Univerzita Hradec Králové

Provozní řád informačních a komunikačních technologií Univerzity Hradec Králové

Obsah

ČÁST PRVNÍ

Článek 1

Úvodní ustanovení

1) Provozní řád informačních a komunikačních technologií Univerzity Hradec Králové stanovuje pravidla pro používání prostředků informačních a komunikačních technologií (dále jen *„ICT“*) v prostředí Univerzity Hradec Králové (dále jen *„UHK“*).

2) Prostředky ICT zahrnují veškeré hardwarové (dále jen *„HW“*) a softwarové (dále jen *„SW”*) vybavení, včetně serverů, osobních počítačů, notebooků, mobilních telefonů, tabletů, datových úložišť, tiskáren, skenerů, audiovizuální techniky, tokenů, síťových prvků, zařízení internetu věcí (IoT), operačních systémů, informačních systémů a aplikací, cloudových řešení a elektronicky zpracovaných informací a dat.

3) Uživatel ICT UHK (dále jen *„uživatel“*) je definován jako zaměstnanec, student, externí osoba nebo systém, který má přístup k ICT UHK. Povinnost dodržovat tento provozní řád ICT UHK se vztahuje na všechny uživatele.

Článek 2

Základní uživatelská pravidla

1) Uživatel je povinen dodržovat ustanovení tohoto provozního řádu a dalších bezpečnostních a právních dokumentů, jako jsou bezpečnostní politiky, výnosy, směrnice a pokyny stanovené UHK. Rovněž je povinen respektovat legislativu kybernetické bezpečnosti jako je Zákon o kybernetické bezpečnosti č. 181/2014 Sb., ve znění pozdějších předpisů, a související vyhlášky.

2) Uživatel je povinen chránit své přístupové údaje a neposkytovat je žádným třetím osobám. Dále je povinen zajistit, aby důvěrné informace (přihlašovací údaje, tiskové výstupy, otevřené dokumenty v informačních systémech, přístupové tokeny apod.) nebyly přístupné neautorizovaným osobám. Při přerušení práce, které má za následek ztrátu dohledu nad svěřenými prostředky ICT, je uživatel povinen řádně zabezpečit tyto prostředky ICT odhlášením z relace operačního systému nebo jiným vhodným způsobem.

3) Uživatel je povinen dodržovat pravidla pro tvorbu hesel, která jsou stanovena v aktuálně platné verzi na oficiálních webových stránkách UHK.

4) Přístup ke klíčovým informačním systémům a aplikacím je podmíněn autentizací prostřednictvím vícefaktorového ověřování. Vícefaktorová autentizace uživatelů je definována samostatným Rektorským výnosem.

5) Uživatel nesmí využít nedbalosti jiného uživatele, například opomenutého odhlášení, k tomu, aby v počítačové síti jednal pod cizí identitou.

6) Uživatel je povinen používat pouze legální a schválené prostředky ICT v souladu s licenčními a právními předpisy. Uživatel je povinen uchovávat veškerou dokumentaci týkající se přiděleného SW a HW. Je zakázáno neoprávněné kopírování nebo modifikování SW nebo dat, která jsou ve vlastnictví či užívání UHK.

7) Uživatel má zakázáno připojovat a používat prostředky ICT pocházející z neschválených, neznámých nebo nedůvěryhodných zdrojů (např. nalezená nebo distribuovaná paměťová média, jako jsou USB disky, kompaktní disky, síťová zařízení apod.).

8) Uživatel má zakázáno stahovat obsah z webových stránek s nevhodným nebo nelegálním obsahem, a to i v případě, že stahování obsahu není blokováno technickými prostředky sítě.

9) Uživatel je povinen využívat prostředky ICT způsobem, který nevede k jejich úmyslnému poškození. Uživatel není oprávněn přemisťovat prostředky ICT v učebnách, měnit jejich konfiguraci, rozpojovat kabely ani provádět jiné technické úpravy prostředků ICT.

