Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

IT Services

ETH Zurich
Anja Harder
IT Security Officer IT Services
OCT G19
Binzmühlestrasse 130
8050 Zurich

+41 44 632 82 29

anja.harder@id.ethz.ch
www.id.ethz.ch

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

IT Guidelines and IT Baseline Protection Rules of ETH Zurich

Edition 2022

Contents

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

based on Art. 11b of the «Organisational Ordinance»[1], as well as Art. 4, Para. 1c of the «ETH Zurich Acceptable Use Policy for Information and Communications Technology» (BOT) [2]and Art. 5, Para. 5a of the «Directive on Information Security at ETH Zurich»[3]

issue the following directive*:*

General provisions

Article 1 Subject matter

These policies and guidelines regulate:

- Tasks, competences, and responsibilities of central roles in ICT[4] operations, and
- the baseline protection of ICT resources, and
- the use of ICT resources

They aim to ensure that a responsible person is identified and can be reached for all ICT resources and that known vulnerabilities are addressed in a timely manner.

Article 2 Scope and binding force

These guidelines are binding for the ICT resources and data of ETH Zurich.

[1] RSETHZ 201.021
[2] RSETHZ 203.21 (BOT)
[3] RSETHZ 203.25
[4] ICT: Information and communications technology

Article 3 Terms

[1]*Defined elsewhere:*

Term	Reference	Definition
User	BOT, art. 2, paragraph. 4	The term “users” includes all members of ETH Zurich (Art. 13 of the ETH Act) and third parties who are authorised to use the ICT resources of ETH Zurich (e.g. guests, congress participants, affiliated organisations, library users at the public work stations, employees of ETH Zurich’s spin-off companies or of other companies, provided a contractual arrangement exists to this effect, professors emeriti and retired employees).
Chief Information Security Officer (CISO)	BOT, art. 2, para. 12 and Directive «Information Security at ETH Zurich», art. 5	The Chief Information Security Officer (CISO) is the person who, in accordance with Art. 5 of the Directive on Information Security at ETH Zurich, is responsible for safeguarding IT security across the university. For this purpose, he/she shall work together with the units in accordance with Arts. 6- 11 of the Directive on Information Security at ETH Zurich.
Cloud computing	ISO/IEC 17788:2014, Information technology - Cloud computing - Overview and vocabulary, paragraph 3.2.5.	Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand. NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.
Cloud service	ISO/IEC 17788:2014, Information technology - Cloud computing - Overview and vocabulary, paragraph 3.2.8	One or more capabilities offered via cloud computing invoked using a defined interface.
Cloud service provider	ISO/IEC 17788:2014, Information technology - Cloud computing - Overview and vocabulary, paragraph. 3.2.15	Party which makes cloud services available.
IT operators	Directive «Information Security at ETH Zurich», art. 3	IT services and infrastructure operators for ETH Zurich include IT Services, the CSCS and IT Support Groups (ISGs) in the academic departments.

Term	Reference	Definition
IT Security Officer Information Technology - Services (ITSO ITS)	Directive «Information Security at ETH Zurich», art. 8, paragraph 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.
ICT resources	BOT, art. 2, paragraph 1	The term “ICT resources” comprises all information and telecommunication resources owned by ETH Zurich or used on behalf of ETH Zurich. In particular, it refers to systems, devices and services of ETH Zurich used for electronic data processing (e.g. data processing equipment, network components, data storage devices, printers, scanners, telecommunication networks and related software, locking systems or services outsourced by ETH Zurich, such as cloud solutions). The definition also includes non-ETH-Zurich-owned systems (e.g. private laptops) connected to the data network of ETH Zurich. It does not include video surveillance in accordance with the Swiss Federal Institutes of Technology Act (ETH Act).
Client (en: tenant)	ISO/IEC 17788:2014, Information technology - Cloud computing - Overview and vocabulary, paragraph 3.2.37	One or more cloud service users sharing access to a set of physical and virtual resources.
Confidential	Directive «Information Security at ETH Zurich», art. 22, paragraph 1	Information, if accessed by unauthorized persons, may significantly affect the interests of ETH Zürich.
Organisational - units	BOT, art. 2, paragraph 6	The term “organisational units” refers to the central or decentralised bodies of ETH Zurich established by the Executive Board pursuant to the ETH Zurich Organisation Ordinance (OV) of 16 December 2003 (e.g. academic departments, institutes, administrative departments, staff units, independent chairs) and the education and research facilities outside the academic departments established pursuant to Art. 61 OV.

