



# TRNAVSKÁ UNIVERZITA V TRNAVE

Smernica rektora Trnavskej univerzity v Trnave  
č. 13/2012

## **Pravidlá používania a správy počítačovej a hlasovej siete Trnavskej univerzity v Trnave**

Obsah: A. Pravidlá používania počítačovej a hlasovej siete Trnavskej univerzity  
B. Pravidlá správy počítačovej siete Trnavskej univerzity

Trnava, november 2012

## § 1 Účel dokumentu

(1) Prevádzkový poriadok počítačovej siete (ďalej len „prevádzkový poriadok“) stanovuje pravidlá prístupu oprávnených používateľov k službám počítačovej siete, ktoré sú v správe Centra informačných systémov (ďalej len „CIS“), alebo iných súčastí Trnavskej univerzity v Trnave (ďalej len „univerzita“), pričom podrobne upresňuje § 7 Bezpečnostnej smernice univerzity.

(2) Prevádzkový poriadok upravuje aj pravidlá spravovania počítačovej siete univerzity, ktoré stanovujú práva a povinnosti správcov počítačovej siete. Odpovedajúce články týchto pravidiel sa primerane vzťahujú na používateľov, ktorí spravujú samostatne svoje výpočtové prostriedky napojené na počítačovú sieť univerzity.

(3) Prevádzkový poriadok je záväzný pre všetkých používateľov počítačovej siete, osobných počítačov a obdobných zariadení pripojených k počítačovej sieti univerzity. Pokiaľ sa daná časť pravidiel vzťahuje iba na študentov, je použitý termín študent. Pokiaľ sa daná časť pravidiel vzťahuje iba na zamestnancov, je použitý termín zamestnanec. Pokiaľ je použitý termín používateľ, potom sa pravidlo vzťahuje na všetkých zamestnancov, študentov a iných používateľov, ktorí majú povolený prístup do príslušného systému alebo k poskytovanej službe.

(4) Používatelia počítačovej siete univerzity sú povinní okrem tohto prevádzkového poriadku dodržiavať aj Všeobecné pravidlá používania siete SANET, ktoré sú uvedené na stránke [www.sanet.sk](http://www.sanet.sk).

## § 2 Základné pojmy a predpisy

(1) Základné pojmy:

- a) **SANET** – Slovenská akademická sieť, ktorú spravuje združenie SANET s cieľom zabezpečiť akademickým i komerčným inštitúciám prístup do siete Internet v súlade so schváleným štatútom a pravidlami pre používanie siete SANET.
- b) **Počítačová sieť** – súhrn technických a programových prostriedkov, ktoré zabezpečujú dátové prepojenie počítačov a obdobných zariadení do univerzitnej počítačovej siete.
- c) **Hlasová sieť** – súhrn technických a programových prostriedkov, ktoré zabezpečujú hlasovú komunikáciu v rámci privátnej hlasovej siete univerzity.
- d) **Správca siete** – *zamestnanec univerzity zodpovedný za prevádzku, správu a údržbu sieťových služieb a aktívnych sieťových prvkov.*
- e) **Server** – obslužný počítač alebo program, na ktorom je zabezpečená prevádzka sieťových aplikácií alebo sieťových služieb pre používateľov.

- f) **Sieťová aplikácia** – počítačový program, ktorý skupine používateľov poskytuje vopred definované sieťové služby.
- g) **Sieťová služba** – schopnosť pomocou sieťových prostriedkov uspokojiť vopred definované požiadavky používateľov.
- h) **Identifikačné údaje používateľa siete** – zahŕňajú meno používateľa v stanovenom formáte a heslo používateľa, ktorých správne zadanie je nevyhnutnou podmienkou pre prístup do počítačovej siete.
- i) **Poštové konto** – názov schránky elektronickej pošty používateľa, ktorá mu po identifikácii umožňuje prístup k službám elektronickej pošty.
- j) **Domovský adresár** – vyhradená časť servera, ktorú po identifikácii môže používateľ využívať na archiváciu svojich údajov.
- k) **Shareware** - skupina programových produktov, ktoré sa vyznačujú tým, že poskytujú možnosť počas autorom definovanej doby (typicky okolo 30 dní) program BEZPLATNE a LEGÁLNE vyskúšať na svojom počítači.
- l) **Freeware** - typ programového vybavenia, kedy sa autor zrieka nároku na zaplatenie registračného poplatku, nezrieka sa však autorstva programu.
- m) **Identity Management System** – systém na správu identít (ďalej aj „systém IDM“) zabezpečuje automatizovaný manažment používateľských účtov (pridávanie, zmenu, odstraňovanie) a synchronizáciu identifikačných údajov používateľov informačných systémov.
- n) **Wifi sieť** – bezdrôtová dátová sieť LAN založená na štandardoch IEEE-802.11, ktorá slúži na prístup k internetu.
- o) **Portál na správu používateľského účtu** – softvérová aplikácia dostupná cez webové rozhranie, ktorá samoobslužným spôsobom zabezpečuje používateľom spravovanie a aktualizáciu svojich prihlasovacích a identifikačných údajov potrebných na prístup k univerzitným informačným systémom (UIS).
- p) **VPN** – virtual private network, slúži na vzdialený prístup do počítačovej siete univerzity z iného umiestnenia.
- q) **HVPS** – hlasová virtuálna privátna sieť je osobitná elektronická komunikačná služba poskytovaná prostredníctvom verejných telefónnych sietí komunikačných operátorov.

