Directive «Information Security at ETH Zurich» RSETHZ 203.25

of 17 December 2024

1. Section: General provisions 2
Article 1 Subject matter 2
Article 2 Applicability 2

2. Section: Goals and requirements 3
Article 3 Goals 3
Article 4 Requirements 3

3. Section: Tasks, responsibilities, competences 5
Article 5 Information security as a management task 5
Article 6 Chief Information Security Officer 5
Article 7 Information Security Officers 6
Article 8 Information owners 7
Article 9 IT operators 7

4. Section: Steering 8
Article 10 Information Security Commission 8
Article 11 Information Security Committees 8
Article 12 Directive Landscape 8

5. Section: Final provisions 9
Article 13 Entry into force 9

Appendix – Information security framework 10

The Executive Board of ETH Zurich,

based on Art. 4 para. 1 (b) of the Ordinance on the Organisation of the Swiss Federal Institute of Technology Zurich of 21 November 2024[1],

hereby decrees:

1. Section: General provisions

Article 1 Subject matter

[1] This directive regulates the objectives and requirements for information security. It defines the tasks, responsibilities and competences as well as the overarching management of information security.

Article 2 Applicability

[1] This directive applies to all units of ETH Zurich in accordance with the Ordinance on the Organisation of the Swiss Federal Institute of Technology Zurich of 21 November 2024 *(Organisation Ordinance ETH Zurich*)[2] and their members, in particular the

a. central organs;

b. departments and their institutes, centres, laboratories and professorships and

c. units outside the departments pursuant to Art. 92 of the ETH Zurich Organisation Ordinance, which are operated solely by ETH Zurich.

[2] Individual arrangements shall be made for units outside the departments that are operated jointly with other universities.

[1] RSETHZ 201.021
[2] RSETHZ 201.021

2. Section: Goals and requirements

Article 3 Goals

[1] Information security ensures the confidentiality, integrity (accuracy and completeness) and availability of information. The information security strategy provides the best possible support for the implementation of ETH Zurich's institutional strategy. IT security is part of information security and means ensuring information security when using IT resources. IT resources are all IT devices and IT services that are owned by or used on behalf of ETH Zurich. This also includes printers, scanners, software, telephony, building technology systems, building automation and outsourced services such as external cloud services. Video surveillance pursuant to Art. 36i of the ETH Act is excluded.

[2] The Chief Information Security Officer (CISO) is responsible for information security at ETH Zurich. The organisational units implement the objectives and the information security strategy independently and in accordance with the specifications and recommendations of the CISO.

Article 4 Requirements

[1] When implementing information security, ETH Zurich complies with the legal requirements and is guided by the standards and norms that have proven themselves in the professional world.

It is orientated towards the following requirements:

a. Information security guidelines are defined, approved by the responsible management, issued, periodically reviewed and, if necessary, revised and publicised to ETH members and relevant external parties;

b. A framework[3] and management system that can be used to initiate, control and report on the implementation of information security at ETH Zurich has been set up;

c. ETH members, research partners and contractors understand and fulfil their responsibilities regarding information security (awareness). Security checks are carried out as required. The protection of ETH Zurich's information security interests must be taken into account when commencing, changing or terminating employment, research cooperation or studies;

d. ETH Zurich inventories and classifies the information collected and processed on its behalf. It defines the responsibilities and accountabilities for the work equipment used and prevents the unauthorised disclosure, modification, removal or destruction of information;

e. Access to information and information-processing facilities is restricted to authorised persons. Users are responsible for protecting their authentication information;

f. The appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of information is ensured;

g. Unauthorised access to information processing facilities as well as damage to and impairment of information are prevented. The loss, damage, theft or endangering of assets and the interruption of organisational activities are prevented;

