Administrative Rules for Information Systems at the University of Applied Sciences

The purpose of the Administrative Rules for Information Systems is to describe all main rules by which the main user or the information system administrator’s special privileges may be utilised in a way that intervene with a user’s privacy. The descriptions are not technically comprehensive. The administration is steered by the legislation attached to this document (Appendix 1: FUSEC/19.11.2012, Guiding Legislation).

Introduction

As the main users, administrators have access possibilities for ”full rights”, which means that an administrator is able, without breaking any protections, to read the contents of any file, start or terminate any programme and monitor all ongoing processes and traffic. Content analysis of telecommunications is required to be monitored by automatic intrusion detection systems (IDS). As the administrator’s technical rights in the administrated environment are in practice unlimited, they are in principle inconsistent with the users’ basic rights and privacy protection.

Therefore each information system administrator is responsible to follow these guidelines defining the good administration practices. In addition, system administrative personnel include administrators ordered by Karelia University of Applied Sciences for administrative services (e.g. the main users of Email and data processing systems and devices).

Obligation of secrecy

An administrator cannot reveal any matters to third parties. An administrator will not use any of the information to non-work related matters. Especially, the administrator commits to not disclose any private matters of the users to third parties that he/she has become aware of because of his/her duties or position.

Respecting the right to privacy

The right to privacy and confidentiality of communications of the users and their communication partners is observed in the administration of the information systems of the University of Applied Sciences. However, the University of Applied Sciences has, while observing these basic rights, a right to control the information content and purpose and define the appropriate use of the information systems in its possession. This also applies to the telecommunications in the telecommunications network owned by the University of Applied Sciences.

Processing emails

As a default, the secrecy of a private email and other electrical message is inviolable.

An email message is considered confidential if it is not meant to be generally received. If a user receives an email message intended for another person, the unintended recipient is obligated to maintain the secrecy of the message and refrain from utilising its contents or the knowledge of its existence.

Confidential messages are never allowed to be read without an agreement. As confidential messages may be demanding to be separated from other messages, the default is that emails of other persons are not allowed to be read without the person’s specific permission.

Users’ email accounts are allowed to be opened by the separate instructions regarding the “Retrieving and Opening an Employee’s Email” and by the following situations:

- With the person’s (user’s) specific permission
- An administrator is allowed to open the email account in when the email system cannot deliver messages due to lacking or damaged structure or content. However, the administrator is not allowed to read any text content meant for the receiver. It may be required, however, to check the address or personal identity of the sender or receiver or other data to repair the situation.

It is to be noted that handling mass mailings, i.e. spam messages is in most cases harmful for the operations of the University of Applied Sciences. Necessary protective steps against mass mailings are taken, e.g. the server may deny accepting messages from certain servers or certain other emails meeting some other set characteristics. The denial of reception may be necessary in order to protect the users and the systems, even though it does limit the users’ rights to free email traffic.

When an email has been received and transferred from the in-box, it is protected by the same regulations as other normal files owned by the user ID.

The rules for email are presented in more detail in the Email rules of Karelia University of Applied Sciences.

Processing other files

An administrator has no general right to read or otherwise process the contents of files owned by users unless their protection allows it.

An administrator has, however, the right to process files under following circumstances:

- When the user has authorised this
- If there is a valid reason to suspect that a user ID has fallen into wrong hands and that it possesses files or programmes that cause danger or threat to the functionality or security of the University of Applied Sciences. The common principle is that an attempt is made to contact the user before any action, but protection and repair actions may have to be done prior to any contact.
- If there is a valid reason to suspect that the owner of a user ID him/herself is guilty of a malpractice, and it may be assumed that certain files owned by the user contain evidence of said malpractice. In these cases the administrator is to inform the suspicions and the grounds to the administrators of the same system, unit head or another authorised person.
- When the user ID owns files, scripts or initialisation files that have a severe effect on the functioning of the system an administrator always has a right to verify the contents of the files and stop their operations if necessary. This is to be reported to the administrators of the same system and the file owner concerned must be informed.

The home directories of users include initialisation files which direct the function of versatile programmes. As a part of normal administration, these files may need to be subject to changes. In addition some initialisation files are monitored by the administration as part of normal safety operations.

In the directories of the temporary files of a system and the temporary files in the home directories of a user may be deleted as a part of normal disc space administration.

Monitoring directories and file lists

Under normal circumstances, an administrator cannot fully avoid requesting and seeing file lists of directories owned by users. Processing directory structures, filenames, modification dates, sizes and protection levels along with other information pertaining to files is a part of normal administration that is done in accordance with good administration practice.

Monitoring programs and processes

An administrator routinely monitors the programs running in the information system as a part of normal administrative operations. An administrator can terminate of a process, should it consume the system's resources to an excessive extent or cause problems. This is also the procedure if the process is against the guidelines and regulations given by the administrator.

In this case the user is notified of the termination of the process and the aforementioned regulations.

If a disturbance in the information system or an extra load is found impairing the information system of the University of Applied Sciences, the traffic may be prevented by the administration.

Processing log files

The majority of the IT systems of the University of Applied Sciences create log files to document users' operations and visits in the system. These logs are necessary when investigating disturbances or misuse situation. Most logs are protected from outsiders in a way that only an administrator is able to monitor them but many mainframe auxiliary services display other users the information pertaining to user IDs besides the administrator.

