TTY/520/002/2013

23.5.2013

Information security policy

The responsibility of the functionality of the University lies with its highest administration. The functionality and services of the University are ever more dependent on the uninterrupted availability and secure function of information technology services. Exploiting information technology and committing resources to information security both on a general level and within the context of information technology are the administration's strategic decisions that will markedly affect the functioning ability of the University. Furthermore, there are legal obligations to maintain information security.
Information security policy is a statement by the Tampere University of Technology administration, in which the goals, responsibilities and means to secure information are laid out. All members of the University community shall be informed of the security policy, and they are obliged to act according to it. The policy is further defined in rules and guidelines of information processing.

Securing information is an essential part of the quality of the services and functions of the University, its total security and the day-to-day processing of information therein. Maintaining a good control on information security requires a continuous monitoring of all activity, long-time planning, preparing against various threat scenarios, adhering to procedures that have been agreed upon, guidelines, training and communication. The goal is to create and maintain a reliable and secure environment to process both University community's own information and information of different liaison groups being handled within the University.

Goals

Information security consists of confidentiality, integrity and usability of information. The goals of the University are to adequately and functionally secure the operation of information, information systems, services and information networks that are important to its functions, prevent their unauthorized use and unintentional or intentional destruction or distortion of information.

Information security shall be maintained in all forms and during the whole lifespan of information when processing it manually as well as with the aid of information technology. The basic nature of each unit of the University and the possible need for increased security must be taken into account. A special care for information security has to be taken in units that process large amounts of confidential or otherwise classified information. In securing information, the administrative, human resources, physical, data, data transfer, hardware, software and usage security are taken into account as separate areas, as per state administration procedures.

Information security work consists of continuous development, planning, implementation and monitoring in order to secure information. Its goal is to prevent damage from internal and external threats to information or limit it to acceptable levels and prepare for recovery from exceptional situations. As a part of securing information processing during normal conditions, the University also prepares for disturbances and exceptional circumstances in a manner which enables it to continue functioning as undisturbed as possible under all circumstances.

The information security of the University shall be maintained according to national and international decrees on information security, and by adhering to

the guidelines and recommendations for information security in state administration.

Organization and Responsibilities of Information Security

All users of University IT systems are responsible to obey the rules and instructions given by the University.

The essential players and roles in addition to their responsibilities and duties related to information security are listed in information security responsibilities document.

Methods of Implementation

Maintaining and developing information security is a continuous process which takes place by administrative, physical and information technological decisions. Actions of users are guided by decrees and guidelines of use included therein, as well as and training and information distribution on secure processing of information. Secure processing of information shall also be agreed upon with organizations and other cooperating partners processing University information.

The necessary level of protection (basic level/enhanced levels) and the necessary protective measures are defined in risk assessment procedures. Significant data and information systems of the University and the units as well as the threats targeting them shall be mapped and grouped. The magnitude of loss, should a threat be realized, shall also be assessed. Risk assessment is repeated periodically and in conjunction with changes.

University information security plan containing the demands of basic security of information processing and requirements of improvement shall be drafted on basis of the information security policy and the risk assessment. Information security decisions and implementations are described in relation to each usage environment, unit, service, application and system in separate plans if necessary. The plans shall state which risks require addressing and which are acceptable in terms of University functionality and legal demands.

Information security is included in the development of University operating procedures and yearly planning of operations and units.

Information security guidelines required in their work are distributed to the personnel. The students are informed about information security and decrees and recommendations concerning them. General information security awareness of the members of the University community shall be increased by advisories and writings on different information channels as well as by organizing training courses. The level of information security in the University's information processing and information systems shall be evaluated by means of internal review and, if necessary, with external review. Shortcomings in information security shall be analysed with maintainers and owners of information systems.

Communications

Matters concerning the information security of the University do not require active external information distribution. General information about information security procedures shall be distributed in order to improve public image, invoke trust in interaction with and using the services of the University and to guide users.

Information distribution about the information security of the University outside the University and, on a general level, inside the University is the responsibility of the Head of Information Management of the University as per the information security plan. Assigned responsible persons in each unit shall also take part in information distribution within their respective units.

Generally speaking, a careless revealing of information technological details can compromise information security. Therefore, information distribution responsibilities must be concentrated to assigned responsible persons in each unit.

Monitoring Information Security and Handling Problem Situations

Maintaining information security demands continuous monitoring that consists of information security monitoring and reporting its level and eventual incidents. The monitoring is carried out both automatically with technical means and by personnel, e.g. as a part of a superior's responsibilities. There are separate guidelines on technical monitoring. Head of Information Management shall coordinate the information security monitoring and reports on information security to the management of the University.

Head of Information Management and the information security administration team are authorized and required by the highest management of the University to conduct surveys of security in processing University information, and to take action in order to remedy any found shortcomings.

The users and the maintenance personnel shall report any shortcomings in information security, inappropriateness concerning information security or suspected information security misdemeanours to the information management liaison person or the head of their unit and head of information management. Separate decrees exist on reacting to information security incidents and repercussions of information security misdemeanours.

Orders and instructions concerning information security

The documentation related to University information security is divided into following main documents.

- Information security policy
- Definitions of information security policy
- Responsibilities of information security
- Acceptable use policies of information systems
- Administrative rules of information systems
- Consequences for IT service abuse
- Abuse penalty table (students, staff members, other users)
- E-Mail rules
- E-Mail filtering
- Retrieving and opening an e-mail
- Relevant legislation

In addition other instructions and supporting documentation will be created to instruct and improve information security. The additional documentation includes for example training material for various responsibility groups and roles.