Policy

2022-05-24

Register number: MIUN 2022/1233

Mittuniversitetet
MID SWEDEN UNIVERSITY

Information Security Policy

Published: 2022-05-24

Deciision makers: Vice-chancellor.

Responsible division: Division of infrastructure

Administrator: Helena Wallskog

Date of decision: 2022-05-24

Period of validity: Until further notice

Last review: 2022-05-24

Sammanfattning: The Information Security Policy summarises the overall objectives and principles of Mid Sweden University's work on information security. The policy follows the Swedish Civil Contingencies Agency's regulations MSBFS 2020:6-7.

Tidigare versioner:

Reg.no. 2021/787, 2021-04-06

Reg.no. 2019/1629, 2019-10-01

Reg.no. 2018/881, 2018-05-30

Table of contents

1 Information Security Policy

The information security policy for Mid Sweden University defines the overall objectives and focus of information security and specifies how responsibility in these matters is distributed. This policy forms the foundation of the University's Information Security Management System (LIS). The policy describes the framework for information security and, together with additional policy documents, shall support the activities of the day-to-day work. The work on information security is based on laws, regulations, regulations, internal and external requirements and agreements.

Information security is the measures taken to prevent the leakage, distortion or destruction of information and to ensure that the information is accessible when needed.

The policy also takes into account the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council, GDPR) which forms an integral part of the overall information security.

1.1 General

Information is one of the university's most important assets and a prerequisite for the operation to function. The information must therefore be made available and protected, for example, from leaking, distorting or destroying.

According to the Swedish Civil Contingencies Agency's Regulation on Information Security for Government Authorities (MSBFS 2020:6), the authority shall carry out systematic and risk-based information security work based on the standards SS-EN ISO/IEC 27001:2017 Information Technology — Security Techniques — Management Systems for Information Security — Requirements and SS-EN ISO/IEC 27002:2022 Information Technology - Security Techniques — Guidelines for Information security measures or equivalent.

Figure 1: Information Security Management System

1.2 TargetSetting

The objective of the information security work is to:

- Maintain a balanced information security with regard to the university, working at the university and the needs of the public.
- Ensure a reasonable level of protection of information assets against various threats.
- Conduct systematic and risk-based information security work with the support of an information security management system.
- Conduct systematic information security work with respect to laws, regulations, regulations, internal and external requirements and agreements.

1.3 Scope

Information assets are all that contains information and all that carries information. Information security is not limited to the security of IT systems, but covers information in all its forms and regardless of how the information is stored, processed and communicated. Information can, for example, be in the form of text, sound, images and film, and can be handled with the support of IT, paper or other means.

1.4 Principles for Information Security Work

Basic for information security work is that it should be conducted systematically through continuous follow-up, improvement and be an integral part of the organisation's corporate governance. This applies to both the allocation of responsibilities and risk management, as well as procedures for planning and budgeting.

1.5 Roles and responsibilities

The responsibility for information security is as follows:

- Responsibility for information security follows the ordinary operational responsibility, from management down to individual employees.
- Each employee must actively work for increased safety and point to shortcomings to superiors.
- According to Mid Sweden University's guidelines for system management, system group owners are responsible for the information security of operational systems.
- Responsibility for information security work lies with the Infrastructure Department (INFRA). The responsibility includes deciding on policies, procedures and processes and supporting management and all other roles that have information security responsibilities in operational, tactical and strategic issues.

Other functions that also provide support in information security work are archives, law, IT and data protection.

1.6 Monitoring and evaluation

1.6.1 Monitoring

Monitoring shall be carried out regularly and if necessary, such as in connection with business follow-up, reorganisation, changes in legal requirements and before deciding to allow the University's information to be processed by another government authority or an external actor.

1.6.2 Evaluation

The University will evaluate how internal rules, working methods and support respond to identified risks and needs. The evaluation is carried out through internal controls, reviews, internal and external audits or equivalent. Internal rules and working methods shall clarify how and when evaluation is to take place.

Information security work is reported to the Executive Board 2 times/year and to the Board 1 time/year

1.7 Education/awarenesstraining

The University's employees shall be offered relevant courses based on their function/role in Mid Sweden University's organisation.

Information shall be provided to employees continuously in order to raise awareness of the current risks and how they should be managed.

1.8 Policy management

The University Administration, through the Infrastructure Department (INFRA), is responsible for maintaining and updating information security policy.