The administration personnel use several log files constantly as a part of their normal administrative work. Monitoring logs is process –and device oriented work and in normal situations the activities of a single user are not monitored. Detailed log files are handled as confidential information and shall not be disclosed to any person to whom the information does not belong due to their tenure. Two exceptions are applicable:

- If log files are requested by a police authority, the information is disclosed in the extent expected by the statutory authority by the Coercive Measures Act or court order. The disclosure is to be registered.
- When preventing attacks, protecting against security breaches or other illegal attempts the University of Applied Sciences may operate together with other universities of applied sciences or service providers to investigate or isolate the origin of the hacker. In these cases it may be necessary to disclose information relating to a single user ID. Then, however, the disclosure is limited to such user IDs that is justifiably suspected to have been fallen into wrong hands or if there is a valid reason to suspect that the owner of a user ID him/herself is guilty of a misuse.

Monitoring data communications network and possible traffic limitations

The monitoring of network traffic does not concern the content of the transferred information but the amount and nature of the traffic. The monitoring of source and target computers is statistical and does not target an individual user. However, the traffic can be monitored in more detail in the case of an individual system, when traffic anomalies, e.g. excessive traffic load, are being investigated. Automatic intrusion detection systems (IDS) may analyse all traffic.

The recommendations and guidelines of Funet are followed in the priorisation and limitation of network traffic.

Further information

The instructions referred to or related to by these instructions are:

- IT Service User Rules
- Email Rules
- Retrieving and Opening an Employee’s Email
- Consequences of IT Service Abuse
- Tables of Penalties of IT Service Abuse
- Administrative Rules for Information Systems (this document)

Appendices

Appendix 1: (FUSEC/19.11.2012) Guiding Legislation

Appendix 1: (FUSEC/19.11.2012) Guiding Legislation

Guiding Legislation

All IT administration and IT service actions must obey the Finnish law, decrees and statuses. They also define the possible consequences of IT service abuse.

The guiding legislations concerning the university, employees and students include:

- The Archives Act (831/1994)
- Administrative Procedure Act (434/2003)
- Personal Data Act (HetiL, 523/1999)
- Act on the Openness of Government Activities (JulkL, 621/1999)
- Act on the Protection of Privacy in Working Life (TETSL, 759/2004, Chapter *6*)
- The Criminal Code (39/1889, Chapter 35:1,2 §; Chapter 38:2 §, Chapter 38:3–4 §; Chapter 38:8 §)
- The Constitution of Finland (731/1999, 10–12§)
- Act on the Protection of Privacy in Electronic Communications (SVTSL, 516/2004)
- Copyright Act (404/1961)
- Universities Act (558/2009 Chapter 5:45 §; Chapter 10:85 §)
- Tort Liability Act (412/1974, Chapter 4; Chapter 5:5-6 §; Chapter 6)
- Employment Contracts Act (55/2001, Chapter 7:1-2 §; Chapter 8:1 §;)

The guiding legislations concerning the university of applied sciences, employees and students include:

- The Archives Act (831/1994)
- Administrative Procedure Act (434/2003)
- Personal Data Act (HetiL, 523/1999)
- Act on the Openness of Government Activities (JulkL, 621/1999)
- Act on the Protection of Privacy in Working Life (TETSL, 759/2004, Chapter 6)
- The Criminal Code (Chapter 38, Data and communications offences)
- The Constitution of Finland (731/1999, 10–12§)
- Act on the Protection of Privacy in Electronic Communications (SVTSL, 516/2004)
- Copyright Act (404/1961)
- Polytechnics Act (351/2003 Chapter 6:28 §; Chapter 9:42)
- Tort Liability Act (412/1974, Chapter 4; Chapter 5:5-6 §; Chapter 6)
- Employment Contracts Act (55/2001, Chapter 7:1-2 §; Chapter 8:1 §;)

The guiding legislations concerning secondary education, employees and students:

- The Archives Act (831/1994)
- Administrative Procedure Act (434/2003)
- Personal Data Act (HetiL, 523/1999)
- Act on the Openness of Government Activities (JulkL, 621/1999)
- Act on the Protection of Privacy in Working Life (TETSL, 759/2004, Chapter 6)
- The Criminal Code (Chapter 38, Data and communications offences)
- The Constitution of Finland (731/1999, 10–12§)
- Act on the Protection of Privacy in Electronic Communications (SVTSL, 516/2004)
- Copyright Act (404/1961)
- Vocational Education and Training Act (630/1998 Chapter 5:35 §; Chapter 6:44)
- Tort Liability Act (412/1974, Chapter 4; Chapter 5:5-6 §; Chapter 6)
- Employment Contracts Act (55/2001, Chapter 7:1-2 §; Chapter 8:1 §;)

The guiding legislations concerning adult education, employees and students:

- The Archives Act (831/1994)
- Administrative Procedure Act (434/2003)

- Personal Data Act (HetiL, 523/1999)
- Act on the Openness of Government Activities (JulkL, 621/1999)
- Act on the Protection of Privacy in Working Life (TETSL, 759/2004, Chapter 6)
- The Criminal Code (Chapter 38, Data and communications offences)
- The Constitution of Finland (731/1999, 10–12§)
- Act on the Protection of Privacy in Electronic Communications (SVTSL, 516/2004)
- Copyright Act (404/1961)
- Vocational Education and Training Act (630/1998 Chapter 5:35 §; Chapter 6:44
- Tort Liability Act (412/1974, Chapter 4; Chapter 5:5-6 §; Chapter 6)
- Employment Contracts Act (55/2001, Chapter 7:1-2 §; Chapter 8:1 §;)