Slezská univerzita v Opavě

Směrnice rektora č. 13/2011

Pravidla užívání počítačové sítě Slezské univerzity

Vydáno: V Opavě, září 2011

Směrnice rektora č. 13/2011

Pravidla užívání počítačové sítě Slezské univerzity

I.

Předmět úpravy, definice základních pojmů

1. Tato směrnice definuje závazná pravidla pro používání počítačové sítě Slezské univerzity (dále jen „SU“). Vztahuje se na všechny uživatele počítačové sítě SU (zaměstnanci, studenti, popř. třetí osoby) a všech počítačů nebo obdobných zařízení, která jsou libovolnými prostředky přímo funkčně připojena k počítačové síti nebo jejím počítačům.
2. Počítačovou sítí (či jen „sítí“) se rozumí všechny technické i programové prostředky výpočetních systémů jednotlivých součástí SU a jejich pracovišť (celouniverzitních pracovišť, fakult, kateder, ústavů apod.) a všech prostředků pro vzájemné propojení těchto systémů.
3. Uživatelem počítačové sítě se rozumí každý, kdo přímo užívá počítačové sítě, počítačů či jiných zařízení k nim připojených.
4. Správcem sítě (resp. její části), serveru nebo počítačové učebny (laboratoře) se rozumí pracoviště SU, které má síť, server nebo učebnu (laboratoř) ve správě.
5. Administrátorem se rozumí osoba, která je správcem konkrétního výpočetního systému pověřena k výkonu činností souvisejících se systémovou správou a údržbou svěřeného systému.
6. Počítačovými prostředky se rozumí výše zmíněné počítače, resp. síť.
7. Počítačovým virem se rozumí jakýkoliv spustitelný kód nebo makrokód, který je na počítači instalován bez vědomí uživatele či správce počítače a jehož primárním účelem jsou uživatelem neautorizované činnosti, zejména, nikoliv však pouze, modifikace dat a programů na počítači, sběr informací o počítači a souborech na něm uložených, rozesílání sebe sama a/nebo dat z počítače na další systémy, zasílání nekorektních dat po síti.

II.

Všeobecná ustanovení

1. Síť SU je distribuovaná síť s určitým stupněm hierarchie. Síť se skládá z jednotlivých domén (podsítí), které jsou vytvářeny podle jednotlivých součástí SU a jejich lokalit. Síť SU je zapojena do větších celků – české akademické sítě CESNET a globální sítě Internet – a je budována v souladu se zásadami budování těchto sítí.
2. Jednotlivé domény jsou spravovány těmi součástmi SU, které je vytvořily, v úzké vzájemné spolupráci. Konkrétní výkon správy zabezpečují zaměstnanci příslušných pracovišť jednotlivých součástí SU, nebo oficiálně pověření pracovníci jednotlivých kateder či ústavů (dále jen „administrátoři").
3. Správce sítě v každé doméně je správcem počítačových prostředků této domény. Dbá o to, aby jejich provozem nebyl omezován nebo dokonce poškozován provoz celouniverzitní sítě. Změny konfigurace sítě v rámci jeho domény jsou plně v jeho kompetenci.
4. Správce sítě je oprávněn monitorovat činnost uživatelů spravované domény v mezích, které neohrožují veřejná, osobní či vlastnická práva jednotlivých uživatelů. Informace, se kterými v rámci této činnosti přichází do styku, je povinen udržovat v naprosté tajnosti a s obsahem soukromých adresářů jednotlivých uživatelů není oprávněn seznamovat další osoby. V případě zjištěného porušení pravidel provozu sítě SU je povinen s touto skutečností seznámit odpovědného vedoucího zaměstnance příslušné součásti SU. V rámci monitorování může správce sítě monitorovat i uživatele subdomén, které spadají pod jeho doménu.
5. Správce sítě může odpojit subdoménu, ke které byly připojeny s ním nekonzultované technické prostředky nebo na níž byla provedena s ním nekonzultovaná změna konfigurace síťového programového vybavení a tyto prostředky či tato změna vedly nebo by mohly vést k závažným poruchám, které ohrožují provoz celouniverzitní sítě.
6. Správce sítě je ve spravované doméně oprávněn stanovit další závazná pravidla, upravující specifické činnosti potřebné k připojení výpočetních systémů (doporučený operační systém včetně povinných update, specifikace nameserverů, komunikační protokoly, míra otevřenosti některých síťových služeb atd.).
7. Za přidělení uživatelského účtu a dalších zdrojů na konkrétním počítači sítě odpovídá administrátor tohoto počítače, nikoliv správce sítě.
8. Uživatel zodpovídá za zálohování svých dat. Způsob zálohování konzultuje s příslušným správcem sítě.

