SBÍRKA ROZHODNUTÍ A OPATŘENÍ
JIHOČESKÉ UNIVERZITY V ČESKÝCH BUDĚJOVICÍCH

Číslo: R 95 *datum: 23. listopadu 2007*

Opatření rektora JU
o užívání počítačů, počítačové sítě a software
na Jihočeské univerzitě v Českých Budějovicích

Toto opatření vychází ze současně platné legislativy ČR, zejména pak ze zákona č. 121/2000 Sb., autorský zákon, ve znění pozdějších předpisů.

I. Základní ustanovení

1. Toto opatření se vztahuje na všechny uživatele výpočetní techniky (počítačů, terminálů, komunikačních serverů a jiných zařízení) provozované na Jihočeské univerzitě v Českých Budějovicích (dále JU) a jeho předmětem jsou:
   a) Pravidla pro užívání počítačů v počítačové síti JU,
   b) Pravidla užívání software na počítačích JU.

2. Práva a povinnosti uživatelů jsou dále upraveny specifickými pravidly platnými na jednotlivých pracovištích a v síti vysokoškolských kolejí.

3. Pod pojmem *počítačová síť* nebo pouze *síť* se v těchto pravidlech rozumí souhrn technických a programových prostředků potřebných k propojení počítačů. Termín *počítačové prostředky* bude dále označovat počítače připojené i nepřipojené do sítě, počítačovou síť nebo obojí. *Uživatelem* se rozumí každý, kdo těchto počítačových prostředků používá.

4. Správu infrastruktury páteřní počítačové sítě JU vykonává Akademické počítačové středisko JU (dále APS).

5. *Odpovědnými pracovníky* se budou dále rozumět osoby, které jsou pověřeny správou počítačových prostředků na některé fakultě či jiném pracovišti JU. Dále uvedené kompetence jsou u každého odpovědného pracovníka omezeny na počítačové prostředky provozované na tomto pracovišti. Odpovědní pracovníci jsou zároveň styčnými osobami pro komunikaci uživatelů tohoto pracoviště se správou sítě.

II. Přístup na počítačové prostředky

1. Všechny počítače zapojené v síti podléhají registraci v databázi vedené a udržované APS.

2. Okruh oprávněných uživatelů každého počítačového prostředku a způsob jeho užívání stanoví vlastník tohoto prostředku, který je přitom povinen respektovat toto opatření, každého oprávněného uživatele s ním seznámit a zajistit jeho dodržování. Obecně mají k počítačovým prostředkům přístup pouze zaměstnanci a studenti JU. Výjimky schvaluje písemně a předem vedoucí příslušného pracoviště JU (katedry apod.), kde má být cizímu

uživateli umožněn přístup. Všichni oprávnění uživatelé musí být zaregistrováni v databázi vedené a udržované APS.

3. Počítačové prostředky, které umožňují přístup ze vzdáleného terminálu, musí být řádně zabezpečeny pomocí spolehlivých hesel. Je nutné se vyvarovat hesel, která jsou jednoduchým způsobem odvozena ze známých osobních údajů uživatele, jakož i samostatných slov používaných v kterémkoliv běžném jazyce. Minimální délka hesla je šest znaků, pokud aspoň jeden z nich není písmenem, anebo osm písmen.

4. Počítačové prostředky, které přístup ze vzdáleného terminálu neumožňují a nemají ochranu pomocí hesla, musí jejich majitel řádně fyzicky zabezpečit proti zneužití.

5. Mechanismus delegovaného ověřování totožnosti, tj. přístup z jednoho počítače na jiný bez zadávání hesla, je povolen výhradně prostřednictvím některé z robustních metod ověřování totožnosti (např. SSH, Kerberos). Je **zakázano** používat tímto způsobem nezabezpečené programy a protokoly typu *rlogin*, *rsh* apod.

6. Terminálový přístup oprávněných uživatelů z externích sítí do počítačové sítě JU je možný pouze jedním z těchto způsobů:
   i. pomocí programu se šifrovaným přenosem autentifikačních údajů a dat (např. VPN koncentrátor, *Secure shell* - SSH) na kterýkoliv server, kde má uživatel zřízen účet. Uživatel je přitom povinen zajistit, aby jeho heslo nebylo v otevřené (nešifrované) formě přenášeno v cizích počítačových sítích. V případě jakékoliv pochybnosti je uživatel povinen postupovat způsobem ii.
   ii. pomocí standardního programu (např. *telnet*) pouze na vyhrazené přístupové servery, a to pomocí mechanismu *jednorázových hesel*.

