ETH Zurich Acceptable Use Policy for Information and Communications Technology (“BOT”) and Appendix
(Partial revision as of 1 April 2019)

1. Section: General provisions
   Art. 1 Purpose
   Art. 2 Definitions
   Art. 3 Scope

2. Section: Responsibilities
   Art. 4 IT Services administrative department, IT support groups and CSCS
   Art. 5 Chief Information Security Officer (CISO)
   Art. 6 IT operator, system and network administrator
   Art. 7 Presence on the intranet/internet

3. Section: Use
   Art. 8 Purpose of use and authorisation for use
   Art. 8bis Private use
   Art. 9 Use of ICT resources outside the ETH Zurich campus
   Art. 10 Private use of software licenced to ETH Zurich
   Art. 11 Data protection
   Art. 12 Software copies
   Art. 13 Use of electronic communication resources

4. Section: Security measures
   Art. 14 Low-risk systems
   Art. 14bis Access protection measures
   Art. 15 High-risk systems
   Art. 15bis Integrity of ICT network

5. Section: Responsibility and liability
   Art. 16 Responsibility
   Art. 17 Liability

6. Section: Abuse
   Art. 18 Logging/Detection of abuses
   Art. 19 Abuses
   Art. 20 Consequences of abuses

7. Section: Special provisions
   Art. 21 Special provisions and instructions

8. Section: Final provisions
   Art. 22 Enforcement
   Art. 23 Abrogation of previous regulations and effective date

Appendix
The ETH Zurich Executive Board,

pursuant to Art. 4 (1) c) of the Ordinance Governing the Organisation of ETH Zurich of 16 December 2003, decree:

1. Section: General provisions

Art. 1 Purpose

1 The information and communications technology (ICT) resources of ETH Zurich should be used in the manner best suited to the pursuit of its mission.

2 The purpose of this Policy is to prevent disruption and misuse of ETH Zurich ICT resources.

Art. 2 Definitions

1 The term "ICT resources" comprises all information and telecommunication resources owned by 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 as well as locking systems). The definition also includes non-ETH Zurich 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).

2 The term "systems" refers to any software and hardware, including portable systems.

3 The term "data" includes personal and academic data.

---

1 Throughout this Policy, the term “telematics” has been replaced with “information and communications technology” or “ICT”. Equally, the term “telematics resources” has also been replaced by the term “information and communications technology resources” or “ICT resources”.

2 Directive on Information Security at ETH Zurich of 9 April 2018 (RSETHZ 203.25en) as amended by decision of the ETH Zurich Executive Board of 9 April 2018 (SLB 09.04.18-09.04 and SLB 26.03.19-07.01).

3 RSETHZ 201.021

4 As amended by decision of the ETH Zurich Executive Board of 17 September 2013, effective as of 1 October 2013; editorial amendment in effect since 1 January 2019

5 Expected Art. 36i ETH Act (as per revision of ETH Act of December 2018).
The term “users” includes all members of ETH Zurich (Art. 13 of the ETH Act) and certain third parties (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) who are authorised to use the ICT resources of ETH Zurich.

The term “electronic communication resources” includes telephone, fax, email, SMS, instant messaging, video conference systems and similar resources.

The term “organisational units” refers to the central or decentralised bodies of ETH Zurich established by the Executive Board pursuant to the ETH Organisation Ordinance (Organisationsverordnung – OV) of 16 December 2003 (e.g. academic departments, institutes, administrative departments, infrastructure units, staff units, independent chairs) and the education and research facilities outside the academic departments established pursuant to Art. 61 OV (e.g. CSCS).

The term “private use” refers to any use of the ICT or telecommunication resources of ETH Zurich that is not for study purposes, or for the purpose of fulfilling one’s duties in the employment relationship.

The term “analysis of anonymous data” refers to the statistical analysis of the log files that does not use personal data.

The term “analysis of pseudonymous or non-personally identifiable data” refers to the analysis of the log files of pseudonymised identifiable persons. The pseudonym must protect the identity of the person in question in the phase of monitoring that does not involve personal data.

The term “logging” refers to the continuous recording of metadata (addresses in the message headers, session data from the log file and similar data) of the ICT resources.

The term “system and network administrators” refers to the specialists described in Art. 3 of the Standards for Responsibilities and System Maintenance.

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.

Art. 3 Scope

This Policy applies to any use or shared use, whether by ETH Zurich members or third parties, of all ETH Zurich-owned ICT resources as well as to any use of non-ETH Zurich devices connected to the ETH Zurich data network.
2. Section: Responsibilities

Art. 4 IT Services administrative department\(^{13}\), IT support groups and CSCS\(^{14}\)

