RSETHZ 203.25en

English is not an official language of the Swiss Confederation. This translation is provided for information purposes only and has no legal force.

Directive on "Information Security at ETH Zurich"

dated 9 April 2018 (last updated: 1 August 2021)[1]

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[2]

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)[3], and their members and, in particular, to

[1] Partial revision to introduce a fourth level for classification on the basis of confidentiality and the use of external cloud services in accordance with the Executive Board's decision of 12 July 2021.
[2] RSETHZ 201.021en
[3] RSETHZ 201.021en

- 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.

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

[3] The use of IT resources at ETH Zurich is governed by the ETH Zurich Acceptable Use Policy for Information and Communications Technology ("BOT")[4].

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".[5]
[3] *Integrity*	"Property of accuracy and completeness".[6]
[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.[7]
[5] *IT security*	Ensuring information security whenever IT resources are used.
[6] *Classification of information and classification note*[8]	*Classification:* allocation to *a classification level in accordance with* Art. 22. *Classification note*: necessary designation* of a classification on the basis of confidentiality (Article 22(1)) by marking information as "confidential" or "strictly confidential". *This requirement only applies to information classified as "confidential" or "strictly confidential".
[7] *Cloud computing and cloud services* [9]	*Cloud computing*: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or

[4] RSETHZ 203.21en; editorial change, version as per the Executive Board decision of 26 March 2019, in force since 1 April 2019.
[5] ISO/IEC DIS 27000:2015 Information technology – Security techniques – Information security management systems – Overview and vocabulary
[6] ISO/IEC DIS 27000:2015
[7] Article 4 of the ETH Zurich Acceptable Use Policy for Information and Communications Technology, BOT
[8] Version according to Executive Board decision of 12 July 2021, in force since 1 August 2021.
[9] Version according to Executive Board decision of 12 July 2021, in force since 1 August 2021.

	virtual resources with self-service provisioning and administration on demand. Source: ISO/IEC 17788:2014, Information technology – Cloud computing – Overview and vocabulary, para. 3.2.5 *Cloud services*: One or more capabilities offered via cloud computing invoked using a defined interface. Source: ISO/IEC 17788:2014, Information technology – Cloud computing – Overview and vocabulary, para. 3.2.8
[8] *External ICT service/external cloud service*[10]	ICT* service purchased by ETH Zurich that is provided by a third-party company outside the ETH Zurich network (e.g. external cloud service). *ICT = information and communications technology Source: IT-Richtlinien und IT-Grundschutzvorgaben (IT guidelines and baseline IT security requirements) directive, RSETHZ 203.23

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

Article 4 General principle

[1] 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.[11]

[2] 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.

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

[10] Version according to Executive Board decision of 12 July 2021, in force since 1 August 2021.
[11] 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)

Article 5 Chief Information Security Officer

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

[2] 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.

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

[4] 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)[12], 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[13]: 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);

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.

[12] Date on which this Act will come into force is not yet known.
[13] Subsequent editorial correction of August 2018.

[5] The CISO has the following powers:

a. defining security measures[14] 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 measures 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

[1] The 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.

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

[3] The 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[15]

[1] 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.

---

[14] Subsequent editorial correction of August 2018.

[15] Version according to Executive Board decision of 12 July 2021, in force since 1 August 2021.

[2] The information owners are responsible for assessing/clarifying which requirements and laws apply to the information they hold (such as data protection for personal data or export control for expertise/technologies with features that could also be suitable for military use, known as dual-use technologies).

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

[1] ETH 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.

[2] Due 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

[1] ETH 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.

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

[3] The 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. rescinded

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 16bis Information requiring a very high level of protection

As a minimum, the following information requires a very high level of protection:

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

Article 17 Requirement to report to the CISO

[1] The 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.

[2] The 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

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

[2] If 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.

[3] Any 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

[1] The CISO defines baseline security. Baseline security 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 or high level of protection, are adequately safeguarded.

[2] Enhanced measures shall be deployed to safeguard information, processes, applications and systems, which require a very 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.

[3] Where information requires a very 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.

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

Article 20 Principles of classification[16]

[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 *classify* the information that falls within their remit (classification obligation) according to risk-based principles pursuant to Article 22. The classification is generally conducted informally.

