UPPSALA
UNIVERSITET

Dnr 2017/651

Information Security Management System

Guidelines for security and safety at Uppsala University

Ratified by the chief security officer	2016-04-26
Latest revision date	2021-03-29
Translation date	2021-03-29

Table of content

1 Introduction

The overall aim of the information security work is to maintain a well-balanced information security with regard to the university, coworkers, students etc at the university, as well as the needs of the public. The information security work must strive for both an adequate level of security, ie. to balance risks against costs for protective measures, as well as a controlled security, ie. controlled and executed according to the university's *information security management system (ISMS)*[1].

The ISMS of Uppsala university is based on the international and Swedish standard SS-EN ISO/IEC 27001:2017, to conform to the demands in the Swedish Civil Contingencies Agency's (MSB) directive on the information security in governmental authorities (MSBFS 2020:6).

The basis for decisions and budgets for the overall LIS work also includes work and follow-up in accordance with the ordinance on state authorities' risk management (SFS 1995:1300), as well as Uppsala University's annual risk and vulnerability analysis in accordance with MSB's regulations on state authorities' risk and vulnerability analyses (MSBFS 2016:7).

The ISMS at the university is described according to the seven sections in ISO27001:2017,

- Context of the organization
- Leadership
- Planning
- Support
- Operation
- Performance evaluation
- Improvement

and covered by security and safety measures in accordance with ISO27002:2017,

- Information security policies
- Organization of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance

[1] In Swedish ”Ledningssystem för informationssäkerhet (LIS)”

The ISMS describes security and safety objectives for which a balanced security level and appropriate security measures must be planned, implemented, followed up and continuously improved when necessary. The continuous cycle of follow-ups and improvements, often described by the so-called PDCA cycle ("Plan-Do-Check-Act"), as well as active dialogue with the University management and core operations are fundamental to the work with security.

The University's ISMS is presented below, in accordance to the seven sections of ISO27001:2017

2 Context of the organization

The overall aim of the information security work is to maintain a well-balanced information security with regard to Uppsala University, active at the University, and the needs of the public in accordance with the assignments in the Higher Education Act (SFS 1992:1434) on teaching, research and public/science outreach.

The information security work must ensure that the University's information resources receive adequate, relevant and comprehensive protection. The work must be managed and carried out in accordance to the University ISMS and strive to balance risks against costs for protective measures.

The *information security procedures (UFV 2017/93)* states what security requirements are imposed on the information systems, both in normal operations and in possible crisis situations.

3 Leadership

Uppsala University's *information security procedures* (UFV 2017/93) – corresponding to the University's *information security policy* in accordance with ISO 27001: 2017 – describes the responsibilities, roles and scope of the information security work at Uppsala university.

All governance documents, guidelines, procedures, etc. within the information security area are published at the Policies and regulations part of the University website[2].

4 Planning

Planning involves a structured way of determining which risks and opportunities that need to be managed in order to prevent or reduce undesirable effects. It also involes how to achieve continuous improvement, as well as planning measures to manage these risks and opportunities and evaluate the impact of the measures.

