Univerzita Hradec Králové

Provozní řád informačních a komunikačních technologií Univerzity Hradec Králové

doc. Mgr. Petr Grulich, Ph.D.,
prorektor pro vnitřní záležitosti

30. června 2016

Obsah

1. Úvodní ustanovení

1.1. Provozní řád informačních a komunikačních technologií Univerzity Hradec Králové (dále jen „provozní řád ICT UHK“) stanovuje pravidla pro používání informačních a komunikačních technologií Univerzity Hradec Králové. Vztahuje se na všechny uživatele ICT využívající možností a prostředků počítačové sítě a služeb ICT provozovaných Univerzitou Hradec Králové.

1.2. Správu počítačové sítě a informačních a komunikačních technologií provozovaných v rámci jednotlivých součástí Univerzity Hradec Králové zajišťuje Centrum informačních technologií UHK (dále jen „CIT“). CIT poskytuje podporu uživatelů, provozuje a systematicky rozvíjí serverovou i síťovou infrastrukturu UHK, zabezpečuje provoz výpočetní techniky pro koncové uživatele. CIT zajišťuje konzultace spojené s výběrem a způsobem provozu vhodných informačních a komunikačních technologií v rámci celouniverzitních i fakultních projektů. CIT provádí technický a metodologický dohled nad centrálně poskytovanými lokálními serverovými službami a nad využíváním služeb externích poskytovatelů informačních technologií (IT).

2. Základní pojmy

Centrum služeb UHK

Pracoviště, které vykonává činnosti související se základní technickou podporou uživatelů na celouniverzitní úrovni.

Cloudová řešení

Služby nebo programy provozované na serverech externích poskytovatelů služeb IT mimo infrastrukturu UHK, případně cloudová řešení provozovaná uvnitř organizace (např. služby Office 365, e-infrastruktura CESNET).

Hardware (HW)

Technické prostředky pro sběr, zpracování, uchovávání a distribuci dat, včetně jejich přenosu (např. PC, notebooky a další prvky počítačové sítě apod.)

ICT (informační a komunikační technologie)

Hardware a software (servery, osobní počítače, notebooky, chytré telefony, tablety, prvky komunikační sítě, datová úložiště, tiskárny, scannery, audiovizuální technika, aplikace apod.) evidovaný v majetku UHK.

PC

Osobní počítač (Personal Computer) na učebnách, v kancelářích a společných prostorách UHK.

Počítačová síť

Technické i programové prostředky používané k propojení výpočetní techniky, včetně této výpočetní techniky.

Server

Fyzické nebo virtualizované zařízení poskytující síťové a aplikační služby klientským zařízením a uživatelům.

Správce aplikace

Pracovník, který je zodpovědný za provozování SW aplikace. Je metodicky podřízený správci ICT.

Správce ICT

Zaměstnanec CIT, který je zodpovědný za chod počítačové sítě nebo výpočetní techniky (servery, počítače, periferie, multimédia a aktivní prvky) na UHK.

Software (SW)

Programové vybavení provozované v rámci ICT.

SW licence

Oprávnění k výkonu práva užívat počítačový program podle licenční smlouvy.

Uživatel

Zaměstnanec, student nebo externí uživatel, který má přístup k počítačové síti a počítačům nebo obdobným zařízením provozovaných v lokalitách UHK.

Uživatelský účet (konto)

Označení, které jednoznačně identifikuje uživatele v prostředí počítačové sítě. 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.)

Zálohování

Pravidelné ukládání dat na externí paměťová média pro případ obnovy.

3. Agendy Centra informačních technologií

3.1. Podpora uživatelů

Uživatelé ICT UHK předávají veškeré požadavky na uživatelskou podporu prostřednictvím:

- aplikace IT Helpdesk,
- elektronickou poštou prostřednictvím e-mailové adresy,
- Centra služeb UHK,
- telefonicky nebo osobně na pracovištích Úseku podpory koncových uživatelů CIT,
- objednávkového listu – v případě požadavku na technické zajištění zvukařské a projekční techniky, případně fotografických prací pro výukové, odborné a společenské akce.

