University of
Hradec Králové

Rules of Operation of Information and Communication Technology of the University of Hradec Králové

Table of Contents

PART ONE

Article 1

Introductory provisions

1) The Rules of Operation of Information and Communication Technology of the University of Hradec Králové set out the rules for the use of information and communication technology (hereinafter referred to as the *"ICT"*) in the environment of the University of Hradec Králové (hereinafter referred to as the *"UHK"*).

2) The ICT assets include all hardware (hereinafter referred to as *"HW"*) and software (hereinafter referred to as *"SW"*) equipment, including servers, personal computers, laptops, mobile phones, tablets, data storage products, printers, scanners, audio-visual equipment, tokens, network elements, Internet of Things (hereinafter referred to as the IoT) devices, operating systems, information systems and applications, cloud solutions, and electronically processed information and data.

3) A user of the ICT UHK (hereinafter referred to as the *"User"*) is defined as an employee, student, external person or system that has access to the ICT UHK. The obligation to comply with these Rules of Operation of the ICT UHK applies to all Users.

Article 2

Basic user rules

1) The User is obliged to comply with the provisions of these Rules of Operation and other security and legal documents such as security policies, decrees, directives and instructions set by the UHK. The User is also obliged to respect the legislation on cybersecurity such as the Act on Cybersecurity No. 181/2014 Sb., as amended, and related decrees.

2) The User is obliged to protect his/her access data and not to provide them to any third parties. He/she is also obliged to ensure that confidential information (login data, printouts, documents open in information systems, access tokens, etc.) are not accessible to unauthorized persons. In the event of an interruption of work that results in loss of control over the entrusted ICT devices, the User is obliged to secure properly these ICT devices by logging out of the operating system session or by other appropriate means.

3) The User is obliged to follow the rules for creating passwords that are set out in the currently valid version on the official UHK website.

4) Access to the key information systems and applications is subject to authentication through multi-factor authentication. Multi-factor authentication of users is defined in a separate Rector's Decree.

5) The User may not take advantage of another User's negligence, such as failing to log out, to act under someone else's identity on the computer network.

6) The User is obliged to use only legal and approved ICT devices in accordance with the licensing and legal regulations. The User is obliged to keep all documentation related to the assigned SW and HW. Unauthorised copying or modification of SW or data owned or used by the UHK is prohibited.

7) The User is prohibited to connect and use ICT devices from unapproved, unknown or untrusted sources (e.g., found or distributed storage media such as USB drives, compact discs, network devices, etc.).

8) The User is prohibited to download content from websites with inappropriate or illegal content, even if the downloading of the content is not blocked by the technical means of the network.

9) The User is obliged to use ICT devices in a way not leading to their intentional damage. The User is not allowed to move ICT devices in classrooms, change their configuration, disconnect cables or make other technical modifications to ICT devices.

10) The User shall use ICT devices in accordance with his/her work or study duties and shall respect the ownership rights to data in electronic form. The user shall follow the same legal and ethical standards as when dealing with objects and information in non-electronic form. The user is responsible for all content of data, texts, visual works or parts thereof intended for publication by ICT devices.

11) The User of the computer network may not perform activities that could affect negatively the operation of the UHK computer network.

12) The User is obliged to educate themselves regularly in the field of cybersecurity. The rules for training employees in the field of cybersecurity are regulated by the internal regulations and security policy documents of the UHK.

PART TWO

Article 3

User accounts

1) The user account is used to access the UHK computer network and the User's e-mail box. A user account is established through the identity management system on the basis of information about a valid study at or employment with the UHK, on the basis of activity in research boards or bodies of the UHK, or on the basis of another contractual relationship with the UHK.

2) The user account and e-mail account expire on the date of termination of employment or studies, on the date of termination of activities in the research boards or bodies of the UHK, or on the day of termination of other contractual relations with the UHK. The user account is then automatically terminated over time via the identity management system, including all data associated with the account.

3) Upon termination of a user account, all documents, e-mails and other data stored on ICT devices, including data stored in cloud-based solutions, become permanently unavailable.

4) A user account with a limited time and function can be provided to external staff and guests who do not have a personal user account. A service account can be set up for the management of ICT devices.

Article 4

User account permissions

1) Access to ICT devices requires unambiguous identification of each User. Each user account is associated with appropriate access rights that determine the User's permissions in relation to ICT devices.

