Directive "Inventory and Classification of Information at ETH Zurich"

of 01 January 2025

The Chief Information Security Officer of ETH Zurich

based on Art. 6, para. 4 (d and f) of the directive "Information Security at ETH Zurich"[1]

hereby decrees:

1. Section: General provisions

Article 1 Subject matter

[1] This directive governs the inventory and classification of information.

[2] Taking inventory makes it possible to obtain an overview of the information assets. Classification means the categorisation of information according to confidentiality, integrity and availability.

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 (ETH Zurich Organisation Ordinance)[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.

2. Section: Taking inventory

Article 3 Obligation to notify the ISO

[1] The information owners report periodically to the Information Security Officer (ISO) for their area of responsibility:

a. the information assets with high and very high protection requirements in accordance with Art. 9 of this Directive and
b. the relevant security measures.

---

[1] RSETHZ 203.25

[2] RSETHZ 201.021

Information owners are persons who are responsible for the information that is collected and processed by them or on their behalf.

[2] The ISO shall keep a register of the reported information assets and security measures.

3. Section: Classification of information

Article 4 Principles

[1] Information is classified according to confidentiality, integrity and availability.

[2] A classification is based on the level of protection required for an information asset (protection requirement).

[3] The classification indicates how the information owners expect users to handle their classified information.

Article 5 Responsibilities

[1] Information owners are responsible for classifying the information available in their area of responsibility (classifying body).

[2] Classifications may only be changed by the classifying body or a higher-level body.

[3] Users process information on behalf of the information owners. They shall comply with the rules of conduct in the appendices to this directive.

Article 6 Classification levels according to confidentiality

[1] Information owners classify the information according to the risk-oriented approach (see Appendix 1a):

a. PUBLIC: Information is considered public if it is authorised for publication by the responsible body.

   Classification aid: For the publication of information (classification as "public") of administrative-technical information, the information owner must be consulted. In case of doubt, a communication centre at ETH Zurich should be consulted (departmental or university communication). The information owner(s) decides on the publication of research results, subject to contractual or legal rights of third parties, such as copyrights[3].

b. INTERNAL: Information is deemed to be "internal" if its knowledge by unauthorised persons could impair the interests of ETH Zurich.

[3] ETH Law, Art. 36 para. 2

Classification aid: Internal information is intended for members of ETH Zurich[4]. Internal information does not have to be labelled as such with a classification note.

c. CONFIDENTIAL: Information is deemed to be "confidential" if its knowledge by unauthorised persons could significantly impair the interests of ETH Zurich.

Classification aid: Information is considered confidential if it is (generally) only intended for a specific group of persons (both internal and external to ETH), group, function or role. Confidential information must be labelled as such with a classification note.

d. STRICTLY CONFIDENTIAL: Information is deemed to be "strictly confidential" if its knowledge by unauthorised persons seriously harm the interests of ETH Zurich.

Classification aid: Information that is intended for a limited, precisely defined and named group of recipients is considered strictly confidential. Strictly confidential information must be labelled as such with a classification note.

[2] Annex 1b contains recommendations for the classification of selected information.

Article 7 Classification levels according to integrity

[1] Information owners classify the integrity of information with a risk-oriented approach on request:

a. NORMAL integrity: Possible effects of unauthorised or unintentional changes to the information are acceptable to the information owners (effects not significant or serious). Access protection and back-up are considered sufficient security measures to ensure normal integrity.

Applies as the default value for all information that is not explicitly categorised as "high" in terms of integrity.

b. HIGH integrity: Unauthorised or unintentional changes to the information are not acceptable to the information owners (significant or serious impact). They must be prevented or at least recognised. Possible examples are archives and the websites of ETH Zurich.

Article 8 Classification levels according to availability

[1] Information owners classify the availability of information with a risk-orientated approach on request:

a. NORMAL availability: Restrictions on access to the information or a complete loss of access for up to 3 working days[5] is acceptable. A loss of the changes made to the information since the last data backup is acceptable. Applies as the default value for all information that is not explicitly categorised as "high" in terms of availability.

