IT Guidelines and IT Baseline Protection Rules of ETH Zurich

of 01 January 2025

The Vice President for Infrastructure and Sustainability of ETH Zurich and the Chief Information Security Officer of ETH Zurich

based on Art. 13, para. 3 (g) of the “ETH Zurich Organisation Ordinance”[1] and on Art. 6 para. 4 (d and f) of the directive "Information Security at ETH Zurich"[2]

hereby decree:

Section 1: General provisions

Article 1 Subject matter

[1] This directive governs:

- tasks, competences and responsibilities of central roles in ICT operations
- the basic protection rules for and the handling of IT resources

[2] The purpose of this directive is to ensure that a responsible person is identified and can be contacted for all IT resources and that known weaknesses are eliminated in a timely manner. It also regulates the use of external IT services. External IT services are IT services purchased by ETH Zurich that are provided by an external company outside the ETH Zurich network (e.g. outsourcing, external cloud service).

[3] 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.

Article 2 Applicability

[1] This directive is intended for system and network zone administrators and service intermediaries at ETH Zurich in accordance with Section 2 of this directive.

Section 2: Rollers

Article 3 Network zone managers

[1] Network zone managers are responsible for the security of their zones and the associated processes.

[1] RSETHZ 201.021
[2] RSETHZ 203.25

[2] The tasks are:

a. participation in the training offered by IT Services for network zone managers;

b. documentation of the purposes of the network zones assigned to them;

c. initial assessment of exception requests for IT resources in their network zone, as well as forwarding the requests supported by him/her to the Chief Information Security Officer (CISO) and

d. knowledge of the system owners for all IT resources in their zones.

[3] The competences are:

a. defining the purposes of the network zones assigned to them. The purpose of a network zone must correspond to the type of network zone requested from IT Services (e.g. DMZ, IoT, BYOD);

b. deciding which IT resources are allowed to connect to their zones, whereby the framework condition should correspond to the type of network zone;

c. deciding on change requests regarding the configurations of their zone firewalls in accordance with Art. 7, para. 5 of this directive;

d. rejection of exception requests relating to IT resources in network zones under its responsibility in accordance with Art. 11 of this directive and

e. applying for exceptions regarding compliance with the IT Guidelines and IT Baseline Protection Rules.

[4] The organisational units may delegate their tasks relating to network zones (including any zone firewalls) to ETH Zurich's internal service providers. The prerequisite for this is the conclusion of a written Service Level Agreement (SLA), taking into account the applicable provisions of this directive. In the event of delegation, the organisational units remain responsible for placing the order and monitoring SLA compliance.

[5] The organisational units report the network zone managers to IT Services. If a zone is protected by a firewall, at least one and no more than three deputies must be registered in addition to the network zone manager.

Article 4 System owners

[1] System owners are responsible for system and system security maintenance and the associated processes within the framework of the applicable provisions of this directive.

[2] The competences are to apply for exceptions in accordance with Art. 11 of this directive.

[3] For IT resources owned by ETH Zurich, the organisational units may delegate their tasks relating to systems to ETH Zurich's internal service providers. In the event of delegation, the organisational units remain responsible for placing the order and monitoring its fulfilment.

[4] For IT resources not owned by ETH Zurich in the ETH Zurich network, such as private IT systems of students (BYOD) or IT systems of third parties such as the order-related use of laptops or

smartphones of external service providers, the registered user is deemed to be the system owner if no system owner is registered.

[5] The organisational units shall report the system administrators and their deputies appointed by them to IT Services (exception: BYOD).

Article 5 Service intermediaries

[1] Service intermediaries may be IT operators and technical/administrative employees of the departments and the central bodies, as well as academic staff in research and teaching, including professors, lecturers and external lecturers at ETH Zurich[3].

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

[3] Service-providing agents procure external IT services (e.g. cloud services, outsourcing) and make them available to ETH Domain members. In this context, they are responsible for contract management with the external provider, in particular in conjunction with responsibility for the technical connection of the service and user life cycle management. This includes:

a. agreeing on the applicable requirements of this directive and monitoring compliance with them; and

b. release of the external service for use within ETH in accordance with the intended purpose (drafting of the terms of use).

[4] The tasks are:

a. monitoring compliance with the contract components and, if necessary, requesting necessary improvements from service providers;

b. if necessary, defining and implementing additional technical or organisational measures to secure the external IT service, e.g. backup, logging, reporting;

c. provision of documentation for users. This explains the intended use and the applicable terms of use, such as the release or prohibition of the processing of confidential information with the external IT service;

d. periodically checking whether and how ETH Zurich data can be migrated to ETH Zurich IT services in the event that the external IT service ceases to be used, and

e. ensuring that ETH Zurich data can be migrated to ETH Zurich IT services when the external IT service ceases to be used.

