INFORMATION SECURITY PRINCIPLES OF THE UNIVERSITY OF JYVÄSKYLÄ

With these information security principles, the University's management specify the information security policy defined in the University of Jyväskylä Security Policy. The information security policy and principles describe the general goals, measures, responsibilities and organisation of information security in order to steer and implement information security at the University.

The information security principles concern everyone working or studying at the University. These principles and responsibilities are described in more detail in the information security principles for internal use available in the intranet.

Information security objectives

Safe management and processing of data is part of operational quality and comprehensive security at the University. The aim of information security is to ensure data security (confidentiality), guarantee the correctness of information (integrity) and enable the usability and availability of data for the purpose it was created. The information security policy, principles, rules and instructions are applied to all processing of data that are received in the assignments of the University and its interest groups, regardless of the form and tools of processing and the processor of the data.

The aim of information security is to secure the functionality of information systems, services and communication networks important for the University's operation, to prevent unauthorised access to them as well as prevent unintentional or deliberate destruction or distortion of data.

The mechanisms of information security management and risk management measures ensure sufficient and appropriate security and undisturbed functionality of the operating environment.

Information security actions ensure the continuity of operations in normal conditions and fault situations as well as in emergency conditions in accordance with the Emergency Powers Act (2011/1552). The University's obligations in emergency conditions are stipulated in the Universities Act (2009/558).

Means to implement information security

Information security is implemented as various process-integrated controls, operation modes, instructions and training as well as with various technical solutions in information systems. The actions are based on continuous development that aims to integrate information security with daily operative activities and modes of operation.

Information security risks are controlled by regular and systematic risk management. Risk assessment helps to steer development, which is implemented in the scope of the University's normal annual planning.

In case of information security deviations, the idea is to react as quickly as possible to minimise their impact. Deviations are controlled in accordance with a defined process.

The continuity, recovery and preparedness planning is directed at least to the critical operations and processes of the University and to the information systems that implement or support them. Ability to function in fault situations or emergency conditions is developed and maintained with regular practicing.

Staff and students are trained and informed about information security in order to increase their competence and awareness of information security.

Guidelines for information security

The University's information security activities comply with the University of Jyväskylä Regulations as well as Finnish and EU law. The information security practices of public administration and the ISO 27000 standard provide a framework for the implementation of information security at the University.

Responsibilities and organisation or information security

The Rector is responsible for information security at the University of Jyväskylä.

Every employee, student or anyone otherwise in a contractual relationship with the University is obligated to follow the information security principles, specifying instructions and guidelines, and the rules for using information systems and networks, computers and other ICT equipment. Neglecting or violating these policies, principles, rules, instructions or guidelines may lead to consequences defined in the information security principles.

Monitoring and supervision

The implementation of administrative and technical information security at the University is monitored with external audits, internal audits, and reviews. Technical information security is also monitored through the means of continuous technical supervision that is partly automatic. The monitoring and supervision is coordinated by the information security manager.

Control of deviations

It is the duty of every employee, student and user of JYU services to notify the information security manager (tietoturva@jyu.fi) about any observed information security deviations or shortcomings as well as suspected misconducts.

Approval and maintenance of information security policy and principles

The University's information security manager is responsible for the preparation and maintenance of the information security policy and principles.

The information security principles are updated at least every two years, and they are approved by the vice rector serving as the chair of the Information Security Development Group.

Jyväskylä, 9 January 2024

_____

Henrik Kunttu, Vice Rector, Chair of the Information Security Development Group

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Tämä dokumentti on allekirjoitettu sähköisesti JYU Sign-järjestelmällä
This document has been electronically signed using JYU Sign

Päiväys / Date: 10.01.2024 13:52:51 (UTC +0200)

Henrik Mikael Kunttu

Vararehtori

Organisaation varmentama (JYU käyttäjätunnus ja puhelintunnistus)
Certified by organization (JYU user account and mobile identification)