Directive on “Information Security at ETH Zurich”
dated 9 April 2018

The Executive Board of ETH Zurich,
pursuant to Article 4(1)(g) of the Ordinance Governing
the Organisation of ETH Zurich dated 16 December 2003

hereby adopts the following Directive:

1. Section: General Provisions

Article 1 Purpose

1 ETH Zurich is responsible for assessing the need to protect information held by it which is
required for the performance of its duties, as set out in Article 2 of the ETH Act (staff and student
data, research data, business-related documents, building plans etc).

2 Within its sphere of responsibility, ETH Zurich shall ensure that information security is
organised, implemented and reviewed in line with scientific and technological developments and
shall adhere to acknowledged Good Practices.

3 This Directive sets out the information security objectives and risk management benchmarks
and defines the relevant responsibilities in relation to controlling and monitoring such objectives
and risks.

Article 2 Scope

1 This Directive applies to all units of ETH Zurich, as specified in the Ordinance Governing
the Organisation of ETH Zurich dated 16 December 2003 (hereinafter referred to as the "ETH
Zurich Organisational Ordinance")

1 RSETHZ 201.021
2 RSETHZ 201.021
- the central administrative units,
- academic departments and their related institutes, centres, laboratories and professorships,
- “teaching and research facilities outside the academic departments”, as defined in Article 61 of the ETH Organisational Ordinance, which are solely operated by ETH Zurich.

Separate procedural arrangements shall be established for teaching and research facilities outside the academic departments that are operated in cooperation with other institutions.

The use of IT resources at ETH Zurich is governed by the Acceptable Use Policy for Telematics Resources (“BOT”)

**Article 3 Definitions**

1. **Baseline security**
   Measures to ensure that information, processes, applications and systems, which require a normal level of protection, are adequately safeguarded.

2. **Information security**
   “Preservation of confidentiality, integrity and availability of information”.

3. **Integrity**
   “Property of accuracy and completeness”.

4. **IT operators**
   IT services and infrastructure operators for ETH Zurich include IT Services, the CSCS and IT Support Groups (ISGs) in the academic departments.

5. **IT security**
   Ensuring information security whenever IT resources are used.

**2. Section: Duties, Responsibilities, Powers (Information Security Governance)**

**Article 4 General principle**

Information security is a management responsibility falling to members of the Executive Board and heads of organisational units at ETH Zurich. They are responsible, as information owners, for any information that is collected and processed by them or on their behalf.

---

3 RSETHZ 203.21
5 ISO/IEC DIS 27000:2015
6 Article 4 BOT
7 Article 6 Richtlinien über den Schutz und den Umgang mit Personaldaten an der ETH Zürich (Guidelines on protecting and processing personal data at ETH Zurich - RSETHZ 612)
The heads of administrative departments, heads of staff units, heads of academic departments and heads of teaching and research facilities outside the academic departments are responsible for implementing information security, as defined in this Directive and as specified by the CISO in accordance with Article 5, and for managing the underlying risks for the organisational unit concerned.

The heads of the organisational units shall cooperate actively with the CISO.

**Article 5  Chief Information Security Officer**

ETH Zurich shall appoint a Chief Information Security Officer (CISO).

In line with the objectives defined in Article 12 of this Directive, the CISO is responsible for coordinating information security across the university, providing advice to information owners and Information Security Officers (ISOs) and reporting to the Risk Management Commission on a regular basis regarding his/her activities.

To ensure the independence of the CISO, he/she shall be incorporated into the units reporting to the President (e.g. the Secretary General).