Kontakty na technickou podporu a informace o provozovaných službách IT jsou uvedeny na webových stránkách UHK (www.uhk.cz) v sekcích Poradna IT a CIT.

3.2. Správa a evidence ICT, serverové a síťové infrastruktury

3.2.1. CIT zajišťuje správu, evidenci a rozvoj ICT, serverové infrastruktury a páteřní sítě UHK.

3.2.2. CIT provádí údržbu ICT jednotlivých pracovišť. Opravy si hradí pracoviště UHK (katedry a útvary) ze svého rozpočtu.

3.2.3. Převzetí ICT do užívání stvrdí uživatel svým podpisem v předávacím protokolu.

3.2.4. Za ICT mimo správu CIT je zodpovědný její vlastník nebo pověřený správce.

3.2.5. CIT provádí pravidelnou údržbu a aktualizace instalovaných operačních systémů a aplikací. CIT administrativně zajišťuje HW a SW podporu provozovaných řešení u dodavatelů.

3.3. Serverové a ostatní služby

3.3.1. Centrálně poskytované služby

CIT zajišťuje celouniverzitní standardní serverové služby. Podrobnější informace o poskytovaných službách jsou v aktuálních verzích k dispozici na oficiálních webových stránkách UHK v sekci Poradna IT.

Primární IT služby centrálně poskytované CIT

- Správa serverů a síťové infrastruktury (DNS, DHCP, síťové a bezpečnostní prvky apod.)
- Správa doménových uživatelských účtů.
- Správa adresářových a autentizačních služeb (LDAP, federované služby).
- Správa poštovních služeb (základní poštovní infrastruktura pro UHK).
- Správa serverů pro provoz virtualizace.
- Správa souborových služeb a systémů ukládání dat v rámci sítě UHK.
- Správa databázových serverů pro centrálně provozované systémy.
- Správa serverů studijní evidence.
- Správa serverů pro podporu e-learningu.
- Správa webové prezentace UHK a vybraných webových aplikací.
- Správa knihovních systémů.
- Správa spisové služby.
- Správa ekonomických systémů.
- Správa celouniverzitně poskytovaných cloudových služeb.
- Správa telefonních a mobilních služeb.
- Správa serverů pro podporu síťového tisku.
- Správa zálohovacích systémů.
- Konzultační činnosti v oblasti služeb ICT.
- Správa dohledových a bezpečnostních systémů.
- Správa hardware, software, konfigurace zařízení ICT.
- Správa a instalace příslušenství prostředků zařízení ICT.
- Zajištění uživatelské podpory při práci s informačními systémy UHK.
- Příprava, koordinace a zpracování technických specifikací pro výběrová řízení.
- Profylaxe multimediálního vybavení.

3.3.2. <u>služby IT pro projekty a podporu výuky</u>

CIT poskytuje další služby pro projekty a podporu výuky na základě jasně vymezených oboustranných dohod s žadatelem. V dohodě jsou definovány role, odpovědnosti a rozsah činností každé ze stran. Pokud projektové záležitosti budou zasahovat do nákladů CIT, je při plánování projektu třeba počítat s prostředky na realizaci, provozní a personální zajištění. Jedná se zejména o tyto služby:

- Správa aplikačních serverů pro výuku nad rámec běžně provozovaných služeb.
- Správa webových serverů, případně správa a rozvoj webových aplikací.
- Správa cloudových služeb pro studium a projektové využití.
- Ostatní služby ICT a správa dle individuální dohody.

3.4. Spolupráce na univerzitních a fakultních projektech

3.4.1. CIT zajišťuje pro projekty, které mají vazbu na celouniverzitní infrastrukturu ICT, konzultační služby s cílem společně navrhnout taková řešení, která budou kompatibilní s provozovanými součástmi infrastruktury a v souladu s konceptem rozvoje ICT UHK. CIT doporučuje, aby řešitel projektu navrhoval technická řešení v souladu s celouniverzitní koncepcí ICT a bylo tak zajištěno efektivní vynakládání finančních prostředků na pořízení a provoz ICT.

