Charles University

Rector's Measure No. 34/2017

- Title:
  Charles University Computer Network Rules

- Effective as of:
  1 September 2017

Charles University Computer Network Rules

In this regulation, Charles University lays down the terms and conditions of access to the Charles University Computer Network, binding rules for the use of the Network and its services as well as the rules for administration and operation of the Network and services provided by the Charles University Computer Network.

Part A.

Rules for Charles University Computer Network Users

Charles University (hereinafter referred to as "CU") hereby stipulates the terms and conditions of access to the Charles University Computer Network, as well as the binding rules for the use of this Network and its services.

I. Definitions of Terms Used

1. The **Charles University Computer Network** (hereinafter the "**CU Computer Network**") means a set of information and communications technology devices (hereinafter "ICT"), including (but not limited to) cabling, network elements, servers, computers, mobile devices and other specialised computer technology devices enabling users access to services provided. The CU Computer Network may be further divided and individual parts may be administered by different operators.
2. CU Computer Network **User** means any person that uses the CU Computer Network, any devices attached thereto or services provided within this Computer Network.
3. CU Computer Network **Service means** a service provided to CU Computer Network Users via ICT.
4. **Central Authentication Service (hereinafter the "CAS")** is a central service of the CU Computer Network run by the Computer Science Centre (hereinafter the "CSC") which serves to verify the identity of Users via usernames and passwords to enable them access to other services.
5. **User Account** means a User identification and verification mechanism (authentication). The User Account permits the User to access the CU Computer Network and services provided.
6. If not provided for otherwise, **an Operator of a part of the Network** (hereinafter the "**Operator**") means, a faculty or another CU unit that has established the given part of the Network or has been authorised to operate that part of the Network on the basis of an internal regulation or a contract. The Operator is entitled to lay down other User rules for the given part of the Network or services which, however, are not in conflict with these Rules or the CU Computer Network Operation Rules. If the character of the workplace requires so, the Operator shall issue operating rules for the workplace in question which shall comply with this regulation.
7. **Administrator** means a natural or legal person (or their organisational unit) that has been authorised by the Operator to conduct activities related to the administration of the operated system, a part of the Network or a service.
8. **Security Incident** means an event that may lead to the violation of confidentiality, integrity, accessibility or non-repudiation of information or services provided within the frame of the CU Computer Network. A Security Incident shall also mean an event recorded in the CU Computer Network or triggered thereby which has or may have a

negative impact on the operation of a part of the Network or services provided or which has a negative impact on other persons, operation of other networks or services.

9. **CSIRT-CUNI (Computer Security Incident Response Team)** means a security team whose main task is to receive information on Security Incidents related to the CU Computer Network, their solutions and co-ordination of solutions in co-operation with Operators of a part of the CU Computer Network, Administrators and Users. In organisational terms, CSIRT-CUNI is run by the Computer Science Centre (hereinafter the "CSC").

II. Basic Principles of CU Computer Network Use

1. The CU Computer Network and the services related thereto may only be used in compliance with the CU mission and activities stated in the CU Statutes[1], and in the CU trade licences.
2. Users are allowed to connect ICT components, such as computers, notebooks and other mobile devices to the CU Computer Network, solely at designated places and by means designed for the purpose.
3. Users are not allowed to:
   a. Connect communications devices (routers, switches, etc.) or entire networks to the CU Computer Network without the prior consent of the relevant Administrator
   b. Install and operate, without an Administrator's consent, any software that excessively burdens the CU Computer Network, servers, or other ICT components, if relevant
   c. Install, copy or publicly communicate any works, software, databases and other results of intellectual creative work that are subject to intellectual property rights (in particular copyright, Personal Data Protection Act and Protection of Classified Information Act) via the CU Computer Network without the relevant authorisation
   d. Modify software, data or technical equipment owned or used by CU without the relevant authorisation (e.g. any computer configuration that would affect the operation of the Network or a service)
   e. Damage or destroy ICT devices (computers, software, communication lines) in the ownership of CU
   f. Ensure access to the Network and other services of the CU Computer Network to other legal entities or natural persons
   g. Use false identity or misuse the negligence of other Users to access data and information of other people
   h. Use such software that permits unauthorised use of another person's User Account
   i. Attempt to obtain access rights to which they are not entitled (should the User gain such rights by mistake resulting from the erroneous operation of software or technical equipment, s/he is obliged to notify the Administrator or CSIRT-CUNI thereof without undue delay)
   j. Develop or use programmes facilitating activities specified in paras d) to i), unless it falls within the scope of their study or work duties (this, however, requires an explicit written consent of the Operator)
   k. Use CU computer devices for activities specified in paras d) to i) against any other organisation whose computer tools are accessible through the CU Computer Network