(2) Počítačová sieť univerzity je súčasťou metropolitnej optickej dátovej siete, ktorá prepája vysokoškolské objekty a tiež niektoré stredné a základné školy v Trnave, ako aj neziskové a štátne organizácie v Trnavskom kraji. Je priamo napojená na uzol siete SANET a prostredníctvom neho na Internet.

(3) Hlasová sieť univerzity je prepojenie telefónnych ústrední alebo telekomunikačných zariadení jednotlivých univerzitných budov v Trnave, ktorým je zabezpečená privátna hlasová komunikácia bez využívania verejnej telefónnej siete.

(4) HVPS univerzity je vytvorená sieť pre uzatvorenú skupinu registrovaných používateľov (manažérov univerzity a jej súčastí), ktorým bol pridelený služobný telefón so SIM kartou na využívanie elektronických telekomunikačných služieb poskytovaných na základe zmluvy s poskytovateľom HVPS.

(5) S touto smernicou súvisia nasledovné predpisy:

- a) Zákon č. 428/2002 Z.z. o ochrane osobných údajov v znení neskorších predpisov
- b) STN ISO/IEC 17799 Informačné technológie. Kódex manažérstva informačnej bezpečnosti.
- c) STN ISO/IEC TR 13335-1 Informačné technológie. Návod na manažérstvo bezpečnosti IT. Časť 1: Koncepcie a modely bezpečnosti IT.
- d) STN ISO/IEC TR 13335-2 Informačné technológie. Návod na manažérstvo bezpečnosti IT. Časť 2: Riadenie a plánovanie bezpečnosti IT.
- e) STN ISO/IEC TR 13335-3 Informačné technológie. Návod na manažérstvo bezpečnosti IT. Časť 3: Techniky pre manažment bezpečnosti IT.
- f) STN ISO/IEC TR 13335-4 Informačné technológie. Návod na manažérstvo bezpečnosti IT. Časť 4: Výber bezpečnostných opatrení.
- g) Bezpečnostný zámer Trnavskej univerzity v Trnave.
- h) Bezpečnostný štandard Trnavskej univerzity v Trnave.
- i) Bezpečnostná smernica Trnavskej univerzity v Trnave.

## Časť A

### PRAVIDLÁ POUŽÍVANIA POČÍTAČOVEJ A HLASOVEJ SIETE UNIVERZITY

#### § 3

#### Prístupové práva a identita

(1) Počítačovú sieť univerzity môžu využívať iba oprávnení používatelia. Oprávnený používateľ (ďalej len „používateľ“) je používateľ, ktorý bol preukázateľne oboznámený s touto smernicou a získal alebo mu boli pridelené identifikačné údaje pre vstup do siete. Zoznam používateľov a ich aktuálne identifikačné údaje uchováva systém na správu identít.

(2) Právo stať sa používateľom počítačovej siete majú zamestnanci a študenti univerzity. Novoprijatí študenti a študenti nastupujúci po prerušení na štúdium získavajú prístupové údaje do počítačovej siete zo systému IDM automatizovane po zaznamenaní ich zápisu na štúdium v akademickom informačnom systéme MAIS. Zamestnanci získavajú prístupové údaje do počítačovej siete automatizovane po zaznamenaní uzatvorenia pracovnej zmluvy v systéme SOFIA modul HR. Na aktiváciu

alebo zmenu prístupového mena (login) a inicializačného hesla do počítačovej siete a k univerzitným informačným systémom slúži používateľovi samoobslužný Portál na správu používateľského účtu. Jeho používanie sa riadi metodickým usmernením správcu systému IDM.

