Univerzita Hradec Králové
Fakulta informatiky a managementu

Provozní řád výpočetní techniky Fakulty informatiky a managementu Univerzity Hradec Králové

Září 2010

Obsah:

1. Účel

1.1. Opatření stanovuje jednotný způsob pro systematické zabezpečování a udržování výpočetní techniky na Fakultě informatiky a managementu Univerzity Hradec Králové (dále jen „FIM"). Popisuje postup, zásady zálohování, archivace, provádění antivirové prevence a popisuje požadavky, kladené na každého zaměstnance a studenta přicházejícího do styku s touto technikou.

1.2. Tento provozní řád se vztahuje na všechny uživatele počítačové sítě FIM a počítačů nebo obdobných zařízení, které jsou libovolnými prostředky přímo funkčně připojeny k počítačové síti FIM nebo jejím počítačům, i na uživatele výpočetní techniky FIM, která není k počítačové síti FIM připojená.

1.3. Při práci v počítačové síti je dodržování zásad zvláště důležité proto, aby činností jednoho uživatele nedocházelo k omezení ostatních uživatelů sítě nadbytečným vytěžováním síťových zdrojů a jejich neoprávněnému využívání.

2. Definice základních pojmů

Administrátor
Zaměstnanec Útvaru informačních systémů (dále jen „UIS") FIM, který je zodpovědný za chod počítačové sítě FIM nebo její části.

Archivace
Ukládání dat do uspořádaného systému na záložní nosiče dat a jejich doplnění o informace, umožňující identifikaci, zpětné vyhledání a použití archivovaných dat.

Centrum služeb FIM
Pracoviště vykonávající tyto činnosti: technická podpora a informace studentům, předávání nahlášených závad od studentů a zaměstnanců na oddělení ÚIS, odblokování uzamčených účtů, změny hesel studentům, tisk a kopírování s asistencí, pomoc při obsluze kopírky a tiskárny, příjem a odesílání faxů pro zaměstnance fakulty, pomoc při nastavování konfigurace wi-fi, dobíjení kreditu, pomoc při odevzdávání závěrečných kvalifikačních prací eVŠKP, kroužková vazba.

Home (domovský) adresář
Přidělený diskový prostor (P) na síti pro ukládání dat jednotlivých uživatelů.

HW
Hardware – technické prostředky pro sběr, zpracování, uchovávání a distribuci dat včetně jejich přenosu (např. PC, notebooky a další aktivní prvky počítačové sítě apod.).

Outsourcing
Zabezpečení služeb IS/IT externím dodavatelem.

PC
Osobní počítač (personal computer).

Počítačové viry
Virus je typ programu, který se dokáže sám šířit tím, že vytváří (někdy upravené) kopie sebe sama. Hlavním kritériem pro posouzení programu jako viru je fakt, že k šíření využívá jiné soubory – hostitele.

Server
Počítač poskytující zejména síťové služby klientským PC.

Síť
Počítačová síť, všechny technické i programové prostředky používané k propojení výpočetní techniky, včetně této výpočetní techniky.

Správce aplikace
Pracovník, který je zodpovědný za provozování SW aplikace. Je metodicky podřízený administrátorovi sítě.

SW
Software – programové vybavení (počítačový program s připojenou dokumentací a případně s připojenými daty, pokud jsou součástí dodávky):

a) standardní – šířený běžně prodejci,
b) nestandardní (individuální) – vytvořený na zakázku, testovací, řídící, údržbový apod.

SW licence
Oprávnění k výkonu práva užívat počítačový program podle licenční smlouvy.

Uživatel
Zaměstnanec nebo student, který má přístup k počítačové síti a počítačům nebo obdobným zařízením, která jsou libovolnými prostředky přímo funkčně připojená k počítačové síti nebo jejím počítačům, i k výpočetní technice, která není k počítačové síti připojená.

Uživatelský účet (konto)
Označení, které jednoznačně identifikuje uživatele v prostředí informačního systému. K tomuto označení jsou pak v systému přiřazeny další vlastnosti, specifické pro daného uživatele (základní informace o uživateli, postavení v organizační struktuře, nastavení jeho výpočetního prostředí, členství ve skupinách, přístupová práva apod.).

UIS
Útvar informačních systémů je organizační jednotka poskytující podporu uživatelů s důrazem především na serverové zdroje, infrastrukturu a služby spojené s informačními a komunikačními technologiemi. UIS systematicky zabezpečuje a rozvíjí výpočetní techniku na FIM.