[4] ETH Law, Art. 13

[5] The following are deemed to be working days in this directive: Monday – Friday, except public holidays

b. HIGH availability: Restrictions on access to the information or a complete loss of access for a maximum of 12 hours per calendar year is acceptable. A loss of the changes made to the information since the last data backup prior to an incident is acceptable or additional measures to protect against data loss are required.

Article 9 Modalities

[1] If different classifications are applicable to a piece of information (e.g. due to contractual agreements), the stricter classification is to be applied or the protection requirement is to be defined.

[2] The need-to-know principle applies to all information. It may be disclosed to authorised persons if this is necessary.

[3] "Confidential" and "strictly confidential" information must bear a classification mark. The information owners decide on the labelling of confidential research data. The classification notes (the labelling of classified information) must be written in capital letters.

[4] The standard classification according to confidentiality at ETH Zurich is "internal". Documents without a classification note are considered "internal". Published (released) information does not have to be labelled with a "public" classification.

[5] Information is classified according to confidentiality when it is created. It must be reviewed throughout the entire life cycle. Classification according to integrity and availability, on the other hand, is usually carried out on request (e.g. as part of IT projects).

[6] Annex 1a-c show the risk-oriented procedure for classifying information according to confidentiality and contain recommendations for classification according to confidentiality as well as examples of labelling (affixing the labelling notes). Annex 2 contains guidelines for the handling of information classified as confidential.

4. Section: Security measures

Article 10 Protection requirements

[1] "Public" information assets do not require confidentiality protection. However, they have at least a normal protection requirement in terms of integrity and/or availability.

[2] Information assets that are considered "internal" and that have normal integrity and normal availability have a normal protection requirement.

[3] Information assets that are considered "confidential" or have high integrity or high availability have a high protection requirement.

[4] Information that is considered "strictly confidential" requires a very high level of protection.

[5] The same applies to processes and IT resources[6] that process information assets with an analogous protection requirement to paragraphs 1 to 4.

Article 11 Basic protection and standardisation

[1] Basic protection offers sufficient protection for normal or high protection requirements.

[2] Information assets, processes and IT resources with very high protection requirements are protected against unauthorised access by more stringent means. This applies in particular also to physical access. Standardised security measures are implemented for this purpose. These packages of measures are defined by the CISO in consultation with the ISOs and the responsible IT operators.

[3] For information assets with very high protection requirements, the information owners shall select the appropriate security measures in accordance with paragraph 2 and ensure their implementation. The responsible ISO advises the information owners on the selection of measures. If the standardised measures cannot be used, alternative measures are taken in consultation with the ISO and the CISO.

[6] 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.

5. Section: Final provisions

Article 12 Responsibility for the instruction

This directive is periodically reviewed by the CISO.

Article 13 Entry into force

This directive enters into force on 01 January 2025.

Zurich, 1 January 2025

Johannes Hadodo
Chief Information Security Officer
ETH Zurich

Appendix 1a: Risk-orientated classification of information according to confidentiality

The recommended procedure for classifying the confidentiality of information according to risk is shown below. The procedure follows the risk management guidelines of ETH Zurich (see section 4.4). The ISO provides information.

Confidentiality is categorised along the following dimensions

- Financial impact [CHF];
- Personal injury;
- Damage to reputation;
- Impairment of business processes (e.g. teaching, research, administrative activities);
- Impact on the environment and additionally
- Impairment of personal rights.