10) Uživatel využívá prostředky ICT v souladu se svými pracovními nebo studijními povinnostmi a respektuje vlastnická práva k datům v elektronické podobě. Uživatel se řídí stejnými právními a etickými normami jako při nakládání s objekty a informacemi v jiné než elektronické podobě. Uživatel odpovídá za veškerý obsah dat, textů, vizuálních děl nebo jejich částí určených k uveřejnění prostřednictvím prostředků ICT.

11) Uživatel počítačové sítě nesmí provádět činnosti, které by mohly negativně ovlivnit provoz počítačové sítě UHK.

12) Uživatel je povinen pravidelně se vzdělávat v oblasti kybernetické bezpečnosti. Pravidla školení zaměstnanců v oblasti kybernetické bezpečnosti jsou upravena vnitřními předpisy a dokumenty bezpečnostních politik UHK.

ČÁST DRUHÁ

Článek 3

Uživatelské účty

1) Uživatelský účet slouží k přístupu do počítačové sítě UHK a uživatelské e-mailové schránce. Uživatelský účet je založen prostřednictvím systému správy identit na základě informací o platném studijním či zaměstnaneckém poměru k UHK, na základě činnosti ve vědeckých radách či orgánech UHK nebo na základě jiného smluvního vztahu s UHK.

2) Uživatelský účet a e-mailová schránka zaniká k datu ukončení pracovního poměru nebo studia, k datu ukončení činnosti ve vědeckých radách či orgánech UHK nebo k datu ukončení jiného smluvního vztahů s UHK. Uživatelský účet je následně s časovým odstupem automaticky zrušen prostřednictvím systému pro správu identit, včetně všech dat spojených s tímto účtem.

3) Po zániku uživatelského účtu se všechny dokumenty, e-mailové zprávy a ostatní údaje uložené v prostředcích ICT, včetně dat uložených v rámci cloudových řešení, stávají trvale nedostupnými.

4) Pro externí pracovníky a hosty, kteří nemají zřízen osobní uživatelský účet, je k dispozici možnost propůjčení uživatelského účtu s časově a funkčně omezenou platností. Pro správu prostředků ICT může být zřízen servisní účet.

Článek 4

Oprávnění uživatelských účtů

1) Přístup k prostředkům ICT vyžaduje jednoznačnou identifikaci každého uživatele. S každým uživatelským účtem jsou spojena příslušná přístupová práva, která určují oprávnění uživatele ve vztahu k prostředkům ICT.

2) Uživatel je oprávněn využívat pouze přístupová práva, která mu byla řádně přidělena. Uživatel je povinen zdržet se jakéhokoli jednání směřujícího k obcházení tohoto ustanovení. V případě, že uživatel jakýmkoli způsobem získá přístupová práva, která mu nebyla přidělena, je povinen tuto skutečnost neprodleně oznámit pracovníkovi Oddělení informačních technologií (dále jen *„OIT“*).

3) Požadavek uživatele na vyšší přístupová práva k prostředkům ICT, která jsou nad rámec přidělených přístupových práv, podléhá schválení OIT. Uživatel je povinen tento požadavek řádně odůvodnit. V případě schválení požadavku je uživatel povinen podepsat prohlášení o přidělení vyšších přístupových práv. Uživatel má odpovědnost za bezpečnostní rizika spojená s těmito právy.

ČÁST TŘETÍ

Článek 5

Provoz v počítačové síti UHK

1) Technickými prostředky lze omezit přístup k portům nebo zdrojům v síti internet. Schvalování přístupu k portům nebo zdrojům je v kompetenci OIT. Pokud jsou určité porty nebo zdroje blokovány, může uživatel požádat OIT o jejich uvolnění. Seznam povolených portů je dostupný na oficiálních webových stránkách UHK.

2) Využívání vnitřní počítačové sítě v rámci spolupráce se studenty a zaměstnanci jiných škol a organizací je možné pouze na základě předchozího souhlasu OIT. Jedná-li se o dlouhodobější vztah, je nezbytné, aby podmínky využívání počítačové sítě, včetně případných sankčních opatření, byly specifikovány ve smlouvě uzavřené mezi UHK a příslušnou organizací, jejíž zaměstnanci nebo studenti využívají počítačovou síť UHK.