(3) Využívanie počítačovej siete univerzity inými osobami, ktoré nie sú študentmi alebo zamestnancami univerzity, je možné, iba ak je to v záujme univerzity, a to buď na základe písomného povolenia, vydaného rektorom univerzity alebo ním povereným zamestnancom, alebo ak to vyžaduje všeobecne záväzný právny predpis a vykonávacie predpisy a usmernenia vydané Ministerstvom školstva, vedy, výskumu a športu SR<sup>1</sup>, a to iba v tomto rozsahu. Pridelenie prístupových údajov do počítačovej siete pre týchto používateľov vykonáva správca systému IDM. Uvedené spôsoby pridelenia prístupových údajov neplatia pre používateľov wifi siete EDUROAM, ktorí sú autentifikovaní voči svojim domovským LDAP serverom.

(4) Používateľ používa na prístup do počítačovej siete výlučne svoje prístupové údaje a je povinný ich udržiavať v tajnosti. Zásady tvorby, používania a aktualizácie hesla používateľa sa riadia metodickým usmernením správcu systému IDM.

(5) V prípade, že používateľ po získaní prístupu do univerzitných informačných systémov (UIS) prostredníctvom Portálu na správu používateľského účtu stratí alebo zabudne svoje prihlasovacie údaje, nevie si ich sám obnoviť a požaduje zmenu hesla od správcu IDM, zaplatí za túto službu poplatok 5 €

(6) Zamestnancom univerzity sa zriaďuje poštové konto v tvare [meno.priezvisko@truni.sk](mailto:meno.priezvisko@truni.sk), ktoré sa používa na služobnú korešpondenciu.

(7) Študentom univerzity sa zriaďuje poštové konto v tvare [meno.priezvisko@tvu.sk](mailto:meno.priezvisko@tvu.sk), ktoré sa používa na korešpondenciu súvisiacu so štúdiom.

(8) Univerzitné poštové kontá podľa ods. 6 a 7 sú jedinými poštovými kontami, na ktoré sa zasiela služobná korešpondencia zamestnancom a študentom, a z ktorých budú akceptované ich požiadavky v rámci univerzity, pričom služba presmerovania na externé poštové servery nie je povolená. Jedinou výnimkou je zaslanie požiadavky na obnovu hesla podľa ods. 5. V tomto prípade je oprávnené použitie súkromného poštového konta zadaného v systéme IDM.

(9) Používateľ je povinný zmeniť svoje heslo pred uplynutím doby jeho expirácie, pričom má právo kedykoľvek zmeniť svoje používateľské heslo v priebehu jej plynutia v súlade s ods. 4 tohto článku. Dobu expirácie stanovuje správca systému IDM.

(10) Používateľ nesmie poskytnúť pridelené meno a svoje heslo inej osobe. Za hrubé porušenie pravidiel sa považuje ich poskytnutie osobe, ktorá nemá nárok na prístup alebo ktorej bol prístup zablokovaný.

(11) Používateľ nesmie zneužiť nedbalosť iného používateľa (napr. zabudnuté odhlásenie) k tomu, aby pracoval pod cudzou identitou.

(12) Prístupové práva používateľ získava v súlade s § 3 ods. 2 alebo sú mu pridelené správcou počítačovej siete. Používateľ sa nesmie žiadnymi prostriedkami pokúšať

---

<sup>1</sup> Napr. prístup pre externých oponentov záverečných, rigorózných a habilitačných prác v zmysle ust. § 8 ods. 1 vyhlášky Ministerstva školstva, vedy, výskumu a športu č. 233/2011 Z.z., ktorou sa vykonávajú niektoré ustanovenia zákona č. 131/2002 Z.z. o vysokých školách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov s prihliadnutím na ods. 29 Manuálu k sprístupňovaniu záverečných, rigorózných a habilitačných prác (č. 2011-12684/31651:2-07, dostupný na [http://www.crzp.sk/dokumenty/prirucka\\_sprístupnovanie.pdf](http://www.crzp.sk/dokumenty/prirucka_sprístupnovanie.pdf))

získať prístupové práva, ktoré mu neboli pridelené. Ak používateľ získa jemu nepatriace prístupové práva chybou systému, je povinný tuto skutočnosť bez zbytočného odkladu ohlásiť správcovi siete (na úrovni súčasti univerzity alebo na adresu [idsm@truni.sk](mailto:idsm@truni.sk)) a tieto práva nesmie použiť.