The ETH Zurich IT Services administrative department (hereinafter “IT Services”) shall provide IT services to the individual users and to the ETH Zurich organisational units. It shall appoint an IT Security Officer for IT Services (ITSO ITS) in accordance with Art. 8 of the Directive on Information Security at ETH Zurich. In particular, the IT Services administrative department is responsible for the following in the area of IT security\(^{15}\):

a) The technical measures with regard to securing the ICT resources and services that are provided by IT Services for the central and decentralised organisational units of ETH Zurich, including the clarification and documentation of security defects, providing information on these as well as resolving and circumventing them\(^{16}\);

b) Providing training and information for users;

c) Monitoring compliance with the Standards for Responsibilities and System Maintenance\(^{17}\) and with the IT Best Practice Rules pursuant to Art. 15 (3);

d) Coordinating the implementation of technical and organisational innovations;

e) Providing the necessary encryption techniques (Art. 13 (2));

f) The duties assigned to it in accordance with the Directive on Information Security at ETH Zurich\(^{18}\) with regards to information security;

g) Granting authorisations pursuant to Art. 15bis;

h) Receiving reports by users concerning security problems (Arts. 14 and 15);

i) Exchanging of information within ETH Zurich and the ETH Domain as well as between the universities, SWITCH and the federal authorities, unless this is done by the CISO in accordance with Art. 5 of the Directive on Information Security at ETH Zurich\(^{19}\);

j) Assisting the CISO\(^{20}\) in fulfilling his/her tasks pursuant to the Guidelines for Monitoring the Use of ICT Resources at ETH Zurich attached as Appendix;

k) Detecting, documenting and correcting security defects (Art. 14 (2)) in the central organisational units;

l) Clarifying the admissibility of a commercial use of the ICT resources and concluding the relevant agreements (Art. 8 (6));

m) revoked\(^{21}\).

The IT support groups in the academic departments shall be for the main part responsible for the same tasks, except for the tasks defined under the letters g), i), k) and l).

---

\(^{13}\) Editorial amendment

\(^{14}\) As amended by decision of the ETH Zurich Executive Board of 17 September 2013, effective as of 1 October 2013

\(^{15}\) As amended by decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019

\(^{16}\) As amended by decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019

\(^{17}\) RSETHZ 203.23

\(^{18}\) RSETHZ 203.25en

\(^{19}\) RSETHZ 203.25en

\(^{20}\) Replacement of term “IT security Officer” with “CISO” throughout this Policy (see Art. 2 (12))

\(^{21}\) As amended by decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019
In its function as national centre, the Swiss National Supercomputing Centre (CSCS) shall be responsible for providing services in the area of supercomputing, except for the tasks defined under the letters g) and k).

Art. 5 Chief Information Security Officer (CISO)\textsuperscript{22}

ETH Zurich has a CISO in order to safeguard information security. He/she has the duties and competencies laid out in Art. 5 of the Directive on Information Security at ETH Zurich\textsuperscript{23}. He/she is not affiliated with a specific department and in organisational terms, is aligned with the President. He/she reports to the Risk Management Commission (RMC) of ETH Zurich.

Art. 6 IT operator, system and network administrator\textsuperscript{24}

There shall be a person responsible for each system integrated in the data network of ETH Zurich.

Every organisational unit shall appoint one or several system administrator(s) and a network administrator to address the technical and operational aspects of the use of the ICT resources.

Based on the reports from the responsible Information Security Officer (ISO)\textsuperscript{25}, the IT operator\textsuperscript{26} determines which systems process high-risk data within the meaning of Arts. 16 and 23 (1) of the Directive on Information Security at ETH Zurich (Art. 15 (1)). The system administrator performs this duty for systems that are not managed by an IT operator.

The system administrator shall delete the data contained on the non-mobile data storage devices (hard disks, etc.) before transfer or disposal (Appendix to BOT, clause 1.7).

The other tasks of the system administrator and of the network administrator are set forth in the implementation provisions, for example the \textit{Standards for Responsibilities and System Maintenance}\textsuperscript{27} and in the \textit{Guidelines for Monitoring the Use of the ICT Resources at ETH Zurich} attached to this Acceptable Use Policy as Appendix.

In the case of non-ETH computing devices, the user with administrator rights shall be at the same time the system administrator.

Art. 7 Presence on the intranet/internet\textsuperscript{28}

The Corporate Communications administrative department shall be responsible for the presentation of ETH Zurich and of its organisational units on the internet or intranet. It shall issue the corresponding implementation provisions in this regard.\textsuperscript{29}

\textsuperscript{22} Wording in accordance with decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019
\textsuperscript{23} RSETHZ 203.25en
\textsuperscript{24} Wording in accordance with decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019
\textsuperscript{25} In accordance with Art. 6 of the Directive on Information Security at ETH Zurich.
\textsuperscript{26} In accordance with Art. 3 (4) of the Directive on Information Security at ETH Zurich (RSETHZ 203.25en).
\textsuperscript{27} RSETHZ 203.23
\textsuperscript{28} Wording in accordance with decision of the ETH Zurich Executive Board of 17 September 2013, effective as of 1 October 2013
\textsuperscript{29} ETH Zurich: Web Policy of 1 September 2016 (RSETHZ 203.22_en) and ETH Zurich Social Media Guidelines of 26 February 2013 (RSETHZ 203.24EN)
In this context, Corporate Communications must comply with the regulations concerning equal treatment of disabled people.\(^{30}\)

Commercial advertising is prohibited. The President may decide on exceptions. This provision does not apply to the mention of sponsors.