The risk assessment is based on the "credible worst case" scenario and refers to the greatest impact/impairment:

- ETH as an institution
- one (or more) departments
- Individuals or groups of people (e.g. ETH members but also people outside ETH who have made data available to ETH, e.g. health data for research purposes)

In the following table, a "credible worst case" scenario is used to assess the confidentiality of the information. The colour code applies:

- Green: the information is to be classified as "internal"
- Yellow: the information is to be classified as "confidential"
- Red: the information is to be classified as "strictly confidential"

Dimensions	very low	low	moderate	essential	high	very high
Financial impact [CHF]	< 0.13 million	0.13 – 1.13 million	1.13 – 13.1 million	13.1 – 66 million	66 – 131 million	> 131 million
Personal injury	Minor injury	Minor injury, outpatient treatment	Medium injury, stationary treatment	Seriously injured	From 10 to 50 seriously injured or dead	More than 50 seriously injured or more than 10 dead
Impairment of reputation	Local media presence	National media presence Up to 1 week, not full coverage	National media presence Up to 1 week area-wide	National and partly international media presence Up to one year	National and international media campaign Up to several years	International media campaign lasting several years, lasting loss of trust with political consequences
Impairment of business processes	½ day failure of non-central functions	½ day failure of central functions	From ½ to 2 days failure of non-central functions	From ½ to 2 days failure of central functions	Longer-term loss of non-central functions	Longer-term loss of central functions
Effects on the environment	Localised environmental impact, no remediation costs	Regional impact on the environment, remediation time < 1 week, small remediation costs	National environmental impact, remediation time < 1 month, average remediation costs	National and in some cases international environmental impact, remediation time > 1 month, high remediation costs	National and international environmental impact, remediation time > 1 year, very high remediation costs	International environmental impact, remediation time > 10 years, immense remediation costs
Impairment of personal rights [above dimensions apply subsidiarily]	Non-sensitive personal data that does not have any particularly negative consequences for the data subject – provided that it is not published in a sensitive context.		Particularly sensitive personal data in accordance with Art. 5 of the Swiss Data Protection Act, which would violate the personal rights of individuals if they were disclosed or processed without authorisation. The misuse of such information could lead to significant negative effects on the economic and/or social status of a person.		Information that is subject to professional secrecy pursuant to Art. 321 or Art. 321bis of the Swiss Criminal Code or that would have a serious impact on a person's health and economic situation (life and limb) if disclosed or processed without authorisation.	

Appendix 1b: Classification recommendations according to confidentiality

The list below contains recommendations for the classification of selected information. These apply subject to a deviating (generally higher) classification by the information owners. Annex 1a in particular should also be taken into account for the classification. The ISO provides information.

Information / Information inventory (selection)	Classification
Web presence of ETH Zurich / Internet documents	**Public**
Press releases / Communications to the press	
Lists of lectures / Timetables for lectures	
Research data, primary and secondary data (published)	
Published dissertations	
Legal collection of ETH Zurich	
Circular mails	**Internal**
Calendar entries (depending on how the information owner handles them)	
Internal telephone book / address directory	
Newsletters/blogs	
Townhall meetings	
Lecture notes (unless made publicly available by the author)	
"Non-sensitive" personal data without any particular need for protection (personal data whose misuse generally has no particular consequences for the data subject, e.g. surname, first name, [company] address, date of birth, [ETH] telephone number or information that has appeared in the media, provided it is not in a sensitive context, see risk levels in the guidelines)	
Project documents: motions, reports, minutes	
Applications from the School Executive Board (“SL-Anträge”) / department incl. minutes; Conference and meeting documents (e.g. from professorial conferences)	**Confidential**
Strategy of ETH Zurich (at least during development)	
Medium-term planning, budgeting & financial planning, annual report in progress	
Financial/risk report	
Management reporting incl. key management figures	
Personal dossiers/documents: job applications, appraisals, employment contracts, staff appraisals, etc. (religious, political, trade union, health [e.g. medical certificates], social welfare, criminal and administrative prosecution and sanctions)	
Student performance assessments, grades, examination documents	
Contracts (co-operations, third-party companies, research, confidentiality)	
IT network plans	
Research data, primary and secondary data before publication	
Planned and ongoing research projects (incl. research projects with third parties, unless otherwise contractually agreed)	
Survey results	
Consultant and supplier contracts	
Export-controlled information assets (risk assessment in consultation with client / partner or export control recommended)	
Library borrowing data (recognisable interest or personality profile of the borrower)	
Personal research data that is not subject to the Human Research Act	
Wage data (risk assessment recommended)	