The duties and responsibilities of the CISO include:

a. initiating, coordinating and assisting in the implementation of information security at ETH Zurich;

b. formulating, coordinating, maintaining and undertaking consultation procedures with respect to information security strategy at ETH Zurich as well as in relation to recommendations, technical approaches, methods, processes and resources in the field of information security;

c. developing security measures in accordance with Article 19 of this Directive;

d. chairing the ISO Committees in accordance with Article 11 of this Directive and coordinating common projects undertaken by ISOs. The CISO may deploy working groups;

e. initiating, undertaking and coordinating measures to raise awareness and provide training in information security, having regard to the information security requirements and principles laid down in the Informationssicherheitsgesetz des Bundes (Swiss Federal Information Security Act), the Swiss Federal Act on Data Protection, Swiss Human Research Act and the applicable implementing ordinances;

f. serving as a centre of expertise for all information security matters;

g. overseeing information security management at ETH Zurich;

h. information security risk management throughout ETH Zurich; consolidating and assessing information supplied by the ISOs in accordance with Article 6 of this Directive;

i. regularly updating the inventory of information that requires a higher standard of protection on the basis of reports submitted by the ISOs (Article 6);

---

8 Date on which this Act will come into force is not yet known.
9 Editorial correction of the phrase dated 1 June 2018.
j. reporting to the Risk Management Commission (RMC) on the status of information security and any unusual incidents or abuses in accordance with Article 19 BOT and any sanctions imposed under Article 20 BOT;

k. chairing the RMC group of experts for information security;

l. representing ETH Zurich on external expert committees.

5The CISO has the following powers:

a. defining security measures\textsuperscript{10} in accordance with Article 19 of this Directive;

b. the power to issue instructions to professors, employees, students, internal and external service provides (where stipulated in the agreement), guests and partners of ETH Zurich regarding adherence to and implementation of mandatory information security standards;

c. requesting information on the status of information security and the associated risks;

d. the power to conduct information security audits throughout ETH Zurich and at external partners appointed to provide services to ETH Zurich, to the extent that this is permitted under the applicable agreement or there is a legal basis for performing such audits;

e. imposing sanctions where there is reason to suspect abuse of the ICT resources of ETH Zurich in accordance with Article 20 BOT;

f. taking immediate action in accordance with section 4 of the Appendix to the BOT in the event of emergencies or imminent threats or attacks that pose a serious risk to information security at ETH Zurich, in cooperation with the authorities specified in this Directive, e.g. the ITSO ITS.

Article 6 Information Security Officers

1The heads of administrative departments, heads of staff units, heads of academic departments and heads of teaching and research facilities outside the academic departments shall each appoint an Information Security Officer (ISO) for their particular areas of responsibility.

2Unless otherwise specified, the within the academic departments shall discharge the function of ISO.

3The duties and responsibilities of the ISOs include:

a. maintaining an up-to-date inventory of information requiring a high level of protection on the basis of reports submitted by the information owners;

b. serving as the first point of contact for advice on all information security matters;

c. submitting reports on the status of information security and the associated risks to the CISO;

d. attending meetings held by the ISO committees and actively participating in ISO working groups.

Article 7 Information owners

\textsuperscript{10} Editorial correction of the phrase dated 1 June 2018.
Information owners are responsible for any information that has been collected and processed by them or on their behalf (see Article 4(1)). As a general rule, the heads of organisation units (professors, heads of administrative departments, heads of non-departmental teaching and research facilities, heads of staff units) will be the information owners. These parties are also responsible for classifying information in accordance with Article 21 of this Directive.

Article 8 IT Security Officer within IT Services

1 The Head of IT Services (ITS) shall appoint an IT Security Officer within IT Services (ITSO ITS).

2 He/she shall have professional responsibility for IT security in relation to the services provided by ITS to the centralised and decentralised organisational units of ETH Zurich and shall serve as the main IT security contact to the CISO. In addition, the ITSO ITS shall provide advice on IT security issues to the CISO and ISOs as required.

3 He/she shall arrange for checks to be carried out on behalf of the CISO, as provided in Article 18(2) BOT.

4 The ITSO ITS may give instructions for protective and precautionary measures to be taken, as specified in section 4(2) of the Appendix to the BOT, in the event of emergencies or imminent threats or attacks posing a serious risk to IT security at ETH Zurich, and shall, in parallel, notify the CISO of any such measures.

