ETH Zurich Acceptable Use Policy for Telematics Resources (“BOT”) and Appendix of April 19, 2005

ETH Zurich Acceptable Use Policy for Telematics Resources (ETH Zurich „BOT“)

dated April 19, 2005

The ETH Zurich Executive Board,

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

promulgates:

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 disruptions to and misuse of ETH Zurich telematics resources.

Art. 2 Definitions

[1]*Telematics resources* include all computing devices, pieces of equipment and services of the ETH Zurich used for electronic data processing, such as hardware, software, networks, data, documentation, consultancy and training services, including non-ETH Zurich devices (e.g. private laptops) connected to the data network[2] of the ETH Zurich.

[2]*Application* means any use of telematics resources.

[3]*Data* includes personal and academic data.

[4]*Users* are all members of the ETH Zurich (Art. 13 of the ETH law) and third parties (e.g. guests, congress participants, affiliated organizations, library users at the public work stations) who are authorized to use the telematics resources of the ETH Zurich.

[5]*Electronic communication means* include telephone, fax, e-mail, SMS, instant messaging, video conference systems and similar means.

[6]*User unit* means any organizational unit of the ETH Zurich (e.g. departments, institutes, chairs, infrastructure units, staff agencies).

[1] RSETHZ 201.021

[2] For more details, see: http://www.id.ethz.ch/services/list/netzwerk/used_ipnetze/index

Art. 3 Scope

This Decree 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 Services

1The ETH Zurich IT department is specifically responsible for the following:

a) Implementing 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) Training and informing the users;

c) Monitoring for compliance with the *Standards for Responsibilities and System Maintenance*[3];

d) Coordinating the implementation of technical and organizational innovations;

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

f) Receiving reports by the system administrators concerning high-risk applications and maintaining a list of such applications (Art. 6 para. 3);

g) Granting authorizations (Art. 15 para. 8);

h) Receiving reports from users concerning security problems (Art. 14 and 15);

i) Managing the information exchange within the ETH Zurich and the ETH area and between the universities and institutions of higher education;

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

Art. 5 IT Security Administrator

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

2He/she should possess the highest level of IT competence possible.

3The IT security administrator is specifically responsible for the following:

a) Identifying, documenting and solving security defects (Art. 15 para. 3 subpara. d; Art. 17 para. 2). He/she shall have authority to give instructions to this effect;

b) Coordinating and supervising the implementation of security measures;

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

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

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

[3] RSETHZ 203.23

Art. 6 System and Network Administrator

[1]There shall be a person responsible for every device operated within the data network of the ETH Zurich.

[2]Every user unit shall appoint one or several system administrator(s) and a network administrator to address the technical and operational aspects of the use of all its systems.

[3]The system administrator shall establish a list of the high-risk applications in his/her user unit and forward it to the IT department.

[4]The other tasks of the system administrator and of the network administrator are set forth in the *Standards for Responsibilities and System Maintenance*[4] 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 shall be at the same time the system administrator.

Art. 7 Appearance and Presence on the Internet

[1]The corporate communications department is responsible for the appearance of the ETH Zurich on the worldwide network and on the ETH Zurich internal network (Internet/intranet). It shall issue the applicable implementing provisions.[5]

[2]In this context, the corporate communications department must comply with the regulations concerning the equal treatment of disabled people.[6]

[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

[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 limit their use of the telematics resources to the appropriate extent within the permitted purposes.

[3]Use of telematics resources for personal purposes is permitted, provided it is not excessive and does not interfere with the user's work or study obligations.

[4]Personal use of ETH Zurich telematics resources should not result in a technical disruption or impair their use for purposes appropriate to the ETH Zurich's statutory missions or cause excessive strain or load on the generally available resources (networks, Internet access, etc.).

[4] RSETHZ 203.23

[5] ETH Zurich Internet Guidelines of May 1,1999 (RSETHZ 203.22)

[6] 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)

5Without 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 modifications to software programs and deactivation, circumvention or removal of security mechanisms. Modifications within the proper use of the telematics resources are excluded.

6Commercial use, e.g. pursuant to spin-off agreements, is subject to the written consent of the Vice-President of Research who will also determine the applicable fee.

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

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

1The employees working at home[8] with the consent of the appropriate authority may use the telematics resources of the ETH Zurich accordingly.

2Unless otherwise provided for in special instructions, the use of portable ETH-owned devices, such as laptops and organizers, is permitted outside of the ETH Zurich campus.

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

1Personal use of the software licensed to the ETH Zurich is permitted to employees of the ETH Zurich on an at least 50% basis and to the students matriculated at the ETH Zurich, to the extent permitted by the applicable license agreement.[9]

2The granting of the right to install the software on a private computer is governed by the applicable license agreement.

3Unless expressly allowed by the license terms, parallel use of software licensed to the ETH Zurich on a private and on an office computer is prohibited.

