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 Telematics Resources ("BOT") and Appendix of April 19, 2005 (Status as of September 17, 2013)

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 Telematics Resources
(ETH Zurich „BOT“)

dated April 19, 2005 (status as of September 17, 2013)

The ETH Zurich Executive Board,

pursuant to Art. 4(1)c) of the Ordinance Concerning the Organization of the Zurich Federal Institute of Technology of December 16, 2003[1],

decrees::

1. Section: General Provisions

Art. 1 Purpose

[1]The telematics resources of the Zurich Federal Institute of Technology 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 telematics resources.

Art. 2 Definitions[2]

[1]The term “*telematics resources”* comprises all information and telecommunication resources owned by the ETH Zurich. In particular, it refers to systems, devices and services of the ETH Zurich used for electronic data processing (e.g. data processing equipment, network components, data storage devices, printers, scanners, telecommunication networks and related software), including non-ETH Zurich systems (e.g. private laptops) connected to the data network of the ETH Zurich.

[2]The term “*systems*” refers to any software and hardware, including portable systems.

[3]The term *“data”* includes personal and academic data.

[4]The term “*users”* includes all members of the ETH Zurich (Art. 13 of the ETH Law) and certain third parties (e.g. guests, congress participants, affiliated organizations, library users at the public work stations, employees of the ETH Zurich’s spin-off companies or of other companies, provided a contractual arrangement exists to this effect, professors emeritus and retired employees) who are authorized to use the telematics resources of the ETH Zurich.

---

[1] RSETHZ 201.021
[2] As amended by decision of the ETH Zurich Executive Board of September 17, 2013, effective as of October 1, 2013

[5]The term "*electronic communication resources*" includes telephone, fax, email, SMS, instant messaging, video conference systems and similar resources.

[6]The term "*organizational units"* refers to the central or decentralized bodies of the ETH Zurich established by the Executive Board pursuant to the ETH Organization Ordinance (Organisationsverordnung – OV) of December 12, 2003[3] (e.g. departments, institutes, infrastructure units, staff positions, independent chairs) and the education and research facilities outside the departments established pursuant to Art. 61 OV (e.g. CSCS).

[7]The term "*private use*" refers to any use of the telematics 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.

[8]The term "*analysis of anonymous data*" refers to the statistical analysis of the log files that does not use personal data.

[9]The term "*analysis of pseudonymous or non-personally identifiable data*" refers to the analysis of the log files of pseudonymized identifiable persons. The pseudonym must protect the identity of the person in question in the phase of monitoring that does not involve personal data.

[10]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 telematics resources.

[11]The term "*system and network administrators*" refers to the specialists described in Art. 3 of the *Standards for Responsibilities and System Maintenance*[4].

Art. 3 Scope[5]

The Policy applies to any use or shared use, whether by **ETH Zurich members** or **third parties,** of all ETH Zurich-owned telematics 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 Department, IT Support Groups and CSCS[6]

[1]The ETH Zurich IT Services Department (hereinafter "*IT Services*") shall provide IT services to the individual users and to the ETH Zurich organizational units and, in the area of IT security, be responsible in particular for the following functions:

a) Implement the technical measures to ensure the integrity of the telematics resources, including identifying and documenting technical defects and coordinating the efforts to remedy or circumvent such defects;

b) Train and inform the users;

c) Monitor for compliance with the *Standards for Responsibilities and System Maintenance*[7] and with the IT Best Practice Rules pursuant to Art. 15 (3);

d) Coordinate the implementation of technical and organizational innovations;

[3] RSETZ 201.201
[4] RSETHZ 203.23
[5] As amended by decision of the ETH Zurich Executive Board of September 17, 2013, effective as of October 1, 2013
[6] As amended by decision of the ETH Zurich Executive Board of September 17, 2013, effective as of October 1, 2013
[7] RSETHZ 203.23

e) Provide the necessary encrypting techniques (Art. 13 (2));

f) *revoked*

g) Grant authorizations pursuant to Art. 15bis;

h) Receive reports by users concerning security problems (Art. 14 and 15);

i) Manage the information exchange within the ETH Zurich and the ETH domain and between the universities, SWITCH and the federal authorities;

j) Assist the IT security Officer in fulfilling his/her tasks pursuant to the *Guidelines for Monitoring the Use of Telematics Resources at the ETH Zurich* attached as Appendix;

k) Detect, document and correct security defects (Art. 14 (2)) in den central organizational units;

l) Clarify the admissibility of a commercial use of the telematics resources and conclude the relevant agreements (Art. 8 (6));

m) Develop a concept of Information Security Management and define a strategy for complete information security at the ETH Zurich.