### 3. Section: Use

#### Art. 8 Purpose of use and authorisation for use\(^{31}\)

1. Use of the ICT resources is permitted for the purposes for which they are made available to the users (“intended use”). This does not apply to applications subject to express authorisation.

2. Users must restrict their use of the ICT resources to the appropriate extent and to the permitted purposes.

\(^{3-4}\) revoked

5. Without the written consent of the responsible system administrator, users may not perform any modification to the ICT resources provided by ETH Zurich, in particular changes and modifications to software programs and the deactivation, circumvention or removal of security mechanisms. This does not apply to the modifications involved in the proper use of the ICT resources.

6. In principle, spin-off companies of ETH Zurich shall use their own ICT resources. Commercial use of ETH Zurich’s ICT resources (e.g. pursuant to spin-off agreements) is not in principle permitted. An exception to this is the use of a network connection in an ETH building. Any costs thereby incurred shall be borne by the respective clients.\(^{32}\)

6bis The operation and use of the supercomputing infrastructure at the CSCS or the use of ICT resources within the framework of a research cooperation shall be contractually agreed upon.

ICT resources are to be disposed of pursuant to Art. 134 of the Financial Regulations of ETH Zurich\(^{33}\) as well as Section 8 of the Guidelines for Inventory Management at ETH Zurich\(^{34}\) of January 2019.\(^{35}\)

#### Art. 8bis Private use\(^{36}\)

1. Use of ETH Zurich’s ICT resources for private purposes, in particular email and internet, is basically permitted, provided it is not excessive, does not conflict or interfere with the user’s work or study obligations, does not violate Swiss law (in particular the provisions of the Criminal Code) or rights of third parties (personal rights, copyrights), is not of a commercial nature, and does not damage the reputation of ETH Zurich.

2. Furthermore, this private use of ETH Zurich ICT resources should not technically disrupt or impair their use for purposes appropriate to ETH Zurich’s statutory missions, or put excessive load or stress on the generally available resources (networks, internet access, storage capacities, etc.).

---

\(^{30}\) Disability Discrimination Act of 13 December 2002 (DDA; SR 151.3); Ordinance on Elimination of Discrimination against People with Disabilities of 19 November 2003 (EPDO; SR 151.31)

\(^{31}\) Wording in accordance with decision of the ETH Zurich Executive Board of 17 September 2013, effective as of 1 October 2013

\(^{32}\) Wording in accordance with decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019

\(^{33}\) Financial Regulations of ETH Zurich of 1 January 2019 (RSETHZ 245en)

\(^{34}\) Available from ETH Zurich > Finance and Controlling > Downloads (last accessed on 21 January 2019)

\(^{35}\) Wording in accordance with decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019

\(^{36}\) Inserted by decision of the ETH Zurich Executive Board of 17 September 2013, effective as of 1 October 2013
Private personal contents of ETH members are not allowed on public ETH web pages, except for curriculum vitae, publications etc. of researchers. IT Services can provide centralised systems required to create personal websites.

Software licenced to ETH Zurich may be used professionally at home (“home office use”) by ETH Zurich employees employed on an at least 50% basis, and by the students matriculated at ETH Zurich, if permitted by the applicable software licence agreement. The right to install software on a private computer and the type of software use (e.g. right to private use) is governed by the applicable licence agreement. Unless expressly permitted by the licence agreement, parallel use of software licenced to ETH Zurich on the private and the office computer is forbidden.

Art. 9 Use of ICT resources outside the ETH Zurich campus

Employees working at home with the consent of the appropriate authority may use the ICT resources of ETH Zurich accordingly.

The use of portable ETH-owned devices, such as laptops, smartphones, etc., is permitted outside of the ETH Zurich campus. The IT Best Practice Rules must be complied with.

Art. 10 Private use of software licenced to ETH Zurich

revoked

Art. 11 Data protection

The processing of personal data is permitted only to pursue ETH Zurich’s statutory missions in compliance with the data protection regulations.

The disclosure of personal data to third parties for authorisation and authentication of electronic services is permitted, provided however that this data is not sensitive and required to use the services.

Mass mailings to ETH internal addressees outside of one’s own organisational unit for information purposes shall be carried out upon written request by the Office of the Rector or IT Services (on behalf of Corporate Communications/HR). Mass mailings may be initiated upon request by the Executive Board or for

---

3 Explanatory information from the IT Services department available from https://idesnx.ethz.ch/SpecialInfo/Heimnutzung_SW.pdf, last accessed on 1 October 2018. The respective licensing conditions apply.

37 Wording in accordance with decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019

38 Pursuant to Art. 43 (3) of the Personnel Ordinance for the ETH Domain (PVO-ETH; SR 172.220.113)

39 Wording in accordance with decision of the ETH Zurich Executive Board of 17 September 2013, effective as of 1 October 2013

40 Wording in accordance with decision of the ETH Zurich Executive Board of 17 September 2013, effective as of 1 October 2013

41 Wording in accordance with decision of the ETH Zurich Executive Board of 17 September 2013, effective as of 1 October 2013

42 Wording in accordance with decision of the ETH Zurich Executive Board of 17 September 2013, effective as of 1 October 2013

43 According to the legal definition of the Federal Act on Data Protection of 19 June 1992 (SR 235.1), personal data includes all data which refers to a certain or determinable natural or legal person.

