General Rules for Computer Infrastructure Users

All Network (LAN) users are obliged to follow the Charles University rules for network users. The rules are applicated for CERGE and EI equivalently.

Institutional computers are computers purchased by institution (CERGE or EI) no matter what source of financing was used. All purchased devices are property of the respective institution during theie whole lifecycle. In addition, network infrastructure rules apply also to any non-institutional computers and other devices like mobile phones connected via institutional wired and WiFi networks.

See also Rector's Measure No. 34/2017 / Computer Network Rules / at https://www.cuni.cz/UKEN-772.html or Opatření rektora č. 34/2017 at
https://cuni.cz/UK-8237.html
PDF version is available at
https://www.cuni.cz/UKEN-772-version1-charles_university_computer_network_rules.pdf

Every CERGE-EI employee (faculty, researchers and staff) and student (further referred to as “users”) will be issued an individual user account. Identity of each user must be explicit. The account is strictly for individual use. The user is obliged to select and keep confidential a security password. The user who allows the abuse of his or her account, or makes such abuse possible, is responsible for any resulting damages caused. If the user suspects abuse of his or her, or any other account, he or she is required to report this fact immediately to the domain administrator. Unless otherwise agreed the user's rights at CERGE-EI expire with the termination of the user's studies or employment contract.

CERGE-EI's computing facilities and network can only be used for approved activities or those activities related to the institution's operations (tuition, projects, individual work, correspondence, etc.). It is forbidden to abuse the computer network by spreading commercial, political, religious or nationalistic propaganda.

E-mail use follows the same ethical rules as ordinary mail. The sender must not assume another person's identity (the same applies to filling out www forms) and must not annoy other users with correspondence. An e-mail letter is considered to be an open correspondence; therefore, the use of vulgarisms is forbidden.

For CERGE-EI users (staff, F&R, students), Windows and Apple Mac computers are provided in the version supported by the manufacturer. These two platforms ensure user comfort, support of the installed software by the IT department, the necessary security of operation and overview of the operation of the equipment owned by the institution (in accordance with the requirements for security according to the applicable laws and regulations), the up-to-date nature of the systems in use, protection of the institution's assets against theft and misuse, compliance with the licensing rules for the installed software, ensuring protection against third parties access.

While using CERGE-EI's computing facilities (like desktop PCs, laptops, tablets etc.), it is forbidden to distribute, install or use software and data for unauthorized purposes (distributing includes placing software on a WWW server), tamper with the hardware (device intrusion, hardware or software reconfiguration, connecting or disconnecting internal computer components, manipulating with the provided computer operating system and tampering with its installed features and components). When using the network, the user must not run software which has not been authorized by the

network administrator. Without such authorization, it is also forbidden to copy and distribute parts of the operation system or installed software that are not in the public domain.

It is forbidden to attempt to gain unauthorized access to programs, computers, information, privileged statuses, peripheries and data of the other users, or to mediate such access. It is forbiden to tamper with installed security and management tools (antivirus, asset management, privilege management etc.). If such a condition occurs unintentionally, the user is obliged to inform the machine or network administrator and, in case of his/her unavailability, to terminate the access. Computer and network administration and overall network and computer security compliance is non-transferable responsibility of the Computer Office.

Users must not deliberately overload the network (e.g., by sending mass mailings or chain letters). They must not change the configuration of the network equipment or manipulate it with devices not intended for public use. Users must follow all rules for handling the technical facilities.

Users must not spread information which contradicts the law or which might damage the honour of Charles University. This also applies to the construction of individual www pages and their direct references.

Users are also obliged to follow the specific rules as well as the laws (e.g., copyright and export laws) of the networks and their respective countries which he/she enters (both within and outside CERGE-EI).

CERGE-EI does not guarantee users in any way the uninterrupted operation of the computer network or its services, their accessibility or quality.

Network traffic is monitored to optimize network operation and to detect and prevent abnormal situations and attempts of unauthorized access. Users agree that their action and data may be monitored; any information acquired will be kept confidential. Neither the network administrator nor CERGE-EI carries any legal accountability for contingent non-delivery, delay or other defects with information transfers.

Text also available at CERGE-EI internal web
https://www.cerge-ei.cz/institutional-support/general-rules-for-lan-users

From:
https://wiki.cerge-ei.cz/ - **CERGE-EI Infrastructure Services**

Permanent link:
https://wiki.cerge-ei.cz/doku.php?id=public:security_rules&rev=1738165452

Last update: **2025-01-29 15:44**