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

ETH Zurich Acceptable Use Policy for IT Resources (BOT) and Appendix RSETHZ 203.21

of 17 December 2024

1. Section: General provisions 2
Article 1 Subject matter 2
Article 2 Applicability 2

2. Section: Usage 3
Article 3 Principles 3
Article 4 Private use of IT resources of ETH Zurich 3
Article 5 Use of private IT devices (bring your own device) 4
Article 6 Handling of business emails 4
Article 7 Use of external IT services (e.g. external cloud services) 5

3. Section: Basic protection requirements for IT resources 6
Article 8 Screen lock 6
Article 9 Identification and authentication 6
Article 10 Software updates 6
Article 11 Deactivating security functions 7

4. Section: Monitoring, data recording and analysis 8
Article 12 Principle 8
Article 13 Recording, storing and analysing data 8

5. Section: Misuse 10
Article 14 Misuse 10
Article 15 Safeguarding and precautionary measures 11
Article 16 Consequences of abuse 11

6. Section: Special regulations 12
Article 17 Data protection 12
Article 18 ETH Zurich's presence on the Internet 12
Article 19 Additional information security regulations 12

7. Section: Final provisions 13
Article 20 Cancellation of previous law and entry into force 13

Appendix 1: Password and PIN rules 14

The Executive Board of ETH Zurich,

based on Art. 4 para. 1 (m) of the Ordinance on the Organisation of the Swiss Federal Institute of Technology Zurich of 21 November 2024[1],

hereby decrees:

1. Section: General provisions

Article 1 Subject matter

[1] This Acceptable Use Policy ("BOT") governs the principles for the proper use of IT resources at ETH Zurich (hereinafter referred to as "IT resources"). This policy is also applicable to non-ETH systems that utilise services in the ETH Zurich data network.

[2] 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 Acceptable Use Policy applies to all use of IT resources by users.

[2] Members of ETH Zurich pursuant to Art. 13 of the ETH Law (namely employees and students) and guests pursuant to the Guest Regulations[2] are deemed to be users.

[1] ETH Zurich Organisation Ordinance (RSETHZ 201.21)

[2] ETH Zurich Guest Regulations (RSETHZ 515.2)

2. Section: Usage

Article 3 Principles

[1] IT resources of ETH Zurich are primarily to be used for business purposes. Any use of IT resources, in particular for study purposes or for the fulfilment of tasks within the scope of the employment relationship or the guest stay, is deemed to be "business". Any other use is considered "private".

[2] Only authorised users may use IT resources. IT resources must be used lawfully, as intended and with care. Users are personally responsible for ensuring that their use of IT resources does not infringe the rights of third parties (e.g. copyright, licence or personal rights).

[3] Authorised users use IT resources for their work that are offered or approved by the IT operators of ETH Zurich. The IT operators for ETH Zurich are in particular the IT Services, the IT Services Groups (ISG) of the departments and the central bodies as well as the CSCS and any professorships with their own IT. IT operators manage, maintain and develop IT resources.

[4] The Chief Information Security Officer (CISO) is responsible for managing information security at ETH Zurich.

Article 4 Private use of IT resources of ETH Zurich

[1] Private use of IT resources of ETH Zurich[3] is possible if the relevant conditions are met (Art. 4 para. 5). However, it is not recommended.

[2] ETH Zurich email accounts should only be used for business purposes. The use of the ETH email account is mandatory for business correspondence.

[3] Private emails may be sent with the prior consent[4] of users. Private emails are then treated by ETH Zurich in the same way as business correspondence (storage; deletion, archiving after 10 years if necessary, etc.). Consent cannot be revoked retroactively.

[4] Excluded from this declaration of consent is the use of services for which the ETH Zurich email is mandatory, e.g. discounts for ETH members, as well as all calendar entries.

[5] The private use of IT resources is prohibited if it, in particular:

a. violates licence terms[5];
b. violates applicable law;
c. is excessive, harassing, offensive or damaging to the reputation of ETH Zurich;
d. has a commercial character;
e. causes a technical malfunction or impairment, or
f. impairs the fulfilment of work or study obligations.