[1] Section 2 of the CU Statutes.

l. Use services of the CU Computer Network to disseminate commercial information, for advertising purposes, political or religious campaigning, or spreading information that is in contradiction with legislation, internal regulations and internal CU standards, ethical or moral rules or information that could be detrimental to the CU reputation (activities conducted within the scope of supplementary activities organised by CU are not considered to be the dissemination of commercial information or information for advertising purposes)
m. Disturb other Users by sending spam through the CU Computer Network or its services
n. Overburden the Network infrastructure and services available and thus restrict other Users in making use of ICT and services.

III. User's Rights and Obligations

1. The basic right of a User who is a student or employee of CU is the right to obtain a User Account to access the CU Central Authentication Service.
2. The User is authorised to use the CU Computer Network for commercial purposes solely in compliance with Act No. 111/1998 Coll., on Higher Education Institutions, as amended, and with the regulation on supplementary activities.
3. Users are obliged to:
   a. Familiarise themselves with the method of and rules for the use of CU Computer Network prior to or during their first connection to the Network
   b. Respect any additional rules or operational rules applicable to the use of devices, services or premises issued by individual Operators of parts of the CU Computer Network
   c. Co-operate in the process of establishment and modification of their User Account
   d. Respect the instructions of the Administrator and other persons authorised by the Administrator and upon request prove their identity (CU identification card, study record book, national ID card, passport, etc.)
   e. Protect their User Account by password or other technical means developed for that purpose and are also obligated to minimise the opportunities for the User's Account misuse
   f. Respect the protection of copyrights and other intellectual property rights, personal and confidential information
   g. Notify CSIRT-CUNI, without undue delay, of any breach of the aforementioned rules, in particular if they suspect that any of the ICT tools or services of the CU Computer Network have been or are being misused or personal access data has been disclosed.
4. Users are liable for the data and ICT components administered by them (Users are fully liable for any potential consequences arising from their conduct, including liability for damage).

IV. Other Provisions

The User hereby confirms and agrees unconditionally with the following:
1. The CSC and Operators have the right to store information on the operation and services provided in the CU Computer Network for administrative, operational, statistical, monitoring and security purposes.

2. The CSC and Operators undertake to ensure that all information obtained in the process of equipment registration or User Account establishment is protected within the meaning of Act No. 101/2000 Coll., on Personal Data Protection, as amended. CU is entitled to communicate the data provided by the User to law enforcement authorities for their purposes in compliance with the applicable legislation.
3. In the event of substantiated suspicion of breach of Czech legal regulations or these Rules, the CSC and Operators are entitled to temporarily restrict the access of the User to the CU Computer Network or its part or selected services, if applicable.
4. In the event of reasonable suspicion of misuse of a User Account or device by another person, the CSC and Operators are entitled to immediately block the User Account (including a CAS account and other User Accounts necessary for the fulfilment of study or work duties) or disconnect such devices from the CU Network and services. CU is obliged to inform the User immediately thereof using the contact information stored for the purposes of the User Account in question or the registered device.
5. In the event of provable violation of these Rules by the User or in the event of a Security Incident caused by the User, the CSC and Operators are entitled to permanently disable the User's access to the CU Computer Network or its part and selected services, if applicable.
6. In order to adhere to the obligations laid down in Act No. 480/2004 Coll., on Certain Information Society Services, as amended, the CSC, Operators and Administrators are entitled, in the event they learn about the existence of User files, parts of files or other information that are of an illegal nature, to immediately delete such information, take all reasonable steps to eliminate such information or make it inaccessible or secure such information for the purposes of criminal proceedings, if any. The User hereby confirms and consents to the fact that the CSC, Operators and Administrators shall not be liable for any direct or indirect damage or other harm that has occurred or may have occurred to the User due to the aforementioned steps.
7. In the event of breach of these Rules by any User, the CSC or Operators may, in compliance with applicable national legislation and international treaties by which the CR is bound, also take other measures not mentioned above.
8. The CSC and Operators do not guarantee the User in any way the uninterrupted operation of the CU Computer Network or its services, their accessibility or quality.
9. In compliance with the general civil and criminal liability of the User pursuant to the relevant provisions of the generally binding legislation, CU shall be entitled to damages should the User violate the obligations laid down herein.