VT
Výpočetní technika FIM (PC, notebooky, prvky sítě, tiskárny, scannery apod., včetně programového vybavení evidované v majetku FIM).

Zálohování
Pravidelné ukládání souborů na externí paměťové médium pro případ obnovy dat a programů.

3. Všeobecné informace

3.1. Správcem sítě je Útvar informačních systémů (UIS), který odpovídá za obsahové vymezení, rozvoj a bezpečný provoz informačního systému.
3.2. Síť se skládá z jednotlivých částí, které jsou vytvářeny podle lokalit budov.
3.3. Síť slouží výhradně k plnění pracovních úkolů zaměstnanců a studijních úkolů studentů.
3.4. Jednotlivé části sítě jsou spravovány zaměstnanci UIS nebo vybranou externí firmou na základě smlouvy (tzn. outsourcing).

4. Organizační struktura

Organizační struktura vyplývá ze Statutu Fakulty informatiky a managementu. UIS je řízen vedoucím UIS, v případě jeho nepřítomnosti jsou jeho pravomoci vykonávány tajemníkem UIS v rozsahu stanoveném jeho náplní práce. Organizační jednotkou UIS je Centrum služeb. Popis prací Centra služeb je dán výnosem děkana FIM.

5. Přidělování a evidence výpočetní techniky

5.1. VT na učebnách a UIS je přidělována a spravována Útvarem informačních systémů v souladu s opatřením o hospodaření s majetkem.
5.2. UIS provádí pouze údržbu VT kateder, opravy si hradí katedry a útvary FIM ze svého rozpočtu.
5.3. Převzetí VT do užívání stvrdí uživatel svým podpisem ve smlouvě o výpůjčce v oddělení evidence majetku.
5.4. VT mimo počítačové učebny a UIS je v inventáři příslušných místností a zodpovídá za ni určený správce místnosti.

6. Zakládání a rušení uživatelských účtů

6.1. Každý nově nastupující zaměstnanec je Osobním oddělením zaveden do příslušného informačního systému (Magion). Požadavek je následně předán do systému ISIT. Požadavek je následně zpracován navazujícími systémy, uživateli je vytvořen účet, založena e-mailová schránka a zřízen přístup k dalším síťovým zdrojům.
6.2. Osobní oddělení zadává požadavky na zrušení zaměstnaneckého konta v systému Magion. Požadavek je následně předán do systému ISIT. Konto je pak s časovým odstupem automaticky zrušeno.
6.3. Studijní oddělení zadává nové studenty do systému ISIT. V dalším kroku dochází k automatickému generování požadavku na založení účtů.
6.4. Administrátor sítě spravuje generování účtů, popř. řeší konflikty při vytváření účtů.
6.5. Studijní oddělení zadává požadavky na zrušení studentských kont v systému ISIT. Konto je následně po určitém čase automaticky zrušeno.
6.6. Každý zaměstnanec je při odchodu z Fakulty informatiky a managementu povinen řádně předat pracovní datové soubory vytvořené v průběhu jeho pracovní činnosti vedoucímu katedry, nebo sekretářce.
6.7. Každý zaměstnanec je při odchodu z Fakulty informatiky a managementu povinen řádně předat veškerou výpočetní techniku správci místnosti.

6.8. Ke dni skončení pracovního poměru končí platnost uživatelského účtu a přístupu do sítě UHK a platnost emailového účtu.

6.9. Datové soubory uložené na síti a e-mailové zprávy se stávají po odchodu zaměstnance a zrušení jeho přihlašovacího účtu k počítačové síti k datu jeho odchodu nedostupné.

6.10. Pro externí pracovníky a hosty, kteří nemají své osobní uživatelské konto, poskytuje Centrum služeb možnost propůjčení časově i funkčně omezeného konta, které bude aktivováno na základě předložení dokladu totožnosti (občanský průkaz, cestovní pas) a vyplněním příslušené žádosti s jasně vymezeným účelem, pro které se dané konto uživateli poskytuje.

7. Instalace aplikací

7.1. UIS provádí evidenci a kontrolu SW instalovaného na FIM. Cílem je zajistit užívání počítačových programů výlučně oprávněnými uživateli na základě licenčních smluv a zajistit důsledný soulad užívání počítačových programů s platnými právními předpisy ČR a příslušnými licenčními ujednáními, a respektovat zákonná práva nositelů autorských a průmyslových práv k jednotlivým softwarovým produktům.