[2]The IT support groups in the 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).

[3] In its function as national center, the Swiss National Supercomputing Center (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 IT security Officer[8]

[1]The ETH Zurich Executive Board shall appoint the IT security officer for the telematics resources. He/she shall report directly to the President[9].

[2]*revoked*

[3]The IT security officer shall be responsible in particular for the following functions:

a) *revoked*

b) Coordinate and supervise the implementation of security measures (Art. 14 et seq.);

c) Investigate suspected abuses, including collecting data which could be used as evidence (Art. 18 et seq.);

d) Impose sanctions in case of abuse (Art. 20);

e) Conduct supervision activities pursuant to the *Guidelines for Monitoring the Use of Telematics at the ETH Zurich* attached as Appendix.

[4]The IT security officer may delegate tasks related to compliance with the Acceptable Use Policy to the IT services.

[5]In case of minor violations of the present Acceptable Use Policy, the IT security officer may issue a warning before imposing sanctions pursuant to Art. 20.

Art. 6 System and Network Administrator[10]

[8] As amended by decision of the ETH Zurich Executive Board of September 17, 2013, effective as of October 1, 2013
[9] Art. 27(2)d) OV
[10] Art. 27(2)d OV

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

[2]Every organizational 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 telematics resources.

[3]Based on the feedback by the users, the system administrator shall identify the systems that contain high-risk data (Art. 15 (1)) in his/her organizational unit, and delete the data contained on the non-mobile data storage devices (hard disks, etc.) before transfer or disposal (Appendix to BOT clause 1.7).

[4]The other tasks of the system administrator and of the network administrator are set forth in the *Standards for Responsibilities and System Maintenance*[11] and in the *Guidelines for Monitoring the Use of the Telematics Resources at the ETH Zurich* attached to this Acceptable Use Policy as Appendix.

[5]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[12]

[1]The Corporate Communications unit shall be responsible for the presentation of ETH Zurich and of its organizational units on the Internet or Intranet. It shall issue implementation provisions on the Use Policy (BOT).[13]

[2]In this context, the Corporate Communications unit must comply with the regulations concerning equal treatment of disabled people.[14]

[3]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 Use Purpose and Use Authorization[15]

[1]Use of the telematics 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 authorization.

[2]The users must restrict their use of the telematics resources to the appropriate extent and to the permitted purposes.

[3]*revoked*

[4]*revoked*

[5]Without the written consent of the responsible system administrator, the users may not perform any modification to the telematics resources provided by the ETH Zurich, in particular changes and

[11] RSETHZ 203.23
[12] As amended by decision of the ETH Zurich Executive Board of September 17, 2013, effective as of October 1, 2013
[13] ETH Zurich Internet Guidelines of May 1,1999 (RSETHZ 203.22)
[14] Law on Equal Treatment of Disabled People, BehiG, of December 13, 2003 (SR 151.3); Decree on Equal Treatment of Disabled People, BehiV, of November 19, 2003 (SR 151.31)
[15] As amended by decision of the ETH Zurich Executive Board of September 17, 2013, effective as of October 1, 2013

modifications to software programs and deactivation, circumvention or removal of security mechanisms. This does not apply to the modifications involved in the proper use of the telematics resources.

[6]Commercial use (e.g. pursuant to spin-off agreements) is permitted where conditions have been contractually agreed in advance, provided the existing contracts between the ETH Zurich and the clients allow it. Any costs thereby incurred shall be borne by the clients.

[6bis]Operation and use of the supercomputing infrastructure at the CSCS or the use of telematics resources within the framework of a research cooperation shall be contractually agreed upon.

[7]Telematics resources are to be disposed of pursuant to the ETH Zurich Equipment Management Guidelines of January 1, 2004.[16]

Art. 8bis Private Use[17]

[1]Use of the ETH Zurich's telematics 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 commercial nature, and does not damage the reputation of the ETH Zurich.

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

[3]On the public ETH web pages, private personal contents of ETH members are not allowed, except for curriculum vitae, or publications, etc. of researchers. The IT services can provide centralized systems required to create personal websites.

