Approved by Rector’s directive No 7 of 4 March 2024

In force from: 04.03.2024

Information Security Policy

Table of Contents

1 General information

The Information Security Policy lays down the principles of information security at Tallinn University of Technology (hereinafter referred to as “the university”) which are based on the requirements of the ISO 27001 standard and provide more precise conditions, bases and principles for ensuring strategic information security. The objective of the Information Security Policy is to set out the university's strategic approach to ensuring information security.
The university will launch an Information Security Management System (ISMS), which consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by the organization in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, operating, monitoring, maintaining, and improving the organization’s information security to achieve its objectives. It is based on a risk assessment and the organization’s risk acceptance levels designed to effectively treat and manage risks.
The information security policy is closely intertwined with the university’s risk management procedures and its regulations governing data protection. Information security is a targeted action carried out to support the university’s core processes, fulfil the objectives of information security and ensure the availability, integrity and confidentiality of information assets.

2 Definitions

"**Information security**" means the protection of the three intrinsic properties of information – availability, integrity and confidentiality, whereas:

- availability – data must be available in time and usable;
- integrity – data must be reliable and authentic, and it must be possible to identify and eliminate unauthorised changes;
- confidentiality – access to data is granted only to those with a justified need-to-know.

“**Information security management system**” means a framework of policies and procedures applied within an organisation to achieve the information security objectives. An information security management system consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, operating, monitoring, maintaining, and improving an organization’s information security to achieve its objectives. It is based on risk assessment and the organization’s risk acceptance levels designed to effectively treat and manage risks.
“**Asset**” means a resource that has value to its owner. Assets include information, data, software, physical assets (infrastructure, buildings, hardware, installations), financial assets, services, human resources (people, qualifications, skills, experience), know-how, non-material assets (reputation, image).
“**Information technology asset** (IT asset)” means a hardware or software within an IT environment that creates value for an organization. IT assets are integral components of the organization’s systems and network infrastructure.
“**Information** or **information asset**” means a collection of knowledge or data, defined and managed as a single unit and that has value as well as risks to the organisation. Information or information assets are defined as assets and are related to information systems and processes.
“**Information system**” means a system that stores and processes information. An information system may consist of several interconnected components or assets (such as functional modules, applications, web services, networks, servers (including virtual ones), computers, operating systems, software and databases), which together form a conceptually complete system.
“**Application**” means a set of various programs designed to perform specific tasks. A set of applications can form an information system.
“**Software**” means the programs, procedures, rules, and associated documentation of an information processing system.
“**Process (business process)**” means a series of activities, actions, or procedures performed within an organisation that produce an outcome contributing to the goal and creating value (e.g. products or services) for the customer. Each process has an owner and a process manager. A process involves strategic goals, legislation, key inputs and outputs, services (including customers and related target groups), indicators, risks, information systems and information assets.
“**Service**” means a value created for a customer, a (potential) result of a process.

"**Incident**" means an unplanned interruption or reduction in the quality of a service, which causes (or may cause) disruption to a service.
"**Information security incident (cyber incident)**" means a special type of incident related to a successful or unsuccessful attempt or attack to destroy, alter, disable, steal or gain unauthorized access or make unauthorized use of an IT asset.
"**Data breach**" means a special type of information security incident involving a breach of security, accidental or unlawful destruction, loss, alteration, unauthorised access to or disclosure of personal data transmitted, stored or otherwise processed.

3 Scope of application

The Information Security Policy and the supporting control measures, processes and procedures apply to all information used at the university. This includes information processed by other organisations when interacting with the university.
The Information Security Policy and the supporting control measures, processes and procedures apply to all persons who have access to university information and technologies, including external persons who provide services to the university or process information in the framework of other forms of cooperation.
The detailed scope, including the breakdown of users, information assets and information processing systems, is laid down in the accompanying documentation outlining the scope of the information security management system.

4 Principles

- The university as the owner of information assets shall select adequate and appropriate measures to protect the information assets.
- In the course of the risk assessment of information assets, the level of significance is determined based on the university's core activities and objectives.
- Information assets shall be used for purposes related to the activities of the university.
- All the employees must comply with the information security requirements.
- Access to information assets is granted based on a justified need-to-know.
- Tasks or responsibilities that conflict with each other shall be kept separate.
- The obligation to maintain confidentiality applies to confidential information and is applied to persons using the university's information assets in accordance with legislation and the contracts entered into.

