PC alebo do zdieľaných sieťových adresárov iba služobné dokumenty, pričom dôležité údajové súbory pravidelne archivuje na určené dátové úložisko.

13) Používateľ PC archivuje služobné dokumenty na prenosné pamäťové médium (USB, prenosný disk) schválené hardvérovým špecialistom iba v prípade, ak to vyžaduje povaha jeho práce a ak to neodporuje bezpečnostnej smernici na ochranu osobných údajov.

14) Používateľ PC je povinný si pravidelne, najmenej však 1 krát za rok, meniť svoje heslo do UIS prostredníctvom portálu na správu používateľského účtu.

Čl. 5 Pravidlá vyradenia a likvidácie PC

1) O vyradení PC z dôvodu neodstrániteľnej poruchy, vysokých nákladov na opravu alebo z dôvodu morálneho zastarania rozhoduje manažér 2.alebo 3. úrovne riadenia. Návrh na vyradenie PC oznámi na predpísanom tlačive oddeleniu pre evidenciu a správu majetku, ktoré zabezpečí potrebné úkony v príslušnom informačnom systéme (SAP-SOFIA).

2) Pred vyradením PC z evidencie majetku je odborný zamestnanec na základe usmernenia od manažéra 2.alebo 3. stupňa riadenia povinný zabezpečiť, aby všetky

potrebné údaje uložené na pevnom disku boli zálohované, resp. archivované na bezpečnom dátovom úložisku danej súčasti alebo univerzity a všetky nepotrebné údaje boli z disku vymazané.

3) Pred odovzdaním PC na centrálne úložisko elektroodpadu musí odborný zamestnanec vybrať z PC pevný disk a pamäťové médiá a vykonať ich fyzické zničenie, aby nebolo možné žiadnym spôsobom rekonštruovať vymazané údaje.

4) S vyradenými PC, ktoré sa stávajú elektroodpadom, nakladá univerzita v súlade so zákonom č.79/2015 Z.z. o odpadoch a o zmene a doplnení niektorých zákonov.

Čl. 6 Záverečné ustanovenia

1) Porušenie povinností uvedených v čl. 4 ods.1) a 3) je v súlade s čl. 12 ods.3. písm. n) Pracovného poriadku TU považované za závažné porušenie pracovnej disciplíny.

2) Opatrenia uvedené v čl.3 ods. 3) je potrebné vykonať do 12 mesiacov odo dňa účinnosti tejto smernice.

3) Táto smernica nadobúda platnosť dňom jej podpisu rektorom univerzity a účinnosť dňom jej uverejnenia na úradnej výveske TU.