III.

Vlastnická práva

1. Uživatelé využívají počítačové prostředky SU ve shodě se svými pracovními a studijními úkoly. Efektivní naplnění těchto úkolů předpokládá vzájemnou spolupráci uživatelů při důsledném respektování vlastnických práv k datům uloženým v elektronické podobě. Uživatelé se musí při přístupu k této formě uložení dat řídit

naprosto stejnými etickými i zákonnými normami jako při přístupu k objektům a informacím v jiné podobě.

2. Všechny složky počítačové sítě SU jsou vlastnictvím SU, případně k nim SU vlastní či vykonává práva užívání. Nepřípustnost odcizení či poškození se pak vztahuje na elektronickou podobu dat a informací stejně jako na vlastní fyzické prostředky.

3. Především zaměstnancům, funkcionářům, jakož i studentům SU je zakázáno:

   a. Připojovat do sítě další počítače a přemísťovat je bez schválení správce sítě.
   b. Instalovat bez schválení administrátorů sítě takové programové vybavení, které by neúměrně zvyšovalo zatížení sítě a serverů.
   c. Šířit a instalovat na síti takové programové vybavení a data, k nimž uživateli nepřísluší vlastnická práva, resp. práva užívání.
   d. Neautorizovaným způsobem kopírovat byť jen části programového vybavení nebo dat, k nimž uživatel vykonává vlastnická práva, resp. práva užívání.
   e. Neautorizovaným způsobem modifikovat programy, data nebo technické vybavení v majetku či užívání SU. Zvlášť přísně je pak zakázáno neautorizovaným způsobem měnit konfigurace počítačů či jiných prostředků, které by mohly mít vliv na provoz sítě jako celku.
   f. Poškozovat nebo ničit počítačové prostředky (počítače, programové vybavení či komunikační linky).
   g. Zneužívat nedbalosti jiných uživatelů (např. opomenutí odhlášení, nevhodná ochrana souborů) k přístupu pod cizí identitou, resp. k cizím datům.
   h. Používat programových prostředků, které mohou vést k získání cizí identity, a používání programových prostředků s cílem získání neodůvodnitelné anonymity (např. posílání anonymní pošty apod.)
   i. Pokoušet se o získání takových přístupových práv, která nebyla přidělena administrátorem (např. neautorizovaný přístup k libovolným neveřejným informačním zdrojům jak na SU, tak i v kterékoli organizaci dostupné prostřednictvím počítačové sítě). Pokud uživatel získá taková práva chybou programového či technického vybavení, je povinen na tuto skutečnost neprodleně upozornit administrátora.
   j. Odposlouchávat či jinak monitorovat provoz sítě a vytvářet kopie zpráv procházejících jednotlivými uzly sítě. Pokud je takovouto činnost nutno vykonávat v rámci výuky specializovaných předmětů odbornou katedrou (ústavem), musí být prováděna výhradně v laboratořích této katedry (ústavu) za podmínek, které určí správce sítě této laboratoře.
   k. Používat počítačové prostředky SU k činnostem uvedeným v bodech a) až j) a namířeným proti jakékoliv další organizaci, jejíž počítačové prostředky jsou dostupné prostřednictvím počítačové sítě SU.

IV.

Ochrana dat a informací

1. SU se snaží chránit občanská, osobní i vlastnická práva všech uživatelů počítačové sítě a v této souvislosti se snaží i chránit soukromí dat a informací uložených na počítačích SU a/nebo přenášených počítačovou sítí.

