LAPIN YLIOPISTO
UNIVERSITY OF LAPLAND

Data Administration and ICT Services
ICT Security, rule
13.5.2016
Public

Administrative Rules of Information Systems

Version	Date	Modifications	Author
1.0	13.05.2016	Document created	Esa Mätäsaho
1.0	13.05.2016	Processed in the employee co-operation council	
1.0	16.05.2016	Approved by the Director of Administration	

1 INTRODUCTION

1.1 DEFINITIONS

In these rules, **administration** refers to

- making necessary changes or corrections in the information systems,
- administering user IDs and usage and access rights in information systems, and
- monitoring and keeping statistics on the operation and usage of information systems

Information system or **system** refers to

- a single data processing device or system, or a collection of such,
- University computer network,
- software and services running in the above-mentioned, and
- the information content within the above-mentioned

User refers to the employees and students of an organization of the Lapland University Consortium (LUC). It also refers to other persons with user privileges issued according to the principles of the user administration of an LUC organization.

Administrator refers to all personnel in charge of the maintenance of the ICT services in LUC. It also refers to the personnel of an external organization with maintenance rights issued by LUC and to persons with some root privileges to a system.

A University unit refers to a University department, division or other functional area of responsibility.

The duty of an administrator of an information system within the University is to take care of the information system technically. The owner of an information system is also the administrator, unless administrative duties have been moved to another unit within the University or outsourced by a contract.

1.2 AUTHORITIES OF ADMINISTRATOR

In order to guarantee the functionality of information systems, an administrator has extensive privileges to inspect the status of the systems and, if necessary, to intervene in the function of the systems, to the use of said information systems by individual users and their data in the information systems.

In order to combat breaches of information security and to eliminate any disturbances targeting information security, an administrator has the right to take necessary steps to ensure information security.

In order to avoid a conflict between an administrator's privileges and the juridical rights of the users of the system, the use of an administrator's privileges is directed through guidelines and regulations that are based primarily on Finnish legislation and additionally on the regulations of the use of the University's information systems along with the information security principles of the University.

These regulations are binding to all administrators in the University, including any students, should they be the administrator of an information system connected to the University information network.

These regulations and other guidelines to the use of the University's information systems are available at the University web server.

2 RESPONSIBILITIES

A unit must document the information systems or system entities in its possession. These systems have to be prioritized and information system administrator and technical administrators have to be assigned. The owner of the information system is responsible for the existence and availability of eventual information system declarations.

The owner of the information system and ultimately the head of the unit are responsible for the adherence to law, good administration practice and the current regulations and policies of the University in the system. The owner always has the ultimate responsibility to the administration of the system. An information system administrator is responsible for the technical administration of the systems in a manner adhering to good administration practice. Every system must have assigned administrators. Administration duties are distributed, where possible, to several individuals with different access rights. Any actions by administrators are logged as well.

The owner or administrator of an information system is not responsible for the content of an individual users data. A user him- or herself is responsible for the legality of his or her data and is required to protect them in accordance to guidelines set by the University. An information system administrator has, however, a legal right and obligation to intervene with a user's data, if there is a reasonable suspicion that it contains information security hazards or illegalities.

If an administrator is under suspicion to have misused his or her privileges, a contact is made to the foreperson of the unit, who along with the Chief Information Officer of the University of Lapland decides on any further and protective measures taken.

3 ACTING PRINCIPLES

3.1 GOOD ADMINISTRATION PRACTICE

The information systems are to be administrated in accordance to good administration practice. A good administration practice means planned, responsible and professional administration, in which the good information management practice, detailed in the Act and decree on the Openness of Government Activities, is being observed.

3.2 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 University's information systems. However, the University has, while observing these basic rights, a right to control the information content 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. The appropriate use is defined in detail in the Acceptable Use Policies of Information Systems or in an individual system's usage regulations.

When users ask an administrator to handle their e-mail or other files, the administrator must secure the person's identity in an appropriate way, e.g. via a legitimate proof of identity, should the administrator not know the user personally.

When an administrator has the need to contact a user, it can be done either to a phone number or an e-mail address available in the University administration's information systems. However, in cases where there is a doubt that the user ID has fallen into wrong hands, e-mail must not be used.

3.3 OBLIGATION OF SECRECY

Obligation of secrecy and non-exploitation bind administrators with regards to any non-work related matters and the existence thereof that they may become aware of while performing their duties. Non-public work-related matters may only be discussed with such persons or officials that are bound by the same confidentiality as the administrator and whose duties the matter involves.

An administrator is specifically bound by the Penal Code, chapter 40, section 5, which states that administrators cannot without authorization reveal or exploit any secret or otherwise legally confidential matters, such as private matters of the users, that they, during or after their tenure, have become aware of because of their duties or position.