2) The User is entitled to use those access rights only that have been duly granted to him/her. The User is obliged to refrain from any action aimed at circumventing this provision. In the event that the User in any way acquires access rights that have not been granted to him/her, he/she shall immediately notify the staff of the Department of Information Technology Services (hereinafter referred to as the *"DITS"*).

3) A User's request for higher access rights to ICT devices beyond the granted access rights is subject to the DITS approval. The User is obliged to justify duly this request. If the request is approved, the User shall be required to sign a declaration of the higher access rights granting. The User shall be responsible for the security risks associated with these rights.

PART THREE

Article 5

Operation in the UHK computer network

1) Technical means can be used to restrict access to ports or resources on the Internet. Approval of access to ports or resources is the responsibility of the DITS. If certain ports or resources are blocked, the User may request the DITS to release them. The list of permitted ports is available on the official UHK website.

2) The use of the internal computer network in collaboration with students and employees of other schools and organizations is only possible with the prior approval of the DITS. In case of a longer-term relationship, the conditions of use of the computer network, including possible sanctioning measures, must be specified in the contract made between the UHK and the respective organisation whose employees or students use the UHK computer network.

3) For security reasons, all computer network traffic is monitored. This data is used for statistical purposes and to resolve security incidents.

Article 6

Electronic mail and communication in the UHK environment

1) Employees are provided with an e-mail address and mailbox upon commencement of employment. Students are provided with an e-mail address and mailbox when they start their studies. Employees and students are obliged to use these only addresses and mailboxes in their work and study communications.

2) The User is obliged to check regularly the contents of the assigned electronic mailboxes, ensure their functionality and bear all consequences resulting from non-receipt of information, for example due to overflowing mailboxes.

3) The User is obliged to maintain the capacity of the assigned e-mail boxes and shared storage within the limits of the quotas. The size of these quotas is specified on the official UHK website.

4) The User is obliged to follow the rules of e-mail etiquette. It is forbidden to use rude and strongly emotional expressions when communicating via e-mail, chat, newsgroups, social networks and other publicly accessible communication platforms. It is prohibited to use electronic means of communication to harass users by disseminating unsolicited or commercial messages.

PART FOUR

Article 7

Protection of data and information

1) Data and information are protected in accordance with Act No. 110/2019 Sb., on the processing of personal data, as amended.

2) Controllers and processors of data, particulars and information to which the provisions of the Personal Data Processing Act apply are fully responsible for their content and security against misuse, as well as for compliance with all other relevant provisions of this Act.

3) To ensure the highest level of privacy and data security, the following activities are prohibited:

   - Taking any action that leads to a breach of another user's privacy, even if the user does not explicitly protect his/her own data.
   - Copying the contents of user folders without the owner's consent, including viewing the folders themselves.
   - Using a computer network to gain unauthorised access to non-public information resources, including those that may be owned or managed by other organisations.

4) For the protection of work data and confidential or secret information, the redirection of work e-mail accounts to external and private e-mail accounts is prohibited. It is forbidden to send work data, confidential and classified information via external and private e-mail accounts.

5) Copying and transmitting work data, confidential and classified information using private data storage and copying and printing devices is prohibited. It is forbidden to transmit data, confidential and classified information via public Internet file-sharing services that are not officially supported by the UHK due to the risk of unauthorised access to sensitive UHK documents, contracts and data.

6) In cases provided for by law and internal regulations, or for other compelling reasons, access to the e-mail and data in ICT devices may be granted. Such access is only possible on the basis of a written court order or a written decision with justification from the Dean of the relevant faculty, the Rector or the Bursar of the UHK. The employer is obliged to inform the employee whose data is to be accessed of the reasons and scope of access. The disclosure of data is also possible in the case of verification of the delivery of the decision through the information system in accordance with the legislation in force.

7) ICT devices are protected by an antivirus programme. Any interference with the anti-virus programme while checking the system is prohibited. The user is obliged to follow the rules of prevention, for example, not to open files from unclear or unknown sources. ICT devices suspected of being infected with a virus may not be used until the malicious files have been removed. In the event of a suspected security threat, the User must notify the DITS.