3) Z bezpečnostních důvodů je veškerý provoz počítačové sítě monitorován. Tyto údaje jsou využívány pro statistické účely a k řešení bezpečnostních incidentů.

Článek 6

Elektronická pošta a komunikace v prostředí UHK

1) Zaměstnancům je e-mailová adresa a schránka zřízena při nástupu do pracovního poměru. Studentům je e-mailová adresa a schránka zřízena při zahájení studia. Zaměstnanci i studenti jsou povinni ve vzájemné pracovní a studijní komunikaci užívat výhradně těchto adres a schránek.

2) Uživatel je povinen pravidelně kontrolovat obsah přidělených schránek elektronické pošty, zajistit jejich funkčnost a nese veškeré důsledky vyplývající z nepřijetí informací, například z důvodu přeplnění schránky.

3) Uživatel je povinen udržovat kapacitu přidělených e-mailových schránek a sdílených úložišť v mezích stanovených kvótami. Velikost těchto kvót je specifikována na oficiálních webových stránkách UHK.

4) Uživatel je povinen dodržovat pravidla etikety e-mailové komunikace. Je zakázáno používat vulgární a silně emotivní výrazy při komunikaci prostřednictvím e-mailu, chatu, diskusních skupin, sociálních sítí a jiných veřejně přístupných komunikačních platforem. Je zakázáno používání elektronických prostředků komunikace k obtěžování uživatelů šířením nevyžádaných nebo obchodních zpráv.

ČÁST ČTVRTÁ

Článek 7

Ochrana dat a informací

1) Ochrana dat a informací probíhá v souladu se Zákonem č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů.

2) Správci a zpracovatelé dat, údajů a informací, na které se vztahují ustanovení Zákona o zpracování osobních údajů, nesou plnou odpovědnost za jejich obsah a za zabezpečení proti zneužití, jakož i za dodržování všech ostatních příslušných ustanovení tohoto zákona.

3) Z důvodu zajištění maximální úrovně soukromí a bezpečnosti dat je zakázáno provádět následující činnosti:

   - Provádění jakýchkoli akcí, které vedou k narušení soukromí jiného uživatele, a to i v případech, kdy uživatel svá vlastní data výslovně nechrání.
   - Kopírování obsahu uživatelských složek bez souhlasu jejich majitele, včetně samotného prohlížení těchto složek.
   - Využívání počítačové sítě k získání neoprávněného přístupu k neveřejným informačním zdrojům, včetně těch, které mohou být ve vlastnictví nebo správě jiných organizací.

4) Z důvodu ochrany pracovních dat a důvěrných či utajovaných informací je zakázáno přesměrování pracovních e-mailových schránek na externí a soukromé e-mailové schránky. Je zakázáno posílat pracovní data, důvěrné a utajované informace prostřednictvím externích a soukromých e-mailových schránek.

5) Je zakázáno kopírovat a přenášet pracovní data, důvěrné a utajované informace pomocí soukromých datových úložišť, kopírovacích a tiskových zařízení. Je zakázáno předávat data, důvěrné a utajované informace prostřednictvím veřejných internetových služeb pro sdílení souborů, které nejsou oficiálně podporovány UHK, z důvodu rizika neoprávněného přístupu k citlivým dokumentům, smlouvám a datům UHK.

6) V případech stanovených zákonem, vnitřními předpisy nebo z jiného závažného důvodu může být poskytnut přístup k e-mailové schránce a k datům v prostředcích ICT. Tento přístup je možný pouze na základě písemného soudního nařízení nebo písemného rozhodnutí s odůvodněním děkana příslušné fakulty, rektora nebo kvestora UHK. Zaměstnavatel je povinen informovat zaměstnance, jehož data mají být zpřístupněna, o důvodech a rozsahu přístupu. Zpřístupnění dat je možné i v případě ověření doručení rozhodnutí prostřednictvím informačního systému dle platné legislativy.