[3] “Confidential” and “strictly confidential information” must be designated as such with a classification note. The decision on the designation of confidential research data shall be taken by the information owners.

[4] Contractual arrangements must be taken into account in the classification and designation of information. If an external partner gives information provided to ETH a higher classification than ETH, the higher classification under Article 22 should be chosen and vice versa.

[5] The principle of freedom of information in the administration (FoIA) continues to apply to classified information.

[16] Version according to Executive Board decision of 12 July 2021, in force since 1 August 2021.

Article 21 Responsibility for classification[17]

[1] Information owners are responsible for classifying information that falls within their remit (authority responsible for classification). If information owners as defined in Article 7 do not provide any indication of the classification, the standard classification can be assumed to apply: “internal” for confidentiality and “normal” for the integrity/availability of information.

[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[18]

[1] Confidentiality classification:

a) PUBLIC:
Public information is any information that has been approved for publication by the relevant authority.

Classification aid: When it comes to publishing administrative and/or technical information (classification as “public”), a communications office of ETH Zurich (departmental or Corporate Communications) must generally be involved. Decisions regarding the publication of research results shall be taken, subject to contractual or statutory rights of third parties, such as copyright, by the information owners.[19]

Published information does not have to be designated as such with a classification note.

b) INTERNAL:
Information is classified as “internal” if unauthorised individuals’ becoming aware of it could damage the interests of ETH Zurich.

Classification aid: Internal information means information intended for members of ETH Zurich[20]. Internal information does not have to be designated as such with a classification note.

c) CONFIDENTIAL:
Information is classified as “confidential” if unauthorised individuals’ becoming aware of it could significantly damage the interests of ETH Zurich.

Classification aid: Confidential information is information that is (generally) intended for a specific group of people, function or role (internal at ETH or external) only. Confidential information must be marked as such with a classification note.

d) STRICTLY CONFIDENTIAL:
Information is classified as “strictly confidential” if unauthorised individuals’ becoming aware of it could severely damage the interests of ETH Zurich.

Classification aid: Information is deemed to be strictly confidential if it is intended for a restricted, clearly defined and named group of recipients. Strictly confidential information must be marked as such with a classification note.

---

[17] Version according to Executive Board decision of 12 July 2021, in force since 1 August 2021.
[18] Version according to Executive Board decision of 12 July 2021, in force since 1 August 2021.
[19] ETH Act, Article 36(2)
[20] ETH Act, Article 13

[1bis] Classification notes (designation of classified information) must be written in capital letters. Information that is not marked with a classification note (e.g. documents) is deemed to be “internal”. This does not include published information.

[1ter] Appendix 1 contains recommendations for the classification of information according to confidentiality. Appendix 1 also contains examples of the designation of information (application of the classification notes).

[1quater] Appendix 2 sets out the requirements for handling information that is classified according to confidentiality.

1[quinques] Responsibility for implementing the requirements set out in the Appendices lies with the information owners.

[2] 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. 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.

[3] Availability classification:

a) Normal:
Restricted access or total loss of access to information for at least one working day[21] 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.

[21] In this Directive, “working days” mean Monday – Friday, excluding public holidays.

Article 22bis Outsourcing of information to external ICT services (e.g., external cloud services)[22]

[1] Where information is outsourced (saving or processing) to external ICT services, this shall be done **at the responsibility of** the information owners.

[2] Information may be outsourced to external ICT services under certain conditions (for further information, see the requirements in Appendix 2, “Electronic information in cloud services” and the IT-Richtlinien und IT-Grundschutzvorgaben (IT guidelines and baseline IT security requirements) directive, RSETHZ 203.23).

[3] Prior to outsourcing information to external ICT services, information owners must conduct a risk assessment (see Appendix 2, “Electronic information in the cloud”).

[4] Strictly confidential information in accordance with Article 22(1) may not be outsourced to external ICT services.

Article 23 Required level of protection[23]

[1] Very high level of protection

A very high level of protection is required for information classified as “strictly confidential” in accordance with Article 22 of this Directive.