Term	Reference	Definition
Service intermediaries, system-, and network zone administrators	BOT, art. 2, paragraph 11	The terms “service intermediaries” and “system and network zone administrators” refer to the specialists described in the “IT-IT Guidelines and IT Baseline Protection Rules of ETH Zurich” and in Art. 6 of this decree.
Strictly confidential	Directive «Information Security at ETH Zurich», art. 22, paragraph 1	Information, if accessed by unauthorized persons, may seriously affect the interests of ETH Zürich.

[2] *External ICT service*:

ICT service purchased by ETH Zurich that is provided outside the ETH Zurich network by an external company (e.g. cloud service).

[3] Remote access:

Access to ICT resources from outside the ETH Zurich data network (remote access).

Roles

Article 4 Network zone administrators

[1] Responsibilities

In addition to the rules laid down in the BOT, they are responsible for the security of their zones and the associated processes, in particular for compliance with the IT Guidelines and IT Baseline Protection Rules of ETH Zurich, applicable in the respective context.

[2] Tasks

a) Participation in IT Services' training for network zone administrators.

b) Documentation of the intended purposes of the network zones assigned to them.

c) Knowledge and implementation of the applicable IT Guidelines and IT Baseline Protection Rules of ETH Zurich.

d) Initial assessment of exception requests for ICT resources in his/her network zone, as well as forwarding the requests he/she supports to the IT Security Officer of IT Services.

e) Network zone administrators must be able to name or promptly find out the system owners for each IT system in their zones.

[3] Competences

a) Determine the intended use of their network zones. The intended use of a network zone must correspond to the type of network zone requested from IT Services (e.g. DMZ, IoT, BYOD).

b) Deciding which ICT resources are allowed to connect to their zones, in accordance with the type of the respective network zone.

c) Deciding on changes regarding the configurations of their zone firewalls in accordance with art. 9, para. 5 of this ordinance.

d) Rejection of exception requests[5], which relate to ICT resources in their network zones.

e) Request exceptions regarding compliance with IT Guidelines and IT Baseline Protection Rules of ETH Zurich.

[4] Appointment

The organisations take network zone responsibility, including responsibility for zone firewalls, themselves or delegate it to ETH Zurich-internal service providers. The prerequisite for this is a written service level agreement (SLA) in which the services to be provided as well as the IT Baseline Protection Rules to be implemented are regulated. In the case of delegation, the organisational units remain responsible in particular for placing orders and monitoring compliance with the SLA[6].

[5] The general conditions for exceptions are set out in Art. 12.
[6] Accountable in the sense of the RACI notation

[5] Registration

a) The organisational units shall register the network zone administrators with IT Services.

b) If a zone is protected by a firewall, at least one, maximum three deputies must be registered in addition to the network zone administrator.

Article 5 System administrators

[1] Responsibilities

In addition to the rules laid down in the BOT, they are responsible for system maintenance and in particular for compliance with the IT Guidelines and IT Baseline Protection Rules of ETH Zurich, applicable in the respective context.

[2] Tasks

a) Maintenance of system and system security

b) Implementation of the applicable «IT Guidelines and IT Baseline Protection Rules».

[3] Competences

Request exceptions[7] regarding compliance with «IT Guidelines and IT Baseline Protection Rules».

[4] Appointment

a) ICT resources owned by ETH Zurich:

The organisational units take system responsibility themselves or delegate it to a service provider[8]. A prerequisite for delegation is a written service level agreement (SLA), in which the services to be provided as well as the IT Baseline Protection Rules to be implemented are regulated. In the case of a delegation of system responsibility, the organisational units remain responsible in particular for placing orders and monitoring compliance with the SLA.[9]

b) Non ETH Zurich-owned ICT resources in ETH Zurich's network:

In the case of non ETH Zurich IT systems in ETH Zurich's network, such as private IT systems of students or IT systems of third parties, the rlogged-in user is deemed to be the system administrator, if no system administrator is officially registered[10] [11].

