LAPIN YLIOPISTO
UNIVERSITY OF LAPLAND

Signed by the Rector of the University of Lapland on 16 May 2016

Information Security Policy at the University of Lapland

Table of Contents

1. Introduction 2
2. Purpose of the Information Security Policy 2
Information security and its significance 2
Definitions 2
3. Factors through which information security activities are controlled 3
4. Threats to information security 3
5. Significance of information security to the organisation 3
Vital services and targets to be secured 3
Information security principles 3
Practices supporting the realisation of information security 4
6. Prioritisation of security measures 4
7. Information security management system 4
8. Responsibilities 5
Organisational responsibilities 5
Responsibilities of the partners of collaboration 5
9. Information security training and instructions 5
10. Communication 5
11. Supervising the realisation of information security 5
12. Course of action in a state of emergency 5

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.

This Policy is supplemented by separate user and maintenance instructions and it shall be followed in all instructions given to the personnel of the University of Lapland.

2. Purpose of the Information Security Policy

The primary objective is to secure the continuity of the services of the University of Lapland.

An action-oriented policy supports the requirements set for the core functions of the university.

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.

Information security is pursued to control all risks threatening the continuity of the information systems and operations. It is essential to carrying out the core operations of the University of Lapland.

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 regulations, instructions, and recommendations. From the viewpoint of information security and protection at the University of Lapland, the most important regulations are the Universities Act/Decree, the Administrative Procedure Act, the Act on Co-operation within Undertakings, the Personal Data Act, the Act on the Openness of Government Activities, the Decree on the Openness of Government Activities and on Good Practice in Information Management, the Act on Electronic Services and Communication in the Public Sector, the Act on the Protection of Privacy in Working Life, the Information Society Code, and the Rules of Procedure of the University of Lapland.

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 organisation

The operation of the University of Lapland is highly dependent on information and on data systems. Special attention must therefore be paid to information risk management.

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.

The aim of protecting these targets is to secure the operation of the internal network and operative systems as well as the provision of services to the university's interest groups and external service providers.

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. The University of Lapland allows its information systems to be used for work-related tasks only. The partners of the university are allowed to use the systems according to the relevant agreements and permissions.

Practices supporting the realisation of information security

The continuity of operations shall be guaranteed by long-term planning that builds on the prevention of disturbances and enables quick recovery.

All security plans, arrangements, and instructions are written and carried out by preparing for subsequent processing of issues arising from negligence, mistakes, or errors in the use of the information systems. The guiding line is to keep the cost-benefit ratio reasonable. The practices are implemented as described in the information security plans.

6. Prioritisation of security measures

The order of security measures in situations of prioritisation 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. Information security management system

The information management system encompasses at least the following operating models and documents:

- Information Security Policy
- information security practices and principles
- information security development plan
- basic and supplementary instructions on information security
- information security training
- processing of deviations from the Information Security Policy
- information security reporting to the management
- operational continuity and readiness plans
- information security processes related to operations
- audit plan

The management system contributes to the strategy and strategy implementation plan of the University of Lapland. It covers the organizing, policies, planning, responsibilities, procedures, processes, and resources related to information security. It is also used for monitoring and assessing the efficiency and usefulness of the information security measures. Continuous development of the system enhances our ability to systematically control information security.

8. Responsibilities

Organisational responsibilities

Information security requires continuous and comprehensive development. In this work, the persons in charge form groups which all have their own tasks.

Information security activities are organized and the related responsibilities are shared according to the agenda of the Administration of the University of Lapland. Each profit unit is in charge of information security in its own sphere of responsibilities.

Headed by the ICT Security Manager of the University of Lapland, the information security operations and management system are developed by the university's Data Administration organization and the ICT Services of the Service Centre of LUC.

The detailed responsibilities are defined in the documentation on information security responsibilities at the University of Lapland.

Responsibilities of the partners of collaboration

Companies providing services to the University of Lapland shall be obligated to appoint an information security liaison responsible for the company's adherence to the security level required by the university. An appendix specifying the applicable information security requirements is to be added to each contract.

9. Information security training and instructions

Information security training is included in the university's orientation process, and it is arranged for every employee on a regular basis.

The ICT Security Manager is responsible for the content and currency of the instructions on information security.

Partners are given specific instructions on information security, and the issue is included in their training.

10. Communication

Issues related to information security are announced when necessary. The ICT Security Manager and the Communications unit are in charge of the internal communication.

The Communications unit is in charge of the university's external communication. Information security issues are not actively communicated to the outside, but if a need should arise, it is carried out as any other external communication.

11. Supervising the realisation of information security

If a staff member encounters any deficiencies, threats, or procedural errors related to information security, he or she is obligated to report them by contacting the ICT ServiceDesk. Each profit unit and each company providing services to the university is individually in charge of implementing the university's instructions on information security.

The realisation of the university's Information Security Policy is monitored by the ICT Security Manager, who reports to the Chief Information Officer.

12. Course of action in a state of emergency

In a state of emergency, the readiness plan of the University of Lapland is followed.

The Director of Administration is in charge of planning the operation in states of emergency.