The same applies to processes, applications and systems where information requiring a very high level of protection is processed or where the loss of such information would severely affect ETH Zurich’s ability to perform its statutory duties or would involve correspondingly high recovery costs.

[1bis] High level of protection

A high level of protection is required for information classified as “confidential” 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.

[22] Version according to Executive Board decision of 12 July 2021, in force since 1 August 2021.
[23] Version according to Executive Board decision of 12 July 2021, in force since 1 August 2021.

6. Section: Concluding Provisions[24]

Article 24

rescinded

Article 24bis Transitional provision for Article 22[25]

The classification according to confidentiality and the handling of information classified in this way applies in accordance with Article 22(1), (1bis), (1ter) and (1quater):

a) to information (documents, data collections, paper-based dossiers, archives, etc.) newly generated on or after 1 December 2021.

b) to already existing information from 1 December 2023. It is the responsibility of the data owners to check whether information that has already been classified as confidential qualifies for classification as “strictly confidential”.

Article 24ter Transitional provision for Article 22bis[26]

Article 22bis on the outsourcing of information to external ICT services (e.g. external cloud services) enters into force on 1 December 2021.

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

[24] Version according to Executive Board decision of 12 July 2021, in force since 1 August 2021.
[25] Version according to Executive Board decision of 12 July 2021, in force since 1 August 2021.
[26] Version according to Executive Board decision of 12 July 2021, in force since 1 August 2021.

Appendix 1a: Classification recommendation (confidentiality)[27]

The list below contains recommendations for the classification of selected information according to confidentiality. This recommendation is subject to differing (generally higher) classifications by the information owners. For correct classification according to confidentiality, please pay attention to Appendix 1b in particular. The Information Security Officer can provide further information if anything is unclear.

Information (selection)	Classification
ETH Zurich website/Internet documents	**Public**
Press briefings/releases	
Lists of lectures/lecture timetables	
Research data, primary and secondary data (published)	
Published dissertations	
Legal Collection of ETH Zurich	
Circular e-mails	**Internal**
Calendar entries (depending on handling by information owner)	
Internal telephone book/address book	
Newsletters/blogs	
Townhall meetings	
Lecture scripts (provided that they have not been made publicly available by the author)	
"Non-sensitive" personal data that is not worthy of special protection (personal data, the abuse of which generally does not have particular consequences for the person affected, such as last name, first name, (company) address, date of birth, ETH telephone number or information that has appeared in the media, provided that it is not of a sensitive nature; see risk levels in the Swiss federal government guide)	
Executive Board/department motions, including minutes	**Confidential**
ETH Zurich strategy (at least while it is being developed)	
Medium-term planning, budget and financial planning, annual report while it is being worked on	
Financial/risk report	
Management reporting including key management figures	
HR files/documents: applications, assessments, employment contracts, etc.	
Student performance assessments, grades, exam documents	
Contracts (cooperation agreements, third-party companies, research, confidentiality)	
IT network plans	
Research data, primary and secondary data prior to publication	
(Planned and ongoing) research projects	
Survey results	
Consultancy and supplier agreements	
Export-controlled information (risk assessment in consultation with customer/partner or export control recommended)	
Library lending data (interest/personality profile of the borrower recognisable)	

[27] Version according to Executive Board decision of 12 July 2021, in force since 1 August 2021. Editorial amendment of various hyperlinks in the Appendices as of 12 January 2022.