(13) Používateľ nesmie zneužívať svoj prístup do UIS a do počítačovej siete univerzity k získaniu neautorizovaných prístupových práv k ľubovoľným informačným zdrojom dostupným prostredníctvom počítačovej siete univerzity.

(14) Prístup k využívaniu služieb HVPS univerzity získa používateľ so súhlasom vedenia príslušnej súčasti univerzity pridelením služobného telefónneho prístroja so SIM kartou zmluvného poskytovateľa komunikačných služieb.

(15) Ukončením posledného štúdia alebo ukončením posledného pracovného pomeru na univerzite zanikajú prístupové práva používateľa k UIS a k službám počítačovej siete a končia oprávnenia na využívanie služieb hlasovej siete a HVPS univerzity.

#### § 4

#### Používanie počítačovej siete

(1) Používateľ môže používať výpočtové prostriedky a počítačovú sieť iba pre vzdelávacie, vedecké, výskumné, vývojové a umelecké účely alebo úlohy súvisiace s prevádzkou a správou univerzity. Za porušenie pravidiel sa považuje predovšetkým použitie pre komerčnú činnosť nesúvisiacu s činnosťou univerzity, šírenie obchodných informácií, politickú, náboženskú alebo rasovú agitáciu, propagáciu drog a šírenie materiálov, ktoré sú v rozpore so zákonom.

(2) Používateľ má právo používať iba legálne nadobudnuté programové vybavenie. Shareware alebo freeware môže používateľ počítačovej siete univerzity používať iba pre účely uvedené v odst. 1 tohto článku.

(3) Zamestnanci majú právo pristupovať z domu alebo z iného umiestnenia do počítačovej siete univerzity pomocou VPN a tak pracovať s možnosťami, akoby sa nachádzali na pracovisku. O tento spôsob pripojenia požiadajú svojho správcu lokálnej siete súčasti univerzity.

(4) Používateľ nesmie na počítače univerzity inštalovať alebo kopírovať programové produkty, ktoré nie sú licenčne zabezpečené alebo sú získané v rozpore so zákonom č. 618/2003 Z.z. o autorskom práve a právach súvisiacich s autorským právom (autorský zákon) v znení neskorších predpisov.

(5) Používateľ nesmie zasahovať do programov, dát a technického vybavenia počítačovej siete bez súhlasu správcu. Zvlášť prísne sú zakázané neautorizované zmeny konfigurácie počítačov či iných prostriedkov, ktoré by mohli mať vplyv na prevádzku počítačovej siete. Študent nesmie inštalovať programy bez súhlasu správcu alebo pedagóga zodpovedného za počítačové laboratórium.

(6) Používateľ má právo používať pridelený domovský adresár na sieťovom disku, výpočtové prostriedky a počítačovú sieť iba s ohľadom na jej celkové zaťaženie. Používateľ nesmie vedome narušovať prácu iných používateľov, ani chod a výkonnosť siete. Musí bez meškania splniť príkaz správcu na zníženie ním generovanej záťaže.

(7) Veľkosť prenášaných súborov prostredníctvom elektronickej pošty a konferencií môže byť obmedzená. Konkrétny limit je daný technickými možnosťami, ktoré stanovuje ich správca. Pri prekročení používateľského limitu využívaného

diskového priestoru na serveri elektronickej pošty môže dôjsť k automatickému zablokovaniu ďalšieho príjmu pošty pre daného používateľa.

(8) Univerzita nezodpovedá za stratu používateľských dát vzniknutú akýmkoľvek spôsobom. Za vytváranie záložných kópií používateľských dát a programov si zodpovedajú používatelia sami. Za ochranu dát uložených v databázach UIS zodpovedajú ich správcovia v súčinnosti so správcom príslušnej databázy.

(9) V prípade, že sa na pracovnej stanici používateľa zobrazí varovanie, že sa na disku alebo vlozenej diskete nachádza vírus, používateľ nesmie toto varovanie ignorovať. Používateľ túto skutočnosť bezodkladne oznámi príslušnému správcovi siete, prípadne po konzultácii s ním vykoná antivírusovú „dezinfekciu“ príslušného pamäťového média.

(10) V prípade, že používateľ objaví vírus v prijatej elektronickej pošte, bezodkladne o tejto udalosti upovedomí správcu siete, ako aj odosielateľa predmetnej elektronickej pošty. V žiadnom prípade zavírenú elektronickejšiu poštu neposiela inému adresátovi.

