LAB University of Applied Sciences

26 May 2020

LAB University of Applied Sciences information security and data protection policy

This information security and data protection policy defines the objectives, principles, responsibilities and operations in the implementation and development of information security and data protection.

Objectives of information security

Information security is a key factor in the quality of the university's operation and services. Information security must be ensured both manually and in computer-aided information processing throughout the life cycle of the information.

Information security refers to the maintenance of the availability, confidentiality and integrity of information. The university aims to ensure the functionality of information, information systems, services and information networks important for the university's operation, and to prevent their unauthorised use or the intentional or unintentional destruction or distortion of information. In addition to everyday procedures, the university also prepares for disturbances and emergencies to ensure that its operations can continue in all conditions.

Implementation of information security

Information security work refers to continuous development, planning, implementation and monitoring that aims for the secure processing of information. Its goal is to prevent any damages caused by internal or external threats to information or to limit them to an acceptable level and to prepare for emergencies.

The university maintains and develops information security through administrative, physical and information technology solutions. Operating instructions and training and communication on the secure processing of information guide the activity of users.
A risk assessment defines the required security level and security measures. External audits may also be conducted to evaluate the security level of information processing and systems at the university, if needed.

Objectives of data protection

Data protection has a close connection to information security. Data protection guards the rights of members and stakeholders of the university community in the processing of their personal data. Data protection pays special attention to the secrecy of personal data and to the fact that those processing personal data are authorised to do so and fulfil their obligations.

Implementation of data protection

Personal data may only be processed for purposes defined by legislation and to the extent and for the duration required for the purpose. The accuracy of the personal data should be verified from the person in question or from reliable sources. Information may be disclosed only on grounds and to recipients explicitly specified or set forth by law. The university controls the use of information systems containing personal data with user management solutions or otherwise documented procedures.

The university is the data controller of personal data filing systems that it compiles and maintains for its operation, fulfilling the obligations that legislation imposes on data controllers. The university draws up the documentation required by legislation for personal data filing systems and informs the persons whose personal data is collected of the processing of the data in accordance with legislation. Each university unit assesses and controls the implementation of data protection in its operations. External audits may also be conducted to evaluate the level of data protection, if necessary.

Liability and organisation

All persons processing data are responsible for information security and data protection for their part and are obligated to observe legislation and the university's instructions regarding information security and data protection.

The information security manager is responsible for monitoring and developing the university's information security at a practical level and for promoting information security awareness at the university. The data protection officer is responsible for data protection matters, monitors that the university complies with data protection legislation, and is a liaison in matters regarding data protection.

Each unit's supervisor is in charge of the unit's information system. The supervisor may appoint an employee as the person in charge, but this will not eliminate the supervisor's responsibility. Information Services and Technology is responsible for the university's information technology infrastructure and the systems it maintains, including their information security and sufficient data protection. If necessary, written agreements concerning the secure processing of information and data protection requirements in the university information systems will be concluded with service providers, consultants and other organisations processing information.

The university management is responsible for the sufficiency of information security and data protection resources. The information security manager and data protection officer notify the management of issues that may compromise information security and data protection. The university's rector is responsible for approving the information security and data protection policy and for assigning responsibilities the university's units.

Monitoring and dealing with problems

Users and administrators must notify their unit's director and the information security manager of any information security or data protection deficiencies, misconduct or suspected breaches they observe. The information security manager must notify the data protection officer if the alleged deficiencies, misconduct or breaches relate to data protection.

The information security manager is notified with the notification form through helpdesk self-service portal or by e-mail helpdesk@lut.fi. If someone suspects or observes that information security or data protection may be compromised, the matter must be investigated without delay. If information security or data protection is compromised, the university's internal instructions and legislation in force must be observed.

Communications

Media Services is responsible for communicating the university's information security and data protection matters to parties beyond the university. Internal communication involving information security issues is the information security manager's responsibility, and that involving data protection is the data protection officer's responsibility.

The university publishes the information security and data protection policy on the university intranet to the members of the university community, who are expected to observe the policy in their university-related activities. The university trains the members of its community in information security and data protection matters and provides related bulletins and instructions.

Students receive information on information security and data protection and rules and recommendations that apply to them.

Entry into force

The university's rector has approved the information security and data protection policy on xx Month 2018, and the policy shall remain in force until further notice. More detailed guidelines are issued by the information security manager and data protection officer.

_____

Turo Kilpeläinen
President and CEO