Auditors' report, audits	
Protocol, usage and traffic data for email, internet or intranet and telephony	
Teaching and learning platforms (student performance and behaviour data recognisable)	
Self-assessments	
Student administration, examination administration	
Process information	
Crisis team documents (alarm organisation, emergency scenarios, BCM, protocols)	
Particularly sensitive personal data and high-risk profiling in accordance with Art. 5 of the Data Protection Act and medical health data subject to the Human Research Act (risk assessment recommended, see in particular Annex 1a and the risk levels in the guidelines)	
Ongoing patent proceedings	
Professional, official and business secrets (risk assessment recommended)	
Intellectual property (IP such as technical inventions, programme code, etc., where there is an obligation of confidentiality) (risk assessment recommended)	
Passwords	
Passwords with very high protection requirements (e.g. administrator passwords)	**strictly confidential**
Information that is used directly to de-identify individuals (e.g. lists for coding or pseudonymisation of patient names and health data)	
Research data (if contractually agreed as strictly confidential, e.g. with cooperation partners, third parties)	
Internal reorganisation projects with staff reductions	
Patient and medical data subject to professional secrecy (cf. Art. 321* or Art. 321bis of the Swiss Criminal Code) or to the Human Research Act** (if indicated in Annex 1a) *Note: Art. 321 also applies to students who disclose a secret that they discover during their studies **if patient and medical data are not irreversibly anonymised in accordance with HRA Ordinance Art. 25	
Research results that could cause high/very high damage if disclosed prematurely (risk assessment recommended, see also Annex 1a)	
Information that is covered by manufacturing or trade secrets pursuant to Art. 162 StGB (risk assessment recommended)	
Company acquisitions and start-ups if premature disclosure could result in high/very high losses	
Highly sensitive personal data (risk assessment recommended: Personal data whose misuse may jeopardise the life of the person concerned; see risk levels in the guidelines)	

Appendix 1c: Recommendations for labelling (classification notes)

Classification notes must be written in capital letters. Information classified as "public" or "internal" does not have to be classified.

- *for Word documents*: Use of a cover sheet labelled "STRICTLY CONFIDENTIAL". The labelling for "CONFIDENTIAL" and "STRICTLY CONFIDENTIAL" is repeated on every (subsequent) page (in the header/footer). Compare also: Templates with classification note. The same applies to Excel sheets, graphics, etc. if applicable

- *Video/films*: "CONFIDENTIAL" or "STRICTLY CONFIDENTIAL" is displayed at the beginning of the video

- *Creating/using a database*: when logging in (initial screen), for example: This data is "CONFIDENTIAL" or "STRICTLY CONFIDENTIAL" (e.g. with ETHIS)

Appendix 2: Handling classified information (confidentiality)[1]

The handling of information varies depending on the level of confidentiality. If anything is unclear, the Information Security Officer will provide information. In the event of data loss, the responsible line manager and the CISO must be informed. In the event of theft, also contact the SHE department.

A. General specifications for classified information

Handling	public	internal	confidential	strictly confidential
Classification takes place	by information owners or on their behalf			
Change of classification	not applicable	is carried out by the information owners or the superordinate body		
Classification labelling	not necessary	not necessary	Mark as "confidential"* *optional for research data	Mark as "strictly confidential"
Allocation of read rights	no restriction	only to authorised persons (e.g. ETH members may in principle access all internal information, provided they have been authorised for access)	to verifiably authorised persons (e.g. authorised groups of persons)	to individually authorised persons, owner keeps list of authorised persons
Read rights check	not applicable	not applicable	as required	immediately when changing access rights or classification

[1] Version in accordance with the Executive Board resolution of 12 July 2021, in force since 1 August 2021.