Personal research data not subject to the Human Research Act	
Salary data (risk assessment recommended)	
Auditors' report, audits	
E-mail, Internet, intranet or telephone log, usage and traffic data	
Teaching and learning platforms (data on students' academic achievement and conduct recognisable)	
Self-assessments	
Student administration, exam administration	
Process information	
Crisis committee documents (alarm organisation, emergency scenarios, BCM, minutes)	
Project documents: applications, reports, protocols	
Personal data of a particularly sensitive nature and personality profiles in accordance with Article 3 of the Federal Act on Data Protection; except medical health-related data, which is subject to the Human Research Act (risk assessment recommended: personal data, the abuse of which can [significantly] impact a person's economic situation or social standing; see the risk levels in the Swiss federal government guide)	
Ongoing patent proceedings	
(Personal) passwords	**Strictly confidential**
Intellectual property, such as technical inventions, program code, etc., for which there is an obligation to maintain confidentiality (risk assessment recommended)	
Information that identifies individuals directly (e.g. tables with keys use to de-identify a patient by means of encoding/pseudonymisation)	
Research data (contractually agreed, e.g. with cooperation partners, third parties)	
Internal reorganisation projects with job cuts	
Data that is subject to professional secrecy and patient and medical data that is subject to professional secrecy for research involving humans or under the Human Research Act* (see Article 321**/Article 321bis of the Swiss Criminal Code (StGB)) *if patient and medical data have not been irreversibly anonymised in accordance with Article 25 of the Human Research Ordinance (HRO) or explicitly given a different classification (risk assessment recommended) **N.B.: Article 321 also applies to students who reveal a secret that they became aware of during their studies	
Research results that could cause serious damage in the event of premature disclosure (risk assessment recommended; see also Appendix 1b)	
Information that is classed as industrial or trade secrets under Article 162 of the Swiss Criminal Code (risk assessment recommended)	
Company acquisitions, foundations	
Highly sensitive personal data (risk assessment recommended: personal data, the abuse of which can endanger the affected person's life; see risk levels in the Swiss federal government guide)	

Appendix 1b: Classification recommendation (confidentiality) taking risk evaluations ("risk assessments") into account[28]

The list below contains recommendations for classifying the confidentiality of selected information on the basis of risk assessments. This recommendation is subject to differing (generally higher) classifications by the information owner. The Information Security Officer can provide further information if anything is unclear.

A risk assessment in accordance with the ETH Zurich Risk Management Manual is recommended (see section 6.3). The risk assessment should be conducted using the following categories:

- Finances
- Reputation
- Applicable law (e.g., personal rights)

The risk assessment shall refer – as appropriate – to at least one of the following points:

- ETH as an institution
- One (or more) departments
- Individuals or groups of individuals (e.g. ETH members but also people external to ETH who have been given access to ETH data, such as health data used for research purposes)

Risk assessment	Classification
Information deemed to be "unclassified" within the meaning of the Federal Act on Freedom of Information in the Administration (FoIA) and/or has been released for publication by the information owner. For information owners: if a risk assessment appears expedient, please conduct one.	**Public**
At most a **low risk** for ETH as an institution. Similar risk assessments can also be conducted for individual (or multiple) departments, individuals or groups of people.	**Internal**
At most a **medium/significant risk** for ETH as an institution. Similar risk assessments can also be conducted for individual (or multiple) departments, individuals or groups of people. Examples: Loss of confidentiality can have the following consequences: - Significant financial or reputational damage - Breach of personal rights, e.g. under the Federal Act on Data Protection	**Confidential**

[28] Version according to Executive Board decision of 12 July 2021, in force since 1 August 2021.

High/very high risk for ETH as an institution. Similar risk assessments can also be conducted for individual (or multiple) departments, individuals or groups of people. Examples: Loss of confidentiality can have the following consequences: - Serious financial damage or lasting reputational damage - Serious legal consequences (e.g. under the Swiss Criminal Code) - Serious consequences for individuals or groups (health, life and limb)	**Strictly confidential**

Key:
The risk ratings of "low", "moderate/significant" and "high/very high" are based on the colours in the risk tables provided in the Risk Management Manual. The same applies to "significant" and "serious" consequences.

Appendix 1c: Recommendations for the designation of information classified as confidential or strictly confidential (classification notes)[29]

Classification notes must be written in capital letters. No classification note must be applied for information classified as "public" or "internal".

- *For Word documents:* Use of a title page with the designation "CONFIDENTIAL" or "STRICTLY CONFIDENTIAL". The designation is repeated on every page (e.g., in the header or footer). See: templates with classification notes. The same applies to Excel sheets, graphics, etc., where applicable.

- *Videos/films*: the words "CONFIDENTIAL"/"STRICTLY CONFIDENTIAL" are shown at the beginning of the video.

- *Creation/use of a database* – display the following words, for example, during the login process (initial screen): "This data is CONFIDENTIAL/STRICTLY CONFIDENTIAL (e.g., in ETHIS)"

[29] Version according to Executive Board decision of 12 July 2021, in force since 1 August 2021.

