**Information security policy**

Effective information security is key to Aalborg University (AAU). All staff members, students and others affiliated with the University must make themselves familiar with the University’s position on information security. This document describes the overall information security policy of Aalborg University.

BACKGROUND

Aalborg University’s information security policy must comply with Danish national legislation and comply with the Information Security Management Systems standards, the ISO 27000 series, whenever relevant.

Any deviation from the ISO standards must be justified by a documented risk assessment.

IDENTIFICATION OF INFORMATION SECURITY

At AAU, information security concerns the protection of any part of the University’s information and communication technology. The University has an inherent need to be able to communicate openly with the outside world and thus cannot guarantee perfect security; therefore, the University aims to strike a balance between openness, security and economy. Naturally, the University must comply with Danish legislation and government guidelines. Moreover, the University wishes to prevent misuse, such as misuse of illegally acquired software, abuse of licence rights or other copyright violations. It must be ensured that information and IT systems are made available within the time frame stipulated by the management.

Information is an asset, and much like any other business asset, information is essential to the business activities of Aalborg University and therefore must be protected accordingly. Increased online information exchange has brought about an increase in both threats and vulnerabilities making information security even more important.

The information we use exists in many forms: printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Regardless of its form, information must always be protected appropriately and in accordance with its importance to the University.

Effective information security is achieved through implementing, monitoring, reassessing and continuously updating an appropriate level of security measures, including policies, practices, procedures, organisational measures or technical functions.

At Aalborg University, information security includes the following three key elements:

A. INTEGRITY

Ensuring that the integrity of information is maintained through the correct function of information systems and through safeguarding its accuracy and completeness.

B. AVAILABILITY

Ensuring that authorised users always have access to information, data and information systems when they need it and when required by AAU.

C. CONFIDENTIALITY

Ensuring that sensitive information (information systems and data) is accessible only to those authorised to use it.

AAU’s IT systems must be secure and meet the requirements for confidentiality and integrity in any given situation in order to protect the University’s reputation. Moreover, the IT systems must be user-friendly and all necessary security measures must be designed so as to not cause unnecessary nuisance to its users. Security measures must protect the University against any natural, technical and human threats. No individual or group are above the security provisions.

VALIDITY

The information security policy applies to all staff members, students and others who make use of AAU’s IT assets. IT assets refer to physical resources, IT equipment, communication equipment, data and software. The information security policy applies to all IT assets owned by or located at Aalborg University.

The information security policy allows for different security levels and security classifications based on the specific usage of IT assets, threats assessment, the costs of security and the possible consequences of security breaches. The information security handbook includes a list of the current security levels and security classifications.

The information security policy must be reviewed by the information security committee and subsequently approved by the Rector.

The information security policy must be reviewed on a regular basis and revised as required.

RESPONSIBILITIES

ROLES AND RESPONSIBILITIES

The Rector has overall responsibility for information security at Aalborg University. The Rector has delegated the authority of the overall management and coordination of information security at AAU to the chair of the information security committee, and in cooperation with the members of the information security committee, the chair will prepare the basis for decisions concerning the joint and overall information security guidelines.

The responsibility for the preparation and compliance of decentralised information security guidelines is delegated in accordance with the organisational structure of the University.

All staff members, students and others affiliated with Aalborg University are jointly responsible for the information security at Aalborg University. This includes the responsibility to point out any information security breaches.

MANAGEMENT

The information security committee is responsible for the day-to-day management of the joint information security. The terms of reference of the information security committee are outlined in the information security handbook.

The day-to-day management of local information security is carried out by the staff members of the local units/departments.

PENALTIES FOR BREACHING INFORMATION SECURITY

Intentional breaches of information security policies, rules and guidelines or attempts to evade these will be sanctioned. Breaches are sanctioned according to the nature of the violation.

RISK ANALYSIS

The extent and nature of the information security system guidelines, rules, procedures and instructions must be based on risk assessments; this allows for all information security solutions to be based on an assessment which identifies the probability of damage occurrence, extent and impact in relation to the costs and risks of implementing preventive measures and/or countermeasures.

The risk analysis must be reviewed and revised as required; however, at least every two years. The procedures for how and when risk analyses must be conducted are outlined in the information security handbook.

INFORMATION SECURITY HANDBOOK

The University must make available an information security handbook, which must be revised on a regular basis. The handbook must include the following:

The overall information security policy of Aalborg University (this document)
A description of the overall information security strategy which provides an action plan for the establishment of the joint principles of information security management and the implementation of the information security system
A set of overall joint guidelines for information security and their associated procedures and rules
A set of specific guidelines for information security and their associated procedures and rules

The content of the information security handbook should be structured in accordance with the Information Security Management Systems standards, the ISO 27000 series.

Rector Per Michael Johansen
25 August 2017

(Aalborg University’s information security handbook is now available in ISMS (Information Security Management System), which may be accessed only via the AAU network - [**https://secureaware.aau.dk**](https://secureaware.aau.dk/))