B. Information on analogue readable media (e.g. paper, film, foil, tape)

Handling	public	internal	confidential	strictly confidential
Processing	no restriction	no restriction	no access by unauthorised persons	no access by unauthorised persons
Filing/storage	no restriction	clean desk	clean desk, keep under lock and key	clean desk, in safe if possible
Internal ETH transfer	no restriction	only to authorised persons	to verifiably authorised persons (e.g. authorised groups of persons)	to individually authorised persons, in a locked container, confirmation of receipt, to be authorised by the owner, non-disclosure agreement
Use with third parties	no restriction	only to authorised persons, non-disclosure agreement* *facultative for research data	to verifiably authorised persons (e.g. authorised groups of persons), non-disclosure agreement** *facultative for research data	to individually authorised persons, in a locked container, confirmation of receipt, to be authorised by the owner, non-disclosure agreement
Erroneous receipt	inform sender	inform sender	inform sender, keep under lock and key, return or destroy according to the sender's instructions	inform sender, keep under lock and key, return or destroy according to the sender's instructions
Erroneous dispatch	inform recipient	inform recipient request destruction or return	inform information owners proceed according to the instructions of the information owner inform recipient	Inform information owners proceed according to the instructions of the information owner report incident to CISO or legal service
Take on business trips	allowed	allowed	Avoid if possible, be careful on public transport!	to be authorised by the owner, be careful on public transport!

Take to home office	allowed	allowed	Avoid if possible, be careful on public transport!	to be authorised by the owner, be careful on public transport!
Disposal / Destruction (office)	Waste paper/waste	class 1 document shredder[1]	class 3 document shredder[2], for destruction by third parties: written confirmation	class 3 document shredder[3], for destruction by third parties: written confirmation

C. Information on removable digitally readable data carriers[4]

Handling	public	internal	confidential	strictly confidential
Filing/storage	no restriction	clean desk	clean desk, keep under lock and key	clean desk, in safe if possible
Dispatch / reception	no restriction	ETH internal: only to authorised persons ETH-external: Only to authorised persons non-disclosure agreement* *facultative for research data	ETH internal: to verifiably authorised persons, encrypted data carrier locked container ETH-external: to verifiably authorised persons, encrypted data carrier locked container, non-disclosure agreement* *facultative for research data	Recommendation: do without medium if possible. If necessary, then: ETH internal: to individually authorised persons, encrypted data carrier in a locked container, confirmation of receipt, to be authorised by the owner, non-disclosure agreement ETH-external: like ETH-internal
Erroneous receipt	same as information on similar readable media			
Erroneous despatch	same as information on similar readable media			
Take on business trips	same as information on similar readable media			
Take to home office	same as information on similar readable media			

[1] according to standard DIN 66399

[2] according to standard DIN 66399

[3] according to standard DIN 66399

[4] e.g. punch cards, memory cards and (USB) sticks, external hard drives/SSDs or removable hard drives, CD/DVD, floppy discs that can be removed from the writing or reading device without major time expenditure

Disposal / destruction (office)	Waste/electrical scrap (environmentally friendly)	Class 1 document shredder[1] or formatting	Class 3 document shredder[2] or destroy, as long as destruction is carried out by third party: written confirmation

D. Electronically readable information (mobile and stationary IT resources)

Handling	public	internal	confidential	strictly confidential
Editing on screen	no restriction	no restriction	no access by unauthorised persons	no access by unauthorised persons
Storage on ETH file server	no restriction	no restriction	group drive with correspondingly restricted access authorisation	group drive with restricted access authorisation, very high protection requirements apply, e.g. encryption (see IT guidelines and IT basic protection specifications)
Access to ETH data using private IT systems (e.g. via PC, smartphone)	allowed	use ETH infrastructure where possible* *where the use of ETH infrastructure is not possible: ETH passwords may be entered for access to ETH accounts via private IT systems		not allowed
		allowed	access only via VPN	
access via publicly accessible IT systems (e.g. Internet café)	allowed	not allowed	not allowed	not allowed
Internal ETH transfer	no restriction	only to authorised persons	to verifiably authorised persons (e.g. authorised groups of persons)	to individually authorised persons, encryption, confirmation of receipt, to be authorised by the owner, non-disclosure agreement