[3] e.g. use of the browser for private purposes

[4] Consent can be given at: www.adressen.ethz.ch ("Personal data and communication data" → Communication data)

[5] Licence conditions can be obtained from the ID Service Desk

[6] The simultaneous use of ETH Zurich-licensed software for professional or study purposes on private and office computers is prohibited, unless explicitly permitted by the licence terms.

[7] Private, personal content of ETH Zurich members is not permitted on the public ETH Zurich websites[6]. Exceptions to this are CVs, job-related publications or similar items from employees.

Article 5 Use of private IT devices (bring your own device)

[1] ETH members and authorised guests who use private IT devices for their work or studies at ETH Zurich are deemed to be system administrators for these IT devices. The corresponding directives apply[7]. The directives applicable to IT operators, in particular Art. 4 Para. 5 of this Acceptable Use Policy, apply. Where direct application is not possible, they apply by analogy.

[2] Private IT devices are used in particular for multi-factor authentication on ETH Zurich IT systems.

[3] The use of private IT devices by ETH Zurich employees (especially laptops and PCs) can be handled more restrictively, depending on the organisational unit.

[4] Strictly confidential data[8] may not be read, edited or used with private IT devices.

Article 6 Handling of business emails

[1] For electronic mail (email), the statutory retention period of 10 years applies until automatic deletion or archiving by the ETH Zurich University Archives[9].

[2] The mass mailing of messages to all ETH employees and/or all students ("mass mailing to all") is generally prohibited. The following exceptions apply, which must be agreed in advance with University Communications:

a. the sender is the president or members of the Executive Board; or
b. these are surveys or similar events that have been authorised by the President or a member of the Executive Board.

Student mailings are primarily based on the regulations of the rectorate[10].

[3] "Mass mailings to all" are also permitted if they contain operational or study-related information that all ETH employees or students must be aware of (e.g. emergencies such as extraordinary building closures) or that is fundamental to their work at ETH Zurich (e.g. setting up multi-factor authentication).

[4] Operational or study-related mass mailings within one's own organisational unit (department, Executive Board domain) are permitted and are carried out by the responsible specialist units.

[6] RSETHZ 203.22 ETH Zurich: Web guidelines

[7] e.g. IT Guidelines and IT Baseline Protection Rules (RSETHZ 203.23), Logging, Analysis and Monitoring (RSETHZ 203.29)

[8] RSETHZ 203.28 "Directive on the inventory and classification of information at ETH Zurich"

[9] See Chapter 14 Financial Regulations (RSETHZ 245)

[10] See Guidelines for the support of written and electronic mailings to ETH Zurich students by the rectorate, filed in the Rectorate's Collection of Directives

[5] Mass mailings to more than 500 addressees ("mass mailing to many") outside of your own organisational unit must be requested in advance in writing from the rectorate (mailings to students) or the University Communications Department (mailings to employees).

[6] No address data of ETH members will be disclosed to external or internal enquirers for mass mailings. Student mailings are primarily based on the regulations of the rectorate.

[7] Newsletters that allow recipients to subscribe and unsubscribe are not considered electronic mass mailings.

Article 7 Use of external IT services (e.g. external cloud services)

[1] The use of external IT services is permitted, provided that these services have been approved by ETH Zurich[11] and the information owners have given their consent to the processing of their data in these services.

[2] The occasional proper use of external IT services to support day-to-day business (e.g. search engines, online translation services, chatbots with artificial intelligence, ChatGPT) that are not approved by ETH Zurich by means of cloud assessment is the responsibility of the user. Personal data requiring special protection in accordance with the Data Protection Act (DSG)[12] Art. 5 (c) and otherwise confidential or strictly confidential (material or personal) data may not be processed using such services.

[3] As a restriction, information owners can prohibit[13] the processing and storage of their data in the cloud. In case of doubt, the information owners should be contacted.