(11) V prípade, ak došlo k napadnutiu počítača trójskym koňom alebo hackerom, je správca LAN povinný daný počítač odpojiť od počítačovej siete do doby, kým nebude počítač spôsobilý na bezpečné pripojenie do počítačovej siete.

(12) Používateľ HVPS sa pri využívaní dostupných služieb riadi usmerneniami správcu HVPS na svojej súčasti, ktorý mu pridelil služobný telefónny prístroj so SIM kartou.

(13) Ukončením posledného štúdia alebo ukončením posledného pracovného pomeru na univerzite zanikajú práva používateľa na využívanie služieb počítačovej siete.

## § 5

### Ochrana súkromia a zverejňovanie informácií

(1) Pre používanie elektronickej pošty a konferencií platia rovnaké pravidlá ako pre používanie normálnej pošty, pričom poštová správa má charakter otvorenej listovej zásielky.

(2) Používateľ je povinný dbať na to, aby jeho správy boli presne adresované a nedochádzalo k nežiadúcemu obťažovaniu ostatných používateľov rozosielaním reťazových správ alebo správ adresovaných na zoznamy poštových kont zhromaždených bez súhlasu adresáta.

(3) Používateľ je povinný pri odosielaní elektronickej pošty používať pridelené používateľské meno (meno schránky). Za hrubé porušenie pravidiel je považované odosielanie správ s falošnou identitou za účelom podvodu, zastrašovania a získania neoprávnených informácií.

(4) Príjem elektronickej pošty z poštových kont, ktoré porušujú ustanovenie odst. 2 a 3 tohto článku, môže byť zablokovaný.

(5) Správca systému má povinnosť rešpektovať súkromie používateľov.<sup>2</sup>

(6) Súborny v domovských adresároch a systémových schránkach pošty sú

<sup>2</sup> V zmysle čl. 7 Charty základných práv Európskej únie (2007/C 303/01), čl. 22 ods. 2 Ústavy SR a § 11 zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov

súkromnými údajmi ich vlastníkov. Používatelia majú nárok na ochranu súkromia, a to i v prípade, kedy svoje adresáre nechránia. Za hrubé porušenie pravidiel je považované vytváranie kópií cudzích dát a nezákonné sledovanie prevádzky na počítačovej sieti za účelom získania obsahu správ alebo dát.

(7) Správca má právo znepřístupniť súbory odporujúce zmyslu čl. 4 odst. 1, prípadne ohrozujúce bezpečnosť systému a počítačovej siete (zavírané programy, nástroje pre odpočúvanie prevádzky, získavanie neprináležiacich práv a pod.), a na výzvu správcu je používateľ povinný ich neodkladne odstrániť.

(8) Univerzita nezodpovedá za možné zneužitie dát pri prenose a uchovaní informácií v počítačovej sieti.

(9) Správca má právo vykonávať všetky úkony nutné k výkonu jeho funkcie, vrátane prípadnej kontroly dát a monitorovanie činnosti používateľov. Pokiaľ používateľ používa pre utajenie informácií šifrovanie, je povinný v prípade pochybností o použití v zmysle čl. 4, odst. 1 sprístupniť správcovi obsah dát.

## § 6

### Pravidlá pre pripojenie k počítačovej sieti

(1) Používateľ je povinný vyžiadať si súhlas správcu siete:

- a) pred pripojením daného zariadenia na počítačovú sieť,
- b) pred zmenou konfigurácie zariadenia, ktorá by mohla mať vplyv na chod siete,
- c) pred trvalým odpojením zariadenia od počítačovej siete.

(2) Správca registruje pripojené zariadenia podľa Pravidiel správy počítačovej siete Trnavskej univerzity v Trnave. Do existujúcej počítačovej siete sa môžu pripojovať len zariadenia vo vlastníctve univerzity. Súkromné, prenajaté a iné zariadenia je možné pripojovať len na základe písomného povolenia správcu počítačovej siete na dobu nevyhnutne potrebnú v súlade s potrebami univerzity. Do wifi siete sa môžu pripájať aj súkromné zariadenia (notebook, iPad, iPhone a podobne) v súlade s metodickým usmernením správcu siete univerzity.

(3) Za správnu a legálnu inštaláciu operačného systému a sieťového programového vybavenia počítača pripojeného k počítačovej sieti zodpovedá buď poverený zamestnanec určený správcou siete, alebo používateľ, pokiaľ má povolené inštalovať operačný systém samostatne (ak to povoľujú Pravidlá prevádzky počítačovej siete na úrovni príslušnej fakulty alebo pracoviska, ktoré musia byť vydané v súlade s týmto prevádzkovým poriadkom).