V. Final Provisions

1. These Rules become binding on the User as soon as s/he expresses his/her consent to the "Rules for Charles University Computer Network Users" document. The Rules are binding for the User for the entire period of use of the CU Computer Network or its services. These Rules as well as other related documents are accessible at https://uvt.cuni.cz/uksit.
2. By clicking **"I agree to the Rules"** or by signing the record enclosed to these Rules, the User confirms that s/he has read the document ("Rules for Charles University Computer Network Users"), understood all the information contained therein and expresses his/her full consent. The User also confirms that s/he has not given his/her consent to the Rules under pressure and that it has been an act of his/her free will.
3. By clicking **"I agree to personal data processing**" or by signing the record enclosed to these Rules, the User confirms that s/he agrees to the processing of the personal data

provided in connection with the establishment of access to the CU Computer Network or use of its services. This personal data is stored and administered pursuant to the "Processing of Personal Data of Students, Applicants, Employees and Other Persons at Charles University" regulation, as amended.

Part B.

CU Computer Network Operation Rules

Charles University hereby lays down the rules for the administration and operation of the Network and services provided by the Charles University Computer Network.

I. CSC Basic Obligations and Rights

1. The CSC provides for the connection of individual university localities to the CU Computer Network, and based on their requirements it ensures their interconnection and connection to the Internet global network. In substantiated cases this obligation may be delegated to the relevant Operator.
2. The CSC is liable for the configuration and operation of central services, assigns Internet addresses to connected networks, registers second level domains, eliminates (in connection with Operators of parts of the CU Computer Network) defects arising from the use of these addresses and domains used in the CU Computer Network, and take measures to prevent their misuse.
3. On the basis of information from the centrally operated information systems the CSC establishes and cancels accounts in the CAS.
4. The CSC checks and provides methodological guidance to Operators of parts of the CU Computer Network to ensure that, in co-operation with Administrators, they see to the proper configuration, functionality and security of ICT components and services provided to their Users and ensure that their operation does not restrict or disrupt the operation of the CU Computer Network or other networks.
5. The CSC operates the CSIRT-CUNI security team.
6. The CSC is entitled to retain information on operation and services provided in the CU Computer Network for administrative, operational, statistical, monitoring and security purposes. The CSC is entitled to analyse information obtained solely to the extent necessary to ensure the proper functioning of the Computer Network and its services and in compliance with the applicable legislation. CSC employees are bound by confidentiality obligations with respect to information that they learn in connection with the aforementioned activities and that could be of confidential nature or relate to individual Users. These obligations remain in validity despite the termination of an employment contract or any contractual relationship with CU. Employees shall not be bound by the confidentiality obligation if handling a Security Incident; in that case they have the right to communicate the information related to the Incident in question to the Administrators dealing with the Security Incident or to the relevant Operator and CSIRT-CUNI members. Furthermore, the confidentiality obligation shall not apply to communication with the Police of the CR or other law-enforcement bodies.
7. In the event of reasonable suspicion of misuse of the CAS User Account by another person, the CSC is entitled block the User Account. The CSC is obliged to inform the User thereof using the contact information maintained for the Account in question.