44 Federal Act on Data Protection of 19 June 1992 (DSG; SR 235.1); Ordinance to the Federal Act on Data Protection of 14 June 1993 (VDSG; SR 235.11); Art. 59 et seq. of Personnel Ordinance (PVO-ETH; SR 172.230.113). Also applicable are Art. 36a to 36e of the ETH Act (SR 414.110), the Regulation on the Processing of Personal Data Collected through the Use of the Electronic Infrastructure of the Federation (Verordnung über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen; SR 172.010.442) and the Guidelines on protecting and processing personal data at ETH Zurich; (RSETH 612)

45 Data within the meaning of Art. 3 c) of Federal Act on Data Protection (SR 235.1)
interdepartmental announcements of courses, etc. (e.g. course information of D-INFK/D-MATH, training instructions of SSHE).

4 When using web analysis tools (e.g. Google Analytics), the guidelines of the Swiss Federal Data Protection and Information Commissioner (FDPIC) must be complied with in any case.

5 Any question concerning data protection in general should be directed to the Legal Office.

Art. 12 Software copies

 revoked

Art. 13 Use of electronic communication resources

1 The confidentiality of messages transmitted through electronic media cannot be guaranteed.

2 Professional, official and business secrets and other confidential information (e.g. files of staff) may only be transmitted out of the ETH Zurich domain using secure ICT resources, in particular using appropriate encryption techniques, where available.

3 The electronic communication resources of ETH Zurich may not be used anonymously, or with a pseudonym, or a false sender.

4. Section: Security measures

Art. 14 Low-risk systems

1 Low-risk systems are systems containing data in accordance with Art. 23 (2) of the Directive on Information Security at ETH Zurich for which the basic measures in accordance with Art. 19 (1) of the Directive on Information Security at ETH Zurich are sufficient.

2 The system administrators responsible for such systems are required to ensure that the applicable IT Best Practice Rules issued by IT Services are complied with. They have to promptly report security problems, defects, etc., to the competent offices of IT Services or the IT support groups.

 revoked

---

46 Statement of the FDPIC of November 2012 on website evaluation tools (https://www.edoeb.admin.ch/edoeb/en/home.html). Any questions should be directed to the Legal Office or Corporate Communications.

47 Wording in accordance with decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019.

48 Editorial amendment, in effect since 1 April 2019.

49 See Art. 16 and 23 (1) of the Directive on Information Security at ETH Zurich (RSETZH 203.25); wording in accordance with decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019.

50 Wording in accordance with decision of the ETH Zurich Executive Board of 17 September 2013, effective as of 1 October 2013.

51 Wording in accordance with decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019.
Art. 14bis Access protection measures

1 Irrespective of the level of protection required in accordance with the Directive on Information Security at ETH Zurich, users shall be responsible for the confidentiality of personal access data and identification mechanisms, such as passwords, PINs, private keys, chip cards, physical keys, tokens, etc. They may not disclose or make available this information to other users. This provision applies in particular to the configuration of personal access data to ETH services that are not operated by ETH Zurich (e.g. mail gateway for mobile phones, external mail server that downloads mails from ETH mail servers).

2 In the event of a reasonable suspicion that access data or an identification mechanism has been disclosed or made available to unauthorised parties, or have been used by such parties, the user must promptly have his/her access blocked and report the incident to the system administrator.

3 The competent offices of IT Services, the IT support groups and the CSCS never request the user to disclose his/her access data by electronic means. If a user is requested to do so, it is an attempt to obtain confidential information for malicious intent (phishing). Such an incident must be promptly reported to the Service Desk of IT Services.

4 The system administrator shall be responsible for defining the requirements for access data and identification mechanisms (e.g. change of password). If greater protection is required, stricter requirements must be introduced.

Art. 15 High-risk systems

1 High-risk systems contain data in accordance with Art. 16 and 23 (1) of the Directive on Information Security at ETH Zurich.

2bis revoked

2 Such systems must be more rigorously protected from being accessed by unauthorised third parties in accordance with Art. 19 (2) and (3) of the Directive on Information Security at ETH Zurich.

3 The responsible system administrators must comply with the applicable IT Best Practice Rules issued by IT Services.

4-9 revoked

10 The loss or disclosure of ETH Zurich data related to administration, education and research within the meaning of Art. 15 (1) must be prevented. Thus, it is incumbent upon each user to ensure that the mobile data storage devices that he/she uses (CDs/DVDs, USB sticks, storage cards, flash storage devices, etc.) and the data on mobile devices are deleted in an appropriate manner and made unreadable before disposal. In case of theft or data loss, the employee’s supervisor and the CISO are to be informed. In the event of theft, the SSHE administrative department must also be notified. In addition, the IT Best Practice Rules issued by IT Services must be complied with.