2. Pro zajištění maximální možné míry soukromí a bezpečnosti dat je uživatelům zakázáno:
   a. Provádět jakékoli akce, které vedou k narušení soukromí jiného uživatele, a to i v těch případech, kdy takovýto jiný uživatel svá vlastní data explicitně nechrání.
   b. Kopírovat jakákoliv data nebo programy z uživatelských adresářů bez souhlasu jejich majitelů. Toto omezení platí i v případě, že uživatelské adresáře jsou svými majiteli ponechány volně přístupné elektronickými prostředky.
   c. Vědomě využívat nelegální programové vybavení a data, případně takovéto programy či data nabízet jiným.
   d. Používat síť pro šíření obchodních informací, pro reklamní účely, pro politickou nebo náboženskou agitaci a pro šíření materiálů, které jsou v rozporu se zákonem, obecnými etickými a morálními normami nebo mohou poškodit jméno SU. Rovněž je zakázáno obtěžování ostatních uživatelů hromadnými zprávami včetně řetězových zpráv či dopisů na náhodně vybrané adresy v síti.
   e. Využívat počítačových prostředků SU k páchání trestných činů či správních deliktů.
   f. Používat počítačovou síť k získání neautorizovaného přístupu k neveřejným informačním zdrojům (i v majetku/správě jiných osob).

V.

Ochrana proti počítačovým virům

1. Proti nebezpečí počítačových virů je na SU zavedena několikastupňová ochrana. Její první a základní součástí je protivirová ochrana jednotlivých počítačů, zajištěná instalací vhodného protivirového programu a jeho korektním užíváním na všech počítačích. Dalším stupněm ochrany proti počítačovým virům je kontrola příchozí a odchozí pošty na SU.
2. Každý uživatel je povinen sledovat informace poskytované protivirovými programy a v případě detekce napadení virem je povinen zamezit dalšímu šíření viru (zpravidla vypnutím počítače), informovat o této skutečnosti správce sítě a spolupracovat při zajištění nápravy.
3. Každý elektronický dopis, jehož adresát je z domény SU (slu.cz), je protivirovým programem ověřen a v případě detekce viru i příslušně označen. Další nakládání s dopisem s detekovaným virem podléhá pravidlům definovaným součástmi SU. Tato pravidla přitom musí zajistit dostatečnou ochranu před automatickou nebo nevědomou aktivací viru u koncového příjemce.
4. Každý elektronický dopis, který je odesílán z SU, je rovněž kontrolován na přítomnost viru. Dopis obsahující virus je smazán a odesílateli je zasláno příslušné upozornění.

VI.

Přístupová práva a identifikace uživatele

1. Přístup k počítačové síti předpokládá možnost jednoznačné identifikace každého uživatele.

2. Každý zaměstnanec SU a každý její student má právo na zřízení uživatelského účtu (dále jen účet) na vhodném počítači sítě. Vhodnost počítače je třeba chápat jak ve vztahu k součásti SU/pracovišti, tak k účelu, pro který uživatel zřízení účtu žádá; uživatelé mohou mít obecně v síti více účtů. S každým jednotlivým účtem jsou spojena příslušná přístupová práva, která rozhodujícím způsobem určují oprávnění uživatele ve vztahu ke zdrojům sítě.
3. Zaměstnanci SU získávají přístup k počítačovým prostředkům sítě na základě žádosti vedoucího pracoviště podané příslušnému správci sítě. Vedoucí pracoviště je také povinen správci oznámit ukončení působení zaměstnance na pracovišti, aby mohl být účet zaměstnance zrušen. Přístupová práva zaměstnanců ke specializovaným serverům (informační systémy SU apod.) přidělují administrátoři těchto serverů na základě přesných požadavků příslušných vedoucích zaměstnanců.
4. Studenti SU získávají přístupová práva k síti SU dnem zápisu ke studiu na SU.
5. Vytváření uživatelských účtů na serverech spravovaných jednotlivými pracovišti je v kompetenci těchto pracovišť.
6. Uživatel, kterému je účet zřízen, je povinen uzavřít svůj účet netriviálním heslem a toto heslo udržovat v tajnosti.
7. Heslo k vlastnímu (individuálnímu) účtu uživatel nesmí sdělit druhé osobě (ani správci počítače, na němž je účet zřízen).
8. Uživatel smí používat pouze přístupová práva, která SU řádným způsobem náleží, a nesmí vyvíjet žádnou činnost směřující k obejití tohoto ustanovení. Pokud uživatel jakýmkoliv způsobem získá přístupová práva, která SU nebyla přidělena (např. chybou programů nebo technického vybavení), je povinen tuto skutečnost neprodleně oznámit správci počítače. Takto získaná práva nesmí použít.
9. Uživatel může zpřístupnit svůj účet i jiným uživatelům počítačové sítě za dodržení následujících podmínek:
   a. Zpřístupnění je umožněno pouze osobě, která má svůj individuální účet, zaregistrovaný v síti SU, resp. je studentem či zaměstnancem SU, případně je k SU v platném smluvním vztahu, do jehož obsahu náleží přístup k počítačové síti SU.
   b. Zpřístupnění není provedeno sdělením hesla, ale jinými prostředky, které umožňuje používaný operační systém. V tomto případě však uživatel spoluodpovídá za případné zneužití účtu k činnostem v rozporu s těmito pravidly.
10. Uživatel nesmí zneužít nedbalosti jiného uživatele (např. opomenutí odhlášení) k tomu, aby v síti pracoval pod cizí identitou.