III. Práva a povinnosti uživatele

1. Uživatel smí používat počítačové prostředky v rámci své pracovní náplně a **v souladu s výzkumným a vzdělávacím posláním** JU. Je zakázáno používat počítačovou síť ke komerčním účelům (inzerce, školení, poskytování informací, programů a dat ze sítě za úplatu apod.). Výjimku může písemně povolit rektor JU. Dále je zakázáno využívat počítačové prostředky a síť v rozporu s autorským zákonem k pořizování a šíření nelegálních kopií autorských děl (např. software, publikací, CD disků a podobně).

2. Je zakázáno vystavovat na serverech pro WWW, FTP či jiné obdobné služby materiály, jejichž obsah je v rozporu se zákony, je nemravný anebo má charakter politické, náboženské či jiné obdobné agitace. Stejně tak je zakázáno využívat elektronickou poštu, konference *Usenet News* apod. k šíření informací tohoto typu.

3. Pro používání elektronické pošty (e-mailu) platí stejná etická pravidla jako pro obyčejnou poštu, přičemž elektronická poštovní zpráva má charakter otevřené listovní zásilky. Uživatel je povinen dbát na to, aby jeho zprávy byly přesně adresované a nedocházelo k obtěžování ostatních uživatelů.

4. Uživatelské účty jsou výhradně individuální. Uživatel tedy pracuje na počítačových prostředcích pouze pod tím uživatelským jménem, které mu bylo přiděleno. Heslo ke svému uživatelskému jménu volí dle výše uvedených zásad a udržuje je v tajnosti.

5. Jestliže uživatel nebude z jakýchkoliv důvodů moci po dobu delší než jeden měsíc pracovat na počítačových prostředcích, na nichž má uživatelský účet, je povinen toto oznámit příslušnému odpovědnému pracovníkovi. Po dobu absence bude účet zablokován.

6. Uživatel odpovídá v plném rozsahu za škody, vzniklé v důsledku zneužití jeho uživatelského účtu, pokud je umožnil vlastním nedbalým zacházením s účtem nebo heslem.

7. Uživatel se nesmí žádným způsobem pokoušet získat přístupová práva nebo privilegovaný stav, který mu nebyl přidělen odpovědným pracovníkem. Jestliže uživatel získá jakýmkoliv způsobem (vinou hardwarové nebo softwarové chyby systému, nedbalostí jiného uživatele apod.) uživatelská práva nebo privilegovaný stav, o nichž se může domnívat, že mu nepříslušejí, je povinen tuto skutečnost neprodleně oznámit odpovědnému pracovníkovi nebo APS. Tato povinnost se vztahuje rovněž na všechny externí počítače a počítačové sítě, ke kterým uživatel získá přístup prostřednictvím počítačových prostředků v síti JU.

8. Uživatel je rovněž povinen neprodleně uvědomit odpovědného pracovníka nebo APS v případě důvodného podezření, že někdo neoprávněně využívá jeho účtu nebo jiných privilegií.

9. Uživatel nesmí vytvářet, vědomě používat a šířit počítačové viry a jiné podobné programy, které mohou poškodit jiné uživatele nebo počítačové prostředky včetně externích. K tomu je uživatel povinen provádět antivirovou kontrolu souborů, zejména před jejich odesláním do elektronické konference. Rovněž je zakázáno používat programy pro odhalování nebo odposlech uživatelských hesel. Odpovědní pracovníci a APS však mohou takové programy používat pro účely kontroly kvality hesel na počítačových prostředcích v rámci své působnosti.

10. Uživatel nesmí vědomě narušovat práci ostatních uživatelů sítě ani chod a výkonnost sítě jako celku nadměrným zatěžováním počítačových prostředků nebo kterýmkoliv jiným způsobem.