3.4.2. Projekty, které nejsou celouniverzitní povahy a přinášejí náklady a požadavky nad rámec běžných služeb poskytovaných CIT, jsou posuzovány individuálně. V případě dohody na spolupráci v rámci projektu bude sepsán protokol vymezující detaily požadavku, konkrétní podmínky, časové termíny trvání projektu, pravomoci a odpovědnosti obou stran dohody. K akceptaci realizace projektu je nutný souhlas žadatele s pravidly vztahujícími se k požadované službě.

3.5. Registrace domén

3.5.1. CIT primárně zajišťuje registraci doménových jmen třetího řádu pro doménu uhk.cz.

3.5.2. V případě registrace nebo potřeby použití jiné domény v rámci ICT služeb je bezpodmínečně nutné, aby vlastníkem této domény byla Univerzita Hradec Králové. Pokud je doména vlastněna jiným subjektem, není možné

s ní spojovat žádné oficiální služby provozované jménem univerzity. Správce domény, která je v majetku UHK, je povinen udržovat aktuální kontaktní údaje u registrované domény a v případě odchodu z organizace provést změnu správce domény.

3.6. Zakládání a rušení uživatelských účtů

3.6.1. Každý nově nastupující zaměstnanec je personálním oddělením zaveden do příslušného informačního systému. Požadavek je následně předán do systému pro správu identit a zpracován navazujícími systémy. Uživateli je vytvořen účet pro přístup k prostředkům ICT, založena e-mailová schránka a zřízen přístup k dalším síťovým zdrojům.

3.6.2. Personální oddělení zadává požadavky na zrušení zaměstnaneckého účtu v informačním systému. Požadavek je následně předán do systému pro správu identit. Uživatelský účet a s ním spojená data je pak s časovým odstupem automaticky zrušen.

3.6.3. Dokumenty, emailové zprávy a ostatní data v elektronické podobě uložené na prostředcích ICT, včetně dat uložených v rámci cloudových řešení, se stávají po odchodu zaměstnance a zrušení jeho uživatelského účtu v počítačové síti trvale nedostupnými.

3.6.4. Každý zaměstnanec je při ukončení pracovního poměru na UHK povinen řádně předat veškeré prostředky ICT v majetku UHK pověřenému správci majetku.

3.6.5. Každý zaměstnanec je při ukončení pracovního poměru na UHK povinen řádně předat pracovní data svému vedoucímu pracovníkovi.

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

3.6.7. Studijní oddělení zadávají nové studenty do studijního informačního systému. V dalším kroku dochází k automatickému generování požadavku na založení účtů v systému pro správu identit.

3.6.8. Studijní oddělení zadává požadavky na zrušení studentských uživatelských účtů ve studijním informačním systému. Uživatelský účet je pak s časovým odstupem automaticky zrušen prostřednictvím systému pro správu identit.

3.6.9. Pro externí pracovníky a hosty, kteří nemají svůj osobní uživatelský účet, nabízí Centrum služeb UHK možnost propůjčení časově i funkčně omezeného uživatelského účtu.

3.7. Instalace software

3.7.1. CIT provádí evidenci a kontrolu SW instalovaného v rámci ICT UHK, který má ve své správě. Na prostředcích ICT UHK je dovoleno používat jen legální SW. Instalaci SW na lokální počítač realizuje pověřený pracovník CIT, případně autor nebo dodavatel SW ve spolupráci s pověřeným pracovníkem CIT nebo pověřený správce aplikace. Součástí požadavku na instalaci individuálního komerčního SW musí být smlouva a faktura na tento SW. Tyto dokumenty musí být uloženy u objednatele pro potřeby případné kontroly po celou dobu užívání software.

3.7.2. V případě instalace komerčního SW či bezplatného a volně šiřitelného SW uživatel přijímá podmínky licenční smlouvy daného SW. Uživatel musí SW používat v souladu s licenčními ujednáními.