(4) Pri samostatnej správe operačného systému a sieťového programového vybavenia počítača pripojeného na počítačovú sieť musí používateľ dodržiavať príslušne ustanovenia Prevádzkového poriadku počítačovej siete univerzity.

(5) Používateľ nesmie používať pre pripojenie k počítačovej sieti inú sieťovú adresu, než mu bola pridelená (či už automaticky alebo staticky).

(6) Využívanie počítačovej siete univerzity v rámci vedeckej a pedagogickej spolupráce s inými organizáciami je možné iba na základe písomného povolenia vydaného rektorom alebo dekanom príslušnej fakulty.



## § 7

### **Postih študentov za porušenie pravidiel používania počítačovej siete**

(1) Porušenie pravidiel používania počítačovej siete je považované za porušenie povinností študenta v zmysle § 71 odst. 2 a 3 zák. č. 131/2002 Z.z. o vysokých školách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

(2) Podľa § 72 citovaného zákona a Disciplinárneho poriadku pre študentov univerzity je možné za porušenie pravidiel študentovi uložiť disciplinárne opatrenie závislé od závažnosti ich porušenia.

(3) Zistené menej závažné porušenia pravidiel používania počítačovej siete dáva správcovi siete alebo ním poverenej osobe právo študenta napomenúť, čo však nie je považované za disciplinárne opatrenie v zmysle bodu 2 tohto článku.

(4) Pri závažnejších porušeníach, či opakovanom menej závažnom porušení pravidiel môže správca alebo ním poverená osoba odňať študentovi na vopred stanovenú dobu právo voľne používať služby počítačovej siete mimo organizovaného vyučovania. Toto právo môže byť využité aj v prípade, ak si študent nesplní všetky povinnosti, ktoré vyplývajú zo zákona č. 131/2002 Z.z. o vysokých školách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Študent má v tomto prípade právo odvolať sa proti rozhodnutiu správcu siete alebo ním poverenej osoby. O odvolaní s konečnou platnosťou rozhodne dekan fakulty alebo riaditeľ pracoviska univerzity. Toto odvolanie nemá odkladný účinok.

(5) Pri opakovanom závažnom porušení pravidiel podľa bodu 4 tohto článku bude prípad riešený takto:

- a) dňom zistenia porušenia pravidiel používania siete stráca študent právo používať služby počítačovej siete,
- b) prípad je postúpený disciplinárnej komisii príslušnej fakulty alebo disciplinárnej komisii univerzity,
- c) na základe záverov rokovania disciplinárnej komisie dekan príslušnej fakulty alebo rektor rozhodne o uložení sankcie podľa bodu 2 tohto článku. Súčasne môže byť pre študenta znepriístupnené služby počítačovej siete univerzity na dobu maximálne dvoch kalendárnych mesiacov.

## § 8

### **Postih zamestnancov za porušenie pravidiel používania počítačovej siete**

(1) Porušenie ustanovení tejto smernice bude u zamestnancov považované za porušenie základných povinností zamestnanca (§ 81 písm. a), c), e) a f) Zákonníka práce) a je možné z neho vyvodiť príslušné pracovno-právne dôsledky vrátane skončenia pracovného pomeru výpoveďou alebo okamžitým ukončením.

(2) Pri zistení porušení pravidiel používania počítačovej siete správca siete alebo ním poverená osoba písomne upozorní zamestnanca, ktorý pravidlá porušil; v prípade hrubého porušenia pravidiel upozorní aj jeho priameho nadriadeného na túto

skutočnosť.

(3) Opakované porušenie pravidiel zo strany zamestnanca bude riešené takto:

- a) dňom zistenia porušenia pravidiel používania siete stráca zamestnanec právo používať služby počítačovej siete univerzity,
- b) dekan príslušnej fakulty alebo rektor v prípade ďalších súčasti univerzity, rozhodne o prípadnom pracovno-právnom postihu zamestnanca podľa ods.1 tohto článku.

(4) Prípadná trestne právna zodpovednosť nie je týmto postupom obmedzená ani vylúčená.

## **Časť B**

### **PRAVIDLÁ SPRÁVY POČÍTAČOVEJ SIETE UNIVERZITY**

#### **§ 9**

#### **Organizačná štruktúra počítačovej siete univerzity**

(1) Počítačová sieť univerzity má hierarchickú štruktúru. Jej členenie je nasledujúce:

- a) metropolitná chrbticová sieť s univerzitným uzlom,
- b) lokálna počítačová sieť súčasti univerzity,
- c) centrálny server,
- d) sieťová aplikácia.