An administrator shall sign a non-disclosure agreement.

4 PRACTICAL ACTIONS

4.1 IDENTITIES AND PASSWORDS

An administrator does not need any user's password to fulfill his duties, and he must not inquire said password from the user.

Should the correcting of a problem require a momentary use of the user's identity, then either the user must be present to input his or her password to the authentication service, or the administrator must assume the identity of the user through an administrators privileges. The user must be informed of the latter as soon as possible. The identity must not be used any longer than what is necessary to correct the problem.

In these situations the administrator must secure the identity of the user in an appropriate manner.

Administrator privileges are to be used only when administrator's duties so require.

4.2 LIMITING USER RIGHTS FOR DURATION OF INVESTIGATION

Should a doubt arise that the University's information security has been compromised or that a user has been guilty of actions contrary to usage guidelines, an administrator has the right to limit the user's access rights for the duration of an investigation.

The sanctions attached to proven misuse are processed in accordance with the applicable legislation.

4.3 PROCESSING E-MAILS

The secrecy of a private letter, call or other confidential message is unbreakable according to the Finnish Constitution, should the law not dictate otherwise. An e-mail message is comparable to a letter. An e-mail message is considered confidential if it is not meant to be generally received.

The normal principles of processing e-mail are defined in the Rules for Handling E-Mail. Administrative Rules of Information Systems (i.e. this document) details specific situations where an administrator has to intervene with e-mail relaying in order to ensure the system's service level or security.

a) When a user requests it from the administrator. The request can be made e.g. in a situation where the user's mailbox cannot be opened with the software in the user's disposal. The authorization by this request concerns one defined instance. If a user asks information about the contents of the mailbox, the administrator must unconditionally secure the identity of the maker of the request (see section 3.2).
b) When a user's mailbox causes disturbances e.g. because of its large size or damaged structure.
c) A mailbox that is disturbing the flow of e-mail must primarily be transferred to another location without opening it. The user must be notified of the location of the mailbox, should the mail system not automatically find it in the new location. If the mailbox due to it large size cannot be placed in a location accessible to the user, a method of transferring the messages to the user must be agreed upon with the user. A mailbox being transferred may be compressed to a less space consuming format, if the user is provided with exact instructions on how to access the e-mails. A large mailbox can also be deleted in a specific exceptional situation, if no other action can be taken on it within reason. This decision is made by the head of the unit administrating the system.

d) An administrator is allowed to repair a structurally faulty mailbox without asking for the user's specific permission. However, the administrator is not allowed to read any text content solely meant for the receiver. The administrator is bound by confidentiality in this as in other situations.
e) The user shall immediately be notified of any non-automatic actions taken on his or her mailbox.
f) When the e-mail system cannot deliver it due to lacking or damaged structure. In this situation the administrator is allowed to investigate and repair the technical guidance data of the message. However, the administrator must, where possible, not read the textual contents solely meant for the receiver of the message.

An administrator also has a right to purge the queue of delivered mail from any messages that are hazardous to the function of the e-mail system and messages that have been generated by a technical error and are apparently unnecessary.

4.4 PROCESSING OTHER INFORMATION

An administrator has no general right to read or otherwise process the contents of files owned by users.

However, an administrator has the right to process said files under following circumstances:

a) When the user has authorized this in order to solve a problem situation.
b) After a specific written request (e.g. should the performance of University duties be impaired through absence, it may be necessary to process files owned by the absent worker/student and protected from others. The head of a unit or equivalent can order the administrator to give an assigned person access rights to the necessary files).
c) If a user ID holds programs or initialization files that cause disturbance to the functioning of the system, to security or to information security of other users. In this case the administrator can verify the contents of the files and, if necessary, stop their operation.
d) If there is a valid reason to suspect that a user ID has fallen into wrong hands and that it possesses files or programs that cause danger or threat to the functionality or security of the University.
e) If an administrator suspects that a user ID has fallen into wrong hands, he or she has the right to temporarily lock the ID. Other action is taken according to the practices of Reacting to Information Security Incidents and Policy of Consequences for IT Offences. 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.
f) If there is a valid reason to suspect that the owner of a user ID himself is guilty of a misdemeanor, and it may be assumed that certain files owned by the user contain evidence of said misdemeanor.
g) An administrator has a right to temporarily lock a user ID in case of a misdemeanor. A misdemeanor by a user is processed according to the University's Acceptable Use Policies of Information Systems, Policy of Consequences for IT Offences and Reacting to Information Security Incidents.
h) The administrators have a right to stop the display of such web pages that are against law, University web policy or Acceptable Use Policies of Information Systems.
i) When the protection of the files otherwise allows it anyway.