[7] General conditions for exceptions are set out in art. 12.
[8] e.g., IT Services
[9] Accountable in the sense of RACI notation
[10] BOT, art. 6, para. 6
[11] Examples of third-party systems are: Laptop or smartphone of a consulting firm. As part of its contractual relationship with ETH Zurich, the company has responsibility for the system

[5] Registration

a) The organisational units shall register the system administrators they have appointed and their deputies with IT Services.

b) If a system administrator is not registerd with IT Services, this information is derived from the available information (such as logs or system states) if possible.

Article 6 Service intermediary

[1] Description

Service intermediaries procure external IT services (e.g. cloud services) and make these services available to members of ETH Zurich. Service intermediaries may be IT operators or technical-administrative or scientific employees of the departments and central bodies of ETH Zürich (e.g. professors, department coordinators, heads of department). Users who obtain an external ICT service exclusively for themselves are not considered service intermediaries.

[2] Responsibilities

Service intermediaries are responsible within ETH Zurich for matters relating to the use and management of one or more external ICT services used by members of ETH Zurich on behalf of ETH Zurich (cloud services, etc.). In particular, they are responsible for contract management, agreeing on the relevant IT Guidelines and IT Baseline Protection Rules in the respective context, monitoring compliance with these rules, and approving the service for specific purposes of use.

[3] Tasks

a) Conduct a risk assessment to evaluate the suitability of the external ICT service for its intended use.

b) Ensure that the IT Guidelines and IT Baseline Protection Rules can be implemented. Contract-relevant specifications should be bindingly agreed with the service provider.

c) Ensure that ETH Zurich is informed or consulted about changes, malfunctions, or incidents and that the relevant information is passed on to the affected users.

d) Consultation with the IT Security Center of IT Services regarding the necessity of security monitoring of the external ICT service. If necessary, prompt delivery of the required unchanged log data to the IT Security Center.

e) Monitoring compliance with the service level agreement and, if necessary, requesting necessary improvements from the service provider.

f) If necessary, define and implement supplementary technical or organisational measures to secure the external ICT service.[12]

[12] e.g., backup, logging, reporting.

g) Provide documentation for users, which explains the purpose and scope of use of the service, the applicable terms of use, such as the release or prohibition of processing confidential information with the external ICT service.

h) Periodically check whether ETH Zurich's data can be migrated to ETH Zurich ICT services in the event of a possible end of use of the external ICT service.

i) Ensure ETH Zurich's data can be migrated to ETH Zurich ICT services, when the external ICT service is no longer used.

[4] Competences

a) Decision on the purpose and scope of use of the external ICT service and the terms of use applicable to members of ETH Zurich.

b) Request exceptions[13] regarding compliance with IT Guidelines and IT Baseline Protection Rules.

[5] Appointment

The organisational units that commission the use of cloud solutions or other external ICT services appoint one or more ETH-internal persons responsible for this purpose. Preferably, the role of «service intermediary» for external ICT services is centralised at department, institute, or division level.

[6] Delegation of tasks

Tasks of a service intermediary can be delegated, the responsibility remains with the person in charge.

[7] Registration

The organisational units shall notify IT Services of the external ICT service, its purpose, scope of use, the service intermediaries, and their deputies.

Article 7 Accessibility of responsible persons

System administrators, network zone administrators, service intermediaries, and their deputies must be reachable via e-mail addresses specified by IT Services and must respond to messages and enquiries regarding possible IT security incidents within one working day.

[13] General conditions for exceptions are set out in Art. 12.

IT Baseline Protection

Article 8 IT baseline protection rules for users

[1] Principle of the use of internal and external ICT services of ETH Zurich

a) In principle, ETH-internal or external ICT services offered or approved[14] by the IT operators of ETH Zurich or the persons responsible for IT at the institutes and professorships, are to be used for data processing and storage. The terms of use for the respective services must be met.

b) For exceptions to this principle, e.g., if ETH Zurich data is to be processed or stored on collaboration platforms or storage services of external cooperation partners[15] or third parties, the approval of the responsible line, research or project management of ETH Zurich must be obtained in advance. Control (e.g., access, protection level) over such data must be always be guaranteed for ETH Zurich and must be regulated in a binding manner. This also applies to cases in which users cannot access the data for a longer period due to extraordinary events (illness, death, etc.).

c) Use of external ICT services during day-to-day business (e.g. online translation services) that are not offered by ETH Zurich is the responsibility of the respective user. Confidential data, strictly confidential data, or personal data may not be processed with such services.

