



University of Hradec Králové

Rector's Decree No. 04/2017

**Rules for Operating Information and Communication  
Technologies  
of the University of Hradec Králové**

*Please note that this translation is non-committal, provided for your understanding. For the legally valid document, see the original in Czech language “Provozní řád informačních a komunikačních technologií Univerzity Hradec Králové”*

## Table of Contents

---

<b>1. Introductory Provisions</b>	<b>3</b>
<b>2. Basic Concepts</b>	<b>4</b>
<b>3. Routines of the Centre for Information Technologies the UHK</b>	<b>7</b>
3.1. User Support	7
3.2. ICT Administration and Records	7
3.3. Provided IT Services	8
3.4. Cooperation on Projects	9
3.5. Domains Registration	10
3.6. Creating and Deleting User Accounts	10
3.7. SW Installation	11
3.8. HW and SW Maintenance and Repairs	11
3.9. Provision of Technical Equipment for Educational, Professional and Social Events	11
<b>4. Computer Network Access Rights and User Identification</b>	<b>12</b>
<b>5. Access Rights to the Internet and External Computer Networks</b>	<b>13</b>
<b>6. Rules for Computer Network Communication</b>	<b>13</b>
<b>7. Property Rights</b>	<b>14</b>
<b>8. Data and Information Protection</b>	<b>15</b>
<b>9. Antivirus Protection</b>	<b>16</b>
<b>10. Data Backup</b>	<b>17</b>
<b>11. Other Obligations of ICT Users</b>	<b>18</b>
<b>12. Security Measures and Sanctions</b>	<b>19</b>

## **1. Introductory Provisions**

- 1.1. The Rules for Operating Information and Communication Technologies of the University of Hradec Králové (hereinafter referred to as the “ICT UHK Operating Rules”) lay down the rules for the use of information and communication technologies (hereinafter referred to as “ICT”) of the University of Hradec Králové (hereinafter referred to as “UHK”). They apply to all ICT users who take advantage of the possibilities, means, computer network services and ICT operated by the UHK.
- 1.2. The computer network and ICT administration within the individual parts of the University of Hradec Králové is provided by the Centre for Information Technologies UHK (hereinafter referred to as “CIT”). CIT provides user support, operates and systematically develops the UHK server and network infrastructure, and ensures the operation of ICT for end users. The CIT provides consultations related to the selection and way of operation of suitable ICT within the framework of the university-wide and faculty projects. CIT carries out technical and methodological supervision of centrally provided local server services and the use of the services of external information technology providers (hereinafter referred to as “IT”).

## **2. Basic Concepts**

### UHK Service Centre

A workplace that carries out activities related to the basic technical support of users at the university-wide level.

### Cloud Solutions

Services or applications operated on servers of external IT service providers outside the UHK infrastructure, or cloud solutions operated within the organization (e.g. Office 365 services, CESNET e-infrastructure).

### Hardware (HW)

Technical means for the collection, processing, storage and distribution of data, including data transmission (e.g. servers, data storage, PCs, notebooks, computer network elements, etc.)

### ICT (Information and Communication Technologies)

Computer technology - hardware elements and software equipment (servers, personal computers, notebooks, smartphones, tablets, communication network elements, data storage, printers, scanners, audio-visual equipment, operating systems, applications, etc.)

### PC

Personal Computer in the classrooms, offices and common areas of the UHK.

## Computer Network

Technical and software tools used for interconnection of computer technology, including that computer technology.

## Authorized System and Application Administrator

A worker who is responsible for the operation of a computer technology that is not primarily under the administration of CIT (e.g. within various projects). If the authorized administrator is not a CIT employee, this administrator is methodically subordinate to the CIT administrator.

## Server

A physical or virtualized device that provides network and application services to client devices and users.

## Domain Administrator

Authorized system and application administrator who administers registered domain data owned by the UHK.

## CIT Administrator

A CIT employee who is responsible for running a computer network and ICT under CIT administration.

## Software (SW)

Software operated within ICT

## SW Licence

Authorization to exercise the right to use the computer programme under the licence agreement.

## User

Employee, student or external user who has access to the computer network and computer equipment or similar facilities operated in the UHK locations.