5 Objectives

The university's information security objectives are the following:

- To provide reassurance to the members of the university (the staff, students and alumni) and its cooperation partners that the university keeps and processes the information assets (data, information) related to them in adherence to legislation and ensures the security (confidentiality, integrity and availability) of the information.
- Information security is an integral part of the university's core and support activities.
- Risks related to information assets are identified, analysed, evaluated and treated in accordance with the agreed risk tolerance level.
- Requirements arising from information security standards are taken into account when developing or procuring information systems and applications.
- The persons managing the university's information assets are aware of their information security responsibilities and obligations. Contractual and legal obligations relating to information security are understood and met.
- The organisational, physical, procedural and technical controls balance user experience.
- Authorised users can securely access and, if necessary, share information in order to perform their roles.
- Efforts are made to minimize incidents affecting the information assets, continuously learning from them and, as a result, improving various information security measures.

The security of information assets is ensured and information security objectives are achieved by implementing a set of Information security management components, including controls, policies, rules, guidelines, processes, organisational structures, resources, actions, software and hardware solutions, in adherence to the Information Security Standard and regulations.

6 Organisation and management of information security

Introduction of information security policy involves planning, creation, implementation, management of security measures and designation of areas of responsibility. The information security roles have been defined for information security purposes. Information security is a collective action of the organisation and a responsibility of all the data users.
The responsibility for information security is divided into general and specific responsibilities:

- data users have general responsibility for information security, which is to comply with information security regulations and to notify of information security incidents;
- specific responsibilities for information security arise from the position in the university structure and the duties. The rector, the structural units and each employee are personally responsible for proper fulfilment of their obligations.

6.1 The rector

- Approves the university's information security policy;
- Approves the university's chief information security officer.

6.2 The rectorate

- Shall demonstrate leadership and commitment with respect to the information security management system;
- Shall make sure that the information security policy is up-to-date and the information security objectives are compatible with the university's goals;
- Shall make sure that information security requirements are integrated into the university's processes;
- Shall make sure that resources required for the information security management system are provided based on risk management principles;
- Shall ensure compliance with the information security management system requirements;
- Shall make sure that the information security management system achieves its intended outcomes and assess the achievement of the objectives;
- Requires members of the organisation to adhere to the Information Security Policy as well as the procedures, guidelines and regulations drawn up within the framework of the information security management system.;
- Directs and supports persons to contribute to the effectiveness of the management system;
- Promotes continual improvement;
- Supports other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility;
- Shall review the organisation's information security management system at regular intervals to ensure that it remains suitable, adequate and effective.

6.3 The chief information security officer

- Is responsible for developing, reviewing and enforcing the information security policy, standards, guidelines and controls to ensure compliance with relevant legislation and regulations;
- Shall make sure that information security measures are implemented and conducts a security audit at least once a year;
- Shall organise information security monitoring and incident response:
- Is responsible for increasing the information security awareness at the university;
- Shall inform, provide advice and training to employees for the implementation of security measures;

- Shall monitor the execution of controls and provide reviews to the relevant parties;
- Shall provide the rectorate an overview of information security at least once a year;
- Is responsible for organizing communication related to the information security management system at the university;
- Identifies and defines the parties involved in the information security management system and their respective needs and requirements;
- Is the contact person in communication with authorities concerning information security;
- Shall make sure that appropriate flow of information takes place at the university with respect to information security (in cooperation with special interest groups, specialist forums, etc.).
- Shall provide input on information security threats for risk management;
- Shall ensure continual improvement of the ISMS.

6.4 A coordinator for protection of personal data and state secrets

- Shall organise the protection of personal data in accordance with the legislation applied to the field;
- Shall organise the protection of state secrets and classified information of foreign states in accordance with the legislation applied to the field.

6.5 An area manager (head of a structural unit)

- Is responsible for implementing the components of the information security management system in his/her field;
- Fulfils the role of the owner regarding the information systems or applications within his/her area of responsibility;
- Appoints the business project manager and superuser of the information systems or applications in his area of responsibility;
- Shall make sure that the personnel within his/her area of responsibility have the necessary competence to maintain information security;
- Shall plan and ensure the availability of resources required for information security in his/her area of responsibility.