7) Prostředky ICT jsou chráněny antivirovým programem. Je zakázán jakýkoli zásah do činnosti antivirového programu při kontrole systému. Uživatel je povinen dodržovat pravidla prevence, například neotevírat soubory z nejasných nebo neznámých zdrojů. Zařízení ICT, u kterých je podezření na virovou nákazu, nesmějí být používána až do odstranění škodlivých souborů. V případě podezření na bezpečnostní hrozbu je uživatel povinen informovat OIT.

8) Uživatel je oprávněn vytvářet záložní kopie pracovních dat výhradně na datová úložiště ve vlastnictví UHK nebo využít cloudové služby, které jsou UHK smluvně poskytovány třetími stranami. Uživatel je povinen dodržovat aktuální bezpečnostní zásady a používat šifrování dat.

9) Návrh na zařazení systémů a dat do zálohovacího plánu předkládají pověření správci systémů a aplikací nebo jejich garanti. Data uložená v cloudových službách a úložištích nejsou zálohována prostřednictvím interních zálohovacích systémů. Návrh na zálohování posoudí OIT s ohledem na technické a kapacitní možnosti aktuálního zálohovacího řešení.

10) Při ukončení pracovního poměru je každý zaměstnanec povinen řádně předat pracovní data svému nadřízenému.

ČÁST PÁTÁ

Článek 8

Správa a evidence ICT UHK

1) Prostředky ICT v majetku UHK určené pro výkon pracovní činnosti jsou evidovány v ekonomickém informačním systému.

2) OIT zajišťuje správu HW a SW vybavení, případně externí servis, profylaxi ICT, náhradní díly a spotřební materiál výhradně pro techniku v majetku UHK.

3) Náklady na opravy, upgrade SW, technické rozšíření, spotřební materiál hradí uživatel nebo příslušné pracoviště UHK z vlastního rozpočtu.

4) Uživatel nesmí blokovat ani jinak omezovat vzdálený přístup za účelem zajištění správy prostředků ICT.

5) V případě, že byly prostředky ICT pořízeny bez předchozí konzultace s OIT, má OIT právo odmítnout převzetí takového prostředku ICT do své správy a odmítnout jeho integraci do provozní infrastruktury z důvodu bezpečnostního rizika, nekompatibility, zvýšených nároků na správu či nepřiměřených nákladů na připojení nebo údržbu.

6) V případě, že uživatel zjistí závadu nebo podezřelé chování prostředku ICT, je povinen tuto skutečnost neprodleně nahlásit OIT. Uživatelé nejsou oprávněni provádět jakékoliv zásahy do svěřených prostředků ICT, které nesouvisí s jejich běžnou obsluhou, bez předchozího schválení OIT. Přípustné jsou pouze zásahy v souladu s provozním řádem ICT UHK.

7) Zařízení ve vlastnictví uživatele (BYOD) může být k infrastruktuře UHK připojeno pouze za podmínky, že budou technickými prostředky vynucována pravidla pro zajištění ochrany univerzitní infrastruktury a dat. Uživatel je povinen zajistit, aby připojované zařízení splňovalo požadavky na bezpečnost, pravidelné aktualizace, SW ochranu a nástroje eliminující rizika šíření škodlivého SW (viry, malware, ransomware apod.). Uživatel je rovněž odpovědný za nainstalovaný SW a dodržování licenčních podmínek. OIT nenese odpovědnost za stav zařízení BYOD.

8) Uživatel je povinen při ukončení pracovního poměru řádně předat veškeré svěřené prostředky ICT v majetku UHK pracovníkovi pověřenému správou tohoto majetku nebo svému přímému nadřízenému.

