jamk

Guidelines for the administration of the data network

Table of contents

1 Purpose

The purpose of the guidelines for the administration of data networks is to confirm the principles referred to in section 12(3) of the Act on Co-operation within Undertakings (1333/2021), the principles of the administration of e-mails and data network approved by the Board of the JAMK University of Applied Sciences which together with the guidelines of use of the network safeguard the implementation of the protection of communications and privacy in the network while ensuring the availability and balanced development of diverse communications services.

2 Scope

These guidelines apply to all computer systems and communication networks maintained by Jamk and to such other systems whose availability or access right has been obtained through the ICT Services of Jamk or which are either directly or indirectly managed and operated by the ICT services. An exception to this are areas isolated from the network, which are used in teaching and research. The administrator or the teacher of such a network is responsible for ensuring that laws, decrees and regulations as well as good information management are followed.

3 Definitions

Administrative personnel refers to the ICT Manager, system planner, technical expert, and other persons that have been separately appointed as administrative personnel.

Jamk's data network refers to the wireless and Ethernet networks maintained by Jamk's ICT services for communication within and between the campuses and the provision of a connection to a public network.

The data network includes services and information systems that are developed and maintained by Jamk's ICT services. The administration of services and information systems requires administrative rights.

4 General principles

Granting administrative rights must be carefully considered. They can only be granted to persons with adequate competence and a clear administrative access need to systems. A person who has been granted administrative rights is responsible for ensuring information security for their part and ensuring that user IDs are used correctly.

26.8.2022

5 Administrative rights

Jamk's ICT service personnel, other Jamk personnel who need administrative rights to systems, and system provider's experts who maintain Jamk's systems can obtain administrative rights to Jamk's information systems. Administrative rights end when the employment relationship ends or in other situations when the person no longer needs the rights.

6 General conditions

6.1 Rights

Administrators have more extensive rights than other users which help them monitor, restrict and control the use and actions of the systems they maintain. If necessary, the administrator can also copy, transfer or delete information stored on hardware or networks. The administrator has the right to in-stall programs that look for harmful material (viruses and spam mails) and prevent their spread.

6.2 Responsibilities and obligations

The administrator is subject to the following responsibilities and obligations:

- Ensuring the functioning and good working conditions of information systems.
- Confidentiality. Information related to the tracking of system use or obtained through administrative duties must not be misused or further handed out.
- Communicating matters related to the system as well as changes and their impacts.
- Providing instructions and guidance on the use of the system. Making guidelines for use available to the users.
- Administrators must manage users and process log data without violating privacy and the confidentiality of communications. The administrator can process log data only if misuse is suspected or when investigating incidents.

6.3 Restrictions

The following restrictions apply to administrators:

- The administrator may only interfere with users' network use and files if it is required by an investigation of a problem or reinstating the system to operational condition, or if there is justified reason to suspect that the guidelines of use have been violated.
- The administrator does not automatically have the right to open a person's emails.

**Guidelines for the admin-
istration of the data net-
work**

5 (6)

26.8.2022

Opening an email is an exceptional situation, and it is only possible in special situations (e.g. death of a person) in accordance with separate instructions.

7   Supervision of guidelines

The ICT services personnel and other persons appointed for the task monitor compliance with the guidelines of the administrators of Jamk's information networks and systems. The implementation of the supervision of the guidelines is the responsibility of supervisory and managerial employees of the University of Applied Sciences. The Jamk Chief Information Security Officer and ICT Manager, who further reports to the Director of Administration, have a special responsibility for the supervision and evaluation of the implementation of the guidelines.

7.1   Personnel supervision

The actions of administrators are primarily supervised by managers. In case of external specialists, monitoring is carried out by system owners.

7.2   Technical supervision

Technical supervision is implemented with various network management and monitoring software, security software and analyses of log files related to information systems.

7.3   Registers

Personal data related to administrators is stored on various registers. Data subjects can view the privacy policy of the register in accordance with the Data Protection Act 1050/2018.

8   Non-compliant activities

8.1   Misuse of administrator rights, information system and information network

Misuse of the administrator rights, information system and the network refers to all intentional or negligent actions that:

- cause harm or damage to system users
- cause harm or damage to another information system or environment
- to which the system is connected
- violate the provided guidelines
- use such parts or properties of the system that
- the user has not been clearly authorised to use
- are prohibited by the system administrator or owner.

jamk

26.8.2022

8.2 Legislation and regulations on misuse

The key laws and regulations guiding most common misuses include the Universities of Applied Sciences Act, University Regulations and Degree Regulations. Jamk's own investigation and restriction measures are primarily applied to the licences in accordance with the following process:

- Jamk's ICT services' own investigation and restriction measures. As a result of actions that go against the guidelines, the access right to a system can be removed immediately either for a fixed period or for the time being.
- If the misuse is illegal, it is submitted to the police for investigation. Authorities process misuses and their consequences according to regulations provided for in Chapter 38 of the Criminal Code of Fin-land, Copyright Act and Data Protection Act.
- Misuses in employment relationships are processed in accordance with the Employment Act.
- You can appeal a decision on a disciplinary matter to the Administrative Court of Hämeenlinna within 30 days of the notification of the decision. A decision on temporary dismissal and removal of access rights can be implemented regardless of whether an appeal has been made.
- The person responsible for misuse may be liable for damages. The misused resources may be subject to charges on material damages and costs of the investigation work caused by the misuse.

9 Entry into force and publication

These guidelines for network administration will be in force until further notice from 15 September 2022. These administration guidelines override all previously created administration guidelines.

The guidelines are published on the JAMK HelpDesk website and on the ELMO intranet.