[2] https://regler.uu.se/, 2021-03-23

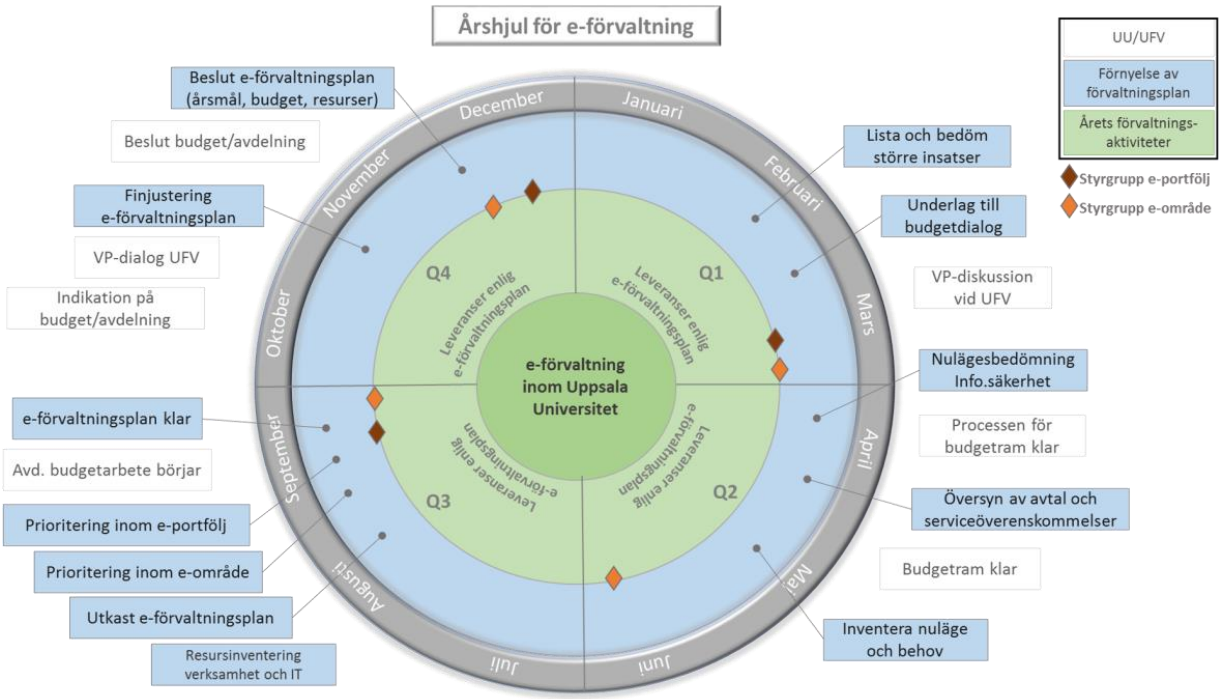
The planning must be based on the risk management procedures (UFV 2018/211). These procedures provide adapted support for continuous risk management of the University's information resources with regard to confidentiality, integrity and availability.

The risk management process contains:

1. Delimitation
2. Impact assessment
3. Information classification
4. Requirement analysis based on the 14 sections of ISO 27002
5. Risk analysis
6. Managing identified security flaws

All part of the process must be documented.

Risk management of the University's information system is an integral part of the system management model. This means that each administrative area must carry out a requirements analysis of their information security once a year. The analysis then forms the basis for priorities and decisions on security improvements in the management plan and budget for the next financial year.
The information security work has been integrated into the annual cycle that states how the administrative work is to be conducted, see picture below.



Information systems not covered by the management model must also carry out an annual analysis of information security.

5 Support

The support for working with Uppsala University's ISMS is divided into resources and competence, awareness, communication and documented information.

Resources for establishing, implementing, maintaining and constantly improving the management system are managed by the University's Security and safety division.

Basic training in information security, as well as integral parts of the University's ISMS, is offered both through workshops and classes as well as via internet-based courses. In addition to this, targeted group-adapted courses and information meetings are offered according to the needs and wishes of each department.

For further support, it is always possible to contact the Security and safety division.

The management system includes documented and established information in accordance with the University's regulations for guidelines and routines. The management system's detailed procedures and routines can be found at the Policies and regulations part of the University website.

The Chief Security Officer is responsible for ensuring that up-to-date and easily accessible information about the university's ISMS and associated regulations is available on the University website. Communication with employees also takes place via e-mail lists, various forums, staff meetings and more.

6 Operation

Planning and managing the activities in terms of information security means planning and controlling the processes required to meet information security requirements and the implementation of measures.

The information security requirements are identified with the help of various measures such as derivation from statutes and internal regulations, risk analyses, analysis of incidents, and results from completed information classifications.

The risk management procedures (UFV 2018/211) describe the process for carrying out delimitation, impact assessment, information classification, requirements analysis, risk analysis and management of identified safety deficiencies.
All steps in risk management are to be documented. Plans for treating risks through various measures will be followed up on an ongoing basis.

7 Performance evaluation

Periodic follow-up, as well as reporting how the security works with regard to set goals, practical experience and compliance, is mainly performed by the Security and safety division.

The head of security reports to the university management regularly.

The university's annual risk and vulnerability analysis contains summaries of this year's work with ISMS, risk areas and improvement proposals.

The tasks for the Security and safety division includes compilation and follow-up of information security incidents, results of completed risk analyses, results of internal or external IT audits, and consequences of any changes in applicable laws, regulations or contractual obligations.

8 Improvement

Continuous improvements of the information security management system with regard to functionality and quality are achieved through

- corrective and preventive measures
- information and education
- external monitoring

Proposals and priorities for improvements in the management system shall be included as part of the Chief Security Officer’s ongoing planning and follow-up of the information security work and form the basis for the annual division business plan.

For each e-area or for an individual information system, proposals and priorities for improvement measures must be included in the ordinary management work and form the basis for the annual management plan.

The annual work with risk management from a safety perspective in the core business is followed up through visits to departments, and equivalents, based on identified needs.