11. Uživatel je povinen dodržovat pravidla, která platí na prostředcích jiných sítí, k nimž získá přístup prostřednictvím sítě JU.

12. Uživatel nesmí svévolně měnit konfiguraci počítačových prostředků připojených do sítě způsobem, který by mohl negativně ovlivnit provoz počítačové sítě. Všechny podobné zásahy do konfigurace je třeba předem projednat s odpovědným pracovníkem.

IV. Povinnosti a práva odpovědných pracovníků a APS

1. APS a odpovědní pracovníci zajišťují provozuschopnost počítačové sítě JU, monitorují její stav a koordinují její rozvoj. Správa sítě rovněž organizuje školení odpovědných pracovníků a vydává metodické materiály pro uživatele a odpovědné pracovníky.

2. APS může podle potřeby monitorovat datový provoz v síti JU. Účelem monitorování je optimalizace provozu počítačových prostředků, zjišťování abnormálních stavů a prevence proti nim a odhalování pokusů o neoprávněné využití počítačových prostředků. **Každý, kdo používá počítačové prostředky JU, vyjadřuje souhlas s takovým monitorováním.**

Pokud monitorování odhalí nepovolenou aktivitu, může být záznam monitorování poskytnut jako podklad pro vyšetřování, disciplinární nebo trestní řízení. Jinak jsou záznamy získané monitorováním důvěrné.

3. Změny v topologii a architektuře sítě provádějí výhradně odpovědní pracovníci a APS. Fyzické připojení jednotlivých počítačových prostředků k existující síti se smí provádět pouze s vědomím správy sítě nebo příslušného odpovědného pracovníka.

4. V případě poruchy na síti, která negativně ovlivňují ostatní uživatele nebo počítačové prostředky, má odpovědný pracovník nebo APS právo odpojit segment sítě, na němž poruchy vznikají, a to na dobu nezbytně nutnou k odstranění závady. O příčinách a postupu odstraňování závad je správa sítě povinna bez zbytečného prodlení informovat dotčený okruh uživatelů.

V. Pravidla užívání software na počítačích JU

1. **Počítačový software je chráněn autorským zákonem** (zákon č. 121/2000 Sb., ve znění pozdějších předpisů) a mezinárodními dohodami o autorských právech. Autorský zákon chrání, mimo jiné, práva držitele autorských práv k softwaru a zaručuje mu řadu exkluzivních práv včetně práva kopírovat software. **Kopírování softwaru bez povolení držitele autorských práv** vyjádřeného licenčním ujednáním **je nezákonné** a kdo se takto proviní, **vystavuje se možnosti zákonného postihu.**
   Kopie softwaru vzniká:
   a) nahráním software do operační paměti počítače při spuštění programu z disku,
   b) kopírováním (instalováním) software na pevný disk vašeho počítače,
   c) spuštěním programu na vašem počítači ze síťového serveru, na kterém je uložen nebo instalován,
   d) vytvořením záložní (archivní) kopie softwaru.
   Autorský zákon povoluje všechny kopie, principiálně nutné k užívání softwaru (např. jeho přenesení do paměti počítače), stejně tak jako případně i záložní (archivní) kopie. Jakákoliv další kopie (např. na druhém počítači) je však již nezákonná, není-li vysloveně povolena držitelem autorských práv.

2. **Užívání softwarových produktů podléhá** kromě autorského zákona i **uživatelské licenční smlouvě** (end user license agreement). Různé produkty mají různé typy licenčních smluv. Smlouva povoluje používat software, zaručuje další práva, ale stanovuje i jistá omezení. Začíná úvodní sekcí Grant of License, která popisuje, jak je možno software používat. Ve smlouvě jsou i jistá omezení týkající se půjčování softwaru, jeho případného dekódování a používání druhé kopie, je-li dodáván na dvou různých médiích. Smlouva obsahuje rovněž omezené záruky za software.

3. Licence také může stanovit pravidla, podle kterých lze současně využívat některé softwarové produkty v počítačové síti. Současné užívání přichází v úvahu pouze u aplikací, nevztahuje se na operační systémy, programovací jazyky a hry. Současné užívání nastává, když jedna kopie, umístěná na síťovém serveru, je používána dvěma nebo více pracovními stanicemi (počítači) v této síti. V tomto případě je rozhodující počet zakoupených licencí pro určení maximálního počtu uživatelů, kteří současně mohou se síťovým softwarem legálně pracovat. Kopie na serveru se nezapočítává do celkového počtu, protože je využívána pracovními stanicemi připojenými k serveru, nikoliv serverem samotným.

