Appendix 1: Information security: responsibilities and organisation

This appendix describes the responsibilities and obligations of information security actors.

The implementation of information security is a continuous and wide-ranging activity that requires cooperation from all parties in the university community. Every staff member and user of the university's information systems and services is responsible for implementing and monitoring information security within their scope of activity. In addition, the control and development of information security requires special expertise and appointed persons in charge.

University rector

The university rector is responsible for the implementation of information security as part of the overall security of the university:

Rector's responsibilities:
- approval of the information security policy and assignment of responsibilities to organisational units.

Chief information officer and information security officer

The chief information officer is responsible for monitoring risks, reporting and communication related to the university's information security. The duties of the chief information officer include:
- the general resourcing and organisation of information security
- organising the monitoring of information security
- reporting to top administration on information security matters
- prioritising information security development projects
- confirming the university's information security regulations and coordinating their preparation
- giving information security instructions to the university units based on the guidelines above
- preparing for emergencies.

The information security officer is largely responsible for monitoring and developing the university's information security at a practical level and for promoting information security awareness at the university.

The duties of the information security officer include:
- communicating information security matters and problems
- increasing the information security awareness of the staff and arranging information security training
- being in charge of the preparation and implementation of information security development projects
- assisting administration and units in the implementation of information security
- taking part in the definition of information security regulations
- handling information security anomalies and monitoring information security
- conducting regular risk analyses
- preparing for emergencies.

Information Services and Technology

Information Services and Technology is responsible for the operation of the university's information technology infrastructure and key information systems. The duties of Information Services and Technology include:
- taking care of technical information security in the university
- the security of the university's telecommunications network
taking care of security in computer classrooms and telecommunications facilities
centralised backups
arranging technical information security training to administrators
providing assistance in technical information security matters.

Owners and administrators of information systems

All information at the university and systems or system parts that process the information are assigned an owner (department, unit, person) who is ultimately represented by the unit head. Owners are responsible for protecting the information and information systems under their responsibility in accordance with laws, good practices and the university's current regulations and policies even if the information is handled or the information systems are maintained e.g. by Information Services and Technology.

The duties of the owner include:
- responsibility for personnel register and information system transcripts
- responsibility for the protection, user rights and backups of the information system and its information; in practice this is taken care of either by the system supplier or Information Services and Technology, depending on the case
- preparing for anomalies and required measures
- monitoring information security in the information system and reporting on incidents to the information security officer
- making sure the information in the system is correct, taking into account information disclosure issues.

The organisational unit appoints an administrator for each information system to perform the duties above.

All units

The duties of the head of a department or other unit include:
- resourcing and implementing information security and related development measures in the unit in accordance with the current information security objectives
- monitoring that the information security regulations are observed in the unit
- acting as the contact person for information security in the unit or appointing a contact person
- appointing administrators for information systems owned by the unit
- reporting on information security and related anomalies to the information security officer.

Users

Everyone who handles information is responsible for information security and obligated to observe related regulations and guidelines issued by the university. The duties of the users include:
- knowing the information security instructions and observing them
- taking part in information security training targeted for them
- reporting problems and activities in breach of regulations and guidelines to the information security officer.

External actors

Consultants and service providers using the university's information systems must observe good practices in information processing and security and maintain and control information security in accordance with general guidelines issued by central government. Owners of information systems must see to it that the external actors above are provided sufficient instructions. If needed, agreements on information security are concluded with organisations and other partners in cooperation that handle university information.
Appendix 2: Key information security rules and guidelines applied in the university

- Rules of IT Service Use
- E-mail rules
- Consequences of IT Service Abuse
- Retrieving and opening employee e-mail
- Key legislation
- Information security policy

Appendix 3: Statutes governing information security in the university

Data administration and the use of IT services are governed by a number of statutes and decrees. They also define the possible sanctions for abuse. Key legislation that applies to the university and its employees and students include:

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