8) The User is entitled to create backup copies of work data exclusively on data storage facilities owned by the UHK or to use cloud services that are contractually provided by third parties to the UHK. The User is obliged to comply with the current security policy and use data encryption.

9) The proposal for inclusion of systems and data in the backup plan shall be submitted by authorised system and application administrators or their guarantors. Data stored in cloud services and repositories are not backed up through internal backup systems. The backup proposal will be evaluated by the DITS with respect to the technical and capacity capabilities of the current backup solution.

10) Upon termination of employment, each employee is required to forward properly the work data to his/her supervisor.

PART FIVE

Article 8

Administration and Evidence of ICT UHK

1) ICT devices owned by the UHK intended for the performance of work activities are registered in the economic information system.

2) The DITS provides HW and SW equipment management, external service, ICT prophylaxis, spare parts and consumables exclusively for the technology owned by the UHK.

3) Costs for repairs, software upgrades, technical extensions, and consumables are covered by the User or the relevant UHK department from its own budget.

4) The User may not block or otherwise restrict remote access to ensure the management of ICT devices.

5) In the event that ICT devices have been acquired without prior consultation with DITS, the DITS shall have the right to refuse to accept such ICT devices into its management and to refuse to integrate them into the operational infrastructure on the grounds of security risk, incompatibility, increased management requirements, or unreasonable connection or maintenance costs.

6) In the event that the User discovers a malfunction or suspicious behaviour of an ICT device, he/she is obliged to report this fact immediately to the DITS. Users are not authorised to make any interventions in the entrusted ICT devices that are not related to their normal operation without prior approval of the DITS. Interventions in accordance with the ICT UHK Rules of Operation only are permissible.

7) User-owned devices (BYOD) may only be connected to the UHK infrastructure on condition that the rules for ensuring the protection of the University infrastructure and data are enforced by technical means. The User is obliged to ensure that the connected device meets the requirements for security, regular updates, SW protection and tools to eliminate the risk of spreading malicious software (viruses, malware, ransomware, etc.). The User is also responsible for the installed software and compliance with the license conditions. The DITS is not responsible for the condition of BYOD devices.

8) Upon termination of employment, the User is obliged to duly hand over all entrusted ICT devices in the possession of the UHK to the employee in charge of the administration of this property or to his/her direct supervisor.

PART SIX

Article 9

Services provided by the DITS UHK

1) **Centrally provided services**

   a) The DITS provides central network and server services. It operates and systematically develops the server and network infrastructure of the UHK, ensures the operation and maintenance of ICT devices of the UHK. The DITS provides consultations related to the selection and operation of appropriate ICT in the context of University-wide and faculty projects. The DITS provides technical and methodological supervision of centrally provided local server services and of the use of services provided by external ICT providers. The management of centrally provided ICT and services is funded from a separate budget where the head of the DITS is the originator of the transaction.

   b) The DITS provides IT support to the Users. The ICT UHK Users submit all requests for user support via:

      - IT Helpdesk application;
      - Electronic mail via the University e-mail address;
      - UHK Service Centre;
      - Phone or in person at the End User Support Unit;
      - An order sheet (Evidence of Requirements for Technical Provision of Events) in the case of a request for technical provision of sound, projection technology, or photographic work for educational, professional and social events.

2) **Cooperation on projects**

   a) The DITS provides consultancy services for projects related to the University-wide ICT infrastructure, with the aim to design jointly solutions compatible with the operational components of the infrastructure and in line with the ICT UHK compatibility. The DITS recommends that the project proponent proposes technical solutions compatible with the ICT in operation to ensure efficient use of funds for ICT acquisition and operation.

b) Projects that present costs and requirements beyond the normal services provided by the DITS are considered on an individual basis. The provision of cooperation on projects is dependent on the DITS's technical and staff capacity. Where the project imposes costs on the DITS, funds for implementation, operation and staffing must be included in the project planning. In the event of an agreement to collaborate on a project, a record will be drawn outlining the details of the request, specific terms and conditions, project timelines, designated system and application administrators, and the authority and responsibilities of both parties to the agreement. Acceptance of the project implementation requires the applicant's agreement to the rules related to the requested service. Any costs associated with the integration of the new solutions into the operational infrastructure shall always be borne by the person who has ordered the service.

c) The authorized administrator of systems and applications is responsible for the operation of the entrusted systems in accordance with the Rules of Operation of ICT UHK. He/she also ensures the protection of data, information and personal data and follows the instructions of the DITS.