[3] For a graphical representation, see appendix "Information security framework"

h. The proper and secure operation of information processing equipment is ensured and protected against malware. Information assets are protected against loss and the integrity of systems in operation is ensured. Events are recorded and evidence is generated. Exploitation of technical vulnerabilities is prevented. The impact of audit activities on systems in operation is minimised;

i. Information in networks and in the supporting information processing facilities are protected and transmitted securely both within ETH Zurich and when dealing with any external bodies;

j. Information security is an integral part of the entire life cycle of information systems and is planned and implemented during the development cycle of information systems. The protection of information and data used for testing is ensured;

k. Information and IT resources of ETH Zurich that are accessible to guests in accordance with the guest regulations[4] (e.g. suppliers, emeriti, lecturers, etc.) are contractually protected in accordance with an agreed level of information security and service provision;

l. Information security incidents, including their notification, are handled consistently and effectively. This includes dealing with weaknesses in processes;

m. Information security is embedded in ETH Zurich's emergency planning, and

n. Information security is implemented in accordance with ETH Zurich policies and procedures and legal, regulatory or contractual obligations. Violations will be appropriately penalised.

[2] The above requirements are adapted to the needs of ETH Zurich as part of the information security strategy using a risk-orientated approach. Information assets, processes, applications and systems as well as people and values are at the centre of this strategy. The principles of expediency, cost-effectiveness and user-friendliness are taken into account.

[3] Reporting on information security is based on a compliance-orientated approach.

[4] RSETHZ 515.2

3. Section: Tasks, responsibilities, competences

Article 5 Information security as a management task

[1] Information security is a management task that is performed by the members of the Executive Board and the heads of the organisational units of ETH Zurich within their areas of responsibility. Information security is a shared responsibility to which all employees actively contribute.

[2] The implementation of information security is the responsibility of the managers of the central bodies, departments and their institutes, centres, laboratories and professorships as well as the managers of the units outside the departments.

[3] The heads of the organisational units work actively with the CISO.

Article 6 Chief Information Security Officer

[1] ETH Zurich appoints a Chief Information Security Officer (CISO).

[2] He/she is administratively assigned to the IT Services department. He/she reports to the Secretary General for the development of regulations and the information security strategy or the performance of audits in the area of information security. He/she coordinates information security throughout the university.

[3] The Chief Information Security Officer:

a. develops and maintains the information security strategy (for the attention of the Executive Board) as well as guidelines, recommendations, specialised concepts, methods, processes and tools;

b. carries out information security controlling as part of the information security management system (ISMS);

c. reports to the Executive Board via the Information Security Commission (see Art. 10);

d. initiates, coordinates and supports the implementation of information security as the highest, technically independent management body;

e. initiates, implements and coordinates awareness-raising and training measures;

f. is the central point of contact and advice centre for the Executive Board and the Information Security Officers (ISOs, see Art. 7);

g. heads the ISO committees and coordinates joint projects of the ISOs. He/she may also set up working groups;

h. is the responsible contact for the "Post and Telecommunications Surveillance Service" (ÜPF) operated by the Swiss Confederation and informs the Legal Service if he/she is contacted by law enforcement authorities and

i. represents ETH Zurich in external specialised committees.

[4] The Chief Information Security Officer has the following competences:

a. may request information on the status of information security and information security risks;

b. orders immediate measures in the event of urgent threats to information security in the event of a significant impairment of the normal use of IT resources or damage to ETH Zurich, its employees or third parties;

c. orders measures to be taken in the event of suspected misuse of ETH Zurich's IT resources;

d. defines the basic protection and is based on the standards and norms that have proven themselves in the professional world. Basic protection includes organisational measures and technologies to adequately secure information assets, processes, applications and systems;

e. has the right to audit information security throughout ETH Zurich and at external partners who provide services on behalf of ETH Zurich, insofar as this is contractually agreed or there is a legal basis for this;

f. is authorised to issue instructions to employees, students and guests of ETH Zurich regarding compliance with and implementation of information security requirements in accordance with the Guest Regulations[5];

g. may grant temporary exemptions within the framework of basic protection, whereby these must be reviewed by the applicant upon expiry and, if necessary, reapplied for, and

h. has the right to withdraw exceptional authorisations or to delegate or withdraw their granting in consultation with the organisational units concerned.