4. Licence také většinou dává právo pořídit si a používat za určitých podmínek druhou kopii produktu na domácím nebo přenosném počítači. Toto právo ale musí být v licenční smlouvě k softwaru výslovně uvedeno. Nevztahuje se to však na produkty, které jsou nainstalovány pouze na síťovém serveru a na systémové prostředky.

5. Obsahuje-li softwarový produkt software na dvou různých médiích (diskety, CD-ROM), je možné použít pouze jedno médium vhodné pro jeden určený počítač. Není možné použít druhé médium na jiném počítači ani na počítačové síti, ani je půjčit nebo přenechat jinému uživateli za podmínek uvedených v licenčním ujednání.

6. Je-li na počítači několik verzí téhož produktu (např. anglickou a českou), musí být uživatel vlastníkem licencí pro každou z použitých verzí. Podobně při aktualizaci produktu na novou verzi (upgrade) se platnou licenční smlouvou stává nová smlouva, doprovázející aktualizovanou verzi (upgrade). S každou další aktualizací uživatel dostane novou licenční smlouvu. Tyto aktualizace (upgrady) tvoří celek se stávajícím produktem, protože z něho ke své funkci využívají mnoho komponentů. Starší verzi produktů nelze proto přenechat někomu jinému, neboť v případě potřeby je nutno doložit vlastnictví všech licencí. Platí to pro aktualizaci aplikací i operačních systémů. V případě, že místo aktualizace je zakoupena kompletní nová verze produktu, pak je možno starší verzi dát k dispozici jinému uživateli.

7. V případě práce s integrovanými produkty, obsahujícími více jednotlivých softwarů (např. Microsoft Office), je možno instalovat pouze celý produkt na jediný počítač, nelze tedy instalovat jednotlivé jeho části na jiné počítače. Uživatel vlastní pouze jedinou licenci na celý soubor, nikoliv více samostatných licencí.

8. V licenčních smlouvách na užívání programovacího jazyka se většinou zaručuje uživateli právo na kopírování a šíření programů vytvořených pomocí tohoto produktu. Podobně je upraveno i právo šíření uživatelem vytvořených tzv. run-time modulů (součástí programovacího jazyka, nutných k funkci vytvořené aplikace).

9. Uživatel zodpovídá za hmotné příslušenství každého softwaru pokud takové je a bylo uživateli předáno (média, manuály, originální obaly apod). Uživatel je povinen zejména média uschovat na takovém místě, aby nemohlo dojít k jejich zneužití a např. i vytvoření kopie bez jeho vědomí.

10. Ke každému počítači je vedena evidence legálně nainstalovaného a užívaného softwaru a hardwaru (tzv. pasport). Aktualizaci tohoto pasportu může provádět pouze osoba pověřená děkanem fakulty. Pracovník potvrdí svým podpisem na pasportu, že pasport je v den jeho převzetí aktuální a že bere opatření rektora o užívání počítačů, počítačové sítě a softwaru na vědomí.

VI. Postihy za nedodržení těchto pravidel

1. JU dbá na své dobré jméno a nebude tolerovat porušování autorských a licenčních práv a vystavovat se tak i nebezpečí trestního stíhání. Proto při porušení tohoto opatření může správa sítě nebo odpovědný pracovník pozastavit uživateli platnost jeho uživatelského účtu až do vyřešení případu.

2. Závažné nebo opakované porušení tohoto opatření bude považováno za hrubé porušení studijních nebo pracovních povinností a kázně se všemi důsledky z toho vyplývajícími, včetně výpovědi či vyloučení ze studia.

VII. Závěrečná ustanovení

1. Toto opatření nabývá platnosti dnem vyhlášení.

2. Zrušuje se Opatření rektora č. 107 z 29. 12. 2003.

prof. PhDr. Václav Bůžek, CSc.
rektor

Rozdělovník: děkanům a ředitelům všech součástí JU