7.2. Instalaci standardního SW na lokální stanici realizuje zpravidla pověřený zaměstnanec UIS.

7.3. Instalaci individuálního SW na lokální stanici realizuje autor nebo dodavatel ve spolupráci s pověřeným zaměstnancem UIS, popřípadě správcem aplikace. Součástí požadavku na instalaci individuálního SW musí smlouva a faktura na tento SW. Tyto dokumenty musí být uloženy u objednatele pro potřeby případné kontroly po celou dobu užívání software.

7.4. Podmínky licenční smlouvy SW na sebe bere každý uživatel při rozbalení obálky s instalačními medii (CD-ROM, DVD-ROM apod.), popř. při jejich prokazatelném převzetí v UIS.

8. Uživatelská podpora

8.1. Zaměstnanci předají veškeré požadavky na uživatelskou podporu prostřednictvím:

8.1.1. Aplikace Help-desku na adrese http://mhd.uhk.cz.

8.1.2. Centrum služeb na tel. čísle 49333 2234.

8.1.3. Telefonicky na tel. číslech (49333) 2223, 2226, 2228.

8.1.4. Osobně na UIS v kanceláři číslo 110.

8.2. Studenti předávají veškeré požadavky na uživatelskou podporu osobně na Centru služeb, kde bude jejich požadavek vyřízen, nebo budou instruováni k dalšímu postupu.

9. Údržba a opravy výpočetní techniky

9.1. UIS zajišťuje záruční a pozáruční servis VT, náhradní díly a spotřební materiál pro tuto techniku. UIS provádí průběžné čištění (vnější i vnitřní) prostředků VT. Současně s čištěním je prováděna i HW a SW pasportizace s následným odstraněním případného nelegálního SW, počítačových her a starého, již nepoužívaného SW. Zároveň jsou odstraňovány i skryté závady VT, které by mohli při jejich včasném neodstranění VT vážně poškodit.

9.2. Pověřený zaměstnanec Útvaru informačních systémů je oprávněn provádět zásahy a úpravy na jednotlivých PC a odstraňovat nelegální či nevhodný SW.

9.3. V případě, že uživatel zjistí závadu či podezřelé chování VT, ohlásí tuto okolnost ihned stejným postupem, jako požadavek na uživatelskou podporu. Je zakázáno, aby uživatelé VT prováděli na VT jakékoli zásahy, které nesouvisejí s běžnou obsluhou VT. Přípustné jsou jen ty zásahy, které předepisuje výrobce VT uživateli a pro které byl uživatel prokazatelně proškolen.

10. Přístupová práva k síti a identifikace uživatele

10.1. Přístup k síti předpokládá nutnost jednoznačné identifikace každého uživatele. S každým jednotlivým uživatelským účtem jsou spojena určitá přístupová práva, která rozhodujícím způsobem určují oprávnění uživatele ve vztahu ke zdrojům sítě.

10.2. Uživatel, kterému je uživatelský účet zřízen, je povinen zabezpečit svůj uživatelský účet netriviálním heslem a toto heslo udržovat v tajnosti. Heslo k vlastnímu (individuálnímu) uživatelskému účtu uživatel nesmí sdělit druhé osobě.

10.3. V případě potřeby přístupu k datům nepřítomných zaměstnanců je nutné zajistit písemný souhlas vedoucího příslušného útvaru k této operaci a kontaktovat zaměstnance Útvaru informačních systémů, kteří zajistí zpřístupnění dat žadateli.

10.4. Uživatel nesmí zpřístupnit svůj uživatelský účet jiným uživatelům počítačové sítě.

10.5. Uživatel nesmí zneužít nedbalosti jiného uživatele (např. opomenuté odhlášení) k tomu, abych v síti pracoval pod cizí identitou.

10.6. Uživatel smí používat pouze přístupová práva, která mu řádným způsobem náleží a nesmí vyvíjet žádnou činnost směřující k obejití tohoto ustanovení. Pokud uživatel jakýmkoliv způsobem získá přístupová práva, která mu nebyla přidělena (např. chybou programu nebo technického vybavení), je povinen tuto skutečnost neprodleně oznámit administrátorovi sítě. Takto získaná práva nesmí použít.