8. In the event of reasonable suspicion of device misuse, the CSC is entitled to block or disconnect such devices. The CSC is obliged to immediately notify thereof the relevant Administrator of the part of the Network to which the device was connected.
9. In the event of violation of these Rules or handling a Security Incident, the CSC is entitled to adopt other measures to ensure the proper functioning of the CU Computer Network and its services. Should such measure lie in the limitation or termination of service provision or connection to the CU Computer Network, the person who has taken this measure must inform the Administration of the relevant part of the Network.
10. In the event of violation of these Rules or the "Rules for CU Computer Network Users", the CSC may adopt other measures in compliance with applicable national legislation and international contracts by which the CR is bound.
11. The CSC does not provide Users with any guarantee regarding the uninterrupted provision of services or their accessibility or connection speed.
12. In cases when the CSC takes on the role of an Operator or Administrator of a part of the Network, it shall be bound by the provisions of Articles II and III, Part B hereof.

II. Basic Obligations and Right of Operators of a Part of the CU Computer Network

1. Operators are liable for the proper configuration, functionality and security of technical means of the part of the Network operated and services provided by them. The administration is delegated to one of their organisational units or an external entity or natural person. Operators shall inform the CSC of the body authorised to carry out the administration.
2. Operators may divide the Network operated into parts and authorise different organisational units, external entities or natural persons to carry out the administration. Furthermore, Operators are entitled to delegate the responsibility for the operation of a certain part to any of their organisational units. Operators shall inform the CSC on the division of the Network and on their decision to delegate the responsibility for the operation of their part.
3. In compliance with the provisions of Section 5 of Act No. 480/2004 Coll., on Certain Information Society Services, as amended, the Operator whose activity lies in the provision of services consisting in storage of information (files) provided by Users is liable for the contents of the information stored at the request of a User only if:
    a. they could, with regard to the subject of their activity and the circumstances and nature of the case, know that the contents of the information stored or action of the User are illegal; or
    b. they have, in a provable manner, obtained knowledge of the illegal nature of the information stored or illegal action of the User, and failed to take, without delay, all measures that could be required to remove or disable access to such information.
4. In compliance with the provisions of Section 6 of Act No. 480/2004 Coll., on Certain Information Society Services, as amended, the service provider whose activity lies in the provision of services consisting in storage of information (files) provided by Users is not obliged to monitor the contents of the information which they transmit or store or actively seek facts or circumstances indicating the illegal contents of information.
5. In order to adhere to the duties laid down in Act No. 480/2004 Coll., on Certain Information Society Services, as amended, the Operator, should they obtain knowledge of User files or parts of files or other information of illegal nature, is obliged to take all measures that could be required to remove or disable access to such information or secure such information for the purposes of potential criminal proceedings.

6. With respect to devices operated by them, the Operator is obliged to ensure adherence to copyrights, the authorised use of products as well as respecting the set licence terms and conditions.
7. The Operator is obliged to retain the identity of Users using a device in the Operator's Network, including such information that proves that the device was used by the User at a given time. This data must be stored for a period of at least 6 months. Upon request of the CSC, the Police of the CR or other law-enforcement authorities, the Operator is obliged to immediately retrieve and provide such information in order to determine the liability for a Security Incident or to communicate the information requested. The Operator shall always inform the CSIRT-CUNI team of Security Incidents that are investigated upon request of the Police of the CR or other law-enforcement authorities or in co-operation therewith. In special cases (e.g. connection of a device to a part of the Network via the eduroam service) the Operator's obligation to retain the identity of Users connecting devices to the Network shall apply appropriately.
8. In exceptional cases (e.g. organization of conferences, seminars and other events without prior participant registration) the Operator is entitled to permit, for a necessary period of time, a technical solution permitting connection of devices to a part of the CU Computer Network with verification shared by multiple Users. This must be communicated to CSIRT-CUNI. If the technical solution fails to enable the Operator to adhere to the obligation to retain the identity of Users connected as specified in the paragraph above, this is not deemed to be a breach of the Operator's obligations.
9. The Operator undertakes to ensure that all information obtained during the registration of a User's device or the establishment of the User Account is protected within the meaning of Act No. 101/2000 Coll., on Personal Data Protection, as amended. The Operator is entitled to disclose the information provided by the User to law-enforcement authorities for their purpose in compliance with the applicable legislation.
10. Should a Security Incident be detected, the Operator is obliged to provide, upon request, co-operation to the CSC, CSIRT-CUNI members, and law-enforcement authorities, if applicable.
11. The Operator is entitled to store operational data and information on services provided in the CU Computer Network for administrative, operational, statistical, monitoring and security purposes.
12. In the event of violation of these Rules or the "Rules for CU Computer Network Users", the Operator may adopt other measures in compliance with applicable national legislation and international contracts by which the CR is bound.
13. The Operator does not provide Users with any guarantee for the uninterrupted provision of services or their accessibility or connection speed.
14. If required, the Operator is entitled to lay down other rules of operation of a part of the Network that are not in conflict with this Regulation.