[11] Link to the directory of shared cloud services

[12] This includes information on religion, ideology, political or trade union activity, health, privacy, race or ethnicity, genetics, biometrics, legal prosecution, social welfare (the legal text is authoritative)

[13] Information owners are responsible for the data collected and processed by them or on their behalf. They are usually managers with budget responsibility for an organisational unit.

3. Section: Basic protection requirements for IT resources

Article 8 Screen lock

Unattended IT equipment must always be secured (even for short periods) by an access-protected screen lock/device lock. This is also recommended for IT devices belonging to students or guests.

Article 9 Identification and authentication

[1] In principle, users of IT resources must identify and authenticate themselves with the user name (user ID) or email address of ETH Zurich. This user data may be disclosed to third parties for the authentication and authorisation of electronic services (namely cloud services).

[2] Means of identification and authentication such as passwords, PINs, private keys or chip cards are personal and "strictly confidential". They must be stored securely and fulfil the requirements of Annex 1 "Password and PIN rules". Disclosure or dissemination is prohibited except for compelling technical reasons.

[3] ETH Offices will never request the disclosure of identification and authentication means. Such requests are unlawful. They represent a malicious attempt (phishing) to gain unauthorised access to ETH Zurich data. They must be reported immediately to the responsible IT Support Personnel[14].

[4] If there is a suspicion of misuse of identification and authentication means by unauthorised persons, the user must have access blocked immediately and report the incident to the responsible IT Support Personnel.

[5] If the user uses an encrypted password manager, the password for opening the manager must comply with the rules in Appendix 1. If technically possible, multi-factor authentication should also be used.

Article 10 Software updates

[1] Patches and security-relevant updates must be installed as soon as possible (generally within two working days) after distribution by the responsible IT Support Personnel and, if necessary, activated by restarting the IT system. In doing so, (scientific) operation must be taken into account depending on the situation, e.g. an ongoing series of measurements. Short extensions must be agreed with the responsible system managers.

[2] An IT system must be shut down or disconnected from the network in the event of a planned absence where there is no possibility of updating the software. The software installed on the device must be updated immediately upon return at the latest.

[3] Negligence may result in the user being warned or the device in question being excluded from the data network by the CISO. If the warning is unsuccessful and the technical possibility exists, security-relevant updates can also be carried out remotely by the responsible system administrator.

[14] e.g. Service Desk of the IT Services or IT Services Group

Article 11 Deactivating security functions

[1] Changes to the IT resources provided by ETH Zurich (e.g. virus protection programmes, local firewalls or security settings) are only permitted with the written consent of the relevant system administrator or, in the case of external IT services, with the written consent of the service provider.

[2] Disabling, circumventing or removing security measures requires the prior authorisation of the CISO.

4. Section: Monitoring, data recording and analysis

Article 12 Principle

[1] The recording, storage and analysis of data are permitted. This includes, in particular, content data or traffic data generated during the use or operation of IT resources, such as user activities or technical security statuses.

[2] Data may also be recorded (e.g. as part of backups).

[3] Technical prevention and the sensitisation and participation of ETH members take priority over monitoring.

Article 13 Recording, storing and analysing data

[1] User activities and technical security statuses of the IT resources may be recorded or logged. As a result, resource access and data changes may be logged, for example saving, reading, modifying, disclosing, deleting and destroying data.

[2] The subject line, date, time, sender and recipient addresses of emails may be logged. When analysing email traffic, the content of private emails is not normally viewed. If the distinction between private and business emails is unclear, ETH Zurich may assume that the email is business-related.

[3] Personal data generated during the use or operation of IT resources or logs may be recorded and evaluated for the following purposes[15]:

a. **not personalised:**
1. to maintain the security of information and services (2 Y);
2. for the technical maintenance of IT equipment (2 Y);
3. to monitor compliance with usage regulations (2 Y);
4. to track access to data collections (2 Y);
5. to record the costs incurred through the use of the electronic infrastructure (2 Y);
6. for data on staff working hours: for the management of working time (5 Y);
7. for data on entering or leaving buildings and rooms and the time spent there: to ensure safety (3 Y).

b. **random non-personalised samples** (e.g. pseudonymised):
1. to control the use of IT resources (2 Y);
2. to control the working hours of staff (5 Y).