Article 9 IT operators

The IT operators are responsible for categorising the level of protection required for systems, applications and processes, which fall within their remit, in accordance with Article 23 of this Directive, as well as for evaluating the information security risks associated with the services for which they are responsible and implementing security measures in accordance with Article 19 of this Directive.

Article 10 IT Services

IT Services is responsible for monitoring the security of all network traffic of ETH Zurich. ITS coordinates and handles information security incidents within its area of responsibility. Except as otherwise provided herein, the responsibilities of IT Services are as set out in Article 4 BOT.

Article 11 Committees

1 The Risk Management Commission (RMC) group of experts for information security is a working group of risk management specialists. The working group shall assist the CISO in the development of information security and operate, alongside the ISOs and ITSO ITS, as an expert review body.

2 The committees consisting of the “departmental ISOs” and the “ISOs of the central administrative units and teaching and research facilities outside the academic departments” are responsible for coordinating cross-cutting projects, sharing information and conducting technical reviews.

3. Section: Information Security Objectives
Article 12  Objectives
To ensure ETH Zurich’s ability to act and prevent loss or damage, the following information security objectives have been defined:

a. Compliance with legal requirements relating to information security;
b. Preserving the availability, confidentiality and integrity of information, processes, applications and IT components in line with requirements;
c. Detecting and dealing with significant information security attacks.

Article 13  Implementation of objectives
The organisational units are responsible for implementing objectives and measures, insofar as is practicable in terms of budget and human resources, both on their own initiative and on the basis of guidelines and recommendations issued by the CISO.

Article 14  Culture of information security
1ETH Zurich shall instil a culture of awareness in relation to information processing by initiating measures to promote understanding and by organising training initiatives in line with requirements.

2Due consideration shall be given at all times to the relevant information security aspects of processes, projects and operations.

4. Section: Management of Risks

Article 15  Risk-based approach
1ETH Zurich adopts a risk-based approach to information security, which includes adhering to acknowledged good practices, standards and guidelines in accordance with Article 1(2) of this Directive.

2Suitable measures should be taken to reduce information security risks to an acceptable level, having regard to the principles of reasonableness, economy and user-friendlyliness.

3The risk-based approach shall be focused primarily on processes, applications and systems requiring a high level of protection in accordance with Article 23 of this Directive.

Article 16  Information requiring a high level of protection
As a minimum, the following information requires a high level of protection:

a. sensitive personal data and personality profiles, as defined in the Swiss Federal Act on Data Protection and Article 59 ff. of the Personnel Ordinance for the ETH Domain (PVO-
ETH), which must be processed in personnel information and study administration systems in accordance with Article 36a and 36b of the ETH Act;

b. health-related data, as defined in the Human Research Act and applicable implementing ordinances;

c. research project data that requires a high level of protection under the terms of an agreement or for other reasons;

d. academic data, including information on student performance and results;

e. financial information (SAP, online banking, accounting production systems etc.);

f. infrastructure data (e.g. building plans and offsite premises plans);

g. archives, and

h. ETH Zurich webpages.

Article 17 Requirement to report to the CISO

1The ISOs are required to report the following matters to the CISO not less than once a year:

- information requiring a high level of protection
- information security risks and security measures.

2The CISO shall maintain a register of all information, risks and security measures reported in accordance with Article 17(1) above.

Article 18 Risk assessment by the CISO

1The CISO shall assess the information, information security risks and measures reported to him/her in accordance with Article 17.

2If the CISO’s assessment differs from the assessment of any information owner, the CISO shall consult the Corporate Risk Manager, the relevant Information Security Officer and the information owner regarding any adjustments that may be required.

2Any conflicts may be submitted for determination by the members of the “RMC group of experts for information security”. Such determination shall be made without the participation of the CISO.

Article 19 Security measures

1The CISO is responsible for determining the measures required to ensure baseline security. The measures providing a basic level of protection shall be aligned with current good practices in accordance with Article 1(2) and ensure that information, processes, applications and systems, which require a normal level of protection, are adequately safeguarded.