III. Basic Obligations and Rights of Administrators of a Part of the CU Computer Network

1. The Administrator ensures, based on the Operator's instructions, the running of the infrastructure and service configuration in the part of the Network that has been entrusted to the Administrator for administration. The Administrator sees to the proper configuration, functionality and security of ICT components and services provided and ensures that their operation does not restrict or disturb the operation of the CU Computer Network or other networks or services.

2. With the Operator's consent, the Administrator may divide the Network entrusted to them into parts and delegate the administration of individual parts to different organisational units, external entities or natural persons.
3. The Administrator permits connection of devices to the Network under the conditions laid down in these Rules and according to the instructions of the Operator of the part of the Network and is in charge of assigning network addresses to such devices. To connect devices to the Network, the Administrator uses suitable technical means.
4. The Administrator establishes and cancels User Accounts (excluding CAS accounts) and registers User devices for access to the CU Computer Network. In the process of account establishing and device registration, the Administrator is obliged to adhere to the administration instructions issued by the Operator and common administration instructions laid down by the CSC.
5. In compliance with the provisions of Section 5 of Act No. 480/2004 Coll., on Certain Information Society Services, as amended, the Administrator whose activity lies in the administration of services consisting in storage of information (files) provided by Users is liable for the contents of the information stored at the request of a User only if:
   a. they could, with regard to the subject of their activity and the circumstances and nature of the case, know that the contents of the information stored or action of the User are illegal;
   b. they have, in a provable manner, obtained knowledge of the illegal nature of the information stored or illegal action of the User, and failed to take, without delay, all measures, that could be required, to remove or disable access to such information.
6. In compliance with the provisions of Section 6 of Act No. 480/2004 Coll., on Certain Information Society Services, as amended, the service provider whose activity lies in the administration of services consisting in storage of information (files) provided by Users is not obliged to monitor the contents of the information which they transmit or store or actively seek facts or circumstances indicating the illegal contents of information.
7. The Administrator is obliged to ensure adherence to copyrights, the authorised use of products, as well as respecting the set licence terms and conditions with respect to devices administered according to the Operator's instructions.
8. The Administrator is obliged to retain the identity of Users using a device or service administered by them or connecting their devices to the part of the Network administered by them, including such information that proves that the device was used by the User at a given time. This data must be stored for a period of at least 6 months. Upon request of the CSC or the Operator, the Administrator is obliged to immediately retrieve and provide such information in order to determine the liability for a Security Incident or to communicate the information requested by the Police of the CR.
9. The obligation to maintain the identity of Users pursuant to para 7 of this Article does not apply in cases in which the Administrator has, upon request of the Operator, implemented a technical solution permitting connection of devices in the part of the CU Computer Network with verification shared by multiple Users. The Administrator is obliged to ensure that such solutions are applied only for a period strictly necessary.
10. The Administrator is obliged to provide the necessary co-operation to the CSC and designated CSIRT-CUNI members when dealing with Security Incidents. In the event the Administrator is notified of blocking or disconnection of a device connected to the part of the Network administered by them pursuant to Article I (8), Part B of this Regulation or other measures taken by the CSC pursuant to Article I (9), Part B of this Regulation lying in the restriction or termination of services provided by or connection to the CU Computer Network, they shall immediately inform the Administrator of the device (or the

Administrator of the subordinated part of the Network, if applicable) and the head of the workplace concerned or the User whose identity data was used to connect the device.