(2) Správu štruktúr počítačovej siete univerzity, ktoré sú uvedené v ods.1, písm. a, c, d tohto článku zabezpečujú správcovia, ktorí sú zamestnancami CIS. Podriadenosť uvedených správcov je v súlade s Organizačným poriadkom CIS.

(3) Správu lokálnej počítačovej siete súčasti univerzity, fakultných serverov a správu fakultných laboratórií zabezpečujú príslušní správcovia lokálnych sietí na jednotlivých súčastiach univerzity. Podriadenosť správcov je v súlade s organizačnou štruktúrou súčasti univerzity. V oblasti prevádzky lokálnej počítačovej siete súčasti univerzity, jej pripojenia cez metropolitnú chrbticovú sieť do hlavného univerzitného uzla, v oblasti pripojenia a správy sieťových zariadení sú podriadení vedúcemu oddelenia komunikačnej siete CIS. Riešenie úloh súvisiacich s funkčnosťou a efektívnou prevádzkou lokálnej počítačovej siete súčasti univerzity má vždy najvyššiu prioritu.

(4) Technické a metodické zabezpečenie správy počítačovej siete postupuje hierarchicky zhora nadol podľa čl. 1 od správcu metropolitnej chrbticovej siete k správcovi sieťovej aplikácie.

(5) Správa jednotlivých sietí môže byť združená, a to z hľadiska hierarchie siete horizontálne (napr.u súčasti univerzity, ktoré sú umiestnené v jednej budove) i vertikálne (napr. správa chrbticovej siete univerzity a správa lokálnej siete súčasti univerzity).

(6) Prevádzku centrálnych informačných systémov a hlavného komunikačného uzla univerzity zabezpečujú zamestnanci CIS. Poslanie a pôsobnosť CIS vymedzuje Organizačný poriadok univerzity a Organizačný poriadok CIS.

## § 10

### Práva a povinnosti správcov v oblasti prevádzky počítačovej siete univerzity

#### (1) Správca sieťovej aplikácie:

- a) zabezpečuje prevádzku aktuálnej verzie aplikácie na serveri, poskytuje súčinnosť pri integrácii aplikácie s inými informačnými systémami univerzity,
- b) definuje používateľom oprávnenia a používateľské roly pre spravovanú aplikáciu,
- c) zodpovedá za bezpečné uloženie záložných dát,
- d) zabezpečuje metodické riadenie používateľov aplikácie a poskytuje im podporu pri správnom používaní aplikácie,
- e) poskytuje aktuálne administrátorské prístupové práva do aplikácie svojmu nadriadenému, ktorý zodpovedá za ich bezpečnú archiváciu,
- f) má právo iniciovať a pripomienkovať zmeny v sieťovej aplikácii a byť informovaný o realizácii všetkých zmien, ktoré sa týkajú sieťovej aplikácie.

#### (2) Správca servera (v prípade, že nie je určený, prechádzajú tieto povinnosti na správcu lokálnej siete):

- a) zabezpečuje prevádzku servera (inštalácia, konfigurácia, aktualizácia) a jeho správne pripojenie do počítačovej siete univerzity,
- b) definuje používateľom oprávnenia a používateľské roly pre správne pripojenie k službám servera,
- c) udržiava konfiguráciu systémov pre počítače, ktorých systém je zavedený zo servera,
- d) zabezpečuje aktualizáciu operačného systému a antivírusovú ochranu servera,
- e) zodpovedá za bezpečné uloženie záložných dát,
- f) poskytuje aktuálne administrátorské prístupové práva k serverom svojmu nadriadenému, ktorý zodpovedá za ich bezpečnú archiváciu.