## User Account

An indication that uniquely identifies a user in a computer network environment. Other properties of the user (basic information about the user, position in the organizational structure, setting up his/her computing environment, group membership, access rights, etc.) are then assigned to this indication in the system.

## Backup

Regular storage of data on external storage media in case of recovery.

### **3. Routines of the Centre for Information Technologies UHK**

#### **3.1. User Support**

ICT UHK users forward all user support requests by means of:

- IT Helpdesk application,
- E-mail via university email address,
- UHK Service Centre,
- Telephone or in person at CIT End-User Support Section workplaces,
- Order sheet - in case of a request for technical provision of sound and projection technology, eventually photographic works for educational, professional and social events.

Contacts for technical support and information on operated IT services can be found on the UHK website ([www.uhk.cz](http://www.uhk.cz)) in the IT and CIT Consulting sections.

#### **3.2. ICT Administration and Records**

- 3.2.1. CIT provides administration, records and development of ICT, server infrastructure and backbone computer network of the UHK.
- 3.2.2. CIT maintains the ICT of individual workplaces. Repairs are paid by the UHK workplaces (departments and divisions) from their budgets.
- 3.2.3. The user confirms the acceptance of ICT for use by his/her signature in the handover protocol.
- 3.2.4. ICT outside the administration of CIT is the responsibility of its owner or authorized system and application administrator.
- 3.2.5. CIT regularly maintains and updates installed operating systems and applications. CIT administratively provides HW and SW support of operated solutions from suppliers.

### 3.3. Provided IT Services

#### 3.3.1. Centrally Provided Services

CIT provides university-wide network and server services. Up-to-date information on provided services is available on the official UHK website in the IT Consulting section.

#### Primary IT services centrally provided by CIT:

- Server and network infrastructure administration (DNS, DHCP, network and security features, etc.)
- Domain user accounts administration.
- Directory and authentication services administration (LDAP, federated services).  
Administration of postal services (basic postal infrastructure for the UHK).  
Virtualization server administration.
- Administration of data storage and sharing systems within the UHK computer network.
- Administration of database servers for centrally operated systems.
- Administration of study records servers.
- Administration of servers for e-learning support.
- Administration of the UHK web presentation and of the selected web applications.
- Administration of library systems.
- Administration of registry service.
- Economic systems administration.
- Administration of university-wide cloud services.
- Administration of telephone and mobile services.
- Administration of servers for network printing support.
- Administration of backup systems.
- Consulting services in the field of ICT services.
- Administration of surveillance and security systems.
- HW and SW administration, configuration of ICT devices.
- Administration and installation of ICT equipment accessories.
- Providing user support for working with the UHK information systems.



- Preparation, coordination and elaboration of technical specifications for tenders.
- Prophylaxis of the multimedia equipment.

### 3.3.2. IT Services for Projects and Teaching Support

The CIT provides additional services for projects and teaching support based on clearly defined bilateral agreements with the applicant. The agreement defines the roles, responsibilities and scope of each party's activities. If project issues interfere with CIT costs, resources for implementation, operational and human resources should be taken into account when planning the project. These services include:

- Administration of application servers for education beyond the scope of commonly operated services.
- Web servers administration, eventually administration and development of the web applications
- Administration of cloud services for studies and project use.
- Other IT services and administration by individual agreement.

## 3.4. Cooperation on Projects

3.4.1. CIT provides consulting services for projects linked to the university-wide ICT infrastructure in order to jointly design such solutions that are compatible with the operating infrastructure components and in accordance with the ICT UHK development concept. CIT recommends that the project researcher propose technical solutions following the university-wide ICT concept in order to ensure efficient spending for ICT acquisition and operation.

3.4.2. Projects that bring costs and requirements beyond the normal services provided by CIT are assessed individually. In case of an agreement on cooperation within the project, a protocol shall be drawn up defining the details of the request, the specific conditions, the time terms of the project duration, the authorized systems and application administrators, the powers and responsibilities of both parties to the agreement. In order to accept the project implementation, the applicant must agree with the rules relating to the requested service.