11. Zásady pro práci s hesly

Mezi zabezpečení síťových prostředků patří zavedení přísných zásad pro hesla. Kromě samotného hesla prosazujeme zásady používání hesel, které zahrnují:

11.1. Pravidelné změny hesla (každých 90 dní).

11.2. Minimální délku hesla (nejméně 8 znaků).

11.3. Požadavek na složitost hesla:

11.3.1. Heslo nesmí obsahovat celé, nebo část přihlašovacího jména.

11.3.2. Heslo musí obsahovat znaky z alespoň tří následujících kategorií:

11.3.2.1. Velká písmena anglické abecedy (A..Z).

11.3.2.2. Malá písmena anglické abecedy (a..z).

11.3.2.3. Číslice (0..9).

11.4. Historii hesla (systém uživateli nedovolí při změně použít heslo již použité – pamatuje si 5 minulých hesel).

11.5. Uzamčení účtu (po 5 chybných pokusech o přihlášení).

11.6. Dobu trvání uzamčení (30 minut).

12. Přístupová práva k Internetu a dalším externím sítím

12.1. Přidělování přístupových práv je omezeno provozními možnostmi sítě. Schvalovat přístup jednotlivých uživatelů do sítě Internet a dalších externích sítí je v pravomoci vedoucího UIS. Možnosti přístupu k Internetu jsou pro všechny uživatele, kterým byla přidělena přístupová práva, kvalitativně stejné.

12.2. Technickými prostředky může být blokován přístup na nežádoucí zdroje. V případě, že jsou blokovány zdroje nezbytné pro pracovní činnost, je možno požádat správce sítě o uvolnění konkrétní zdrojů. Je nepřípustné stahování obsahu z webových stránek s nežádoucím obsahem (erotické, vulgární, propagující nenávist, politickou, náboženskou a rasovou agitaci, dále pak software, audio a video soubory chráněné autorským zákonem) a to i v případě, že stahování obsahu není blokováno síťovými prostředky. Je zakázáno hraní počítačových her. Provoz sítě je z bezpečnostních důvodů (napadení sítě atd.) monitorován. Lze tedy vyhledat důkazy o činnosti uživatelů až na úroveň PC, na kterém se tato činnost vykonávala.

13. Pravidla pro komunikaci v síti

Při komunikaci v síti i s jinými sítěmi je uživatel povinen dodržovat následující pravidla:

13.1. Je zakázáno používat vulgárních a silně emotivních výrazů při komunikaci otevřené dalším účastníkům (chat, diskusní skupiny, news, ...).

13.2. Je zakázáno používat síť pro politickou, náboženskou a rasovou agitaci.

13.3. Je zakázáno využívat elektronických prostředků (především elektronické pošty) k obtěžování nebo zastrašování jiných uživatelů. Do této kategorie spadá i rozesílání řetězových dopisů či e-mailových zpráv na náhodně vybrané adresy v síti.

13.4. Je zakázáno zneužívat elektronickou poštu k reklamním a jiným účelům, sloužícím k získání osobního prospěchu.

13.5. Je zakázáno využívat VT k páchání trestných činů.

13.6. Je zakázáno používat VT k činnostem namířeným proti jakékoliv další organizaci, jejíž počítačové prostředky jsou dostupné prostřednictvím počítačové sítě.

13.7. Uživatel sítě je povinen dodržovat, 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 s UIS a řídit se jeho pokyny.

13.8. Využívání sítě v rámci spolupráce se zaměstnanci jiných organizací je možné na základě souhlasu UIS. V případě, že se jedná o dlouhodobější vztah, je nezbytné konkrétní podmínky využívání sítě, včetně případných sankčních opatření, specifikovat ve smlouvě mezi FIM a organizací, jejíž pracovníci využívají naší sítě.

13.9. Velikost přílohy elektronické pošty by neměla přesáhnout 5 MB u studentů a 10 MB u zaměstnanců. UIS si vyhrazuje právo systémově omezit velikost příloh a blokování nebezpečného obsahu (např. nebudou doručovány zavirované soubory).

13.10. Uživatel není oprávněn využívat nedovoleným způsobem data systému, systémy a sítě nebo neoprávněně zkoušet, zkoumat či testovat zranitelnost systému nebo sítí.

