Aarhus University's information security policy

This policy forms the overall framework for information security at Aarhus University on the basis of the university's overall strategy **2025:**

> *Aarhus University is a strong university that is internationally recognised for the high quality of its research, research-based degree programmes and public sector government consultancy, in addition to value-creating collaboration with private businesses, public sector institutions and civil society. The curiosity-driven creation of knowledge rooted in strong disciplines to benefit society is the university's reason for existing.*

In order to maintain confidence in Aarhus University, critical information is protected with measures to ensure the necessary level of information security. Our work is based on three cornerstones:

1. **Confidentiality:** Only people with a legitimate need have access to information.
2. **Integrity:** Information must be consistent and in a form that can be trusted.
3. **Accessibility:** Information must be accessible for the right people when they need it.

Anyone associated with Aarhus University can find out about the guidelines applying for information security in the information security policy. The guidelines reflect requirements in legislation and from relevant authorities such as the Ministry of Higher Education and Science, e.g. requirements to use the common information security standard, ISO 27001.

1.1 Scope of the information security policy

The information security policy covers all of Aarhus University's information assets, i.e.:

l. any information belonging to Aarhus University.

2. information for which Aarhus University can be held responsible.

3. resources to use, produce or store the information described in points 1 and 2.
This applies regardless of the form of information, including oral information.

Examples of information assets are:

- experimental and research data.
- information about employees.
- information about financial matters.
- information that contributes to the administration of Aarhus University.
- information transmitted to Aarhus University by others.
- laboratories, research equipment, computers and computer networks.

The information security policy applies for:

- all employees without exception – hence also people who work temporarily for Aarhus University, as well as emeritus professors, examiners and external supervisors.
- students who use, generate or store Aarhus University's information assets in connection with their studies.
- others who use, generate or store Aarhus University's information assets. For example alumni, suppliers, consultants, builders and guests.

The senior management team has decided that:

- the senior management team is to be kept informed of the current risk landscape for information security.
- the senior management team is responsible for ensuring that the management system for information security at Aarhus University is continuously adapted and improved to reflect the threat landscape faced by the university.
- the Information Security Department recommends the objectives and framework for information security, which are then approved by the Central Information Security Committee (CISU) and the senior management team.
- the Information Security Department coordinates work on information security with the data protection officer (DPO), the information security committees at the faculties (FISU), in the Administration (EISU), as well as other relevant stakeholders. If necessary, the Information Security Department will obtain approval from the Central Information Security Committee and the senior management team.

- risks against information security at Aarhus University are to be countered with appropriate protective measures. The measures must be substantiated by a risk assessment, the university's risk appetite and commercial risks. For personal data, a risk assessment must also be carried out for the data subjects.
- risk assessments must be updated annually and in the event of significant changes in the general threat landscape or in the organisation, strategy or operational environment of the university.
- measures are to be designed such that Aarhus University complies with contractual requirements and legal requirements – e.g. the GDPR and the University Act.
- the following security principles must be complied with:
    - Access to information assets must be provided as needed.
    - Security must be designed into processes and solutions.
    - Necessary separation of functions must be introduced.

1.2 Responsibility and security awareness

The following responsibilities apply with respect to protecting Aarhus University's information assets:

- The senior management team has overall responsibility for information security at Aarhus University.
- The senior management team is responsible for ensuring that staff and students are informed about their responsibilities with regard to information security at Aarhus University.

1.3 Breach of information security, exemptions and infringements

If an employee or student discovers threats against or breaches of information security, the employee or student must inform the Information Security Department.

Exemptions from following the information security policy may be granted in exceptional cases by sending a request for exemption to the Information Security Department, which will submit the request to the Central Information Security Committee.

Infringements of the information security policy will be treated as a security incident with corresponding sanctions.

1.4 Approval

Aarhus University's information security policy is approved by the rector on the basis of recommendations from the Central Information Security Committee.

As part of overall security management, on the basis of the ongoing management reporting of the risk landscape, the senior management team will review the information security policy at least once a year.

Approved by Rector Brian Bech Nielsen 11 February 2021