Art. 11 Data Protection

1Processing of personal data[10] is permitted only to pursue the ETH Zurich's statutory missions in compliance with the data protection regulations.[11]

2The disclosure of personal data to third persons for authorization and authentication of electronic services is permitted, provided however that this data is not sensitive[12] and is required for using the services.

[7] RSETHZ 220

[8] Pursuant to Art. 43 para. 3 PVO (SR 172.220.113)

[9] The applicable compilation is to be found under: http://www.id.ethz.ch/services/list/einkauf/heimnutzung

[10] 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

[11] 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)

[12] Data within the meaning of Art. 3 c) of Data Protection Law (SR 235.1)

Art. 12 Software Copies

Unless otherwise expressly stated in the license terms or the copyright law[13], 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 Means

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

2Professional, official and business secrets and other confidential information (e.g. personal dossiers) may only be transmitted electronically out of the ETH Zurich domain using appropriate encrypting techniques.

3The electronic communication means of the ETH Zurich may not be used anonymously or under a pseudonym.

4. Section: Security Measures

Art. 14 General Security Measures

1**Normal-risk** applications or systems are such which do not require special protective measures.

2The system administrators responsible for the applications or systems in this category must themselves take the following security measures: Installing and activating the most recent antivirus software, installing the security updates for the operating systems, performing regular and comprehensive data backups, promptly reporting any security problems, defects, etc., to the IT department.

3The users of the applications or systems in this category must ensure the confidentiality of access information.

Art. 15 Special Security Measures

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

2High-risk applications or systems must be more rigorously protected from being accessed by unauthorized third parties. This applies to access to the applications and data as well as to physical access to the computers themselves.

3Access authorization and identification mechanisms, such as password, PINs, chip cards, physical keys, tokens, etc., must be kept confidential. In particular, to ensure more rigorous protection, the following steps should be taken, depending on the case in question:

a) Enhanced password protection with regular controls;

b) Logging out when leaving the work place;

c) Promptly reporting security problems;

[13] Art. 24 of Copyright Law of October 9, 1992 (SR 231.1)

d) Periodical controls by the IT security administrator;

e) Data protection through encrypted data transmission;

f) Creation of a data backup policy;

g) Appointment of a substitute system administrator;

h) Emergency strategy for long downtimes;

i) Safeguarding data carriers outside the processing site;

j) Access control through e.g. lists of persons, turnstiles, identification through badge, photo or magnetic card.

[4]It is absolutely forbidden to transfer or disclose personal access authorization means and identification mechanisms to other users.

[5]As stipulated in the regulations governing proxies which apply to the user concerned, such information may be transferred or disclosed to the proxy system administrator where it is indispensable in the absence of a reasonable alternative.

[6]The system administrator of the user units shall establish the terms governing the access authorization and identification mechanisms (e.g. change of passwords). If more rigorous protection is needed, the terms must be tightened accordingly.

[7]If a user suspects that an access authorization or identification mechanism has become known or been disclosed to unauthorized third parties, he/she must promptly notify the system administrator.

[8]Installation and use of direct accesses to non-ETH Zurich communication networks and the installation of direct accesses to the ETH Zurich-owned communication networks (e.g. per modems) are subject to the written consent of the IT department.

[9]Access protection mechanisms on the Internet and intranet (e.g. IP restrictions) may not be deactivated through search or acceleration mechanisms (proxy and cache engines) without authorization.

5. Section: Responsibility and Liability

Art. 16 Responsibility

[1]Every user is 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]If the user makes use of a fee-based service without the written consent of the responsible superior or teacher, he/she shall have to assume any costs incurred.

Art. 17 Liability

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

[2]The technical and operating instructions issued by the IT department, by the system administrator of the user units or by the IT security administrator strictly apply to all users. Every user has to follow these instructions.

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

[4]In every case, the user shall be liable for damages or technical disruptions in the telematics resources of the ETH Zurich caused by 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 the ETH Zurich by third parties.

[6]In other respects, the Law on Responsibility applies to the employees of the ETH Zurich[14].

6. Section: Abuse

Art. 18 Records/Detection of Abuses

[1]Transactional data (addressing data on message headers, session data on transaction logs and similar data) may be recorded as usage data, in particular for the ETH Zurich server systems and ingoing and outgoing traffic; invoice and license compliance data may also be gathered.

[2]To monitor compliance with the provisions of this Acceptable Use Policy, logs may be examined on a random and anonymous basis as instructed by the IT security administrator.

[3]If abuses within the meaning of Art. 19 are discovered or suspected, the records may be examined by the IT security administrator in order to identify the violators, pursuant to the applicable Appendix: *Guidelines for Monitoring Use of Telematics Resources at the ETH Zurich*.

[4]Detailed rules concerning records on user behaviour, responsibilities, recording of abuses, retention and analysis of usage data are to be found in the Appendix of this Acceptable Use Policy.

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

Art. 19 Abuses

[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:

a) Processing, storing or transmitting illegal or immoral materials, such as violent images, pornography (Art 197 of the Swiss Penal Code – 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.).