[15] Art. 57l ff. Government and Administration Organisation Act (RVOG; SR **172.010**) in conjunction with Art. 4 f. Ordinance on the Processing of Personal Data Resulting from the Use of the Federal Electronic Infrastructure of 22 February 2012 (SR **172.010.442**); see also the directive "Logging, Analysis and Monitoring of log data at ETH Zurich" (RSETHZ 203.29).

c. **personalised**:
   1. to clarify a concrete suspicion of misuse of IT resources or penalisation of proven abuse (2 Y);
   2. to analyse and rectify faults in the electronic infrastructure and to defend against specific threats to this infrastructure (2 Y);
   3. for the provision of required services (2 Y);
   4. for recording and invoicing services rendered (2 Y);
   5. to control individual working hours (5 Y).

The permitted retention period for personal data, including log data, is indicated in brackets; the data will be deleted after this period at the latest. Shorter retention periods and paragraphs 4 and 5 are reserved. Art. 59 ff. of the ETH Domain Personnel Ordinance apply to personnel dossiers and medical personnel data [16] (personnel dossier: Retention period 10 years).

4 In order to clarify a concrete suspicion of misuse of IT resources or to penalise proven misuse (Article 3 [c1] above), data may be backed up without informing the person concerned in writing. The retention period pursuant to Article 3 (c1) does not apply in this case. The personalised analysis of the seized data is only permitted after the data subject has been informed in writing of the suspicion or misuse[17].

5 If there is a concrete suspicion of the existence of criminal offences, the relevant data shall be secured for the attention of the competent criminal authority. Further personalised analyses are the sole responsibility of the criminal justice authorities. The President of ETH Zurich is responsible for deciding whether to press charges against offending members of the teaching staff or employees of ETH Zurich.[18]

6 Users are obliged, as far as permissible, to co-operate in the investigation of misuse or cases of financial loss.

7 For the processing and storage of data recorded in the electronic personnel and student information systems pursuant to Art. 36a and 36b of the ETH Act, the implementing provisions of the ETH Board[19] and the Executive Board of ETH Zurich shall apply.

[16] Personnel Ordinance ETH Domain (PVO-ETH; SR **172.220.113**)

[17] Art. 57o para. 1 (a) Government and Administration Organisation Act (RVOG; SR **172.010**) in conjunction with Art. 11 Ordinance of 22 February 2012 (SR 172. 010.442). Art. 11 Ordinance on the Processing of Personal Data Resulting from the Use of the Electronic Infrastructure of the Confederation of 22 February 2012 (SR **172.010.442**).

[18] Art. 14 para. 2 Rules of Procedure of the Executive Board of 10 August 2004 (RSETHZ 202.3).

[19] Personal Data Protection Ordinance ETH Domain, PDV-ETH (SR **172.220.113.42)**

5. Section: Misuse

Article 14 Misuse

[1] Any use of ETH Zurich IT resources that disregards the provisions of this Acceptable Use Policy, violates overriding law (in particular, violates professional obligations, e.g. regarding integrity in research) or violates the rights of third parties is improper use.

[2] In particular, the following behaviours are considered abusive and are prohibited:

a. the processing, storage or transmission of material with unlawful or immoral content, such as depictions of violence, pornography[20], incitement to crime or violence[21], disturbance of religious freedom and freedom of worship[22] or discrimination and incitement to hatred[23];

b. the production, instruction in the production or intentional distribution of harmful programmes or programme components within the meaning of Art. 144bis para. 2 Swiss Criminal Code, SCC (viruses, worms, Trojans, etc.). The production and instruction in the production of such programmes for the purposes of teaching and research is permitted if appropriate precautions are taken against their harmful use;

