

## Information Security Policy for Halmstad University

Replacing Information Security Policy for Halmstad University, ref-10-2010-2654.

According to the Swedish Civil Contingencies Agency concerning governmental information security (MSBFS 2016: 1), Halmstad University is required to have an information security policy and other governing documents in order to work effectively with the university's information security.

The university's information is a very important resource. This policy aims to highlight, guide, as well as clarify the objectives and responsibilities concerning information security at the university.

Information is available in many forms - printed or written, electronically stored, via mail or electronic post as well as in film or by word of mouth. All information at Halmstad University should be handled to meet the desired basic information security requirements. Good information security is a prerequisite for the University to be able to fulfill its mission of providing education, conducting research, and interacting with the surrounding community.

Information security work is to be coordinated with other security work at the university and should be based upon prevention, risk-analysis, sustainability and cost-effectiveness. Work is required to be performed in a well-structured way and in agreement with the university's management. An important aspect is the commitment of all employees.

### Aims

The aim of the University's information security work is to protect Halmstad University's information against various threats and to create effective protection by ensuring the following:

- Correctness/Accuracy – All information should be protected from accidental as well as deliberate distortion.
- Accessibility – All information should be available to authorised persons according to their needs in the expected manner and to the extent required.

- Confidentiality - All information should be protected so that it is not intentionally or accidentally made available or disclosed to unauthorised persons or may be used in another unauthorised manner.

## Roles and responsibilities

Each employee and student is responsible for the information he/she handles, and to independently follow the rules and guidelines that concern their own tasks.

The Head of IT is responsible for information security at Halmstad University. The job consists of developing and monitoring information security work at the University. In addition, he or she is allowed to set demands regarding activities that do not fully comply with Halmstad University's rules concerning information security, and contact Halmstad University's crisis organisation whenever appropriate.

All information handled at Halmstad University has a so-called information owner i.e. a person responsible for the given information. Information owners for information found in Halmstad University's IT systems are the respective system owners. Information owners for other information is the person(s) who created the information. The information owner is responsible for ensuring that the information is correct, complete and up-to-date, and that it is handled in accordance with laws and regulations.

The Vice-Chancellor decides protective measures concerning the entire university, or the person, he or she designates. Regarding IT systems, maintenance object owners, system owners, heads of department and IT managers are jointly responsible for investigating and proposing security levels and safeguards. The Head of IT and the University Director(s) have joint responsibility when it comes to IT infrastructure.

All persons operating as system administrators or similar, and those having higher authorisation of systems than ordinary users at the university are required to a contingent liability where ones rights and obligations are stated.

When another party performs a task or assignment for the university where IT services or IT systems constitute an important role, the university shall ensure, via agreements, that the party maintains the information security that meets the requirements of the university.

## Description

All information is protected, however, in various ways. Therefore, a decision between the desired level of protection and the effective use of the University's resources is required. An effective and secure management of information requires that both information in need of safeguarding is identified and that relevant risks are assessed.

This is done by all information handled within the university's central and administrative IT systems undergoing an information classification, and where information protection requirement is assessed. Object owners, system owners and heads of departments are jointly responsible for this. Information classification, with subsequent risk assessment and actions, can also be done for specific operation sectors / research projects when the head(s) of department/school so wishes. Information classifications shall be reviewed every two years.

Risk assessment with regard to information security is also carried out. Object owners, system owners and head(s) of department/school are jointly responsible for these actions. In addition, risk assessment should be carried out prior to any replacement of IT systems, or change of operating system of IT systems. The object owner is the person responsible for such events.

Protection measures to be implemented are decided after a risk assessment.

In the case of procurement and development of IT systems and IT services, information security requirements shall be included in the requirement specification and the agreement.

The University should have tested the procedures for reporting both information security and personal data incidents. Reporting shall be made to the University's management and, where applicable, to other authorities if required.

Each employee is required to participate in a refresher course concerning information security on a regular basis (preferably every two years) to ensure that they have sufficient competence of the subject in order to perform his/her duties in the correct manner.

The University shall have procedures for continuity management in cases where the handling of the university's information is affected by major disturbances and interruptions. At least every two years, exercises will be conducted to test and develop these routines.

All work concerning information security at the University is required to be reviewed on a regular basis. The results of the review shall be reported to the Board and the Vice-Chancellor twice a year. The information security officer is responsible for such details.

## **Underlying documents**

Documented procedures: Information classification

Documented procedures: Risk assessment with regard to information security

Documented procedures: the handling of incidents with regard to information security

Documented procedures: Continuity plan for IT

Documented procedures: Continuity review and follow-up of information security

Documented procedures: Acquisition of IT solution

Rules & regulations for the use of IT resources

Rules and responsibilities for system administrators

Rules and responsibilities for IT staff