ČÁST ŠESTÁ

Článek 9

Služby poskytované OIT UHK

1) Centrálně poskytované služby

a) OIT zajišťuje centrální síťové a serverové služby. Provozuje a systematicky rozvíjí serverovou a síťovou infrastrukturu UHK, zabezpečuje provoz a údržbu prostředků ICT UHK. OIT poskytuje konzultace spojené s výběrem a způsobem provozu vhodných ICT v rámci celouniverzitních i fakultních projektů. OIT provádí technický a metodologický dohled nad centrálně poskytovanými lokálními serverovými službami a nad využíváním služeb externích poskytovatelů ICT. Financování správy centrálně poskytovaných ICT a služeb je hrazeno ze samostatného rozpočtu, kde příkazcem je vedoucí OIT.

b) OIT zajišťuje IT podporu uživatelů. Uživatelé ICT UHK předávají veškeré požadavky na uživatelskou podporu prostřednictvím:

- aplikace IT Helpdesk,
- elektronické pošty prostřednictvím univerzitní e-mailové adresy,
- Centra služeb UHK,
- telefonicky nebo osobně na pracovištích Úseku podpory koncových uživatelů,
- objednávkového listu (Evidence požadavků na technické zajištění akcí), v případě požadavku na technické zajištění zvukařské, projekční techniky, případně fotografických prací pro výukové, odborné a společenské akce.

2) Spolupráce na projektech

a) OIT poskytuje konzultační služby pro projekty, které se vztahují k celouniverzitní ICT infrastruktuře, s cílem společně navrhnout řešení kompatibilní s provozovanými součástmi infrastruktury a v souladu s kompatibilitou ICT UHK. OIT doporučuje, aby řešitel projektu navrhoval technická řešení v kompatibilní s provozovaným ICT, čímž bude zajištěno efektivní využití finančních prostředků na pořízení a provoz ICT.

b) Projekty, které představují náklady a požadavky přesahující běžné služby poskytované OIT, jsou posuzovány individuálně. Poskytnutí spolupráce na projektech je závislé na technických a personálních kapacitách OIT. V případě, že projektové záležitosti přinášejí náklady pro OIT, je při plánování projektu nutné zahrnout prostředky na realizaci, provoz a personální zajištění. V případě dohody o spolupráci na projektu bude sepsán protokol vymezující detaily požadavku, konkrétní podmínky, časové termíny trvání projektu, pověřené správce systémů a aplikací, pravomoci a odpovědnosti obou stran dohody. K akceptaci realizace projektu je nutný souhlas žadatele s pravidly vztahujícími se k požadované službě. Případné náklady spojené se zapojením nových řešení do provozní infrastruktury hradí vždy objednatel služby.

c) Pověřený správce systémů a aplikací je zodpovědný za provoz svěřených systémů v souladu s provozním řádem ICT UHK. Zajišťuje také ochranu dat, informací a osobních údajů a řídí se pokyny OIT.

3) IT Služby pro podporu digitalizace procesů

a) OIT poskytuje služby pro podporu digitalizace procesů na základě sběru požadavků, jejich prioritizace dle shody jednotlivých organizačních součástí UHK a stanovení realizace požadavků kolegiem rektora. Jedná se o služby:

- Analýza aktuálních procesů ve všech organizačních složkách.
- Návrh jednotného digitalizovaného procesu.
- Podpora výběru vhodného SW řešení.
- Podpora při integraci systémů.
- Tvorba uživatelské dokumentace pro interních aplikace.
- Podpora během uživatelského testování a akceptace řešení.
- Školení koncových uživatelů.
- Ověření implementace řešení z hlediska podpory daného procesu.

b) Pro zařazení požadavku mezi žádosti určené k digitalizaci musí být ke každému požadavku na digitalizaci procesu dodány následující informace:

- Podrobný popis požadavku zahrnující požadované cíle (důvody a očekávané přínosy).
- Garant nebo vlastník procesu.
- Osoba projektového manažera.
- Zodpovědná osoba za proces zajišťující metodiku.

c) V případě, že je k požadavku přiložena kompletní analýza a návrh sjednoceného digitalizovaného procesu, musí požadavek obsahovat:

- Cíle a očekávané výstupy.
- Rizika a kritická místa.
- Požadované termíny realizace.
- Požadavky na spolupráci s dalšími útvary organizace a externími subjekty.
- Očekávané investiční a neinvestiční náklady.
- Požadované rozdělení rolí a odpovědností všech zúčastněných stran.

d) Náklady na implementaci nového SW řešení jsou plně v gesci garanta procesu. Pokud tyto náklady zasahují do rozpočtů spravovaných OIT, je nezbytné při plánování projektu zahrnout nové jednorázové prostředky na realizaci, ale i následné náklady na provozní a personální zajištění pro zajištění udržitelnosti.