13.11. Uživateli není dovoleno porušovat bezpečnostní opatření a ověřovací procedury klientských stanic, serverů a na nich provozovaných aplikací.

14. Vlastnická práva

14.1. Uživatelé využívají VT ve shodě se svými pracovními úkoly. Efektivní plnění pracovních 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 než elektronické podobě.

14.2. Všechny prvky sítě jsou vlastnictvím UHK, případně k nim FIM vlastní či vykonává práva užívání; nepřípustnost krádeže a vandalismu (poškození) se pak vztahuje na elektronickou podobu dat a informací stejně jako na vlastní fyzické prostředky.

14.3. Uživatelé VT nesmí jakýmkoliv způsobem dále šířit (a to ani bezúplatně) jakýkoliv SW, který je součástí počítačové sítě FIM. SW se může používat a šířit pouze v souladu s licenčními podmínkami pro daný typ SW.

Je proto dále zakázáno:

14.3.1. Neautorizované kopírování SW i jeho částí a kopírování dat, k nimž FIM vykonává vlastnická práva, resp. práva k užívání.

14.3.2. Neautorizovaná modifikace SW nebo dat v majetku či užívání FIM.

14.3.3. Vědomě využívat nelegální SW a data, případně takovýto SW či data nabízet jiným osobám.

14.3.4. Používat síť k získání neautorizovaného přístupu k neveřejným informačním zdrojům (i v majetku/správě jiných organizací).

15. Ochrana dat a informací

15.1. UIS chrání (v souladu se zákonem č. 101/2000 Sb., o ochraně osobních údajů ve znění pozdějších předpisů), občanská, osobní i vlastnická práva všech uživatelů sítě a v této souvislosti chrání soukromí dat a informací uložených na VT nebo přenášených sítí. FIM nemůže technicky zabezpečit úplné soukromí a bezpečnost dat uložených na PC nebo přenášených počítačovou sítí. Vysoce citlivá data a individuální statistické údaje proto nemohou být na PC uložena bez použití dodatečných prostředků jejich zabezpečení (minimálně na úrovni šifrování).

15.2. Správci a zpracovatelé datových souborů, na něž se vztahují ustanovení zákona č. 101/2000 Sb., o ochraně osobních údajů, jsou plně odpovědní za obsah a ochranu těchto datových souborů před zneužitím jakož i za plnění veškerých dalších ustanovení tohoto zákona, vyplývajících pro oblast zpracování osobních údajů, včetně oznamovací povinnosti dle §16 zákona.

15.3. Pro zajištění maximální možné míry soukromí a bezpečnosti dat je uživatelům dále zakázáno:

15.3.1. Provádět jakékoli akce, které vedou k narušení soukromí jiného uživatele, a to i případech, kdy uživatel svá vlastní data explicitně nechrání.

15.3.2. Kopírovat jakákoliv data nebo programy z uživatelských adresářů bez souhlasu jejich majitele (to zahrnuje i samotné prohlížení těchto adresářů).

15.3.3. Používat síť k získání neautorizovaného přístupu k neveřejným informačním zdrojům (i v majetku/správě jiných organizací).

16. Antivirová ochrana

16.1. V síti je nainstalován antivirový program, který zabezpečuje antivirovou kontrolu souborů PC, sítě a zpráv elektronické pošty, včetně jejich příloh. Program vytváří na každém PC rezidentní štít, který brání vniknutí a šíření viru do PC. Antivirová databáze je po síti průběžně aktualizována. Uživatele nesmí přerušovat aktualizaci antivirového prostředku a jsou povinni se řídit pokyny antivirového programu, především pokynu pro opětovné spuštění (restart) PC.

16.2. Je důležité dodržovat pravidla antivirové prevence:

16.2.1. Nespouštět SW s nejasným či neznámým původem.

16.2.2. Používat jen legální SW odsouhlasený Útvarem informačních systémů.

16.2.3. PC podezřelý z infikování virem nesmí být do odstranění viru dále používán.

17. Zálohování a archivace dat

17.1. Smyslem zálohování a archivace dat je vytvoření bezpečnostních kopií souborů na záložní nosič dat.

17.2. Z uživatelského hlediska jsou pravidelně silami UIS zálohována zejména data v přiděleném domovském (disk P) adresáři na síti, obsah schránek elektronické pošty. Tato záloha je prováděna v pravidelných intervalech dle zálohovacího plánu a délka uchování zálohy je popsána na webu FIM v sekci návody a rady. V případě potřeby je možno požádat administrátora sítě v příslušné lokalitě o individuální obnovu dat (např. při ztrátě v důsledku chyby ze strany uživatele). Za zařazení aplikací odborných útvarů do zálohovacího plánu odpovídají příslušní odborní garanti.