Appendix 2: Handling classified information (confidentiality)[30]

Information must be handled differently depending on the level of confidentiality. The Information Security Officer can provide further information if anything is unclear.

General requirements for classified information

Handling	Public	Internal	Confidential	Strictly confidential
Classification is carried out	by the information owner or on his/her behalf			
Change of classification	Not applicable	Is carried out by the information owner or his/her superior		
Designation of classification	Not necessary	Not necessary	Mark as "confidential"* *optional for research data	Mark as "strictly confidential"
Grant access/assign access rights	No restriction	Only to authorised individuals	To verifiable authorised individuals (e.g., authorised groups of people)	To individually authorised persons; Owner keeps a list of authorised individuals
Verification of access/ access rights	Not applicable	Not applicable	As required	Immediately if access rights or classification are changed

Information on physical media/data storage devices (paper, film, slides, etc.)

Handling	Public	Internal	Confidential	Strictly confidential
Processing	No restriction	No restriction	May not be viewed by unauthorised individuals	May not be viewed by unauthorised individuals
Filing/storage	No restriction	Clear desk	Clear desk, keep under lock and key	Clear desk, keep in safe if possible
Forwarding within ETH	No restriction	Only to authorised individuals	To verifiable authorised individuals (e.g., authorised groups of people)	To individually authorised persons, use encrypted data storage devices, confirmation of receipt, to be approved by owner, confidentiality agreement
Use with third parties	No restriction	To authorised individuals only, confidentiality agreement* *optional for research data	To verifiable authorised individuals (e.g. authorised groups of people), confidentiality agreement* *optional for research data	To individually authorised persons, encrypted data storage devices, confirmation of receipt, to be approved by owner, confidentiality agreement

[30] Version according to Executive Board decision of 12 July 2021, in force since 1 August 2021.

Received by mistake	Inform sender	Inform sender	Inform sender, keep under lock and key, return or destroy according to sender instructions	Inform sender, keep under lock and key, return or destroy according to sender instructions
Sent by mistake	Inform recipient	Inform recipient, request destruction or return	Notify information owner, Follow information owner's instructions, Inform recipient	Notify information owner, Follow information owner's instructions, Report incident to CISO or the Legal Office
Take on business trips	Permitted	Permitted	Avoid if possible, take care on public transport!	To be approved by owner, take care on public transport!
Take home	Permitted	Permitted	Avoid if possible, take care on public transport!	To be approved by owner, take care on public transport!
Disposal/destruction (office)	Waste paper/waste	Class 1 shredder[31]	Class 3 shredder[32], destruction by third parties: written confirmation required	Class 3 shredder[33], destruction by third parties: written confirmation required

[31] pursuant to standard DIN 66399
[32] pursuant to standard DIN 66399
[33] pursuant to standard DIN 66399

Electronic information

Handling	Public	Internal	Confidential	Strictly confidential
On-screen processing	No restriction	No restriction	May not be viewed by unauthorised individuals	May not be viewed by unauthorised individuals
Stored on ETH file server	No restriction	No restriction	Shared drive with restricted access rights	Shared drive with restricted access rights; security requirements are very high, e.g., encryption (see IT-Richtlinien und IT-Grundschutzvorgaben (IT guidelines and baseline IT security requirements) directive)
Access to ETH data via private ICT resources (e.g via PC, smartphone)	Permitted	Use ETH infrastructure if possible* (*where the use of ETH infrastructure is not possible: the entry of ETH passwords in order to access ETH accounts via private ICT resources is permitted)		Not permitted
Access via publicly accessible ICT resources (e.g. Internet café)	Permitted	Not permitted	Not permitted	Not permitted
Forwarding within ETH	No restriction	To authorised individuals only	To verifiable authorised individuals (e.g., authorised groups of people)	To individually authorised persons, encryption, confirmation of receipt, to be approved by owner, confidentiality agreement
Use with third parties	No restriction	To authorised individuals only, confidentiality agreement* *optional for research data	To verifiable authorised individuals (e.g., authorised groups of people), confidentiality agreement* *optional for research data	To individually authorised persons, encryption, confirmation of receipt, to be approved by owner, confidentiality agreement
Received by mistake (e.g., e-mail)	Inform sender	Inform sender	Inform sender, no forwarding, delete if possible, according to sender's instructions	Inform sender, no forwarding, delete if possible, according to sender's instructions
Sent by mistake (e.g., e-mail)	Contact recipient	Inform recipient, request deletion	Notify information owner, Follow information owner's instructions, Inform recipient	Notify information owner, Follow information owner's instructions, Report incident to CISO or Legal Office
Received by mistake (mobile data storage device)	Inform sender	Inform sender	Inform sender, Keep under lock and key, Return or destroy according to sender instructions	Inform sender, Keep under lock and key, return or destroy according to sender instructions
Sent by mistake (mobile data storage device)	Inform recipient	Inform recipient, request destruction or return	Notify information owner, Follow information owner's instructions, Inform recipient	Notify information owner, Follow information owner's instructions, Report incident to CISO or Legal Office