c. unauthorised intrusion into a data processing system (Art. 143bis SCC "Hacking"): spying on passwords, unauthorised scanning of internal and external networks for vulnerabilities (e.g. port scanning), taking precautions and implementing measures to disrupt networks and computers (e.g. denial of service attacks). “Hacking" in a closed environment for the purposes of teaching and research is permitted;

d. the sending of messages with misleading sender details or content (e.g. fraudulent emails such as phishing, CEO fraud, etc.). Justified exceptions are only permitted if they are absolutely necessary for teaching and research and are accompanied by appropriate transparency measures[24];

e. unauthorised data procurement (Art. 143 SCC) and data damage (Art. 144bis para. 1 SCC);

f. the use of ETH Zurich IT resources in deliberate violation of licence terms or copyrights;

g. harassment of members of ETH Zurich or third parties through messages (e.g. with offensive, sexist, racist, reputation-damaging or discriminatory content), in particular through content that contradicts ETH Zurich's Code of Conduct «Respect»[25];

h. violation of the regulations on bulk mailing pursuant to Art. 6;

i. setting up unassigned direct connections to the ETH Zurich communication networks (e.g. via WLAN access points) without the prior written consent of IT Services and the respective system managers.

[20] Art. 197 of the Swiss Criminal Code (SCC; SR **311.0**)

[21] Art. 259 StGB

[22] Art. 261 StGB

[23] Art. 261bis SCC

[24] e.g. subsequent information of data subjects or disclosure of the circumstances in the scientific publication publication

[25] Code of Conduct “Respect” or https://ethz.ch/staffnet/en/employment-and-work/working-environment/living-respect.html

[3] The following are deemed grave:

a. misuse in accordance with the Swiss Criminal Code, in particular para. 2 (a, b, c, d), insofar as this is wilful or intentional;

b. wilful infringement of Art. 10 or

c. other abuse in case of recurrence.

[4] Knowledge of serious misuse obliges direct superiors, IT operators and service intermediaries to report it to the CISO.

Article 15 Safeguarding and precautionary measures

Where it is feared that the normal use of ETH Zurich's IT resources may be significantly impaired or that damages are likely or known to have occurred to ETH Zurich, its members or third parties, the following protective and precautionary measures may be ordered:

a. blocking access to IT resources from which misuse has been detected or which are affected by it;

b. blocking of data and

c. securing and storage of data for evidentiary purposes.

Article 16 Consequences of abuse

[1] If misuse or a concrete suspicion of misuse pursuant to Art. 14 is identified, the CISO may hear the persons involved and/or order the following measures:

a. warning for minor offences;

b. precautionary blocking of access to IT resources that are affected;

c. blocking of abusive and/or illegal data;

d. removal or deletion of abusive and/or unlawful data;

e. securing and storage of data for evidentiary purposes.

[2] Furthermore, the CISO may temporarily or permanently block the offending user's access to IT resources, restrict their use or prohibit their use.

[3] In addition, disciplinary or personnel measures may be taken against users at fault[26], civil proceedings (action for damages) may be initiated or criminal charges may be brought[27]. For employees, any type of abuse is considered a breach of labour law obligations[28]. Serious cases pursuant to Art. 14 para. 3 may lead to dismissal.

[4] The costs caused by misuse and its consequences, including investigation and sanctioning (including investigation, court and legal costs), may be passed on by ETH Zurich to the offending users.

[26] Students: pursuant to Art. 2 ff. ETH Zurich Disciplinary Ordinance of 10 November 2020 (SR **414.138.1**);
Employees: in accordance with Art. 58a of the ETH Domain Personnel Ordinance of 15 March 2001 (PVO-ETH; SR **172.220.113**).

[27] Cf. Art. 22a of the Federal Personnel Act (FPA; SR **172.220.1**).

[28] Art. 25 Federal Personnel Act (SR **172.220.1**) or Art. 53 PVO-ETH

6. Section: Special regulations

Article 17 Data protection

[1] When processing personal data, the legal requirements of data protection must be complied with. In particular, Art. 36a-36f of the ETH Act[29] apply.