[1] according to standard DIN 66399

[2] according to standard DIN 66399

Use with third parties	no restriction	only to authorised persons, non-disclosure agreement* *facultative for research data	to verifiably authorised persons (e.g. authorised groups of persons), non-disclosure agreement** *facultative for research data	to individually authorised persons, encryption, confirmation of receipt, to be authorised by the owner, non-disclosure agreement
Erroneous receipt (e.g. email)	inform sender	inform sender	inform sender, no forwarding, if possible, delete according to the sender's instructions	inform sender, no forwarding,, if possible, delete according to the sender's instructions
Erroneous dispatch (e.g. email)	contact recipient	inform recipient request deletion	inform information owners proceed according to the instructions of the information owner inform recipient	inform information owners proceed according to the instructions of the information owner report incident to CISO or legal service
ETH external reuse/sale/donation PC[1]	no restriction	reset PC		overwrite/"wipe" PC-internal data carrier[2] and set up again

[1] Personal Computer

[2] A procedure that only marks the memory cells as deleted is not permitted.

E. Electronic information in cloud services (additional "cloud"-specific requirements)

<table>
<tr><th>Handling</th><th>public</th><th colspan="2">internal</th><th>confidential</th><th>strictly confidential</th></tr>
<tr><td>Personal data in accordance with the Data Protection Act (excluding medical data in accordance with the Human Research Act)</td><td>no restriction</td><td colspan="3">possible in compliance with the Data Protection Act (DSG) and, in particular, compliance with the FDPIC's guidelines/explanations on cloud computing:
• data processing only within the meaning of Art. 9 FADP
• cloud provider fulfils data security according to Art. 8 DSG and 1 ff. GDPR
• disclosure of data abroad only if Art. 16 et seq. FADP (see also statement, explanations and explanatory notes as well as list of countries FDPIC and model contract for data transfer abroad [SCC])
• only if the right to information pursuant to Art. 25 FADP and the right to erasure and rectification pursuant to Art. 41 para. 2 FADP are guaranteed
• list of processing activities Art. 12 FADP
risk assessment necessary*</td><td>not permitted</td></tr>
<tr><td>Research data according to the rules of export control</td><td>not applicable</td><td colspan="4">If research data is subject to export control regulations and is also destined for abroad, official authorisation is mandatory for uploading to a cloud. Authorisation is granted by SECO (via the Export Control Office of ETH Zurich).
The same applies to data/information that is uploaded to clouds whose server is in Switzerland, but the data/information is made accessible to recipients abroad (deemed export).</td></tr>
<tr><td>Factual data</td><td>no restriction</td><td colspan="3">permitted with risk assessment* (by information owners), appropriate organisational and any necessary technical protective measures, taking into account existing legislation (e.g. export control), contractual agreements and the rights of third parties (e.g. personal rights or copyrights)</td><td>not permitted</td></tr>
<tr><td rowspan="2">Labelling of the data</td><td rowspan="2">No</td><td>mark as "internal"**
facultative</td><td colspan="2">mark as "confidential "
**facultative for research data</td><td rowspan="2">not applicable</td></tr>
<tr><td colspan="3">specification of the cloud services for which the respective information is intended**
**facultative for research data</td></tr>
</table>

Use of external cloud services (e.g. backup service)	Permitted, provided that the service has been released and a declaration of consent from the information owner(s)* is available.	not allowed

*supporting material (template) is available from the CISO