Owner: Information Security Officer
Approved:
Published at: 15.10.2013; jory
Updated: 01.02.2023; JuhaSe

1 GENERAL

1.1 The four dimensions of information security

- Confidentiality: Identifying confidential information and ensuring its confidentiality.
- Integrity: Ensuring the accuracy, integrity and long-term preservation of information.
- Availability: Ensuring the right access to information.
- Authenticity: The authenticity, integrity, internal integrity, completeness, timeliness, accuracy and usability of the data or information system.

The information security policy is a statement by SAMK's management that defines the objectives, responsibilities and means of implementing information security. The Security Policy is communicated to all SAMK employees and they are expected to act in accordance with it. The policy is further specified in the security rules and guidelines.

1.2 Implementing information security

Ensuring information security requires well-chosen and implemented measures at all stages of the information lifecycle (processing → storing → sending → printing → disclosing → handling → storing → sending → printing → disclosing → handling), and the tools, organisation and methods used to process the information, as well as rules and guidelines and training to guide the actions of those handling the information. These are collectively referred to as security mechanisms.

Implementing information security is about selecting and implementing security mechanisms that are appropriate to the known security risks. The choice of security mechanisms must be balanced between the four dimensions of information security and the cost and usability of using security mechanisms. Costs can be of a direct financial investment nature but can also be indirectly caused by slowing down work.

The objectives of data security are set and its implementation methods are chosen so that the data protection and data security guaranteed by law are implemented in the university of applied sciences in the best possible way.

1.3 Motivations for data security

- Complying with laws and other binding standards
- Safeguarding business conditions in all situations
- Ensuring cooperation and compliance with contracts
- Minimising financial risks
- Creating a good working and learning environment - Fostering reputation and trust

2 GUIDANCE VALVES

2.1 Compliance and security

Information security and information security measures are measured and implemented in accordance with the law and the agreements concluded by the UAS, and based on risk assessment. The UAS also prepares for disruptive and exceptional circumstances so that operations can continue as smoothly as possible under all circumstances.

2.2 Implementing the UAS strategy

The strategy of the UAS determines the choice of priorities for implementing information security.

2.3 Managed information security and information risk management

Information security and risk management related to information and information systems are organised and implemented in a coherent and systematic way, documented in writing. Information security and data protection are part of overall security. Data protection principles and responsibilities are defined in the data protection policy. Risk management and the choice of security mechanisms are also forward-looking to enable the secure and timely introduction of new technologies and systems. Descriptions of data security and personal data processing will be integrated and documented in the ARC system and linked to the descriptions in the Quality Manual, Architecture and Strategy. The descriptions will cover, inter alia

- the organisation of risk management for information and information systems,
- the organisation of the monitoring of information security requirements arising from the standard environment and the agreements binding the university of applied sciences, and
- information security roles, responsibilities and delegations.

Information security is part of the quality of operations. Information security management is integrated into the overall quality management of the UAS.

2.4 Adapting information security to an open international environment

International standards can be used to determine the level of information security. International and national standards and recommendations and their terminology are used to set information security objectives, measure and select security mechanisms.

Internationalisation is supported by offering the UAS's information security-related material and training in English, if necessary.

2.5 Support for research, education and cooperation on information security

The aim of information security is to enable the secure and effective use of the information processing and communication methods needed for research, teaching and collaboration. Security measures scale from the level of the individual researcher or teacher, through research projects and teams, courses and subjects, to the whole university of applied sciences.

2.6 2.6 Information security support for administration and other support functions

Information security is taken care of as part of the development of administrative systems and processes. Information security activities aim to promote the introduction of new and efficient systems and practices in all process activities.

2.7 2.7 Transferring good practice from the UAS to society

Information security is based on applicable domestic standards and recommendations. Information security guidance and training is targeted at different groups of staff and students and at different levels of the organisation. Students and staff who have adopted the security practices of the UAS transfer good practices to the surrounding society.

3 ORGANISATION

3.1 Management

Information security and its maintenance are part of the quality assurance of the UAS. The management and monitoring of road safety are integrated into the overall management of the UAS.

3.2 Responsibility

The CEO/Rector is ultimately responsible for the information security of the UAS. Process and competence area managers are responsible for information security in their area of responsibility. ICT and Digital Services is responsible for technical security. The Chief Information Security Officer is responsible for the development and monitoring of information security and for external cooperation on information security. The ICT Services management team prepares security development measures in cooperation with the ICT and Digital Services security team. Each UAS student is responsible for the implementation of information security in his/her own activities and is also obliged to inform his/her supervisor, the ServiceDesk or the Information Security Officer of any information security deficiencies he/she detects.

The organisation of information security work and the distribution of responsibilities are described in more detail in the ARC system.

4 COMMUNICATION

Communication related to information security follows the communication and crisis communication plans of the University of Applied Sciences.
Under normal circumstances, the Information Security Officer is responsible for the internal information security communication of the UAS, together with the IT Manager. Internal security communication within the process and competence area is the responsibility of the respective director. In the event of a crisis, responsibilities for security communication shall be distributed in accordance with the Crisis Communication Plan.

5 REFERENCES TO OTHER DOCUMENTS

Strategy

UAS strategy

Communication plan

Communication plan of the UAS

Crisis Communication Plan

A crisis communication plan for a UAS.

Information security management system

Descriptions in the ARC system

Privacy policy

Contingency plan

Laws and norms affecting the information security and data protection policy of Satakunta University of Applied Sciences