[4]Software licensed to the ETH Zurich may be used privately by ETH Zurich employees on an at least 50% basis, and by the students matriculated at the ETH Zurich, if permitted by the applicable software agreement[18]. The right to install software on a private computer is governed by the applicable license agreement. Unless expressly permitted by the license agreement, parallel use of software licensed to the ETH Zurich on the private and the office computer is forbidden.

Art. 9 Use of Telematics Resources outside the ETH Zurich Campus

[1]The employees working at home[19] with the consent of the appropriate authority may use the telematics resources of the ETH Zurich accordingly.

[2]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[20].

Art. 10 Private Use of Software Licensed to the ETH Zurich[21]

revoked

[16] RSETHZ 220
[17] Inserted by decision of the ETH Zurich Executive Board of September 17, 2013, effective as of October 1, 2013
[18] The applicable list can be found under: http://id.ethz.ch/services/list/einkauf/heimnutzung
[19] Pursuant to Art. 43(3) PVO (SR 172.220.113)
[20] As amended by decision of the ETH Zurich Executive Board of September 17, 2013, effective as of October 1, 2013
[21] As amended by decision of the ETH Zurich Executive Board of September 17, 2013, effective as of October 1, 2013

Art. 11 Data Protection[22]

[1]Processing of personal data[23] is permitted only to pursue ETH Zurich's statutory missions in compliance with the data protection regulations.[24]

[2]The disclosure of personal data to third person for authorization and authentication of electronic services is permitted, provided however that this data is not sensitive[25] and required to use the services.

[3]Mass mailings to ETH internal addressees **outside of** one's own organizational unit for information purposes shall be carried out upon written request by the Office of the Rector or the IT services (on behalf of HK/HR). Mass mailings may be initiated upon request by the Executive Board or for interdepartmental announcements of courses, etc. (e.g. course information of D-INFK/D, training instructions of SGU).

[4]When using web analysis tools (e.g. Google Analytics), the guidelines of the Swiss Data Protection Commissioner (EDOEB) must be complied with in any case[26].

[5]Any question concerning data protection in general should be directed to the legal department.

Art. 12 Software Copies

Unless otherwise expressly stated in the license terms or the copyright law[27], duplicating in whole or part of the software licensed to the ETH Zurich (programs and documentation) is prohibited, irrespective of its origin.

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 appropriate encryption techniques.

[3]The electronic communication resources of the ETH Zurich may not be used anonymously, or with a pseudonym, or a false sender[28].

4. Section: Security Measures

Art. 14 Low-Risk Systems[29]

[1]**Low-risk** systems are systems containing data which do not require special protective measures.

---

[22] As amended by decision of the ETH Zurich Executive Board of September 17, 2013, effective as of October 1, 2013
[23] According to the legal definition of the Data Protection Law of June 19, 1992 (SR 235.1), personal data includes all data which refers to a certain or determinable natural or legal person
[24] Data Protection Law of June 19, 1992 (SR 235.1); Data Protection Decree of June 14, 1993 (SR 235.11); Art. 59 et seq. of Personnel Ordinance (SR 172.230.113). Also applicable are Art. 36a and 36b of the ETH Law, the Regulation on the Processing of Personal Data Collected through the Use of the Electronic Infrastructure of the Federation (SR 172.072) and the Directives on the Protection and Use of Personal Data of the ETH Zurich (RSETH 612)
[25] Data within the meaning of Art. 3 c) of Data Protection Law (SR 235.1)
[26] Statement of the EDOEB of October 10, 2011 on website evaluation tools (www.edoedb.admin.ch). Any question should be directed to the legal department or the corporate communications unit
[27] Art. 24 of Copyright Law of October 9, 1992 (SR 231.1); backup copies are allowed
[28] As amended by decision of the ETH Zurich Executive Board of September 17, 2013, effective as of October 1, 2013
[29] As amended by decision of the ETH Zurich Executive Board of September 17, 2013, effective as of October 1, 2013

[2]The system administrators responsible for such systems are required to ensure that the applicable best practice rules issued by the IT services are complied with. They have to promptly report security problems, defects, etc., to the competent offices of the IT services or the IT support groups.

[3]*revoked*

Art. 14bis Access Protection Measures[30]

[1]The users shall be responsible for the confidentiality of personal access data und 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 the ETH Zurich (e.g. mail gateway for Blackberry cellular phones, external mail server that downloads mails from ETH mail servers, etc.).

[2]In the event of a reasonable suspicion that access data or an identification mechanism has been disclosed or made available to unauthorized 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 the 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 the 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[31]

[1]**High-risk** systems contain data, the loss of which would substantially impair the pursuit of the ETH Zurich's statutory missions, or result in substantial recovery costs.