### **3.5. Domains Registration**

- 3.5.1. CIT primarily provides for the registration of third-level domain names for the uhk.cz domain.
- 3.5.2. In case of registration or need to use another domain within ICT services, it is absolutely necessary that the owner of this domain is UHK. If the domain is owned by another entity, it is not possible to associate with it any official services operated on behalf of the UHK. The domain administrator, which is owned by the UHK, is obliged to keep up-to-date contact information with the registered domain and in case of leaving the organization change the contact information to the new domain administrator.

### **3.6. Creating and Deleting User Accounts**

- 3.6.1. Each new employee is introduced into the relevant information system by the HR department. The request is then forwarded to the identity management system and processed by the downstream systems. An account for accessing ICT means is created, an e-mail box is created and access to other network resources is established for the user.
- 3.6.2. The HR Department enters requests to cancel an employee account in the information system. The request is then forwarded to the identity management system. The user account is then automatically cancelled with time lag, including the account associated data.
- 3.6.3. Documents, e-mails and other electronic data stored on ICT means, including data stored in cloud solutions, become permanently unavailable after the employee leaves and cancels his/her user account on the computer network.
- 3.6.4. Each employee is obliged to duly hand over all ICT means owned by the UHK to the employee in charge of the administration of these assets upon termination of the employment at the UHK.
- 3.6.5. Every employee is obliged to duly transmit work data to his/her manager at the termination of employment at the UHK.
- 3.6.6. Upon termination of employment, the validity of the user account, access to the UHK computer network and the email account expire.

- 3.6.7. The Study Department enters new students into the Study Information System. The next step is to automatically generate a request to create accounts in the identity management system.
- 3.6.8. The Study Department enters requests for cancellation of students' user accounts in the Study Information System. The user account is then automatically cancelled with time lag, including the account associated data.
- 3.6.9. For external workers and guests who do not have a personal user account, the UHK Service Centre offers the possibility of lending a limited time and function user account.

### **3.7. SW Installation**

- 3.7.1. The CIT records and controls SW installed within the ICT UHK that administers. Only legal SW is allowed on ICT UHK means. The installation of the SW on a local computer is carried out by the CIT administrator, possibly by the author, a SW supplier or an authorized system and application administrator in cooperation with the CIT administrator. The requirement to install individual commercial SW must include a contract and an invoice for this SW. These documents must be deposited with the order party for the purposes of possible inspection during the entire period of the software use.
- 3.7.2. In the case of installation of commercial SW or free software, the user accepts the terms of the licence agreement of that SW. The user must use the SW in accordance with the licence agreements.

### **3.8. HW and SW Maintenance and Repairs**

- 3.8.1. CIT provides warranty and post-warranty service of HW and SW, prophylaxis of ICT, spare parts and consumables for CIT-administered technology.
- 3.8.2. The CIT administrator is authorized to perform interventions and adjustments on individual ICT UHK means and to remove any possible illegal SW from them.
- 3.8.3. If the user discovers an ICT defect or suspicious behaviour, he/she will immediately report it to the CIT administrator. ICT users are not entitled to independently make any interventions in the entrusted ICT means that are not related to their normal operation. Only those interventions that are in accordance with the ICT Operating Rules or they were immediately agreed with the CIT administrator, are allowed.

### **3.9. Provision of Technical Equipment for Educational, Professional and Social Events**

- 3.9.1. CIT provides technical preparation of sound and projection technology, including photographic works during educational, professional and social events at the UHK.
- 3.9.2. The application for technical provision is submitted via a form, which can be found on the UHK website in the CIT section.
- 3.9.3. After taking over the request, the order party specifies the specific scope of services according to the technical and personnel capabilities of CIT.

#### **4. Computer Network Access Rights and User Identification**

- 4.1. Access to the computer network implies the necessity of unambiguous identification of each user. Each user account is associated with certain access rights that decisively determine the user's authority in relation to the computer network resources.
- 4.2. The user is obliged to secure his/her user account with a password and keep this password secret and not to disclose it to another person.
- 4.3. A user must not access his/her user account to other computer network users.
- 4.4. A user must not misuse another user's negligence (e.g. omitted logout) to work on a computer network under the identity of somebody else.
- 4.5. A user may only use the access rights that he or she duly possesses and may not engage in any activity to circumvent this provision. If a user obtains access rights in any way that have not been assigned to him (e.g. by a programme or hardware error), he/she is obliged to notify the CIT administrator immediately.
- 4.6. The user must adhere to the conditions for creating passwords, which are listed in the current version on the UHK website in the IT Consulting section.