[3] e.g. professors, department coordinators, heads of department

[5] The competences are:

a. deciding on the purpose of the external IT service and the terms of use applicable to members of ETH Zurich.

b. applying for exceptions in the event of non-compliance with the requirements of this directive in accordance with Art. 11.

[6] The service intermediaries notify the Chief Information Security Officer (CISO) of the external IT service, its purpose and conditions of use. The CISO is responsible for information security.

[7] Users who obtain an external IT service exclusively for themselves are not deemed to be service intermediaries. Members of ETH Zurich pursuant to Art. 13 of the ETH Law (namely employees and students) and guests pursuant to the Guest Regulations are deemed to be users.

Article 6 Availability

System owners, network zone managers, service intermediaries and their deputies must respond to reports and enquiries regarding possible IT security incidents within one working day.

Section 3: IT Baseline Protection Rules

Article 7 Guidelines for network zone managers

[1] If possible, IT resources should only be placed or connected in those zones of the ETH Zurich network that have similar protection requirements and purposes.

[2] If a zone contains IT resources for which the requirements of this directive are not met for more than 20 days, the zone must be isolated in such a way that any vulnerabilities cannot be exploited from outside the zone. Alternatively, the affected systems can be moved to an already isolated zone.

[3] The network zone managers know the responsible system owners in their network zone for all IP addresses/IT resources or can find them out promptly.

[4] The use of IP addresses must be checked regularly (DHCP snooping). Unused IP addresses must be returned to IT Services.

[5] Firewalls must be configured so that all services are closed by default, and only services that are really needed are open ("whitelist"). IT Services will only open ports and/or protocols with the authorisation of the person responsible for the network zone. The network zone administrator also assesses firewall rules against the background of the stability and vulnerability of the network and the protection requirements of the data.

[6] Activations, changes and deactivations of firewall rules must be traceable. For each firewall rule, the applicant, the executor, the purpose/functionality and the time must be documented.

[7] Firewall rules must be reviewed and updated at least once a year. Rules that are no longer required must be removed.

[8] Firewall logs must be periodically checked for irregularities by the network zone administrators.

[9] Users and IT systems must authenticate or authorise themselves via Network Access Control (NAC) technologies in order to be connected to a zone. The list of authorised users and IT systems (certificates, MAC addresses) is checked regularly. Authentication and authorisation logs are periodically checked for irregularities by the network zone administrators (RADIUS).

[10] Every IT system must have an entry in the IT Services Domain Name System (DNS). The DNS configurations of a zone must be checked and updated regularly.

[11] Network connections must be protected against unauthorised access using NAC technologies. Network connections that are not protected with NAC may only be located in closed rooms to which only authorised persons have access (exception e.g. lecture halls or similar).

Article 8 Specifications for system owners

[1] Keeping software up to date

a. Firmware, operating systems, applications, apps, etc. must be used in the latest versions supported by the manufacturer and must be kept up to date with the latest security updates.

b. Security updates must be tested as soon as they are released and distributed as quickly as possible. Updates must be distributed to the target systems no later than ten calendar days after their release date, unless operational problems and risks prevail.

c. Updates and any restart of the target systems must be carried out no later than two working days after distribution unless operational problems and risks override this.

d. In the event of an emergency, the CISO or the responsible IT operator can order the immediate distribution and installation of security updates.

[2] Protection against malware

a. Where available and useful, IT resources must be operated with malware scanners.

b. The protection programmes must be up to date with regard to software version, updates and protection signatures and must be configured so that files are automatically checked on access.

c. During the runtime of an IT system, updates must be checked for and installed automatically – if possible, at least every hour.

[3] Storage media on desktops and mobile devices such as laptops, tablets and smartphones must be fully encrypted where possible.

[4] A screen lock must be activated on the IT equipment after 10 minutes of inactivity at the latest (exceptions e.g. through adequate access protection). This can only be unlocked by entering a password, PIN, fingerprint or similar authentication methods.

