17 September 2022

Information about the computer network in Karlín

The following IT administrators take care of the network and computer services in Karlín:

Name	Contact (office, phone, e-mail)	Main responsibility
Jaroslav Richter	K381, 95155 3206, richter@karlin.mff.cuni.cz	User support, account creation, computer registration
Martin Trčka	K381, 95155 3237, trcka@karlin.mff.cuni.cz	Computer classrooms and computer lab K10
Oldřich Ulrych	K387, 95155 3216, ulrych@karlin.mff.cuni.cz	Network and servers

(If you are not sure who to contact, please contact any of the people above.)

Services for faculty, staff, PhD students, guests

- computer classrooms (K11, K4, K10A, K10B) - for access to the rooms, for setting up a teacher user account (LABK domain) or for installing the necessary software -> M. Trčka
- connecting to the Internet via the eduroam Wi-Fi network (login details must be set up by the user in the CAS system: *Other accounts -> Set password for eduroam realm cuni.cz*)
- connecting your computer to the wired network (computer registration) -> Jaroslav Richter
- Karlín user account (MSEKCE domain, see https://www.mff.cuni.cz/en/math/internal-affairs/net-and-computers/msekce) -> Jaroslav Richter, account offers:
  - the possibility to log in to the desktop computers in the Karlin building (e.g. computers in classrooms K1–K9 except for computer classroom K4)
  - an e-mail box with the address name@karlin.mff.cuni.cz (IMAP/SMTP or https://webmail.karlin.mff.cuni.cz)
  - Possibility to have your own website
  - Data space with backup
- furthermore, on request (-> Jaroslav Richter) we offer:
  - Remote access to a terminal (Windows) or SSH (Linux) server
  - VPN (remote access to local network e.g. from home)
- computing cluster (and Git) - see https://cluster.karlin.mff.cuni.cz/

For details of these services, see https://www.mff.cuni.cz/en/math -> *Internal Affairs*.

Note on security (phishing)

None of the Karlín administrators need to know the **password** to your account, and they certainly won't ask for it via email. So, if you receive an email asking you to provide or enter your login credentials on some (dubious) website (or else all your data will be blocked or deleted within 24 hours), it will most likely be a phishing scam.

The only known exception to this is the university's CAS system, which reminds users once a year that their password will expire in 14 days and that they should change it at https://ldapuser.cuni.cz/account/password/nomenu/1. But with the administrator J. Richter or O. Ulrych, you can also change the expired password (or at least extend its validity).

If you are in doubt whether an email message is genuine or a scam, you should contact any of the IT administrators.

17 September 2022

University and Faculty Computer Network Rules (unofficial summary)

Summary of the rules in one sentence:
You are joining an academic computer network - behave yourself.

The user shall:

1. become familiar with the **rules** of the network to which he/she is connecting; respect these rules and the instructions of the relevant administrator.
2. provide assistance in the creation of the **user account** and in any modifications to it; prove his/her identity when requested by the administrator; protect his/her user account from misuse.
3. connect his/her **device** (desktop computer, laptop, mobile phone, etc.) only in designated places and only by designated means (in some cases the device must be registered with the administrator before connection); the user is fully responsible for his/her device.
4. report any breach of **security** of their account or any element of the UK network or computer system that they become aware of, either to the administrator (of that network or system) or to the University Security Team (abuse@cuni.cz).
5. employees are required to use only **work e-mail accounts** under the domain "cuni.cz" for work-related matters (including communication with students).

The user shall not:

6. use the network in a manner contrary to the **mission** of the university (advertising, political and religious agitation and anything that damages the reputation of the university is prohibited).
7. violate any **law** (e.g. copyright law).
8. **harm** or damage (place unreasonable load on the network or servers, restrict or harass other users, damage technical equipment).
9. **hack** (attempt to obtain someone else's rights, work under someone else's identity, make unauthorized changes to programs or settings, create malicious programs).
10. connect **other people** or unauthorized network elements (e.g., switches or entire other networks) to the university network.

User acknowledges that:

11. the administrator does **not guarantee** 100% functionality and is not legally responsible for outages or possible loss of data - protection (e.g. backups) is therefore entirely the responsibility of the user
    - However, in Karlín, we normally back up all server (network) drives, with justifiable exceptions (e.g. the working directory for a computing cluster).
12. network operation is **monitored** to the extent necessary to ensure proper functioning of the network and to prevent security incidents.

Details:

- Rector's Directive No. 34/2017 (Charles University Computer Network Rules)
- Dean's Directive no. 4/2018 (Rules for administering and using devices connected to the MFF UK network)
- Guidelines of the Data Protection Officer: Guideline 3 – Use of private e-mail addresses