Article 7 Information Security Officers

[1] The heads of division, heads of staff, heads of department and heads of units outside the departments shall each appoint an Information Security Officer (ISO) for their area of responsibility.

[2] The Information Security Officer:

a. is the first point of contact and advice centre for all information security issues in their own area of responsibility;

b. keeps an up-to-date inventory of the information assets based on the reports from the information owners and reports these periodically to the CISO. The procedures to be used are defined in the directive "Inventory and Classification of Information at ETH Zurich";

c. reports at least once a year on the status of information security to the CISO and

d. participates in the meetings of ISO committees and actively contributes to ISO working groups.

[5] RSETHZ 515.2

Article 8 Information owners

[1] Information owners are responsible for the information assets that are collected and processed by them or on their behalf. As a rule, they are heads with budget responsibility for an organisational unit (professors, heads of units outside the departments, heads of department, heads of staff).

[2] The information owners:

a. know which regulations and laws are applicable to their information assets and are familiar with the relevant specialised bodies, such as the export control office or the data protection advisors within ETH Zurich, and

b. inventory and classify their information according to confidentiality, integrity and availability requirements.

Article 9 IT operators

[1] IT operators manage, maintain and develop IT resources. The IT operators for ETH Zurich are in particular the IT Services department, the IT Services Groups (ISG) of the departments and the central bodies as well as professorships with their own IT and the CSCS.

[2] The IT operators:

a. implement the specifications of the CISO;

b. are responsible for categorising the protection requirements of IT resources;

c. guarantee the information security of their IT resources;

d. monitor their IT resources and

e. are responsible for dealing with information security incidents in their area of responsibility.

[3] Reporting of information security incidents:

a. IT operators are obliged to report[6] to the IT Services department immediately, at the latest within 24 hours[7] of becoming aware of it.

b. In addition, IT operators shall report data security breaches involving personal data immediately, at the latest within 72 hours, to the data protection advisor[8] at ETH Zurich.

[4] IT Services (ID) are also responsible for monitoring the IT security of all IT resources in order to identify vulnerabilities and information security incidents.

a. They ensure that IT security incidents can be detected and dealt with appropriately.

b. They will support the CISO with technical investigations into information security incidents.

[6] Email address: security@ethz.ch
[7] Cybersecurity Ordinance (CSV) SR 120.73, Art. 21, para. 1
[8] Email address: ds@ethz.ch

4. Section: Steering

Article 10 Information Security Commission

[1] The Information Security Committee recommends to the Executive Board in the sense of a pre-decision committee:

a. updating the information security strategy, including the definition and implementation measures, and

b. the report on the status of information security.

[2] The CISO prepares the aforementioned documents and discusses them with the Information Security Commission.

[3] The Information Security Committee meets as often as business requires, but at least once a year.

Article 11 Information Security Committees

[1] The two information security committees are the "ISOs of the departments" and the "ISOs of the central bodies and units outside the departments".

[2] The committees serve to coordinate overarching projects, the mutual exchange of information and the professional review. The two committees also act in an advisory capacity to the CISO.

Article 12 Directive Landscape

The information security directive landscape distinguishes between the following hierarchical levels (see appendix "Information security framework"):

a. The Executive Board issues directives for the implementation of the strategic management guidelines;

b. The CISO enacts directives that define ETH Zurich-wide information security procedures, and

c. if necessary, the management functions of the organisational units specify the procedures (information security procedures) in their own directives, taking into account the technical and organisational circumstances.

5. Section: Final provisions

Article 13 Entry into force

The directive enters into force on 01 January 2025.

Zurich, 17 December 2024

On behalf of the Executive Board:

The President: Prof. Joël Mesot

The Secretary General: Katharina Poiger Ruloff

Appendix – Information security framework