[5] Access control

a. Access to privileged accounts, such as "admin" or "root", or to groups with administration privileges, such as "administrators" or "sudoers", must be restricted to as few people as possible who are authorised for the respective role (need-to-know principle).

b. Accounts for system administration must be restricted to the necessary minimum (least privilege) and checked regularly.

c. Access to confidential or strictly confidential databases or to IT resources with high or very high protection requirements in terms of integrity or availability may only be made available to verifiable or individually authorised persons. Access rights are also checked regularly.

d. Shared accounts are only permitted if they are absolutely necessary. Access may only be made available to authorised persons. Access authorisations must be checked regularly.

e. Unused, preconfigured user accounts (e.g. "guest") must be deleted. If this is not possible, they must be deactivated or blocked for login. The preset password must be changed.

[6] The password and PIN rules of ETH Zurich must be configured, if technically possible, e.g. in the IAM, in Active Directory or on the local media.

[7] Data backup

a. Data backup must be regulated as part of the contract or otherwise documented.

b. The recoverability of backups must be checked periodically on a random basis.

[8] Remote access means access to IT resources from outside the ETH Zurich data network. The following applies:

a. Remote access may only be carried out using encryption protocols that are currently considered secure.

b. When using Virtual Private Network (VPN) as an access technology, access must terminate on the VPN endpoint of IT Services.

c. Alternative remote access methods to VPN (such as "jump hosts", SCION, protocol tunnelling, proxy technologies) must be protected and monitored.

d. Systems that access ETH Zurich IT resources via remote access shall comply with the provisions of this directive.

[9] Unauthorised persons must not have access to IT resources. Unauthorised persons are persons who do not need to enter the relevant premises in order to perform their duties at ETH Zurich. The necessary safety measures must be adapted to the spatial conditions. The physical security requirements applicable to the respective organisational unit apply.

Article 9 Specifications for service intermediaries

The following requirements apply to external IT services if they are relevant in the respective context.

[1] Contracts with such service providers or the GTC of ETH Zurich regulate in particular:

a. For reasons of legal enforceability, the following preference applies with regard to place of jurisdiction and applicable law: 1. Switzerland, 2. EU, 3. other.

b. Personal data is processed and stored in Switzerland or the EU. If the level of data protection in the country of storage/processing is inadequate (see the Federal Data Protection Commissioner's list of countries), personal data must be protected by agreeing standard contractual clauses (SCC) or comparable contractual measures.

c. Service providers confirm that they comply with the laws and regulations relevant to ETH Zurich in the context of the application, e.g. the General Data Protection Regulation (GDPR) of the European Union[4].

d. All responsibilities are clearly assigned to one party.

e. External service providers undertake to carry out regular independent audits of IT security and provide audit reports or certification documents or grant ETH Zurich the right to audit.

f. Mutual contact persons, guaranteed response times and communication channels are defined.

g. ETH Zurich data must be (logically) separated from the data of other customers and the administrative area of the service providers.

h. In the event of cancellation of the external service, the contract must regulate the takeover of the data and the usage logs (log data) by ETH. In addition, the irretrievable deletion of this data on the part of the service provider is agreed.

[2] *Internal* data may be released for processing if the following conditions are met:

a. Users and administrators of ETH Zurich and the external service providers work with personal user accounts and authenticate themselves with at least one factor (e.g. password).

b. Data is encrypted during transport and storage, in each case using methods that are considered secure according to the current state of the art.

c. The activities of ETH Zurich users and administrators are traceable. The log data must be available for at least one year and will be irretrievably deleted after two years at the latest.

d. An interface is available for ETH Zurich to transfer log data ("near realtime") on the activities of ETH Zurich users and administrators. If this is not possible or does not make sense in the respective context, the responsible departments of ETH Zurich should be able to access this information in another way, e.g. via corresponding programme interfaces (APIs) or online management functions (dashboards) of the service.

e. Activities of the service providers in which ETH Zurich data is accessed must be recorded by the service providers and retained for at least two years.

f. The availability of ETH Zurich data must be ensured in accordance with ETH Zurich's requirements. This is preferably ensured by a regular backup of all data, the functionality of which is checked periodically.

[4] General Data Protection Regulation (GDPR) of the European Union: EUR-Lex - 32016R0679 - EN - EUR-Lex (europa.eu) (accessed 1 July 2022)

g. The availability of ETH Zurich data must also be ensured for extraordinary events (illness, death, etc.). The service intermediary or an IT administrator and their deputies should be able to access the data if necessary.

h. It must be possible to transfer ETH Zurich data back to ETH Zurich IT services if required.