3.8. Údržba a opravy hardware a software

3.8.1. CIT zajišťuje záruční a pozáruční servis HW a SW, profylaxi ICT, náhradní díly a spotřební materiál pro techniku ve správě CIT.

3.8.2. Pověřený pracovník CIT je oprávněn provádět zásahy a úpravy na jednotlivých prostředcích ICT UHK a odstraňovat z nich případný nelegální SW.

3.8.3. V případě, že uživatel zjistí závadu či podezřelé chování ICT, ohlásí tuto skutečnost ihned uživatelské podpoře CIT. Uživatelé ICT nejsou oprávněni samostatně provádět jakékoliv zásahy do svěřených prostředků ICT, které nesouvisejí s jejich běžnou obsluhou. Přípustné jsou jen ty zásahy, které jsou v souladu s provozním řádem ICT, popř. byly bezprostředně dohodnuty s odpovědným správcem ICT.

3.9. Zajištění technického vybavení pro výukové, odborné a společenské akce

3.9.1. CIT zajišťuje po technické stránce přípravu zvukařské a projekční techniky, včetně fotografických prací při výukových, odborných a společenských akcích na UHK.

3.9.2. Žádost na technické zajištění se podává prostřednictvím formuláře, který je umístěn na webových stránkách UHK v sekci CIT.

3.9.3. Po převzetí požadavku je s objednavatelem upřesněn konkrétní rozsah služeb dle technických a personálních možností CIT.

4. Přístupová práva k síti a identifikace uživatele

4.1. 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.

4.2. Uživatel je povinen zabezpečit svůj uživatelský účet heslem a toto heslo udržovat v tajnosti a nesdělovat jiné osobě.

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

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

4.5. Uživatel smí používat pouze přístupová práva, která mu řádným způsobem náleží a nesmí vyvíjet žádnou činnost směřující k obejití tohoto ustanovení. Pokud uživatel jakýmkoli způsobem získá přístupová práva, která mu nebyla přidělena (např. chybou programu nebo technického vybavení), je povinen tuto skutečnost neprodleně oznámit správci ICT.

4.6. Uživatel musí dodržovat podmínky pro tvorbu hesel, které jsou uvedeny v aktuální verzi na webových stránkách UHK v sekci Poradna IT.

5. Přístupová práva k Internetu a dalším externím sítím

5.1. Přidělování přístupových práv je omezeno provozními možnostmi počítačové sítě. Schvalovat přístup k blokovaným zdrojům v rámci sítě Internet a dalších externích počítačových sítí je v pravomoci vedoucího CIT. Seznam aktuálně povolených portů je k dispozici na oficiálních webových stránkách UHK v sekci Poradna IT.

5.2. Technickými prostředky může být blokován přístup na nežádoucí zdroje v rámci sítě Internet. V případě, že jsou blokovány zdroje nezbytné pro pracovní nebo studijní činnost na UHK, je možnost požádat pověřeného správce ICT o uvolnění konkrétních zdrojů. Je nepřípustné stahování obsahu z webových stránek s nežádoucím obsahem (erotické, vulgární, propagující nenávist, politickou, náboženskou a rasovou agitaci, dále pak nelegálně poskytovaný software a multimediální soubory chráněné autorským zákonem) a to i v případě, že stahování obsahu není blokováno síťovými prostředky.

6. Pravidla pro komunikaci v síti

6.1. E-mailová adresa a schránka je studentovi zřízena jako součást síťového účtu při zahájení studia, pracovníkovi je zřízena při nástupu do pracovního poměru. Studenti i pracovníci jsou povinni ve vzájemné studijní a pracovní komunikaci těchto adres užívat.

6.2. Pracovníci i studenti jsou povinni pravidelně kontrolovat obsah schránky elektronické pošty a schránku udržovat funkční. Důsledky plynoucí z případného nepřijetí informace (např. pro přeplnění schránky) nese v plné míře adresát.