3) IT services to support the digitisation of processes

a) The DITS provides services to support the digitization of processes based on the collection of requirements, their prioritization according to the agreement of the individual organizational units of the UHK and the determination of the implementation of requirements by the Rector's Board. These services are:

- Analysis of current processes in all organizational units;
- Design of a unified digital process;
- Support for the selection of a suitable SW solution;
- Support in system integration;
- Creation of user documentation for internal applications;
- Support during user testing and solution acceptance;
- End user training;
- Verification of the implementation of the solution in terms of support for the process.

b) In order to classify a request as a request for digitisation, the following information must be provided for each request for process digitisation:

- A detailed description of the requirement including the desired objectives (reasons and expected benefits);
- The guarantor or owner of the process;
- Project manager person;
- The person responsible for the process providing the methodology.

c) If the request is accompanied by a comprehensive analysis and design of the unified digitized process, the request must include:

- Objectives and expected outcomes;
- Risks and critical points;
- Required implementation dates;
- Requirements for cooperation with other units of the organization and external entities;
- Expected investment and non-investment costs;
- Required division of roles and responsibilities of all stakeholders.

d) The process guarantor is fully responsible for the costs of the new SW solution implementing. If these costs impinge on the budgets managed by the DITS, it is necessary to include new one-off implementation funds in the project planning, as well as subsequent operational and staffing costs to ensure sustainability.

4) Domain registration

a) The DITS provides registration of third-order domain names for the domain uhk.cz.

b) In the event of the need to register or use another domain, it is necessary that the UHK is the owner of the domain. If the domain is owned by another entity, no official services operated on behalf of the UHK may be associated with it. The administrator of a domain owned by the UHK is obliged to keep the contact details of the registered domain up to date and to update the contact details of the new domain administrator in the event of a departure from the organisation.

5) **SW installation**

a) The installation of the software is performed by the DITS, or by the software supplier, or by an authorized administrator of systems and applications in cooperation with the DITS. The request for installation of individual commercial software must include a contract and invoice for that software. These documents must be kept on file with the orderer for possible inspection during the entire period of use of the software.

b) In case of SW installation, the User accepts the terms of the license agreement of the software. The User is obliged to use the SW in accordance with the license agreement. The DITS is entitled to remove any illegal SW or SW used in violation of the license agreement.

6) **Provision of technical equipment for teaching, professional and social events**

a) The DITS provides technical support and preparation of audio-visual equipment for teaching, professional and social events at the UHK within its technical and capacity capabilities.

b) The application for technical support must be submitted using the form available on the official UHK website. After receiving the request, the specific scope of services is specified with the client. The provision of services is dependent on the technical and personnel capacities of the DITS.

7) **Energy consumption of ICT devices**

The DITS is working to reduce the energy consumption of ICT devices through the optimisation of HW and SW, especially in the process of tenders for ICT supply.

PART SEVEN

Article 10

Security measures and sanctions

1) It is forbidden to try, investigate, test or exploit vulnerabilities of ICT devices, both on the internal network and on the Internet. If the activity is related to teaching, the User must consult such activities in advance with the DITS and follow its instructions.

2) The DITS is authorized to suspend access to the computer network for Users who have proven to have violated the Rules of operation of ICT UHK for the time necessary to resolve the case.

3) The DITS is entitled to interrupt the access of ICT devices to the UHK computer network or disconnect ICT devices from the computer network if they threaten the security and operation of the UHK computer network.

4) The DITS reserves the right to restrict the delivery of electronic messages showing the features of unsolicited electronic mail (spam) and to block dangerous content in electronic mail, such as infected files, etc.

5) Deliberate or repeated violation of the Rules of Operation of ICT UHK may be considered a violation of obligations arising from the employment contract, from regulations related to the work performed (breach of work discipline) or from the UHK Disciplinary Code.

Article 11

Final provisions

1) This Regulation repeals Rector's Decree No. 4/2017.

2) These Rules of Operation shall come into force and effect on the date of their signature.

In Hradec Králové on XX. XX. 2025

Assoc. prof. RNDr. Jan Kříž, Ph.D.
Rector