[1bis]Based on the feedback by users, each organizational unit of the ETH Zurich shall identify the systems in its own area that contain high-risk data.

[2]Such systems must be more rigorously protected from being accessed by unauthorized third parties. This applies to access to the applications and data and to physical access to the computers themselves.

[3]The responsible system administrators must comply with the applicable IT best practice rules issued by the IT services.

[3]*revoked*

[4]*revoked*

[5]*revoked*

[6]*revoked*

[7]*revoked*

[30] Inserted by decision of the ETH Zurich Executive Board of September 17, 2013, effective as of October 1, 2013
[31] As amended by decision of the ETH Zurich Executive Board of September 17, 2013, effective as of October 1, 2013

[8]*revoked*

[9]revoked

[10]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 und made illegible before disposal[32]. In case of theft or data loss, the employee's supervisor and the IT security officer are to be informed. In addition, the IT best practice rules issued by the IT services must be complied with[33].

Art. 15bis Direct Access[34]

Installation and use of direct access to non-ETH Zurich communication networks and installation of direct access to ETH Zurich's own communication networks (e.g. via access points) are subject to the written consent of the IT services.

5. Section: Responsibility and Liability

Art. 16 Responsibility[35]

[1]Every user shall be personally responsible for ensuring that her/his use of the telematics 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, license terms, personal rights).

[2]*revoked*

Art. 17 Liability

[1]It is expected that the users use the telematics resources provided by ETH Zurich with all due care.

[2]The technical and operating instructions issued by the IT services, by the IT support groups, by CSCS, or by the system administrator, and the instructions issued by the IT security officer strictly apply to all users. Every user has to follow these instructions[36].

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

[4]In any case, the user shall be liable for damages or technical disruptions in the telematics resources of the ETH Zurich caused by his/her gross negligence or willful 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 license terms), the user shall also be liable for any claims eventually brought against ETH Zurich by third parties.

---

[32] Cf. also Appendix 1 to BOT 1(7)
[33] See Article 21
[34] Inserted by decision of the ETH Zurich Executive Board of September 17, 2013, effective as of October 1, 2013
[35] As amended by decision of the ETH Zurich Executive Board of September 17, 2013, effective as of October 1, 2013
[36] As amended by decision of the ETH Zurich Executive Board of September 17, 2013, effective as of October 1, 2013

[6]In other respects, the Law on Responsibility applies to the employees of the ETH Zurich who use the telematics resources to carry out the Federation's public tasks.[37]

6. Section: Abuse

Art. 18 Logging/Detection of Abuses[38]

[1]The telematics resources maintain log files of the most important activities.

[2]Upon instruction by the IT security officer, 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 concrete threats to the infrastructure, the IT security officer may use the personally identifiable data contained in the log files to identify the violators, in accordance with the applicable principles set forth in the Appendix: *Guidelines for Monitoring Use of Telematics Resources at the ETH Zurich*.

[4]Detailed provisions concerning records of user behavior, responsibilities, recording of abuses, storage of usage data and analyses are set forth in the Appendix to this Acceptable Use Policy.

[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[39]

[1]Any use of the telematics resources of the 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 Penal Law – Schweizerisches Strafgesetzbuch – "StGB"), incitement to crime or violence (Art. 259 StGB), violations of the freedom of faith and worship (Art. 261 StGB) or racial discrimination (Art 261bis StGB).

b) Writing, providing instruction in writing or intentionally distributing destructive programs or program parts within the meaning of Art. 144bis no. 2 StGB (viruses, worms, trojans, 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) Unauthorized access into a computer system (Art. 143bis StGB, „Hacking"): Cracking passwords, scanning internal and external networks without authorization in order to identify vulnerabilities (e. g. port scanning), conceiving and executing strategies to disrupt

[37] SR 170.32
[38] As amended by decision of the ETH Zurich Executive Board of September 17, 2013, effective as of October 1, 2013
[39] As amended by decision of the ETH Zurich Executive Board of September 17, 2013, effective as of October 1, 2013

networks and computers (e. g. denial of service attacks). In particular cases, “hacking” may be permitted in a secure test environment for teaching and research purposes[40], subject to the prior written consent of the ETH Executive Board or its designee; the responsible system administrator may scan a restricted area for vulnerabilities in order to eliminate them.

d) Data theft (Art. 145 StGB) and data damage (Art. 144bis no. 1 StGB);

e) Using the telematics resources of ETH Zurich in intentional breach of license terms and copyrights;

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

g) Harassing or misleading members of ETH Zurich or third parties through messages transmitted by electronic communication means (e. g. offending, sexist, racially offensive, defamatory or discriminating messages);

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

i) 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.