---

52 Inserted by decision of the ETH Zurich Executive Board of 17 September 2013, effective as of 1 October 2013; wording in accordance with decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019.

53 Wording in accordance with decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019.

54 See also Appendix to BOT 1 (7)
Art. 15bis Integrity of ICT network

The ICT network of ETH Zurich may not be expanded or modified by users or third parties in an unauthorised manner. Exceptions to this require written consent from IT Services.

5. Section: Responsibility and liability

Art. 16 Responsibility

1 Every user shall be personally responsible for ensuring that her/his use of the ICT resources does not violate the provisions of this Acceptable Use Policy or of the applicable laws (e.g. criminal law, data protection regulations), or infringe third-party rights (e.g. copyrights, licence terms, personal rights).

2 revoked

Art. 17 Liability

1 Users are expected to use the ICT resources provided by ETH Zurich with all due care.

2 The technical and operating instructions issued by IT Services, by the IT support groups, by the CSCS, or by the system administrator, and the instructions issued by the CISO strictly apply to all users. Every user has to follow these instructions.

3 Unless the responsible bodies have given a guarantee in writing, ETH Zurich shall not be liable for any defects in the ICT resources and their consequences.

4 In any case, the user shall be liable for damages or technical disruptions in the ICT resources of ETH Zurich caused by his/her gross negligence or wilful misconduct. In case of non-intended use, the user concerned shall be liable also for slight negligence.

5 In case of grossly negligent or intentional infringement of third-party rights (in particular copyrights and licence terms), the user shall also be liable for any claims eventually brought against ETH Zurich by third parties.

6 In other respects, the Government Liability Act applies to the employees of ETH Zurich who use the ICT resources to carry out the Federation’s public tasks.

55 Wording in accordance with decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019.
56 E.g. through a connection to a third-party ICT network via a direct connection (e.g. to the internet) or by installing routers, switches, access point, firewalls, load balancers etc.
57 Wording in accordance with decision of the ETH Zurich Executive Board of 17 September 2013, effective as of 1 October 2013.
58 Wording in accordance with decision of the ETH Zurich Executive Board of 17 September 2013, effective as of 1 October 2013.
59 SR 170.32 (Verantwortlichkeitsgesetz)
6. Section: Abuse

Art. 18 Logging/Detection of abuses

1 The ICT resources maintain log files of the most important activities they are used to perform.

2 Upon instruction by the CISO, non-personally identifiable data contained in the log files may be viewed for spot checks to monitor compliance with the provisions of this Acceptable Use Policy.

2bis In work-related emails, the log file contains the subject line, date, time, sender and recipient addresses, etc. The users must clearly mark their private emails as “PRIVATE”, or save them in a separate folder.

3 To address detected or reasonably suspected abuses within the meaning of Art. 19, or to identify and correct technical malfunctions, and to ward off specific threats to the infrastructure, the data contained in the log files may be analyzed on behalf of the CISO with a view to personal references, in accordance with the applicable principles set forth in the Appendix of the Guidelines for Monitoring the Use of ICT Resources at ETH Zurich.

3bis The Head of the Safety, Security, Health and Environment administrative department is responsible for determining (data recording, sighting, securing) and potentially sanctioning (themselves or via criminal complaint) any abuses, security breaches or crimes via video recordings or electronic access control for buildings or sites of ETH Zurich. The provisions of this Section 6 of the BOT as well as the Appendix shall apply analogously unless any other standards take precedence.

4 Detailed provisions concerning records of user behaviour, responsibilities, recording of abuses, storage of usage data and analyses are set forth in the Appendix (Guidelines for Monitoring the Use of ICT Resources at ETH Zurich).

5 The users and system administrators are obliged to assist in investigating the cases of abusive and illegal use, and of damage.

Art. 19 Abuses

1 Any use of the ICT resources of ETH Zurich which disregards the provisions of this Acceptable Use Policy, or breaches applicable higher-level laws or infringes third-party rights constitutes an abuse.

2 In particular, abuses include the following and are forbidden:

   a) Processing, storing or transmitting illegal or immoral materials, such as violent images, pornography (Art. 197 of the Swiss Criminal Code “SCC” [SCC; SR 311.0]), incitement to crime or violence (Art. 259 SCC), violations of the freedom of faith and worship (Art. 261 SCC) or racial discrimination (Art. 261bis SCC).

   b) Writing, providing instruction in writing or intentionally distributing destructive programs or program parts within the meaning of Art. 144bis no. 2 SCC (viruses, worms, trojan horses, etc.). Providing instruction in writing such programs for teaching and research purposes may be permitted, provided appropriate measures against malicious use are taken, and subject to the prior written consent of the ETH Executive Board or of its designee.

   c) Unauthorised access into a computer system (Art. 143bis SCC, “Hacking”): Cracking passwords, scanning internal and external networks without authorisation in order to identify vulnerabilities.