6.3. Je zakázáno používat vulgárních a silně emotivních výrazů při komunikaci otevřené dalším účastníkům (e-mail, chat, diskusní skupiny, sociální sítě a jiné).

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

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

6.6. Je zakázáno zneužívat elektronickou poštu k reklamním a jiným účelům, sloužícím k získání osobního prospěchu. CIT si vyhrazuje právo systémově omezit doručování zpráv s charakteristikou nevyžádané pošty (spam) a blokovat nebezpečný obsah v elektronické poště (např. nebudou doručovány zavirované soubory).

6.7. Je zakázáno využívat ICT k páchání trestných činů.

6.8. Je zakázáno používat ICT k činnostem namířeným proti jakékoli další organizaci, jejíž počítačové prostředky jsou dostupné prostřednictvím počítačové sítě.

6.9. Uživatel počítačové sítě nesmí provádět takové činnosti, které by negativně ovlivňovaly možnosti využití počítačových prostředků dalšími uživateli. To se týká jak neúměrného zatěžování linek a provozovaných systémů, tak i neúměrného zatěžování jednotlivých počítačů a serverů. Uživatel není oprávněn zkoušet, zkoumat či testovat zranitelnost systému nebo sítí. Pokud by se jednalo o činnost spojenou s výukou, je třeba takovéto činnosti předem konzultovat s CIT a řídit se jeho pokyny.

6.10. Využívání vnitřní počítačové sítě v rámci spolupráce se studenty a zaměstnanci jiných škol a organizací je možné na základě souhlasu CIT. V případě, že se jedná o dlouhodobější vztah, je nezbytné konkrétní podmínky využívání počítačové sítě, včetně případných sankčních opatření,

specifikovat ve smlouvě mezi UHK a organizací, jejíž pracovníci nebo studenti využívají počítačovou síť UHK.

6.11. Provoz počítačové sítě je z bezpečnostních důvodů (napadení sítě atd.) monitorován. Tyto údaje jsou využívány pro statistické účely a pro potřeby řešení bezpečnostních incidentů.

7. Vlastnická práva

7.1. Uživatelé využívají ICT ve shodě se svými pracovními či studijními úkoly a respektují vlastnická práva k datům v elektronické podobě. Uživatelé se řídí stejnými etickými i zákonnými normami jako při nakládání s objekty a informacemi v jiné než elektronické podobě.

7.2. SW se může používat a šířit pouze v souladu s licenčními podmínkami pro daný SW. Je proto dále zakázáno:

- Neautorizované kopírování SW i jeho částí a kopírování dat, k nimž UHK vykonává vlastnická práva, resp. práva k užívání.
- Neautorizovaná modifikace SW nebo dat v majetku či užívání UHK.
- Vědomě využívat nelegální SW a data, případně takový SW či data nabízet jiným osobám.
- Používat počítačovou síť k získání neautorizovaného přístupu k neveřejným informačním zdrojům (i v majetku/správě jiných organizací).

7.3. Uživatel nese plnou odpovědnost za obsah veškerých dat, textů, vizuálních děl či jejich částí určených uživatelem k uveřejnění prostřednictvím prostředků ICT nebo síťových úložišť.

8. Ochrana dat a informací

8.1. CIT 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 prostředcích ICT UHK nebo přenášených sítí UHK.

8.2. 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.

8.3. Pro zajištění maximální možné míry soukromí a bezpečnosti dat je uživatelům zakázáno:
- Provádět jakékoli akce, které vedou k narušení soukromí jiného uživatele, a to i v případech, kdy uživatel svá vlastní data explicitně nechrání.
- Kopírovat jakákoli data nebo programy z uživatelských adresářů bez souhlasu jejich majitele (to zahrnuje i samotné prohlížení těchto adresářů).
- Používat síť k získání neautorizovaného přístupu k neveřejným informačním zdrojům (i v majetku/správě jiných organizací).