[3]The serious abuses include:

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

b) or other abuses where repeated.

[4]The immediate supervisor and the system or network administrators are obliged to report any serious or repeated abuses to the IT security officer

Art. 20 Consequences of Abuses

[1]Should an abuse within the meaning of Art. 19 of this Acceptable Use Policy be detected or reasonably suspected, the IT security officer may take the following measures:

a) Suspend the access to the telematics resources[41] affected as a precaution;

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

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

[2]As sanctions against abuses, the violators may have their access to the telematics resources suspended, or their use restricted or prohibited. These sanctions shall be imposed by decree. The violators shall have their sanctions 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.

[3]An appeal against the measures decreed pursuant to para. 2 can be filed with the ETH Complaint Committee (ETH Beschwerdekommission) within 30 days following effective date.

[4]In addition, disciplinary measures[42], civil proceedings (action for damages) or criminal complaints may be initiated or lodged against violators[43]. In case of serious abuse (Art. 19 para 3), disciplinary

[40] e. g. Information Security Lab, D-INFK
[41] See also point 4 of Appendix

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 Rules[44]. For employees, any type of abuse shall be deemed a breach of duties under labor law[45].

[6]The costs resulting from the abuses and their consequences, including investigation and imposition of sanctions (including investigation, court costs and attorney fees) may be charged to the violator by the ETH Zurich.

7. Section: Special Provisions

Art. 21 Special Provisions and Instructions[46]

[1]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 the ETH Zurich on the Internet (ETH Zurich Internet Guidelines) of August 2009[47];

c) Instructions by the Vice President Finance and Controlling at the ETH Zurich of January 1, 2004[48];

d) Standards for Responsibilities and System Maintenance of February 6, 2003[49];

e) Regulation on the Processing of Personal Data Collected through the Use of the Infrastructure of the Federation[50];

f) Art. 36a (Personnel Information Systems) and Art. 36b (Student Information Systems) of the ETH Law [51]

g) IT Best Practice Rules issued by the IT services of August 2009 http:// www.id.ethz.ch/documentation/rechtliches/IT-Best_Practice_Rules.pdf)

8. Section: Final Provisions

Art. 22 Enforcement[52]

The units of ETH Zurich, particularly the IT services, the Security, Health and Environment unit, the ETH library, CSCS,the IT support groups of the departments as well as Corporate Communications may, on the basis of this document, issue additional rules within their respective sphere of competence.

---

[42] Students: pursuant to Art. 3 of ETH Zurich Disciplinary Rules of November 2, 2004 (SR 414.138.1); employees: pursuant to Art. 58a of Personnel Ordinance for the ETH Zone of March 15, 2001 (SR 172.220.113)
[43] The procedure
[44] SR 414.138.1
[45] Art. 25
[46] As amended by decision of the ETH Zurich Executive Board of September 17, 2013, effective as of October 1, 2013
[47] RSETH 203.22; the guidelines are under review at the moment
[48] RSETH 220
[49] RSETHZ 203.23
[50] SR 172.072
[51] SR 414.110
[52] As amended by decision of the ETH Zurich Executive Board of September 17, 2013, effective as of October 1, 2013

Art. 23 Abrogation of Previous Regulations and Effective Date

[1]The following decrees are revoked:

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

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

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

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

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

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

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

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

[2]This decree is effective as of Mai 1, 2005.

Zurich, April 19, 2005

On behalf of the ETH Executive Board

President: Kübler

Representative: Kottusch

Appendix[53]

Guidelines for Monitoring the Use of Telematics Resources at the ETH Zurich

1. Data Collection, Storage and Deletion

[1]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.

[2]The data that are collected through the use of the telematics resources by the ETH Zurich or on its behalf are collected for the following purposes[54]:

a. all data, including content of electronic mail: for backup purposes (backups);
b. data on use of the telematics resources (metadata):
   - 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 the ETH Zurich and times of stay: for security purposes.

[3]To the extent required by the purpose of the analysis, data mentioned in para. 2 can be stored at the most as follows:[55]

a. data mentioned para. 2(a): until the basic underlying information is filed in the ETH archives[56]; if it is not included: 2 years:
b. data mentioned in para. 2(b): 2 years
c. data mentioned to para. 2(c): 3 years

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

[5]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[57] of their electronic mail.