[2] External storage or processing of confidential data

a) In principle, an external ICT service (e.g., cloud service) may be used to process and store confidential data, provided it has been approved for use with confidential data by the responsible service intermediary.

b) As a restriction, an information owner can prohibit processing and storage of information in the cloud.[16] In case of doubt, the information owner should be contacted.

[3] Software updates

a) If users receive IT security-relevant updates of system software and applications (patches and updates), they must install them as soon as possible, at the latest within two working days after distribution by the IT support in charge, and if necessary, activate them by restarting the IT system. Short extensions of this deadline are possible in consultation with the responsible system administrator.

b) In case of planned absence of the responsible user, the IT system must be shut down or disconnected from the network. Upon return, it must be updated immediately. IT systems that are not shut down despite the absence of the responsible user, must be looked after by a deputy.

[14] e.g., self-managed systems owned by ETH Zurich or systems not owned by ETH Zurich (e.g., "Bring Your Own Device").
[15] e.g., with other universities or industry partners
[16] Directive Information Security, Annex 2, "Electronic Information in the Cloud" RSETHZ 203.25

[4] Do not deactivate safety functions

Security measures implemented by system administrators, such as virus protection programs, software which identifies vulnerabilities, local firewalls, or security settings, may only be changed in consultation with the system administrator or the service intermediary in charge.

[5] Encryption of mobile data storage

Mobile data storage on which data[17] classified as «confidential» or «strictly confidential» is stored, must be encrypted and protected with a secure password or other means of authentication.

[6] Screen lock

Unauthorised access to unattended IT systems must be prevented by an access-protected screen lock ,unless users log out of the IT system completely.

[7] Handling means of authentication

a) Means of authentication such as passwords, PINs, private keys, smart cards, and other physical tokens are personal and classified as «strictly confidential». They must not be disclosed or passed on to other persons.

b) If sharing of a user account[18] and the associated password is mandatory for technical reasons, the password may be passed on to the authorised persons.

c) If passwords or PINs are written down, they must be kept protected so that unauthorised persons cannot gain access to them.

d) Electronic storage of authentication means must be encrypted by means currently considered to be sufficiently secure. The password for opening the repository must at least comply with the ETH Zurich password rules[19] and be different from any other password of the user(s) concerned. If possible, the electronic repository shall be protected with multifactor authentication.

[8] Passwords and PINs

The password and PIN rules according to the appendix of this document must be followed.

[9] System responsibility for self-managed systems

Users of self-managed systems[20] assume the role of system owners and must also comply with art. 10 accordingly.

[17] Definition of confidentiality levels Directive Information Security, Art. 22, RSETHZ 203.25
[18] "shared account"
[19] see appendix to this document: ETH Zurich password and PIN rules
[20] ETH Zurich "self-managed" systems or BYOD

Article 9 IT baseline protection rules for network zone administrators

[1] Only IT systems may be connected to a zone of ETH Zurich's network, which correspond to the intended use of the respective zone. If possible, IT systems with the same protection requirements should be protected in specific zones or sub-zones.

[2] If a zone contains IT systems which have not been compliant to the IT Guidelines and IT Baseline Protection Rules ETH Zurich for more than 20 days, the zone must be isolated in such a way that vulnerabilities are not exploitable from outside the zone. Alternatively, the affected systems can be moved to an already isolated zone.

[3] For all IP addresses in a zone, the responsible system administrators are known to the network zone administrators or can be found out at short notice.

[4] The use of the limited number of available IP addresses must be kept restrictive. Unused IP addresses must be returned to IT Services. The use and consumption of IP addresses must be checked regularly (DHCP fixations).

[5] Zone firewalls are generally closed. Ports and/or protocols are opened by IT Services only with the approval of the network zone administrator. The network zone administrator shall in advance carry out a risk assessment regarding the stability and vulnerability of the network, as well as considering the protection requirements of the affected data. IT Services have a veto right regarding the implementation of changes, which could affect the stability of the network or cause the network or ICT resources to become vulnerable.

[6] Activations, changes and deactivations of firewall rules must be traceable. For each firewall rule, the applicant, the user, and the purpose/functionality must be documented. The name of the person implementing the rule and the time of activation and deactivation must also be documented.

