TTY/520/002/2013

23.5.2013

Administrative Rules of Information Systems

Definitions

In these rules, *administration* refers to maintaining information systems and keeping them secure, 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(s) or service(s) refers to data processing device(s) or system(s), or a collection(s) of such, University computer network, software and services running in the above-mentioned, and the information content within the above-mentioned.

Administrator refers to persons responsible for the computer administration and technical management of the University information systems, and other University IT support personnel, who with the above-mentioned take care of the administrative tasks of the systems, user support and guidance. In the broadest sense, administrator refers to all and any person(s) having administrative rights in the information system. Also student(s) responsible of maintaining and managing information system connected to University network is considered to be an administrator.

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

A *responsible owner of an information system* within the University is the unit for which functioning and data processing the information system has been procured, and which defines the persons entitled to use the information system. Author of programs, web pages and other such material can also be considered to be the responsible owner of the material according to the Copyright Act.

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.

Authorities of administrator

In order to guarantee the functionality of information systems, an administrator has adequate 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.

The administrator privileges are directed through guidelines and regulations that are based 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 and other guidelines to the use of the University's information systems are available at the Tutka and POP ”IT > Rules and recommendations” and at IT Helpdesk.

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 and privacy 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 users data, if there is a reasonable suspicion that it contains information security hazards or illegalities (see Policy of Consequences for the Information Management).

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 Head of Information Management decides on any further and protective measures taken. These measures must be in accordance with Policy of Consequences for the Information Management.

Acting principles

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 and on Good Practice in Information Management.

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 Rules of IT service use 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.

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. Any private matter is considered to be an example of such information.

An administrator shall sign a non-disclosure agreement according to current TUT practices.

Practical actions

Identities and passwords
An administrator does not need any user's password to fulfil 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 and the use of such assumption must be logged or otherwise recorded as verifiable documentation. 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.

Limiting User Rights for Duration of Investigation
Limiting user rights is defined in consequences for IT system abuse document.

Processing E-Mails
Rules for E-Mail processing is defined in rules for E-Mail document.

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:

- When the user has authorized this in order to solve a problem situation.
- 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).
- 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.
- 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.
- If an administrator suspects that a user ID has fallen into wrong hands, he or she has the duty to temporarily lock the ID. Other action is taken according to the university rules and regulations. 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 himself is guilty of a misdemeanour, and it may be assumed that certain files owned by the user contain evidence of said misdemeanour.

An administrator has a right to temporarily lock a user ID in case of a misdemeanour.

A misdemeanour by a user is processed according to the University's rules for IT service abuse documentation.

The administrators have a right to stop the display of such web pages that are against law or University’s rules for IT service use.

When the protection of the files otherwise allows it anyway.

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

- 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.
- 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.
- 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.

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.

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 head 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.

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.

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), or contain recognition information that falls under the scope of the Act on the Protection of Privacy in Electronic Communications (516/2004).

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.

Supervision of These Rules
These rules are supervised by Information Management of the University and the owner of possible other information systems of University units. Offenses against these rules shall be dealt with according to the Policy of Consequences for IT Offences. The rules shall be updated when necessary, or when the common recommendations of the Universities are changed. The need for updates shall be monitored by the Director of Information Management.

Guiding legislation
The legislation guiding the operations of Tampere University of Technology are listed in relevant legislation document.