Sending/receipt of mobile data storage devices[34]	No restriction	Internally at ETH: To authorised individuals only Outside ETH: To authorised individuals only Confidentiality agreement* *optional for research data	Internally at ETH: To verifiable authorised individuals, encrypted data storage devices, locked container Outside ETH: To verifiable authorised individuals, encrypted data storage devices, locked container, confidentiality agreement* *optional for research data	Recommendation: avoid using mobile data storage devices if possible If necessary, then: Internally at ETH: To individually authorised persons, Encrypted data storage device, in locked container, Confirmation of receipt, approved by owner, Confidentiality agreement Outside ETH: as internally at ETH
Disposal/destruction of mobile data devices	Waste/electronic waste (environmentally friendly)	Class 1 shredder[35]/formatting	Class 3 shredder[36]/destroy, destruction by third parties: written confirmation required	
Reuse/sale/donation of PC outside ETH[37]	No restriction	Reinstall PC	Overwrite/wipe PC's internal data storage device [38] and reinstall it	

[34] e.g., CD/DVD/Blu Ray, USB, SSD/flash memory, cameras, interchangeable hard disks, etc.
[35] pursuant to standard DIN 66399
[36] pursuant to standard DIN 66399
[37] Personal computer
[38] Processes that only mark the memory cells as deleted are not permitted.

Electronic information in cloud services (additional cloud-specific requirements)

Handling	Public	Internal	Confidential	Strictly confidential
Personal data under the Federal Act on Data Protection (excluding medical data under the Human Research Act)	No restriction	Possible if Federal Act on Data Protection (FADP) and in particular the Federal Data Protection and Information Commissioner's guide to cloud computing (FDPIC) are complied with: • Data processing only within the meaning of Article 10a FADP • Cloud provider meets data security requirements pursuant to Article 7, 8ff/20ff of the Ordinance to the Federal Act on Data Protection (OFADP) • Data disclosure abroad only if compliance with Article 6 FADP is guaranteed (see also position paper, guide, explanations, list of countries and standard contract from the FDPIC) • Only if right to information under Article 8 FADP and right to deletion under Article 5 FADP are guaranteed • If applicable, registration of data files, Art. 11a • Risk assessment necessary*		Not permitted
Research data according to export control rules	Not applicable	If research data is subject to export control rules and is also intended to be exported abroad, it is essential to obtain official approval prior to uploading it to a cloud. Approval is granted by the SECO (via the ETH Zurich export control office). The same applies to data/information that is uploaded to clouds on which, although the server is in Switzerland, the data/information will be accessible to recipients abroad (deemed export).		
Technical data	No restriction	Permitted with risk assessment* (by information owner), appropriate organisation and, if necessary, technical security measures, taking into account existing laws (e.g., export control), contractual agreements and rights of third parties (e.g., personal rights or copyright)		Not permitted

< Continued on next page >

<table>
<tr><td rowspan="2">Designation of data</td><td rowspan="2">No</td><td>Mark as “internal”**
optional for research data</td><td>Mark as “confidential”
**optional for research data</td><td rowspan="2">Not applicable</td></tr>
<tr><td colspan="2">Indication of which cloud services the respective information is intended for**
**optional for research data</td></tr>
</table>

*Supporting material (template) is available from the CISO.