In addition to aforementioned privileges, an administrator always has a right:

a) to access and change initialization files, e-mail forwarding or sorting files and other files that have an effect on the functioning of the systems, should these files threaten the functionality or security of the system or the information security of the users. If the possible modifications cannot be done without erasing the modifications made by users themselves, the old version modified by the user is transferred to another file name and the user is notified of the change.
b) to certify that common disk areas have no files that are illegal or threaten the functionality or security of the system or the information security of the users. Such files include e.g. malware, recordings that are in violation of copyright or data that is illegal as per the Penal Code.

c) to manually or automatically delete files from disk areas assigned for temporary storage. This deletion must happen in adherence to predefined principles. The deletion principles must be available to the users, but deletions adhering to them do not have to be reported to the user concerned.

4.5 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.

Should a file's or a directory's protection found to be too weak in relation to its nature, administrator has the right to upgrade the protection to necessary levels.

An administrator is bound by confidentiality. In performing administrator's duties care is taken to not display filenames etc. unnecessarily. E.g. when file listings are needed to solve a problem case, "private" is printed in place of such files that do not pertain to the matter at hand.

4.6 MONITORING PROGRAMS AND PROCESSES

The administrator and the information system administrator together define what software shall be available in the system. Programs can be prohibited or removed from use, if the use of said programs is not necessary for the functioning of the University and the present a threat to the service level and security. This decision is made by the [administration team foreperson] of the unit administrating the system.

An administrator routinely monitors the programs running in the information system.

An administrator can adjust the processing priority of a process, should it consume the system's resources to an excessive extent.

An administrator can terminate a process if

- the function of the process has clearly been disturbed
- the process impairs the function of the rest of the system by extra load and is not contributing to the University's functioning or
- the process is connected to software, the use of which 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.

4.7 MONITORING DATA COMMUNICATIONS NETWORK

An administrator of the University data communications network monitors the traffic of the University network and its external connections with monitoring software and by reviewing log data in order to guarantee a reasonable service level and security as well as to take care of financially efficient use of the external connection.

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.

An administrator of the data communications network can contact the person responsible for the computer that causes excessive traffic or other anomalies in order to investigate a possible disturbance or misuse situation.

An administrator of the data communications network may deny communications or the use of a certain service from a computer or a part of the network,

- that causes traffic which threatens the service level or security of the network,
- if there is a valid reason to suspect that a computer or computers have fallen into wrong hands or are infected by malware,
- in which the Acceptable Use Policies of Information Systems are being breached
- which is not properly administrated especially with view to information security.

In all cases, the responsible administrator of the computer or the part of the network shall be contacted immediately after the denial of traffic.

4.8 PROCESSING LOG FILES

The University's information systems create log files to document the functioning of the system, to investigate eventual disturbance or misuse situations and to collect billing information. In the University, the logged information is only used in the technical duties of administrators bound by confidentiality as well as to enable billing. The principles of processing log files are defined in detail in Log File Processing Regulations. Log files can form a registry that falls under the scope of the Personal Data Act (523/1999).

4.9 DATA STORAGE

The provider of information system services must, as a part of system administration, take care of backing up their systems. Back-ups in case of disk failure shall be taken sufficiently frequently. At least modified files must be backed up daily.

Back-ups shall be stored appropriately, and the administrator shall make sure that the back-ups are accessible. The information on back-ups shall be processed in adherence to the same principles as equivalent information in an information system. The deletion of back-ups shall take place in such a manner that the confidentiality of the information contained therein will not be compromised.

5 SUPERVISION OF THESE RULES

Compliance with these rules is overseen by the ICT Security Manager of University of Lapland in cooperation with the ICT Services of the Service Centre of the Lapland University Consortium, as well as by superiors within their job descriptions. Breaches of the rules lead to sanctions according to the applicable Legislation.

The rules shall be updated when necessary. The need for updates shall be monitored by the ICT Security Manager.

Appendix I Guiding Legislation

In all administration, Finnish law shall be followed. Laws considering administration are:

- The Constitution of Finland (731/1999)
- Personal Data Act (523/1999)
- Act on the Openness of Government Activities (621/1999)
- Decree on the Openness of Government Activities and on Good Practice in Information Management (1030/1999)
- Information Society Code (917/2014)
- Act on the Protection of Privacy in Working Life (759/2004)
- Act on Changing the Act of Cooperation in Government Bureaus and Institutions (651/1988) (479/2001)
- Act on Electronic Services and Communication in the Public Sector (13/2003)
- Penal Code (39/1889)
- Coercive Measures Act (450/1987)

and the decrees, other statutes and orders issued under the aforementioned.