[7] Firewall rules must be checked and updated every six months. Rules that are no longer required must be removed.

[8] Network zone administrators must periodically check the firewall logs for irregularities.

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

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

[11] Physical security:
Network connections must be protected from outside access using NAC (Network Access Control) methods. Network connections that are not protected with NAC, may only be located in closed rooms to which only authorised persons have access.

Article 10 IT baseline protection rules for system administratos

[1] Up-to-dateness of software

a) Firmware, operating systems, applications, apps, and other software must be used in current versions which are supported by the manufacturer. They must be kept up to date with regard to security updates.

b) Security updates must be tested immediately after their release and distributed to the IT systems as quickly as possible. Provided that the tests do not reveal any operational problems and the operational risks are not disproportionately high compared to the security gain, the updates must be distributed to the target systems no later than ten calendar days after their release.

c) In emergencies, in case of urgency, the IT Security Officer of IT Services or the IT operators in charge may order immediate distribution and installation of security updates.

d) In ICT environments, where it is possible and operationally justifiable, the installation of updates and any restart on the target systems shall be enforced by technical means no later than two working days after distribution.

[2] Protection against malware

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

b) Malware scanners must be up to date, regarding software version and protection signatures.

c) Malware scanners are to be configured to check files «on access».

d) During runtime of an IT system, malware scanners must check for updates, if possible, at least every hour, and the updates must be imported automatically.

[3] Encryption of storage media

If possible, storage media of desktops and mobile devices such as laptops, tablets, smartphones are to be fully encrypted using the respective manufacturer's standard solutions.

[4] Screen lock

On end-user IT systems (desktops, laptops, tablets, etc.) and servers, a screen lock shall be automatically activated after 10 minutes of inactivity by the user. It can only be unlocked by entering a password, PIN, fingerprint, or by similar authentication methods.

[5] Access control

a) Access to accounts with increased access rights, such as «admin» or «root», or to groups with administration privileges, such as «administrators» or «sudoers», must be restricted to as few persons as possible. The persons have to be authorised for the respective role.[21]

[21] Need-to-Know

b) Access rights of user accounts with system administration rights must be restricted to the necessary minimum[22] and checked regularly.

c) Access rights to confidential or strictly confidential data or to ICT resources with a high need for protection in terms of integrity or availability must be restricted to the necessary minimum[23] and reviewed regularly.

d) Shared user accounts[24] are only permitted if there is a compelling need for them. Access to shared user accounts must be limited to the minimum necessary and checked regularly.

e) Preconfigured user accounts, such as «guest», must be deleted. If this is not possible, they must be deactivated or blocked from logging in. The preset password must be changed.

[6] Password and PIN Policies

If technically possible, the password and PIN rules of ETH Zurich[25] must be enforced by configuring password policies, e.g. in the IAM, Active Directory or on the local IT systems.

[7] Data backup

a) Data backup must be regulated and documented in a service level agreement or otherwise.

b) Resore of backuped data must be checked periodically on a random basis.

[8] Remote Access

a) Remote access may only take place using encrypted protocols currently considered secure.

b) If VPN (Virtual Private Network) is used as the access technology, the access must terminate on the VPN endpoint of IT Services.

c) If other remote access methods (such as «Jump Hosts», SCION, protocol tunneling, proxy technologies) are used, the access logs must be permanently monitored for anomalies (e.g. failed login attempts, cyber attacks).

d) IT systems used for remote access must have at least the level of security required by the IT Guidelines and IT Baseline Protection Rules of ETH Zurich.

[9] Physical security

Unauthorised persons must not have access to ICT resources. The necessary security measures must be adapted to the spatial conditions. The physical security requirements

[22] least privilege
[23] need-to-know
[24] "shared accounts"
[25] see appendix to this document: ETH Zurich password and PIN rules

applicable to the respective organisational unit, such as the room concept of IT Services[26], shall apply.

[10] Traceability

Operational and security-relevant system use and system activities, as well as changes to system configurations, must be logged.

Article 11 Basic IT protection requirements for service intermediaries

In addition to art. 10 of this ordinance, the following requirements apply to external ICT services used by ETH Zurich, insofar as they are relevant in the respective context.