2Enhanced measures shall be deployed to safeguard information, processes, applications and systems, which require a high level of protection, from unauthorised access, including logical and physical access control to systems, applications and information as well as physical systems access. Standardised security measures shall be implemented for this purpose. The CISO shall define the sets of measures required in consultation with the ISOs and IT operators responsible.

3Where information requires a high level of protection, the relevant information owners shall select appropriate security measures in accordance with Article 19(2) above and ensure that
such measures are implemented. The ISO concerned shall advise the information owner responsible on selecting appropriate measures. Where standardised measures are impracticable, alternative measures shall be taken in consultation with the ISO and CISO.

6. Section: Classification of Information and Required Level of Protection

Article 20 Principles of classification
1 Information shall be classified in accordance with the levels indicated in Article 22 only to the extent necessary and, where feasible, for a limited period of time.
2 Information owners shall indicate which information is confidential or requires a high level of integrity or availability.

Article 21 Responsibility for classification
1 Information owners are responsible for classifying information that falls within their remit (authority responsible for classification).
2 Classification levels may only be changed or removed by the authority responsible for classification or the next level authority in the reporting structure.

Article 22 Classification levels
Confidentiality classification:

a) Public:
   Public information is any information that has been approved for publication by the relevant authority (e.g. the Executive Board or Corporate Communications). All information is deemed to be internal or confidential unless or until such approval has been granted.

b) Internal:
   Internal information means information intended for members of ETH Zurich\(^{11}\). ETH information is deemed to be internal unless a different classification level has been assigned by the information owner.

c) Confidential:
   Information that is intended for a restricted, clearly defined group of recipients.

Integrity classification:

a) Normal:
   The potential consequences of unauthorised or unintentional changes to the information are deemed to be acceptable by the information owner. Careful management of information in day-to-day operations and the deployment of baseline security (e.g. protected access and backups) are deemed to constitute adequate security measures.

---

\(^{11}\) ETH Act, Article 13
This is the standard value assigned to any information that is not explicitly categorised as requiring a "high" level of integrity.

b) High:
Unauthorised or unintentional changes to the information are unacceptable as far as the information owner is concerned. Such changes must be prevented or at least identified.

Availability classification:

a) Normal:
Restricted access or total loss of access to information for at least one working day\(^{12}\) is deemed to be acceptable.
The loss of any changes made to information since the data was last backed up prior to an incident is deemed to be acceptable.
This is the standard value assigned to any information that is not explicitly categorised as requiring a "high" level of availability.

b) High:
Restricted access or total loss of access to information for up to 12 hours is deemed to be acceptable.
The loss of any changes made to information since the data was last backed up prior to an incident is deemed to be acceptable or additional protective measures against data loss are required.

**Article 23  Required level of protection**

\(^1\)High level of protection
A high level of protection is required for information classified as “confidential” or as requiring a “high” level of integrity or availability in accordance with Article 22 of this Directive.
The same applies to processes, applications and systems where information requiring a high level of protection is processed or where the loss of such information would materially affect ETH Zurich’s ability to perform its statutory duties or would involve substantial recovery costs.

\(^2\)Normal level of protection
A normal level of protection is required for information, processes, applications and systems that do not require a high level of protection.

**7. Section: Concluding Provisions**

**Article 24  Transitional provisions**
The Head of Safety, Security, Health and Environment, acting in the capacity of IT Security Officer, and the Head of IT Services, who is the acting CISO, will continue to be responsible for information security matters until the CISO takes office.

---

\(^{12}\) In this Directive, “working days” mean Monday – Friday, excluding public holidays
**Article 25  Commencement**

This Directive takes effect on 1 May 2018.

Zurich, 9 April 2018

For and on behalf of the Executive Board:

The President: Lino Guzzella

The Secretary General: Katharina Poiger Ruloff