[3] *Confidential* data may be released for processing if the conditions for processing internal data and the following requirements are met. Information is deemed to be confidential if unauthorised persons could gain knowledge of it and significantly impair the interests of ETH Zurich:

a. Administrators of external service providers who access ETH Zurich data and services use secure authentication methods such as multi-factor authentication or FIDO2.

b. Users and administrators of ETH Zurich authenticate themselves with multi-factor authentication.

c. The providers of the service use keys for encrypted storage exclusive for ETH Zurich. Other keys are used for data from other customers.

d. User accounts and access rights are managed centrally by ETH Zurich. A connection to the identity management and federation services operated by IT services (e.g. ADFS, DirX) must be implemented where possible and appropriate.

e. It must be possible to assign granular access rights to individual databases for users or groups of users (e.g. create, read, modify, delete).

[4] Release for the storage or processing of *strictly confidential* data is not permitted. Information is considered to be strictly confidential if knowledge of it by unauthorised persons could seriously harm the interests of ETH Zurich.

[5] Keeping software up to date

a. If applicable in the respective context, it must be checked selectively whether the service provider installs security updates within the agreed deadlines. Violations of the contract components must be addressed with the service providers and warnings issued in the event of recurrence.

b. If the responsibility for importing security updates lies with ETH Zurich, the procedure described in Art. 8, para. 1 and para. 2 of this directive must be followed.

[6] In addition, Art. 10 applies.

Article 10 Principles for the provision and use of external cloud services

[1] IT Services and the IT Services Groups provide a selection of external cloud services that cover the majority of ETH members' needs. The following applies to service intermediaries for the provision and release of external cloud services beyond this:

a. In addition to IT Services (e.g. professors, department coordinators, heads of department and other IT operators such as the IT Services Groups in the departments), service providers are permitted to provide additional cloud services as required and to release them for internal ETH use.

b. Prior written assessment of the degree of fulfilment of the requirements of this directive is required for the approval of external cloud services (self-assessment).

c. The CISO maintains a central register of external cloud services (reporting obligation)[5].

d. Service intermediaries must obtain temporary exemption authorisations from the CISO for the provision and release of external cloud services that cannot comply with the requirements.

[2] For the outsourcing (storage and processing) of information assets in external cloud services, the following applies to information owners:

a. The use of external cloud services is the responsibility of the information owner[6] or by users acting on behalf of the information owner.

b. The outsourcing (storage and processing) of confidential information using external cloud services is permitted, provided

- the cloud service fulfils the requirements for storing and processing public, internal or confidential data, in particular Art. 9 and Art. 10 para. 1 (b) and
- the information is suitable for outsourcing to the intended cloud service. A self-assessment is available to assess the suitability of the information. The outsourcing of strictly confidential information remains prohibited.

c. The information owners can obtain a second opinion from the CISO regarding the information to be outsourced.

Section 4: Exceptions / Compliance

Article 11 Exceptions to the aforementioned requirements

[1] For external IT services for which the requirements of this directive cannot be complied with, an exceptional authorisation must be obtained from the CISO.

[2] The Director of IT Services and the CISO may decide that an external IT service may not be used or must be discontinued if it persistently violates legal, contractual or internal requirements of ETH Zurich.

[3] The following applies to IT resources in the ETH Zurich network for which the provisions of this Directive applicable in the respective context cannot be complied with:

a. Non-compliant IT resources must be placed in isolated zones of the ETH Zurich network. Any weak points must not be exploitable from outside the isolated zones.

[5] Register of external cloud services: https://ethz.ch/staffnet/en/service/information-security/usage-external-cloud-services/list-external-cloud.html
[6] Information owners are responsible for the information assets that are collected and processed by them or on their behalf. Source: Directive "Information Security at ETH Zurich", RSETHZ 203.25

b. An exemption permit must be obtained for IT resources that do not have to be operated in an isolated zone, even though the requirements are not met for more than 10 working days.

[4] The IT Services carry out the exception process on behalf of the CISO.

[5] Exceptional authorisations are limited in time. Upon expiry, the applicant may review a new application.

Section 5: Final provisions

Article 12 Responsibility for the instruction

This directive is reviewed annually and put into effect by the Vice President for Infrastructure and Sustainability of ETH Zurich and the Chief Information Security Officer of ETH Zurich.

Article 13 Cancellation of previous law

The following decrees are cancelled:

1. Previous versions of the IT Guidelines and IT Baseline Protection Rules (RSETHZ 203.23)

Article 14 Transitional provision

None

Article 15 Entry into force

This directive enters into force on 01 January 2025.

Zurich, 01 January 2025

Prof. Dr Ulrich A. Weidmann Vice President for Infrastructure and SustainabilityETH Zurich

Johannes Hadodo
Chief Information Security Officer
ETH Zurich