APPROVED BY
Order of KTU Rector
No. A-357 of 06 06 2008

RULES FOR THE USE OF KTU COMPUTER NETWORK

I. GENERAL INFORMATION

1. Kaunas University of Technology (hereinafter – University) provides its employees and students with a possibility to use information technologies and internet resources via the University's computer network.
2. The University respects the personal right to communication, diversity of values and views characteristic to the academic community, as well as privacy of all the members of the University's community.
3. Each user of the University's computer network is responsible for his/her actions performed while using the University's computer network.
4. These rules stipulate the proper use of the University's computer network.

II. DEFINITIONS

5. The user of the University's computer network – person using the University's computer network for the access to the services of the University's computer network or other computer networks (internet).
6. Resources of the University's computer network – digital resources of the computers connected to the University's computer network (processor's working time, used main memory hard disc location) as well as bandwidth of the University's computer network.
7. Computer security incident – the event having real or potentially undesirable effect to the computer's or computer network's performance which results in fraud, loss or misuse, threat to information, loss of the ownership of information or its damage.
8. Network administrator – University's employee who, at the assignment of the head of division, is authorised to manage a defined part of the computer network or computer system (install, change operational parameters, perform other maintenance work).

III. PURPOSE

9. The purpose of these rules is to define ethical, legal and secure principles of the use of computers and computer network to all the users of the University's computer network. Violations of these rules can pose a threat to the University and operation of the University's computer systems.

IV. APPLICATION

10. The requirements of these rules are binding to all the users of the University's computer network: employees, students, persons on temporary visits to the University, staff of the third parties who use the University's equipment or resources. These rules are applied during the use of the equipment of the University's computer network or the equipment rented to the University.

V. GENERAL PRINCIPLES OF USE

11. The resources of the University's computer network are intended for studies, scientific work and informal learning.

12. The users of the computer network are responsible for rational and ethical use of the University's resources.

13. The user has to follow the instructions of the authorised employee while using the resources of the University's computer network.

14. The University's divisions may have additional rules of the use of computer equipment and computer network that cannot contravene these rules.

15. The University's computer network guarantees the privacy of its users; however, the users have to know that comprehensive confidentiality of the information stored in the devices of the University's network is not guaranteed. It is recommended for the users to encrypt all the information they consider confidential.

16. To ensure compliance with these rules the University reserves the right to perform regular inspections of computer networks and systems.

17. To perform the functions of maintenance and security of computer network, the authorised persons of KTU ITPI Computer Network Centre (hereinafter – KTC) can monitor and check the network equipment, system and network traffic at any time.

VI. SECURITY

18. The users of the University's network have to preserve the resources of computer network and take all required security measures for the disposable digital resources to be used only for their intended purpose.

19. The users have to protect and never disclose their passwords, as well as do not let anyone to use their system login name.

20. All the computers of workplaces and laptops connected to the University's computer network have to be protected using password and screen saver with password that automatically logs out the user or locks the desktop after 10 minutes of idle at the latest (the provisions of this paragraph may be changed during the teaching process or events in accordance with the decree of the head of the division).

21. All the computers of workplaces and laptops connected to the University's computer network have to have installed constantly operating and regularly updated antivirus software.

22. The users of the University's network have to be careful while opening the files attached to emails, because they may contain viruses, bugs or other malware.

VII. VIOLATIONS

23. The users of the University's computer network are prohibited to:

23.1 Perform the actions violating the rights of any natural person or legal entity protected by the laws on copyright, related rights and intellectual property rights. Such actions include installation, use, storage or distribution of software without licence, copying of the works protected by copyrights;

23.2 Launch malware in the computer network, service or workstation (i.e., computer viruses, bugs, Trojan horses, etc.);

23.3 Reveal the login information of the University's systems (login name, password) or allow other persons to use the user's login name;

23.4 Disseminate false information using the University's network systems or send such information using the University's name;

23.5 Disturb the network operations. Such actions include flooding of the network with unnecessary packages, falsifying of network packages, etc.;

23.6 Perform network intelligence activities (scanning of ports, service stations or security of services) without a prior agreement with KTC;

23.7 Monitor network traffic intercepting the data not intended for the user's computer, except for the cases when such actions are part of the duties;

23.8 Consciously use the information when the user is not the intended recipient of the information;

23.9 Login to the service station or account when the user has not received a direct permission for such login, except for the cases when such login is performed while performing direct duties;

23.10 Bypass or otherwise violate the authentication or security systems of any computer, network or account;

23.11 Disturb the operation of the computer system or eliminate the possibility to use the provided service or information;

23.12 Upload harmful or intolerable information and links to such information in the University's computer network or online using the University's computer network or the University's name. examples of such information: information in breach of the law; pornography or other improper material; information fuelling national, racial, ethnic, religious hate, advocating violence and terrorism; information discrediting or offending the University, other organisations, countries or private persons;

23.13 Use the University's resources for development of commercial activities or for benefit;

23.14 Individually change the set computer's parameters (IR address, etc.);

23.15 Violate the rules for the use of the other networks which services are being used or equivalent rules;

23.16 Perform any other activities violating the laws of the Republic of Lithuania and international agreements.

24. While using email and other means of communication, it is prohibited to:

24.1 Send advertising messages when their receiver has not expressed any wish to receive such messages or when the University's administration has not provided a special permission for such messages;

24.2 Any form of abuse and harassment using email, telephone or other means of communication;

24.3 Falsify the information of official headings of the email messages;

24.4 Send chain emails.

25. The user of the University's computer network who notices the listed violations of the rules or other incidents of computer security, has to

25.1 Save the proof of violation;

25.2 Immediately notify the administrator of the network or service station;

25.3 Follow the instructions of the person responsible for the analysis of the computer security incident (KTC employee or administrator of the network, service station or workstation).

VIII. RESPONSIBILITY

26. The University is not responsible for the damage and loss incurred using the University's computer network.

27. The user of the University's computer network is responsible for the damage to computer, computer network or information resources caused by the failure to follow these rules and other rules for the use of computer network and information services approved at the University, under the procedure set by the University and by the legislation of the Republic of Lithuania.

28. The user of the University's computer network is responsible for the violation of the law committed while using the University's computer network according to the current Administrative Code, Criminal Code and Civil Code of the Republic of Lithuania.

29. The user of the University's computer network is responsible for the material loss committed while using the University's computer network according to the current Labour Code and Civil Code of the Republic of Lithuania.

30. The user of the University's computer network who fails to follow these rules may be prohibited to access the resources of the computer network; disciplinary penalties are imposed for serious violations under the procedure set by the University, including termination of the employment contract or removal from the student lists.

_____