[1] The contract, the service level agreement, and the general terms and conditions regulate in particular:

a) Jurisdiction and applicable law. For reasons of legal enforceability, the following preference applies: 1. CH, 2. EU, 3. other.

b) Personal data is processed and stored in Switzerland or in the EU. With appropriate contractual protection, personal data may also be processed or stored in other countries, including countries with an insufficient level of data protection, according to the list of countries of the Federal Data Protection and Information Commissioner (FDPIC). If the level of data protection in the country of storage/processing is insufficient, personal data must by law be protected by an agreement of standard contractual clauses (SCC) or comparable contractual measures.

c) The service provider confirms that it complies with the applicable laws and regulations[27].

d) All responsibilities are clearly assigned to one party.

e) The external service provider agrees to conduct regular independent IT security checks (audits, certifications) and provides audit reports, or grants ETH Zurich the right to audit.

f) Mutual contact persons and guaranteed response times, as well as the communication channels to be used, are regulated so that in the event of operational malfunctions or security incidents, a reliable and rapid response can be made.

g) The separation of ETH Zurich's data from data of other clients and from the administrative area of the service provider must be ensured (multi-client capability).

h) The service termination regulation must specify the acquisition of the ETH Zurich data and the usage logs by ETH Zurich and the deletion of this data on the part of the service provider.

[2] *repealed*

[26] IT Services room concept: https://sherlock.sp.ethz.ch/221b/policies/VPPR%20readonly%20Lib/2019_01_RL_Raum_Konzept_ID.pdf, available on request.

[27] e.g., the General Data Protection Regulation (GDPR) of the European Union EUR-Lex - 32016R0679 - EN - EUR- Lex (europa.eu) (retrieved 22.2.2021)

[3] Approval for processing of *internal* data may be given if the following conditions are met:

a) Users and administrators of ETH Zurich and the external service provider 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 considered secure according to the current state of the art.

c) Activities of users and administrators of ETH Zurich should be traceable. The logs should be available for at least one year and must be irretrievably deleted after two years at the latest, as specified in the BOT[28].

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

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

f) The availability of ETH Zurich data must be ensured in accordance with the requirements of ETH Zurich. Preferably, this is ensured by a regular backup of all data, the functioning of which is checked periodically.

g) ETH Zurich must have access to its data. This must also be ensured for cases in which users cannot access the data for a longer period due to extraordinary events (illness, death, etc.). At a minimum, 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 data of ETH Zurich back to ICT infrastructure of ETH Zurich if required.

[4] Approval for processing of *confidential* data may be given if the conditions for processing of internal data and additionally the following requirements are fulfilled:

a) Administrators of the external service provider who access ETH Zurich data and services use multifactor authentication.

b) Users and administrators of ETH Zurich authenticate with multifactor authentication.

c) The service provider uses the encryption key for the repository of ETH Zurich exclusively for ETH Zurich. For other customers, different keys are used.[29]

d) The administration of user accounts and access rights is carried out at a central internal unit of ETH Zurich. A connection to the identity management and federation services operated by IT Services[30] is to be implemented, insofar as this is possible and makes sense in the respective context.

[28] RSETHZ 203.21, annex 1, no. 3b
[29] The service provider uses different keys for different customers / tenants.
[30] e.g., ADFS, DirX

e) Users or groups of users must be able to be given granular access rights[31] to individual datasets.

[5] It is prohibited to store or process *strictly confidential* data on external ICT services.

[6] Up-to-dateness of the software

a) If applicable in the respective context, selective checks must be carried out to ensure that the service provider installs security updates within the agreed deadlines. Violations of the service level agreement must be discussed with the service provider and a warning issued in the event of repeated violations.

b) If the responsibility for importing security updates lies with ETH Zurich, the procedure in Art. 10 of this Ordinance must be followed.

Article 12 Exceptions to the above provisions

[1] External ICT services

For external ICT services for which the IT Guidelines and Baseline Protection Rules to be applied cannot be complied with, exceptions must be obtained from the CISO.

[2] ICT resources in the ETH Zurich network

a) IT systems for which the requirements of this ordinance cannot be complied with must be placed in isolated zones of the ETH Zurich network. Any vulnerabilities must not be exploitable from outside the isolated zones.

b) For IT systems that are to be operated in a non-segregated zone, even though IT Guidelines and IT Baseline Protection Rules are not complied with for more than ten working days, exceptional approvals must be obtained.

c) IT Services are conducting the approval process on behalf of the CISO of ETH Zurich.

d) The following applies to the approval process:

- Application submission by the system administrator:

  An initial assessment is made by the responsible network zone officer: He/she forwards the applications supported by him/her to the IT Security Officer IT Services.