---

60 Wording in accordance with decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019.
61 Wording in accordance with decision of the ETH Zurich Executive Board of 17 September 2013, effective as of 1 October 2013.
Data theft (Art. 145 SCC) and data damage (Art. 144bis no. 1 SCC);

Using the ICT resources of ETH Zurich in intentional breach of licence terms and copyrights;

Transmitting messages through electronic communication means with forged or falsified sender information (including technical address) or unsolicited promotions (spam);

Harassing or misleading members of ETH Zurich or third parties through messages transmitted by electronic communication means (e.g. with offensive, sexist, racist, defamatory or discriminatory content);

Setting up direct access to ETH Zurich communication networks (e.g. through modems or WLAN access points) without prior written consent of IT Services and the responsible system administrator;

Sending mass advertising without direct links to requested content and without prior consent of the clients, correct sender information or offer of a possibility to decline without problems and costs (spam); this provision does not apply to ETH internal mass mailings within the meaning of Art. 11(3) of this Acceptable Use Policy.

Serious abuses include:

a) abuses pursuant to paragraph 2a), b), c), d) where deliberate or intentional;

b) or other abuses where repeated.

The immediate supervisor and the system or network administrators are obliged to report any serious or repeated abuses to the CISO.

Art. 20 Consequences of abuses

Should an abuse within the meaning of Art. 19 of this Acceptable Use Policy be detected or reasonably suspected, the CISO may take the following measures:

a) Issue a warning for minor breaches of the applicable Acceptable Use Policy;\(^\text{63}\)

b) Suspend access to the ICT resources\(^\text{64}\) affected, as a precaution;

c) Block abusive and illegal data, and store and safeguard them as evidence;

d) Delete abusive and illegal data where this is required for security reasons.

As sanctions against abuses, the violators may have their access to the ICT resources suspended, or their use restricted or prohibited. These sanctions shall be imposed by decree. Sanctions shall be revoked if disciplinary proceedings have not been initiated, or a criminal complaint has not been lodged, within three months. Upon completion of the disciplinary proceedings, the sanctions, if any, shall be determined anew.

An appeal against the measures decreed pursuant to para. 2 can be filed with the ETH Appeals Commission (ETH Beschwerdekommission) within 30 days following the effective date.

\(^{62}\) E.g. Information Security Lab, D-INFK

\(^{63}\) Wording in accordance with decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019

\(^{64}\) See also point 4 of Appendix
In addition, disciplinary measures, civil proceedings (action for damages) or criminal complaints may be initiated or lodged against violators. In case of serious abuse (Art. 19 para 3), disciplinary proceedings will be opened in all cases. Particularly serious offences may result in exclusion or dismissal from ETH Zurich.

A serious abuse by students does not constitute a petty offence within the meaning of the Art. 8 of the ETH Zurich Disciplinary Code. For employees, any type of abuse shall be deemed a breach of duties under labour law.

ETH Zurich may charge the violator for the costs resulting from the abuses and their consequences, including investigation and imposition of sanctions (including investigation, court costs and attorney fees).

7. Section: Special provisions

Art. 21 Special provisions and instructions

In other respects, the users must comply with the following regulations, where applicable, in their then current version.

a) Any special instructions issued by the user units concerning use of individual systems, in particular concerning data protection and data security;

b) Implementing Provisions Concerning the Appearance of ETH Zurich on the Internet (ETH Zurich Internet Guidelines) of August 2009;

c) Guidance for inventory management at ETH Zurich of January 2019;

d) Standards for Responsibilities and System Maintenance of 6 February 2003;

e) Regulation on the Processing of Personal Data Collected through the Use of the Electronic Infrastructure of the Federation;

f) Art. 36a to Art. 36e of the ETH Act (Personnel Information Systems, Student Information Systems; managing personal data in research projects); and

g) IT Best Practice Rules issued by IT Services.
8. Section: Final provisions

Art. 22 Enforcement\(^{76}\)

*revoked*

Art. 23 Abrogation of previous regulations and effective date\(^{77}\)

1 The following decrees have been revoked:

a) Acceptable Use Policy for Telematics Resources (BOT) of 12 January 1999 (RSETHZ 203.21en).

b) Rules governing the Use of ETH Zurich IT Resources “at Home” of 12 September 1995 (SLB 120913-95).

c) Instructions on the Students’ Use of Computers of 20 October 1992/CAZ.

d) Software Use Guidelines for Teaching with IT Resources at ETH Zurich of 20 July 1987 (RSETHZ 305.50).

e) ETH Zurich IT Network of 13 September 1977 (RSETHZ 222.01).

f) Software Use Rules for Teaching with IT Resources at ETH Zurich of 15 July 1987 (RSETHZ 305.52).

g) Acceptable Use Policy for ETH Zurich Educational Computers of 15 September 1987 (RSETHZ 305.51).

h) Educational Software Use Guidelines for Teachers of 26 April 1988 (RSETHZ 305.53).

2 This decree is effective as of 1 May 2005.

Zurich, 19 April 2005

On behalf of the ETH Executive Board

President: Kübler
Representative: Kottusch

Partial revision of 26 March 2019, on behalf of the Executive Board:

________________________________________________________
President
Joël Mesot

________________________________________________________
Secretary General
Katharina Poiger Ruloff

\(^{76}\) Wording in accordance with decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019.