9. Antivirová ochrana

9.1. V síti je nainstalován antivirový program, který zabezpečuje antivirovou kontrolu souborů uložených na koncových zařízeních ICT UHK, antivirovou kontrolu sítě a zpráv elektronické pošty, včetně jejich příloh. Program vytváří na každém koncovém zařízení ICT UHK rezidentní štít, který brání vniknutí a šíření viru do zařízení. Antivirová databáze je po síti průběžně aktualizována.

9.2. Je důležité dodržovat pravidla antivirové prevence, např. nespouštět SW s nejasným či neznámým původem. Zařízení ICT podezřelé z infikování virem nesmí být do odstranění viru dále používáno. V případě podezření na bezpečnostní hrozbu je uživatel povinen kontaktovat pověřeného pracovníka CIT.

10. Zálohování dat

10.1. Smyslem zálohování dat je vytvoření bezpečnostních kopií pracovních dat na záložní nosiče dat.

10.2. Pověřenými pracovníky CIT jsou pravidelně zálohována data v přiděleném domovském adresáři, v adresáři s webovou prezentací a ve složce pro projekty umístěné na sdíleném síťovém disku. Tato záloha je prováděna v pravidelných intervalech dle zálohovacího plánu. CIT si vyhrazuje právo na změnu zálohovacích plánů. V případě potřeby je možno požádat pověřeného správce ICT o individuální obnovu dat.

10.3. V případě ukládání dat do jiných síťových umístění nebo na lokální úložiště koncových zařízení ICT UHK přechází odpovědnost zálohování na osobu uživatele. Uživatel má možnost zabezpečit zálohování vlastními prostředky (záloha na vysokokapacitní média, externí disky, zálohované síťové disky,

cloudové služby, např. prostředí Office 365 a prostředí datových úložišť CESNET).

10.4. Žádost o zařazení ostatních systémů a dat do zálohovacího plánu podávají pověření správci systémů a aplikací nebo jejich garanti (v případě realizace studentských projektů). Žádost bude posouzena pověřenými pracovníky CIT podle technických možností aktuálního zálohovacího řešení.

11. Další povinnosti uživatelů ICT UHK

11.1. Uživatel je povinen používat svěřené prostředky ICT pouze k plnění pracovních povinností a v souladu s účelem, ke kterému byly určeny.

11.2. Uživatel je povinen pracovat s prostředky ICT tak, aby je nedošlo k jejich poškození.

11.3. Uživatel není oprávněn na učebnách přemísťovat prostředky ICT, měnit konfiguraci zde instalovaných počítačů či jiných prostředků ICT, rozpojovat kabely a provádět jiné technické úpravy na těchto prostředcích ICT.

11.4. Uživatel je povinen uchovávat veškeré doklady ke svěřenému SW a HW.

11.5. Uživatel je povinen zamezit neoprávněným osobám v přístupu k prostředkům ICT UHK.

11.6. Při přerušení práce se ztrátou dohledu nad svěřenými prostředky ICT (i při krátkodobém opuštění pracoviště) je uživatel povinen dostatečným způsobem zabránit neoprávněnému použití těchto odhlášením z relace operačního systému popř. jiným způsobem.

12. Bezpečnostní opatření a sankce

12.1. Správce ICT je oprávněn přerušit přístup k síti uživatelům, kteří prokazatelně porušili ustanovení tohoto řádu, na dobu do vyřešení případu.

12.2. Správce ICT je oprávněn přerušit přístup zařízení ICT k síti UHK nebo odpojit zařízení ICT z počítačové sítě, pokud v důsledku neautorizovaných změn do zařízení ze strany uživatele nebo v důsledku instalace škodlivého software došlo k takové změně konfigurace zařízení ICT, které ohrožuje bezpečnost sítě UHK nebo jinak narušuje její provoz.

12.3. Úmyslné nebo opakované porušení pravidel provozního řádu ICT UHK může být považováno za porušení povinností vyplývajících z pracovní smlouvy, z předpisů vztahujících se k vykonávané práci (porušení pracovní kázně) nebo z disciplinárního řádu pro studenty UHK.