17.3. Lokální disky PC (zejména disk C:) nejsou primárně určeny pro ukládání dat. V případě takto nestandardně uložených dat přechází povinnost zálohování výhradně na osobu uživatele, který je povinen zabezpečit zálohování vlastními prostředky (záloha na vysokokapacitní média, externí disky, popř. kopie dat na síti). Za takto umístěná data nenese UIS odpovědnost.

18. Další povinnosti uživatelů výpočetní techniky

Uživatelé VT jsou dále povinni:

18.1. Používat svěřené prostředky VT pouze k plnění svých pracovních povinností a v souladu s účelem, ke kterému byly určeny.

18.2. Pracovat s VT tak, aby ji nepoškodili, zejména mechanicky.

18.3. Nepřemísťovat VT, neměnit konfiguraci PC či jiných prostředků VT, nerozpojovat kabely a neprovádět technické úpravy na VT.

18.4. Uchovávat veškeré převzaté doklady k nainstalovanému SW a HW.

18.5. Zamezit cizím osobám přístup k VT.

18.6. Při přerušení práce se ztrátou dohledu nad PC (i při krátkodobém opuštění pracoviště) je uživatel povinen dostatečným způsobem zabránit neoprávněnému použití PC, například odhlášením z PC, nebo standardním ukončením práce. Zaměstnanci mají možnost uzamčení PC pomocí kláves ALT+CTRL+DEL s volbou "Uzamknout počítač".

18.7. Důsledně dodržovat pravidla antivirové prevence.

18.8. Důsledně zálohovat, popřípadě archivovat, veškerá data, pokud nejsou uživateli uložena na centrálních zálohovacích prostředcích.

18.9. Uživatelé VT nesou odpovědnost za obsahovou správnost jimi vytvořených dat.

19. **Povinnosti administrátorů sítě**

Administrátoři sítě jsou v rozsahu svých oprávnění odpovědni za řádný chod počítačové sítě nebo jejich částí a zabezpečují zejména:

19.1. Monitorování provozu počítačové sítě a kontrolu stavu serverů sítě a síťových prvků včetně zálohovacího systému. Pravidelnou kontrolu systémových zpráv (tzv. logů).

19.2. Provádění pravidelné kontroly využití diskových prostorů jednotlivých serverů a zabezpečují potřebná nápravná opatření.

19.3. Dohled nad generováním uživatelských účtů.

19.4. Vedení provozní dokumentace.

19.5. Administrátor sítě je oprávněn monitorovat činnosti uživatelů spravované sítě v mezích, které neohrožují 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 zjištění porušení pravidel provozu sítě je povinen s touto skutečností seznámit odpovědného zaměstnance (vedoucího UIS).

19.6. Administrátor sítě je zároveň správcem VT v části sítě, kterou má ve své správě. Dbá o to, aby jejím provozem nebyl omezován nebo dokonce poškozován provoz sítě. V případě naléhavé potřeby může administrátor sítě požádat uživatele o přerušení práce v síti na dobu nutnou pro zásah do sítě nebo instalaci SW a uživatelé jsou povinni mu v maximální možné míře vyhovět.

19.7. Administrátor sítě je oprávněn odpojit VT, na níž byla provedena změna konfigurace síťového SW.

19.8. Administrátor sítě je oprávněn stanovit další závazná pravidla, upravující specifické činnosti v částech sítě (specifikace serveru, komunikační protokoly, míra otevřenosti některých síťových služeb apod.).

20. Sankce

20.1. Administrátor má právo přerušit přístup k síti uživatelům, kteří prokazatelně porušili ustanovení tohoto řádu, a to na dobu do vyřešení tohoto případu.

20.2. Porušení povinností, kladených na uživatele v jednotlivých ustanoveních Provozní řádu výpočetní techniky, bude považováno za porušení pracovní kázně resp. disciplinárního řádu UHK.

V Hradci Králové dne 15. 9. 2010

doc. Ing. Václav Janeček, CSc.
děkan
Fakulty informatiky a managementu
Univerzity Hradec Králové