[2] Data breaches relating to personal data must be reported to the Data Protection Advisor immediately, but no later than 72 hours after discovery (email address: ds@ethz.ch).

[3] ETH Zurich has a data protection advisor. The data protection page of the Legal Service provides further information on data protection[30].

Article 18 ETH Zurich's presence on the Internet

University Communications issues the implementation provisions[31] for the presence of ETH Zurich and its organisational units in online media.

Article 19 Additional information security regulations

[1] The following apply in particular:

a. the «Directive on Information Security at ETH Zurich»[32]

b. for system and network zone managers: the directive «IT Guidelines and IT Basic Protection Requirements of ETH Zurich»[33];

c. for information owners: the directive on the «Inventory and Classification of Information»[34];

d. for service intermediaries and information owners in the context of using external cloud services: the directive «IT guidelines and basic IT protection requirements of ETH Zurich»[35]

e. for system and network zone managers and service mediators, the directive «Logging, Analysis and Monitoring of Log-Data»[36]

[2] Users of self-managed IT resources, for example professorships with their own IT, fulfil the role of system administrators.

[29] See also the Data Protection Act (DSG, SR **235.1)** and Ordinance (DSV, SR **235.11**), in some situations also the EU General Data Protection Regulation (GDPR); regulations of the ETH Domain such as the Personal Data Protection Ordinance of the ETH Domain (PDV-ETH), guidelines of the Federal Data Protection Commissioner FDPIC (www.edoeb.admin.ch).

[30] https://ethz.ch/staffnet/de/service/rechtliches/datenschutz.html

[31] e.g. Web Guidelines (RSETHZ 203.22), Social Media Guidelines (RSETHZ 203.24), Guidelines on the Use of the Logo (RSETHZ 202.4)

[32] RSETHZ 203.25

[33] RSETHZ 203.23

[34] RSETHZ 203.28

[35] RSETHZ 203.23

[36] RSETHZ 203.29

7. Section: Final provisions

Article 20 Cancellation of previous law and entry into force

[1] ETH Zurich Acceptable Use Policy for Information and Communications Technology of 19 April 2005 (BOT; RSETHZ 203.21) are hereby repealed.

[2] This policy enters into force on 01 January 2025.

Zurich, 17 December 2024

On behalf of the Executive Board:

The President:	Prof. Joël Mesot
The Secretary General:	Katharina Poiger Ruloff

Appendix 1: Password and PIN rules

1. Passwords

a. Passwords must be difficult to guess. Names, dates of birth, telephone numbers, sequences of letters and numbers, unchanged entries from dictionaries or similar easy-to-guess terms may not be used.
b. Where technically possible, passwords must be at least:

  - 12 characters long. Exception: A length of 10 characters is sufficient for the ETH Zurich network (RADIUS authentication);
  - Include at least three of the following categories
    - Uppercase letters
    - Lowercase letters
    - Numbers
    - Special characters

c. If you change your password, you must choose a new password that has not been used before.
d. The password for the "virtual private network" – VPN – of ETH Zurich (VPN with RADIUS authentication) must be different from each of the other passwords, e.g. from the login to Windows, 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 commissioning the IT equipment. Initial passwords that are assigned when a new user account is opened, for example, must be changed the first time the user account is used.
g. If a user account is misused or misuse is suspected, the password concerned must be changed immediately from a secure IT system.
h. If the group of persons authorised to access a shared user account (where a password must be shared) changes, the password must be changed if this is technically possible.

2. PINs

a. If PINs are used to protect IT resources, they must be at least 6 digits long if technically possible.
b. PINs must be difficult to guess. Dates of birth, sequences of numbers (such as 123456) or repetitions (e.g. 111111) are not permitted.
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 previously must be selected.
e. PINs preset by the manufacturer must be changed immediately after commissioning the IT systems.
f. If the group of people working with a shared PIN changes, the PIN must be changed if this is technically possible.