## **5. Access Rights to the Internet and External Computer Networks**

- 5.1. The allocation of access rights is limited by the operational capabilities of the computer network. It is the responsibility of the CIT Manager to authorize access to blocked resources within the Internet and other external computer networks. A list of currently allowed ports is available on the official UHK website in the IT Consulting section.
- 5.2. Access to unwanted resources within the Internet computer network can be blocked by technical means. If the resources necessary for work or study at the UHK are blocked, it is possible to ask the CIT administrator to release specific resources. Downloading content from websites with unwanted content (erotic, vulgar, hate-promoting, political, religious, and racial agitation, illegally provided software and copyrighted multimedia files) is prohibited, even if the download is not blocked by network means.

## **6. Rules for Computer Network Communication**

- 6.1. A student's e-mail address and mailbox are set up as part of the network account at the start of his/her studies. An employee has an e-mail address and a mailbox set up when he/she starts his/her employment. Students and employees are obliged to use these addresses in their mutual study and work communication.
- 6.2. The employees and students are obliged to regularly check the contents of their e-mail box and to keep their mailbox functional. The consequences of any failure to receive information (e.g. due to overfilling of the mailbox) are fully born by the addressee.
- 6.3. It is forbidden to use vulgar and strongly emotional expressions in communication open to other participants (e-mail, chat, discussion groups, social networks, etc.)
- 6.4. It is forbidden to use a computer network for political, religious and racial agitation.
- 6.5. It is forbidden to use electronic means (especially electronic mail) to bother or intimidate other users. This category includes unauthorized sending of chain letters or e-mail messages to randomly selected addresses in the computer network. It is forbidden to send spam.

- 6.6. It is forbidden to misuse electronic mail for advertising or other purposes for personal gain. CIT reserves the right to systematically restrict the delivery of messages with the characteristic of spam and block unsafe content in e-mail (e.g. infected files will not be delivered).
- 6.7. It is prohibited to use ICT for committing crimes and for activities directed against any other organization whose computer means are accessible through a computer network.
- 6.8. The user of the computer network must not perform such activities that would negatively affect the possibility of using computer means by other users. This applies both to disproportionate load on lines and operating systems and to disproportionate load on individual computers and servers. The user is not authorized to probe, investigate or test system or computer network vulnerabilities. In the case of teaching-related activities, such activities should be consulted with the CIT administrator in advance and be subject to his/her instructions.
- 6.9. The use of the internal computer network in cooperation with students and employees of other schools and organizations is possible with the consent of CIT. In the case of a longer-term relationship, it is necessary to specify the specific conditions for using the computer network, including any sanction measures, in a contract between the UHK and an organization whose employees or students use the UHK computer network.
- 6.10. The computer network operation is monitored for security reasons. These data are used for statistical purposes and security incident resolution.

## **7. Property Rights**

- 7.1. Users use ICT in accordance with their work or study tasks and respect the property rights to the data in electronic form. Users are subject to the same ethical and legal standards as when handling objects and information in a non-electronic format.

7.2. SW may be used and distributed only following the licence terms for the specified SW. It is therefore further prohibited:

- Unauthorized copying of SW and its parts and copying data to which the UHK exercises property rights, resp. rights of use.
- Unauthorized modification of SW or data owned or used by the UHK.
- To knowingly use illegal SW and data, or offer such SW or data to others.
- To use a computer network to gain unauthorized access to non-public information sources, including those that may be owned or administered by other organizations.

7.3. The user bears full responsibility for the content of all data, texts, visual works or parts thereof designated by the user for publication via ICT means or network storage.

## **8. Data and Information Protection**

8.1. CIT protects (in accordance with Act No. 101/2000 Coll., On the protection of personal data, as amended) civil, personal and property rights of all users of the computer network and in this context protects the privacy of data and information stored at ICT UHK means or transmitted by the UHK computer network.

8.2. Administrators and processors of data files subject to the provisions of Act No. 101/2000 Coll., On the protection of personal data, are fully responsible for the content and protection of these data files from misuse, as well as for compliance with any other provisions of this Act arising from in the area of personal data processing, including the reporting obligation pursuant to Section 16 of the Act.