6.6 A process manager

- Is responsible for implementing the components of the information security management system within his/her process;
- Shall identify, analyse and assess risks related to the information systems and applications within his/her process in collaboration with the business project manager, the superuser, the IT project manager, and the system manager;
- Is the owner of the data or information generated during the process.

6.7 Members of the organisation

- Shall be aware of the information security policy and the information security procedures and regulations that apply to them;
- Shall understand their role within the information security management system and adhere to the policies, rules, guidelines, controls, organisational structures, and processes arising from the system in their work as well as recognise the benefits of enhancing information security performance;
- Shall be aware of the consequences of non-compliance with the requirements of the information security management system;
- Contribute to the continual improvement of information security activities.

7 Resolving an information security incident

- A data user must notify the IT Helpdesk of any information security incident as soon as possible.

- The resolution of information security incidents is conducted in accordance with the established incident resolution procedure.
- To resolve an information security incident, parties related to the information assets must grant the chief information security officer and authorized personnel access to information required to resolve the incident.
- The chief information security officer shall inform the relevant parties, including external parties about information security incidents as required by regulations.
- If elements of criminal offence, misdemeanour or disciplinary offence are discovered in the course of solving a security incident, the case is referred to the authority who has the right to conduct the relevant proceedings.
- The information collected in the course of solving an incident shall be documented, analysed and used to prevent similar incidents in future.

8 Compliance and non-conformities

The university ensures compliance with its information security policy and management system through regular reporting, feedback from information asset owners, risk assessment, and internal and external audits.
All deviations and exceptional cases in the implementation of information security measures shall be documented and approved by the chief information security officer before their implementation.
In the event of non-compliance:

- react and take action to control and correct it and deal with the consequences;
- assess the situation, determine if any similar non-conformities exist elsewhere and, if necessary, address the root cause to eliminate it;
- review effectiveness of the corrective action;
- if necessary, make changes to the information security management system (e.g. by supplementing procedures, rules, guidelines, etc.);
- document the non-conformities (incl. the nature of the non-conformity, the steps and measures to be taken, and the results of corrective actions).

The chief information security officer is responsible for documenting non-conformities.
Members of the organization who have violated the principles of the information security policy will be subject to disciplinary action as outlined in the applicable procedures.

9 Review by the rectorate

The rectorate shall review the organisation's information security management system at regular intervals to ensure that it remains suitable, adequate and effective.
A rectorate's review must include at least the following:

- The status of actions from previous management reviews;
- Changes in the internal and external issues that are relevant to the purpose of the information security management system;
- Changes in the information security management system related to the needs and expectations of interested parties;
- Feedback on the information security performance, including trends (non-conformities and corrective actions; monitoring and measurement results; audit results; fulfilment of information security objectives).
- Feedback from stakeholders;
- Results of risk identification, analysis and assessment and a risk treatment plan;
- Opportunities for continual improvement.

The rectorate's review of the ISMS shall be prepared by the chief information security officer. The outputs of the rectorate's review should include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

10 Implementation

The Information Security Policy is a public document published on the university website at oigusaktid.taltech.ee. The Information Security Policy shall be made available to all the persons within the scope of application of the ISMS.
The annexes to the Information Security Policy and information security management system include the following procedures and instructions, approved separately from the Policy. It is crucial to ensure consistency across the entire information security management system, various policies, regulations, procedures, and guidelines. The procedures and guidelines of the information security management system shall be approved by an order of the Director for Administration.

- The scope of information security
- Administrative management
- Data protection and exchange of information
- Rules for information technology development work
- Physical security
- Management of IT assets
- Access management
- Remote work and mobile devices
- Crisis management
- Cryptographic operations
- Logging policy
- Principles of the management and use of end user devices
- Change management
- Partnerships and agreements
- Human resource management
- Enquiry, incident, event and problem management
- Risk management
- Basis of server and network management
- Internal audit and compliance
- Service continuity

Information security policies, along with supplementary procedures and guidelines, are reviewed annually and amended as needed based on various impact factors (e.g. changes in objectives, the external environment, information security risks, etc.) and the outputs of reviews or audits conducted by the rectorate.

Annex 1

Figure 1 Chart of the information security management system