LAPIN YLIOPISTO
UNIVERSITY OF LAPLAND

Signed by the Rector of the University of Lapland on 14 Sep 2022

Information Security Policy at the University of Lapland

Table of Contents

1. Introduction

The Information Security Policy is an internal ordinance signed by the Rector of the University of Lapland. It is delivered to the personnel of the university and it concerns everyone. The principles of the Policy are also followed when making agreements with partners and when writing instructions for users belonging to various interest groups.

2. Purpose of the Information Security Policy

The primary objective of information security is to ensure the uninterrupted operation of information systems and information networks that are important for the core functions of the university, to prevent the unauthorized use of data and information systems and the accidental or intentional destruction or distortion of information.

2.1. Information security and its significance

Information security measures are taken to ensure the availability, integrity, and confidentiality of information. It requires the appropriate protection of information, systems, services, and data communication in normal and unusual conditions through administrative, technological, and other measures. The confidentiality, integrity, and availability of information is secured against equipment and system failures, natural events, as well as threats and damages caused by intentional, negligent, or accidental acts.

The development and maintenance of information security are part of general security activities and risk management.

2.2. Definitions

The most important information security-related terms and their explanations are as follows:

Confidentiality: Refers to protecting the confidentiality of information and the rights related to information, information processing, and data communication against threats and infringements.

Integrity: Refers to information or information systems that are authentic, genuine, internally coherent, comprehensive, current, valid, and usable. Also means that information or messages have not been changed without authorization and that the possible changes can be verified from a list of entries.

Availability: Means that information, an information system, or a service is available to those with access rights at a desired time and by desired means.

Authentication: Ensuring the authenticity, validity, and origin of an object or ensuring the authenticity of a user at a desired level of confidentiality.

Indisputability: Refers to evidence, gained in a digital network through various methods, on the fact that a person has sent a certain message (indisputability of origin), a person has received a certain message (indisputability of transfer), or a message or event has been submitted for processing.

3. Factors through which information security activities are controlled

Information security work is controlled by national and international regulations on information security and in accordance with best practices and recommendations in information security.

4. Threats to information security

Information security is threatened when the confidentiality, integrity, or availability of information, information systems, or data communication is compromised.

Information security at the University of Lapland is strongly affected by the possible ignorance, carelessness, or indifference of a user. Other threats include intentional misuse of information, hacking, deficient software and devices, technical problems, and actions by external service providers.

5. Significance of information security to the organization

The core functions of the organization are highly dependent on information systems. Special attention must therefore be paid to information risk management.

5.1. Vital services and targets to be secured

The most important targets to be secured are the personnel, premises, equipment, data transfer, information systems, services, knowledge, and information materials of all types.

5.2. Information security principles

The principles are early prevention, real-time monitoring and development, and continuous surveillance of the operation and use of the information systems.

When defining, planning, and implementing the systems, potential risks must be observed and measures must be taken to prevent them from happening. In the implementation phase, the appropriate preventive measures are verified to provide a system environment that matches user needs.

5.3. Adapting information security to open international activities

International standards can be used to determine the level of information security. International and national standards and recommendations and the terminology adopted in them are used in the setting of information security objectives, measurements and the selection of security mechanisms.
Internationalization is supported by providing guidelines and training related to information security also in English, if necessary.

5.4. Information security support for research, teaching and cooperation

The objective of information security is to enable the safe and efficient use of the information processing and communication methods needed for research, teaching and cooperation. Security measures scale from the level of an individual researcher or teacher through research projects and groups, courses, subjects and units to apply to the entire organization.

5.5. Information security support for administration and other support functions

Information security is taken care of as part of the administration's system and process development. Information security measures aim to promote the adoption of new and efficient systems and practices in all operations.

5.6. Practices that support the implementation of information security

The continuity of operations must be ensured through continuity planning, which includes the prevention of disturbances and enables rapid recovery from them.

The security plans, arrangements and instructions of information systems provide for the subsequent investigation of omissions, damages or errors concerning information security, based on the principle that the costs are reasonable in relation to the benefits received. The principles will be implemented as described in the information security plan.

6. Prioritization of security measures

The order of security measures in situations of prioritization is as follows:

- protecting the life or health of an individual
- keeping delicate or otherwise essential information confidential
- protecting the integrity of data systems and registers
- protecting the availability of the user and operating environment

7. Responsibilities

7.1. Organizational responsibilities

The Rector of the University of Lapland is responsible for information security. Technical information security is the responsibility of LUC IT Services. The Director of Information and Digital Services is responsible for the development of information security and the implementation of monitoring, as well as for external cooperation on information security. The group which is responsible of comprehensive security of University together with the IT management team will develop information security measures.
All the people working or studying at the University of Lapland are responsible for the implementation of information security in their own operations and are also obliged to report any shortcomings they notice in information security.

7.2. Responsibilities of service providers

With service providers, information security requirements and responsibilities are defined by agreements

8. Developing information security awareness

Information security has been included in the personnel induction process. The aim is to develop the personnel's awareness of information security through training and topical bulletins and instructions.

The content and timeliness of the information security guidelines are ensured according to the changing operating environment.

9. Communication

Personnel are informed about information security issues as needed. Informing the personnel is handled by the IT management and IT services unit.

Information security issues are not actively communicated outside the university, but if there is a need for public information, it is handled in accordance with the principles of external communication of the university.