\(^{77}\) Editorial amendment, effective as of 1 April 2019.
Appendix

Guidelines for Monitoring the Use of ICT Resources at ETH Zurich

1. Data collection, storage and deletion

Technical prevention, raising awareness and involvement of members of ETH should be given priority over monitoring. ETH Zurich shall ensure that the protective technical measures are regularly updated to the latest state of the art.

If the ICT resources of ETH Zurich are used or ICT resources are operated on the latter’s behalf, any data collected may be recorded for the following purposes:

a. all data, including content of electronic mail: for backup purposes (backups);

b. data on the technical state of the ICT resources (e.g. patch statuses, virus protection notifications, vulnerability scans) and marginal data about their use:
   - to ensure information and service security,
   - to conduct maintenance of the electronic infrastructure,
   - to carry out spot checks for compliance with the BOT,
   - to record access to data collections,
   - to control costs;

c. data on entry and exit to and from buildings and rooms of ETH Zurich and times of stay: for security purposes.

To the extent required by the purpose of the analysis, data mentioned in para. 2 can be stored at the most as follows:

a. data mentioned in para. 2 (a): until the basic underlying information is filed in the ETH archives, if it is not included: 2 years

b. data mentioned in para. 2 (b): 2 years

c. data mentioned in para. 2 (c): 3 years

The collected data must be deleted by the competent bodies upon expiration of the storage period.

For electronic mail (email) data commercially or legally relevant to ETH Zurich, the statutory storage period of 10 years is applicable. ETH Zurich employees shall be responsible for storage or deletion of their electronic mail.

For processing and storage of data stored in the personnel and student information systems of ETH Zurich pursuant to Art. 36a and 36b of the ETH Act, the relevant implementation provisions of the ETH Board or of the ETH Zurich Executive Board are applicable.

78 Wording in accordance with decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019.
79 Recording for the purposes under Art. 57 of the Ordinance on the Organisation of the Government and the Federal Administration (GAOO; SR 172.010); editorial amendment effective as of 1 January 2019.
80 Art. 4 of the Regulation on the Processing of Personal Data Collected through the Use of the Electronic Infrastructure of the Federation of 22 February 2012 (SR 172.010.442).
81 The ETH Library has been given the function of public archives for ETH Zurich and the ETH Board pursuant to the Federal Act on Archiving (RSETHZ 420.1).
82 IT Services deletes the email archives on request by the employee to the Service Desk.
83 Guidelines for the Protection and Use of Personal Data at ETH Zurich of 15 November 2011 (RSETH 612).
The storage period and deletion of data on printers, scanners, etc., depend on the storage capacity of the device on which they are stored. These data must be deleted irrecoverably at latest at the time of transfer or disposal of the device.84

For the storage of research data, Art. 11 of the Guidelines for Research Integrity and Good Scientific Practice at the ETH Zurich is applicable.85

2. Responsibilities

2.1 IT operators and system administrators of the organisational units

a) To install and operate the ICT resources allowing to record data pursuant to Section 1 of this Appendix.

b) To carry out spot checks pursuant to Section 3 as instructed by the CISO.

c) To support the CISO and/or ITSO ITS in fulfilling his/her tasks pursuant to these Guidelines.

2.2 Network administrators
To support the IT security officer in fulfilling his/her tasks pursuant to these Guidelines.

2.3 IT Services of ETH Zurich:
To support the CISO in fulfilling his/her tasks pursuant to these Guidelines and to monitor the ICT resources (i.e. ICT network) of ETH Zurich.

2.4 IT Security Officer of IT Services (ITSO ITS)
Unless otherwise regulated in Art. 8 of the Directive on Information Security at ETH Zurich86, the ITSO ITS is specifically responsible for mandating the random checks on behalf of the CISO pursuant to Section 3 (1) of this Appendix.

2.5 Chief Information Security Officer (CISO)
Unless otherwise regulated in Art. 5 of the Directive on Information Security at ETH Zurich87, the CISO is specifically responsible for the following duties:

a) Contacting the Post and Telecommunications Surveillance Service (PTSS);

b) Instructing that spot checks be carried out in accordance with clause 3 (1) of this Appendix;

c) Taking preventive measures in accordance with clause 4 of this Appendix;

d) Deciding on the analysis of personally identifiable data in accordance with clause 5 (1a) of this Appendix;

e) Questioning members of ETH Zurich in accordance with clause 3 (2) of this Appendix;

f) Ordering the recording of personally identifiable data in consultation with the responsible direct line manager (for employees) / the Director of Studies (for students) in accordance with clause 5.

84 Art. 5 of the Regulation on the Processing of Personal Data Collected through the Use of the Electronic Infrastructure of the Federation of 22 February 2012 (SR 172.010.442).

85 Guidelines for Research Integrity and Good Scientific Practice at ETH Zurich (RSETHZ 414en)

86 Directive on Information Security at ETH Zurich of 9 April 2018 (RSETHZ 203.25en)

87 Directive on Information Security at ETH Zurich of 9 April 2018 (RSETHZ 203.25en)
2bis Analysis of recorded log files

The analysis of the recorded log files can concern both non-personally identifiable data and personally identifiable data and must comply with the principles laid down in these Guidelines.