#### (3) Správca lokálnej siete súčasťou univerzity:

- a) zabezpečuje používanie lokálnej siete od prípojného miesta chrbticovej siete univerzity ku koncovým staniciam,
- b) zabezpečuje správnu funkciu lokálnych serverov (pokiaľ nie je menovaný správca príslušného servera),
- c) definuje používateľom oprávnenia na prístup k zariadeniam a službám, ktoré sú súčasťou ním spravovanej lokálnej počítačovej siete,
- d) spolupracuje s univerzitným správcom e-mailového servera a poskytuje podporu používateľom elektronickej pošty z danej súčasťou univerzity,
- e) udržiava konfiguráciu počítačov v lokálnej sieti podľa jednotných pravidiel a usmernení pre správu PC a terminálových klientov,
- f) udržiava aktuálny zoznam MAC a IP adries všetkých pripojených zariadení a zmeny hlási správcovi chrbticovej siete univerzity,
- g) v spolupráci so správcom chrbticovej siete univerzity realizuje všetky zásahy do lokálnej siete (zmeny topológie, výstavba siete atď.),
- h) informuje používateľov o pravidlách práce v sieti,
- i) inštaluje a konfiguruje vpn a wifi klienta používateľom,
- j) zodpovedá za bezpečné uloženie záložných dát.

#### (4) Správca metropolitnej chrbticovej siete:

- a) zabezpečuje bezpečnú prevádzku metropolitnej univerzitnej siete v súlade so schválenou topológiou, pričom spolupracuje so správcom mestského uzla siete SANET,
- b) zaisťuje pre univerzitu konektivitu naväzujúcich počítačových sietí,
- c) vykonáva pravidelné monitorovanie chrbticovej siete,
- d) zaisťuje používanie centrálnych serverov (DNS, FireWall, DHCP a pod.),
- e) sleduje vývojové trendy v oblasti počítačových sietí a navrhuje vedeniu CIS spôsob ich implementácie do metropolitnej siete univerzity,
- f) organizuje nasadzovanie nových sieťových služieb,
- g) poskytuje odborné konzultácie správcovi podriadených sietí,
- h) poskytuje aktuálne administrátorské prístupové práva k serverom svojmu nadriadenému, ktorý zodpovedá za ich bezpečnú archiváciu.

(5) Pravidlá pre všetkých správcov na všetkých úrovniach:

- a) zaisťujú používanie a dostupnosť siete, servera alebo sieťovej aplikácie,
- b) kontrolujú dodržiavanie pravidiel používania siete,
- c) monitorujú používanie siete a riešia prípadné kolízie,
- d) zálohujú a archivujú dáta na zverených zariadeniach.

(6) Správca počítačovej siete má právo stanovovať obmedzenia, ktoré sú v záujme efektívnej prevádzky aplikácií a počítačovej siete univerzity.

## **§ 11**

### **Práva a povinnosti správcov v oblasti bezpečnosti počítačovej siete univerzity**

(1) Správcovia (bez ohľadu na postavenie v hierarchii metropolitnej počítačovej siete) sú povinní zaisťovať bezpečnosť prevádzky počítačovej siete v súlade s prijatou bezpečnostnou politikou univerzity.

(2) Správca lokálnej siete je povinný upozorniť bez zbytočného odkladu správcu metropolitnej chrbticovej siete na zistené bezpečnostné incidenty a tieto incidenty zdokumentovať.

(3) Správca má právo kontrolovať dáta používateľov a monitorovať ich činnosť v sieti, a to buď námatkovo, alebo v prípadoch vzniku podozrení na porušenie pravidiel prevádzky počítačovej siete univerzity. Pri tejto činnosti je správca povinný zachovávať mlčanlivosť o informáciách, ktoré získa, pokiaľ nezistí porušenie pravidiel prevádzky počítačovej siete. Pokiaľ porušenie pravidiel zistí, je povinný postupovať podľa odpovedajúcich ustanovení § 7 a 8 v časti A tejto smernice.

## **§ 12**

### **Záverečné ustanovenia**

(1) Pravidlá používania počítačovej siete na úrovni fakulty alebo ďalších súčasti univerzity môžu byť doplnené pravidlami vydanými dekanom príslušnej fakulty alebo riaditeľom príslušnej súčasti univerzity. Pravidlá používania na úrovni fakulty a ďalších súčasti univerzity nesmú byť v rozpore s Pravidlami prevádzky a správy počítačovej siete univerzity.

(2) Táto smernica nadobúda účinnosť dňom podpisu.

(3) Prechodné obdobie na zosúladienie skutočného stavu s ustanoveniami tejto smernice, najmä s § 3, sa stanovuje na 3 mesiace od jej podpisu rektorom univerzity.

- (4) Ruší sa Smernica rektora Trnavskej univerzity v Trnave č.20/2006 Prevádzkový poriadok počítačovej siete Trnavskej univerzity v znení Dodatku č. 1 zo dňa 25.1.2011.

V Trnave, dňa

.....  
prof. doc. JUDr. Marek Šmid, PhD.  
*rektor Trnavskej univerzity v Trnave*