- Application submitted by the network zone administrator:

  The application is submitted directly to the IT Security Officer IT Services.

- Decision by the IT Security Officer IT Services:

  He/she is responsible for assessing and approving or rejecting requests for exceptions.

[31] e.g., create, read, change, delete

- Escalations to the CISO of ETH Zurich:

  She/he is the escalation point in case of conflict. Furthermore, he/she is entitled to check the inventory of exception requests.

- Inventory:

  The IT Security Officer IT Services shall keep an inventory of the exception requests processed. It must be comprehensible, which requests were approved or rejected with which reasons, which time limits apply and which conditions, if any, are linked to an approval.

[3] Exception permits are limited in time, with the permits being reviewed by the applicant upon expiry and a new application submitted if necessary.

Article 13 Discontinuation of the use of external ICT services in the event of persistent non-compliance with mandatory requirements

The use of external ICT services must comply with the legal requirements and internal guidelines of ETH Zurich. The Director of IT Services and the Chief Information Security Officer may decide that an external ICT service may not be used or that its use must be discontinued if it persistently violates legal, contractual, or internal requirements of ETH Zurich.

Final Provisions

Article 14 Responsibility for the regulation

The ordinance «IT Guidelines and IT Basic Protection of ETH Zurich» is compiled up by the IT Services department, reviewed annually and submitted to the Vice President for Infrastructure and the Chief Information Security Officer of ETH Zurich on an annual basis.

Article 15 Repeal of previous regulations

The following decrees are repealed:

1. Standards for Responsibilities and System Maintenance of 6 February 2003 (RSETHZ 203.23)

2. The IT Best Practice Rules, Version 1.4 of 6 March 2019

3. Previous versions of IT Guidelines and IT Baseline Protection Rules of ETH Zurich (RSETHZ 203.23)

Article 16 Transitional provision

Edition 2022 of the IT Guidelines and IT Baseline Protection Rules of ETH Zurich must be implemented by March 2023 at the latest.

Article 17 Entry into force

These guidelines come into force on 1 August 2022.

Zurich, 14 July 2022

Prof. Dr Ulrich Weidmann
Vice President for Infrastructure
ETH Zurich

Dr Domenico Salvati
Chief Information Security Officer
ETH Zurich

Appendix: ETH Zurich password and PIN rules

1. Passwords

a) Passwords must be complex and difficult to guess. Names, dates of birth, telephone numbers, sequences of letters and numbers, terms from dictionaries, or similar easy-to-guess terms must not be used.

b) Where technically possible, passwords must be at least:
   - 12 characters long[32]
   - Include at least three of the following categories
     - Capital letters
     - Lower case letters
     - Numbers
     - Special characters

c) When changing a password, a new password that has not been used so far must be selected.

d) The password for ETH Zurich's network (RADIUS authentication) must be different from any of the other passwords (LDAP, Active Directory, etc.).

e) A password used in a private environment may not be used for a user account at ETH Zurich and vice versa.

f) Passwords preset by the manufacturer, must be changed immediately after the IT systems are put into operation.

g) Initial passwords that are assigned, for example, when a new user account is opened, must be changed when the user account is used for the first time.

h) If a user account is misused or misuse is suspected, the affected password must be changed immediately from a secure IT system.

i) If the group of persons authorised to access a shared user account changes, it's password must be changed if this is technically possible.

[32] Exception: For the ETH Zurich network (RADIUS authentication), a length of 10 characters is sufficient.

2. PINs

a) If PINs are used to protect IT systems, they must have at least 6 digits, if technically possible.

b) PINs must be difficult to guess. Dates of birth, number sequences (such as 123456) or repetitions (e.g. 111111) are not allowed.

c) In the event of misuse or suspected misuse, the PIN concerned must be changed.

d) When changing a PIN, a new PIN that has not been used so far must be selected.

e) PINs preset by the manufacturer must be changed immediately after the IT systems have been put into operation.

f) If the group of persons working with a common PIN changes, the PIN must be changed if this is technically possible.