3. Spot checks of non-personally identifiable data

1 On instruction by the CISO, the system administrators may carry out spot checks of non-personally identifiable data to monitor the use of the ICT resources.

1bis For the purpose of monitoring ICT security, the analysis of data not connected to individuals by name (anonymously or pseudonymously) can be carried out by IT Services at any time and without the CISO’s instruction in accordance with Art. 1 (2) (b).

2 When monitoring email traffic, the content of private emails of ETH members may not be accessed (Art. 18 (2bis)). If the private and work-related emails are not marked as such, and if the address elements give no clue or indication as to the nature of certain messages, ETH Zurich may assume that the email is work-related. In case of doubt, the issue is to be clarified with the ETH member in question.

3 The abuses actually detected or reasonably suspected in such spot checks must be promptly reported by the system administrators to the CISO.

4. Protective and precautionary measures

1 If spot checks of non-personally identifiable data give rise to a reasonable suspicion that an abuse within the meaning of Art. 19 BOT has been taking place which threatens to jeopardise substantially the use of ETH Zurich ICT resources, or cause damages to ETH Zurich, or to its members, or to third parties, the CISO shall be authorised to take the following protective and precautionary measures:

   a) To block access to the ICT resources in which the detected abuse occurs or which are affected by it;

   b) To block the data, and store and safeguard them as evidence.

2 In emergency cases, the ITSO ITS may also request that the measures set forth in para. 1 be taken; the CISO must be promptly notified and shall decide whether the measures taken should remain in effect.

5. Analysis of personally identifiable data

1 If the analysis of non-personally identifiable data reveals abuses within the meaning of Art. 19 BOT, or gives rise to a reasonable suspicion of such abuses, the CISO may direct that recorded personally identifiable data be analysed according to the following principles:

   a) Depending on the seriousness of the abuse, together with the immediate line manager and the Head of HR (employees) or the relevant personnel manager, or with the Director of Studies or the Rector (students), he/she may decide whether the personally identifiable data are to be analysed at once to identify the violator, or only when the abuse is repeated.

   b) In any case, further analyses may be carried out only after the person concerned has been informed about the suspected abuse.

   c) If the suspected abuse could reasonably constitute a criminal offence pursuant to the Swiss Criminal Code, the relevant pieces of evidence consisting of log files and, if any, backups, must be secured.

---

88 Art. 57o (1a) of the Ordinance on the Organisation of the Government and the Federal Administration (GAOO; SR 172.010) in conj. with Art. 11 of the Regulation on the Processing of Personal Data Collected through the Use of the Electronic Infrastructure of the Federation of 22 February 2012 (SR 172.010.442).
such cases, follow-up investigations of personally identifiable data are not permitted, and are the
sole responsibility of the competent criminal prosecution authorities. If the guilty parties are ETH
teaching staff or employees, the decision whether to lodge a complaint rests with the President.

d) revoked

Investigations conducted to detect and correct technical malfunctions in the ICT resources and to address
concrete threats to that infrastructure are permitted only where they are indispensable to search for the
cause of the malfunction, or to remedy it, or to ward off a real threat, namely when:

a) the use of the ICT resources has been precluded or substantially impaired by a defect or excessive
use by a single user; or

b) there exists a direct risk of damage to the ICT resources, or to the data of the users (spread of
malware).

6. Sanctions

The responsibility for imposing sanctions for abuses is governed by Art. 20 BOT.

7. Confidentiality

The data collected pursuant to section 1 of this Appendix must be treated in confidence; the system
administrators must take the appropriate measures to prevent members of ETH Zurich and third parties from
gaining unauthorised access to, or knowledge of, such confidential information.

The results of the spot checks and of the analysis of personally identifiable data as well as the protective
and precautionary measures must be kept in strict confidence by the persons involved. Information may be
disclosed only when and to the extent that the disclosure is permitted pursuant to the present and future
applicable provisions.

8. Monitoring of the telephone network

The CISO is responsible for contacting the Post and Telecommunications Surveillance Service (PTSS)
operated by the Federation. The PTSS monitors post and telecommunications in order to investigate
serious crimes. The CISO and the other units of ETH Zurich also shall promptly inform the Legal Office if
they are contacted by the PTSS, or by the criminal prosecution authorities in relation to the monitoring of
the telephone network.

Monitoring shall specifically be conducted pursuant to Arts. 4, 18 et seq., 28 and 51 et seq. of the Ordinance
on the Surveillance of Post and Telecommunications of 15 November 2017 (VÜPF; SR 780.11; not available in
English).

---

89 Art. 14(2) of the Procedural Rules of the ETH Executive Board (RSETH 202.3).
90 Art. 57o (1b) of the Ordinance on the Organisation of the Government and the Federal Administration (GAOO; SR
172.010) in conj. with Art. 12 of the Regulation on the Processing of Personal Data Collected through the Use of the
Electronic Infrastructure of the Federation (SR 172.010.442).