11. In the event of substantiated suspicion of misuse by another person of a User Account administered by them, the Administrator is entitled to temporarily block the User Account. The Administrator is obliged to inform the User immediately thereof using the contact information retained for the purpose of the User Account in question or via another person designated by the Operator.
12. In the event of substantiated suspicion of device misuse, the Administrator is entitled to temporarily block or disconnect such devices. The Administrator is obliged to immediately communicate this to the device Administrator or the User whose identity data was used to connect the device or to other persons designated by the Operator.
13. In the event of violation of any of the provisions of the "Charles University Computer Network Rules" or supplementary rules issued by the Operator or in the event of handling a Security Incident, the Administrator is entitled to adopt relevant measures to ensure the proper operation of the CU Computer Network and Computer Network services. Should the measure adopted lie in the temporary limitation of service provision or connection to the CU Computer Network, the person who has taken this measure shall inform the head of the workplace concerned and the administrator of the device (or part of the Network) or service concerned. If this refers to a device connected to the CU Computer Network which has no Administrator assigned by the Operator, the information on the measure taken is communicated to the User whose identity data was used to connect the device to the Network. In the event of permanent restriction or termination of service provision, the Administrator is obliged to inform the Operator or the persons designated by the Operator.
14. The Administrator is entitled to retain, in compliance with the Operator's instructions, the operational data and information on services provided in the CU Computer Network for administrative, operational, statistical, monitoring and security purposes. The Administrator is entitled to analyse information obtained solely to the extent necessary for ensuring the proper functioning of the Computer Network and its services and in compliance with the applicable legislation. The information that the Administrator learns in connection with the aforementioned activities and that could be of confidential nature or relate to individual Users are subject to the confidentiality obligation. This obligation remains in validity despite the termination of an employment contract or any contractual relationship with CU. The Administrator shall not be bound by the confidentiality obligation if handling a Security Incident; in that case they have the right to provide the information related to the Incident to the Operator and CSIRT members. Furthermore, the confidentiality obligation does not apply to contacts with the Police of the CR or other law-enforcement bodies.

IV. Final Provisions

1. Each and every Operator is obliged to demonstrably acquaint all their employees with these Rules. If the administration is carried out externally, the above shall also apply to the employees of such Administrators or a natural person in charge of the administration of any part of the Network.
2. Each and every Operator is obliged to ensure that the access to the CU Computer Network or the access to authenticated services provided within this Network is enabled only after it has been verified that the User has given consent to the Rules and consent to personal data processing pursuant to paras V(2) and V(3), Part A hereof. Furthermore, the

Operator undertakes to immediately disable any User to further access the Network or use the services provided should the User withdraw any of the aforementioned consents.

3. The Operator's obligation stipulated in para 2 does not apply to services that are necessary for the fulfilment of study duties and other special services. The list of services which are not subject to the verification of the User's consent to the Rules and consent to personal data processing is published at https://uvt.cuni.cz/uksit.
4. Any potential violation of this Regulation by employees may be considered a breach of work duties and may affect, among other things, the employment relationship.
5. This Regulation No. 34/2017 issued by the Rector shall take effect on 1 September 2017.
6. To ensure adherence to the obligations of Operators and Administrators arising from this Regulation, a transitional period of one year has been set. Within this period any potential breach of any Operator's or Administrator's obligations arising herefrom caused by limited technical means shall not be considered a violation of the Regulation.

In Prague, on 11 August 2017

prof. MUDr. Tomáš Zima, DrSc., MBA
Rector