[6]For processing and storage of data stored in the personnel and student information systems of ETH Zurich pursuant to Art. 36a and 36b of ETH Law, the relevant implementation provisions of ETH Council or of the ETH Zurich Executive Board[58] are applicable.

[7]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[59].

---

[53] As amended by decision of the ETH Zurich Executive Board of September 17, 2013, effective as of October 1, 2013
[54] Within the meaning of Art. 57 RVOG (SR 172.010)
[55] Art. 4 of the Regulation on the Processing of Personal Data Collected through the Use of the Electronic Infrastructure of the Federation (SR 171.072)
[56] The ETH Library has been given the function of public archives pursuant to the Federal Law on Archives; RSETH 420.1
[57] The email archives are deleted by the IT services on request to the service desk
[58] Guidelines for the Protection and Use of Personal Data at ETH Zurich of November 15, 2011 (RSETH 612)

[8]For the storage of research data, Art. 11 of the Guidelines for Research Integrity and Good Scientific Practice at the ETH Zurich is applicable.[60]

2. Responsibilities

2.1 System Administrators of the Organizational Units

a) To install the telematics 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 IT security officer.

c) To support the IT security officer 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 the ETH Zurich:

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

2.4 IT Security Officer

a) To maintain contact with the federal communication authorities;

b) To mandate the random checks pursuant to Section 3;

c) To take the precautionary measures pursuant to Section 4;

d) To decide whether the personally identifiable data contained in the log files are to be used pursuant to Section 5 a);

e) To interview members of ETH Zurich pursuant to Section 5 d);

f) In consultation with the responsible direct superiors (for employees) or with the Rector (for students), to give instructions to collect personally identifiable data pursuant to Section 5 b).

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 IT security officer, the system administrators may carry out spot checks of non-personally identifiable data to monitor the use of the telematics resources.

[1bis]Basically, for the purpose of monitoring network security, analysis of anonymous data can be carried out at any time and without the security administrator's instruction.

[59] Art. 4 of the Regulation on the Processing of Personal Data Collected through the Use of the Electronic Infrastructure of the Federation (SR 172.072)
[60] RSETHZ 414

[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 security administrator.

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 jeopardize substantially the use of ETH Zurich telematics resources, or cause damages to ETH Zurich, or to its members, or to third parties, the IT security officer shall be authorized to take the following protective and precautionary measures:

a) To block the access to the telematics 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 head of the group “Network Security” of ETH Zurich IT services may also request that the measures set forth in para. 1 be taken; the IT security officer 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 IT security officer may direct that recorded personally identifiable data be analyzed according to the following principles:

a) Depending on the seriousness of the abuse, together with the immediate superior (employees) and with the director of the department or with the competent head of personnel, or with the Rector (students), he/she may decide whether the personally identifiable data are to be analyzed at once to identify the violator, or only if 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[61].

c) If the suspected abuse could reasonably constitute a **criminal offence** pursuant to the Swiss Penal Code, the relevant pieces of evidence consisting of log files and, if any, backups, must be secured. **In 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 culprits are ETH employees, the decision whether to lodge a complaint rests with the President[62].

d) *revoked*

[2]Investigations conducted to detect and correct malfunctions in the telematics 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:

[61] Art. 570(2)a) RVOG
[62] Art. 14(2) of the Procedural Rules of the ETH Executive Board (RSETH 202.3)

a) the use of the telematics 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 telematics resources, or to the data of the users (spread of malware).[63]

6. Sanctions

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

7. Confidentiality

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

[2]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

In the course of investigation of criminal offences, the IT security officer shall contact the Telephone Monitoring Service operated by the Federation[64]. The IT security officer and the other units of ETH Zurich also shall promptly inform the legal department when they are contacted by this service, or by the criminal prosecution authorities in the context of monitoring the telephone network.

[2]Monitoring shall be designed and conducted pursuant to Art. 28 and 29 of the Decree on Monitoring the Postal and Telephone Network of October 31, 2001 (VüPF; SR 780.11).

[63] Art. 12 of the Regulation on the Processing of Personal Data Collected through the Use of the Electronic Infrastructure of the Federation (SR 172.072)
[64] Art. 28 and 29 of the Decree on Monitoring the Post and Telephone Traffic (VÜPF; SR 780.11)