8.3. To ensure maximum privacy and data security, users are prohibited from:

Taking any action that results in another user's privacy violation, even if the user does not

- explicitly protect his/her own data.
- Copying any data or programmes from user directories without the owner's consent (this also includes only browsing the directories).
- Using a computer network to gain unauthorized access to non-public information sources, including those that may be owned or administered by other organizations.

8.4. In legitimate cases or for serious reasons, it is possible to provide designated persons with access to e-mail at the UHK, data on IT devices (PCs, notebooks, drives, USB drives, backup media) and user data stored in the UHK operating infrastructure, including cloud environments but always only on the basis of a written court order or on the basis of a written decision with the justification of the relevant faculty's Dean, Rector or Bursar of the University of Hradec Králové. The employer is obliged to demonstrably inform the employee whose data are to be made available about the extent of access, the reasons and the method of implementation. The disclosure of data is possible, subject to the condition of a written order, also in cases of verification of the delivery of decisions where the Higher Education Act and the internal regulation allow delivery via the internal information system.

## **9. Antivirus Protection**

- 9.1. An antivirus programme, which provides antivirus control of files stored on ICT UHK terminal devices, antivirus control of the computer network and e-mail messages, including their attachments, is installed in the computer network. The programme creates a resident shield on each terminal device of the ICT UHK that prevents the intrusion and spread of the virus into the device. The antivirus database is continuously updated over the computer network.
- 9.2. It is important to follow the rules of antivirus prevention, for example not to run SW with unclear or unknown origin. ICT device suspected of being infected by a virus must not be used until the virus is removed. If a security threat is suspected, the user must contact the CIT administrator.



## **10. Data Backup**

- 10.1. The purpose of data backup is to create safety copies of working data on backup data carriers.
- 10.2. CIT administrators regularly back up data in the assigned home directory, web presentation directory, and in the folder for projects located on a shared network drive. This backup is performed at regular intervals according to the backup plan. CIT reserves the right to change backup plans. If necessary, it is possible to ask the CIT administrator for individual data recovery.
- 10.3. In case of storing data to other network locations or local storage of the ICT UHK terminal devices, the responsibility of the backup passes to the user. The user has the option of securing backups with his/her own means (backup to high-capacity media, external drives, backed up network drives, cloud services such as the Office 365 environment and the CESNET data storage environment).
- 10.4. Requests for inclusion of the other systems and data in the backup plan shall be submitted by authorized system and application administrators or their guarantors (in case of implementation of the student projects). The request will be reviewed by CIT administrators according to the technical capabilities of the current backup solution.

## **11. Other Obligations of ICT Users**

- 11.1. The user is obliged to use the entrusted ICT means only for the performance of work or study duties and in accordance with the purpose, for which they were intended.
- 11.2. The user is obliged to work with ICT devices in such a way that they are not damaged.
- 11.3. The user is not allowed to move ICT devices in classrooms, to change the configuration of computers or other ICT devices installed there, to disconnect cables and to make other technical adjustments to these ICT devices.
- 11.4. The user is obliged to keep all documents to the entrusted SW and HW.
- 11.5. The user is obliged to prevent unauthorized persons from accessing the ICT UHK means.
- 11.6. In the case of interruption of work with the loss of supervision of the entrusted ICT means (even in the case of short-term leaving the workplace), the user is obliged to sufficiently prevent unauthorized use of the ICT means by logging out of the operating system session or in another way.

## **12. Security Measures and Sanctions**

- 12.1. The CIT administrator is entitled to suspend access to the computer network to users who have been proven to have breached the provisions of these Regulations for the period until the case is resolved.
- 12.2. The CIT administrator is entitled to interrupt the access of the ICT device to the UHK computer network or to disconnect the ICT device from the computer network if the ICT device endangers the security of the UHK computer network or otherwise interferes with its operation.
- 12.3. Intentional or repeated violation of the principles of the ICT UHK Operating Rules may be considered a violation of obligations arising from the employment contract, regulations related to the work performed (violation of work discipline) or from disciplinary rules for students of the UHK.

In Hradec Králové on March 17, 2017

prof. Ing. Kamil Kuča, Ph.D., in his own hand

**Intended for:** all UHK employees