4) Registrace domén

a) OIT zajišťuje registraci doménových jmen třetího řádu pro doménu uhk.cz.

b) V případě potřeby registrace nebo využití jiné domény je nezbytné, aby vlastníkem dané domény byla UHK. Pokud je doména vlastněna jiným subjektem, není povoleno s ní spojovat žádné oficiální služby provozované jménem UHK. Správce domény, která je ve vlastnictví UHK, je povinen udržovat aktuální kontaktní údaje u registrované domény a v případě odchodu z organizace provést aktualizaci kontaktních údajů na nového správce domény.

5) Instalace SW

a) Instalaci SW provádí OIT, případně dodavatel SW nebo pověřený správce systémů a aplikací ve spolupráci s OIT. Součástí požadavku na instalaci individuálního komerčního SW musí být smlouva a faktura za tento SW. Tyto dokumenty musí být uloženy u objednatele pro potřeby případné kontroly po celou dobu užívání SW.

b) V případě instalace SW uživatel přijímá podmínky licenční smlouvy daného SW. Uživatel je povinen používat SW v souladu s licenční smlouvou. OIT je oprávněno odstraňovat případný nelegální SW nebo SW používaný v rozporu s licenční smlouvou.

6) Zajištění technického vybavení pro výukové, odborné a společenské akce

a) OIT zajišťuje technickou podporu a přípravu audiovizuální techniky pro výukové, odborné a společenské akce na UHK v rámci svých technických a kapacitních možností.

b) Žádost o technické zajištění je nutné podat prostřednictvím formuláře, který je dostupný na oficiálních webových stránkách UHK. Po obdržení požadavku je s objednavatelem specifikován konkrétní rozsah služeb. Poskytnutí služeb je závislé na technických a personálních kapacitách OIT.

7) Energetická náročnost prostředků ICT

OIT spolupracuje na snižování energetické náročnosti prostředků ICT prostřednictvím optimalizace HW a SW, a to především v procesu výběrových řízení na dodávku ICT.

ČÁST SEDMÁ

Článek 10

Bezpečnostní opatření a sankce

1) Je zakázáno zkoušet, zkoumat, testovat nebo zneužívat zranitelnosti prostředků ICT, a to jak v interní síti, tak na internetu. V případě, že činnost souvisí s výukou, je uživatel povinen konzultovat takové činnosti předem s OIT a řídit se jeho pokyny.
2) OIT je oprávněno pozastavit přístup k počítačové síti uživatelům, kteří prokazatelně porušili ustanovení provozního řádu ICT UHK, a to po dobu nezbytnou k vyřešení případu.
3) OIT je oprávněno přerušit přístup prostředků ICT k počítačové síti UHK nebo odpojit prostředky ICT z počítačové sítě, pokud ohrožují bezpečnost a provoz počítačové sítě UHK.
4) OIT si vyhrazuje právo systémově omezit doručování elektronických zpráv s charakterem nevyžádané elektronické pošty (spam) a blokovat nebezpečný obsah v elektronické poště, například zavirované soubory apod.
5) 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 UHK.

Článek 11

Závěrečná ustanovení

1) Tímto řádem se ruší rektorský výnos č. 4/2017.
2) Tento provozní řád nabývá platnosti a účinnosti dnem jeho podpisu.

V Hradci Králové dne 04. 03. 2025

doc. RNDr. Jan Kříž, Ph.D., v. r.
rektor