VII.

Všeobecné povinnosti

1. Při komunikaci s jinými sítěmi je uživatel povinen dodržovat pravidla, která platí v těchto sítích.
2. Uživatel se snaží, aby jeho činnost jen v minimálním rozsahu negativně ovlivňovala možnosti využití počítačových prostředků dalšími uživateli. To se týká jak neúměrného zatěžování linek v době jejich maximálního využití, tak i neúměrného zatěžování jednotlivých počítačů. Všechny takovéto činnosti je vhodné konzultovat se správcem počítače/sítě a řídit se dále jeho pokyny.
3. Využívání sítě SU v rámci vědecké a pedagogické spolupráce studenty a zaměstnanci jiných organizací je možno na základě písemného svolení vydaného vedoucím zaměstnancem příslušné součásti nebo rektorem. V případě, že se jedná o vztah trvající

déle než akademický rok, je nezbytné konkrétní podmínky využívání počítačové sítě SU včetně případných sankčních opatření specifikovat ve smlouvě mezi SU (konkrétní součástí) a organizací, jejíž zaměstnanci využívají sítě SU. Tato smlouva nemusí být uzavřena v případě, že se jedná o spolupráci se zaměstnanci či studenty jiných vysokých škol či ústavů Akademie věd.

4. Použití sítě SU pro účely nesouvisející přímo s posláním SU je možno pouze na základě písemného svolení, vydávaného rektorem SU.

VIII.

Sankce

1. Správce sítě má právo na dočasné nebo stálé omezení, resp. odebrání, uživatelských přístupových práv k počítačové síti uživatelům, kteří prokazatelně porušili ustanovení této směrnice. Uživatel má právo požádat vedoucího zaměstnance příslušné součásti nebo v případě pracovišť s celoškolskou působností rektora SU o přehodnocení tohoto opatření.
2. Porušení ustanovení této směrnice studentem bude považováno za disciplinární přestupek ve smyslu §64 zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), za nějž lze v souladu s citovaným zákonem a disciplinárním řádem SU uložit sankci podle §65 odst. 1 zákona č. 111/1998 Sb.
3. Porušení ustanovení této směrnice bude u zaměstnanců považováno za porušení základních povinností zaměstnance (§ 301 písm. c) a d) Zákoníku práce) a lze z něj vyvodit příslušné pracovně-právní důsledky včetně rozvázání pracovního poměru.
4. Porušení pravidel protivirové ochrany, zejména pak svévolné vypnutí této ochrany s následným zavirováním počítače či počítačů sítě SU bude vždy posuzováno jako závažné porušení pracovní kázně.

IX.

Závěrečná ustanovení

1. Tato směrnice nabývá účinnosti dnem vydání.
2. Tato směrnice ruší směrnici rektora č. 17/2004.
3. Kontrolou dodržování těchto pravidel a jejich bližším výkladem pověřuji příslušné správce sítě SU.
4. Každý správce sítě má právo vydat interní směrnice a nařízení, kterými zpřísní, konkretizuje či upřesní ustanovení této směrnice vztahující se na konkrétní pracoviště.

V Opavě dne 13. 9. 2011

Prof. PhDr. Rudolf Žáček, Dr.

rektor

Název účetní jednotky:	Slezská univerzita v Opavě
Označení:	**Směrnice rektora**
Číslo:	**13/2011**
Název normy:	**Pravidla užívání počítačové sítě Slezské univerzity**
Schvaluje:	Ing. Jaroslav Kania
Derogace:	Směrnice rektora č. 17/2004
Platnost:	13.9.2011
Datum vydání:	13.9.2011
Vydává:	rektor
Zpracoval:	Mgr. Nosek
Spolupracoval:	
Počet stran:	6
Počet příloh:	