[14] SR 170.32

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 networks and computers (e.g. denial of service attacks). In a particular case, “hacking” may be permitted in a secure test environment for teaching and research purposes[15], 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 the 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 the 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 accesses to the ETH Zurich communication networks (e.g. through modems or WLAN access points) without prior written consent of the IT department and the responsible system administrator;

3The serious abuses include:

a) Abuses pursuant to para. 2 subpara. a, b, c, d where deliberate or intentional;

b) or other abuses where repeated.

4The immediate superiors and the system or network administrators are obliged to report any serious or repeated abuses to the IT security administrator.

Art. 20 Consequences of Abuses

1Should an abuse within the meaning of Art. 19 of this Acceptable Use Policy be detected, the IT security administrator may take the following measures:

a) Block the access to the telematics resources[16] concerned as a precaution;

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

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

2As 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 where disciplinary proceedings have not been initiated or a criminal complaint not been lodged within three months. Upon completion of the disciplinary proceedings, the sanctions, if any, shall be determined anew.

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

[15] e.g. Information Security Lab, D-INFK

[16] See also point 4 of Schedule

4In addition, disciplinary measures[17], 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.

5A serious abuse by students does not constitute a petty offence within the meaning of the Art. 8 of the ETH Zurich Disciplinary Rules[18].

6The 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

1In 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 May 1, 1999 (as of July 2003) (RSETHZ 203.22);

c) ETH Zurich finance department's Instructions on Equipment Management at the ETH Zurich of January 1, 2004 (RSETHZ 220);

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

8. Section: Final Provisions

Art. 22 Enforcement

The units of the ETH Zurich, particularly the IT department, the security and environmental protection department, the ETH library department, the CSCS and the corporate communications department may, on the basis of this decree, issue additional rules within their respective sphere of competence.

Art. 23 Abrogation of Previous Regulations and Effective Date

1The following decrees are abrogated:

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.

[17] 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)

[18] SR 414.138.1

d) Software Use Guidelines for Teaching with IT Resources at the 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

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

1. Data Recording

[1]The ETH Zurich shall ensure that the technical protective measures to prevent technical disruptions are regularly updated to the latest state of the art.

[2]In case of technical disruptions, logs may be consulted to detect the causes.

[3]The following data may be recorded as usage data on the ETH Zurich telematics resources:

a) Transactional data (addressing data on message headers, session data on transaction logs and similar data), in particular concerning the use of the ETH Zurich server systems and of the ingoing and outgoing traffic;

b) Invoice data for fee-based telematics services provided;

c) Data to monitor compliance with the license terms (license server).

[4]In exceptional cases, the individual user units of the ETH Zurich (departments, institutes, chairs, infrastructure units, staff agencies) may issue, with the IT security administrator's approval, written guidelines for recording, saving and deleting transactional, invoice and/or license data concerning the telematics resources for which they are responsible. In so doing, they should take into account the peculiar nature of the telematics resources in question, their intended use and general use requirements. This information may not be kept longer than 3 months following termination of the relevant transaction.

[5]These guidelines must be made known to the users in an appropriate manner.

2. Responsibilities

2.1 System Administrator of the User Units

a) To install the telematics resources allowing to record data pursuant to point 1 of this Appendix.

b) To perform the random checks pursuant to point 3 as instructed by the IT security administrator.

c) To support the IT security administrator in fulfilling his/her tasks pursuant to these guidelines.

2.2 Network Administrator

To support the IT security administrator in fulfilling his/her tasks pursuant to these guidelines.

2.3 IT Services ETH Zurich:

To support the IT security administrator in fulfilling his/her tasks pursuant to these guidelines.

2.4 IT Security Administrator

a) To contact the special tasks service (Dienst für Besondere Aufgaben – "DBA").

b) To instruct the system administrator to perform the random checks pursuant to point 3.

c) To take the precautionary measures pursuant to point 4.

d) To decide whether the personal data analysis contained in the records is to be examined in order to identify the violator pursuant to point 5 a).

e) To interrogate members of the ETH Zurich on the contents of electronic messages (e.g. E-mails) pursuant to point 5 d).

f) To instruct the system administrator, in agreement with the responsible direct superiors (for employees) or the Rector (for students) pursuant to point 5 b), to examine the recorded data.

3. Anonymous Random Checks

[1]Concerning the data collected pursuant to point 1, the system administrators may, on instruction by the IT security administrator, perform anonymous random checks for abusive use within the meaning of Art. 19 B.OT.

[2]When monitoring the exchange of electronic messages (e.g. e-mail), the specific content of the messages may not be inspected.

[3]The actually detected or suspected abuses in such random checks must be promptly reported by the system administrators to the IT security administrator.

4. Protective and Precautionary Measures

[1]If, on the basis of the anonymous control, there is a reasonable suspicion that an abuse within the meaning of Art. 19 BOT by ETH Zurich members or third parties has been taking place which threatens to jeopardize the use of the ETH Zurich telematics resources or cause damages to the ETH Zurich, the IT security administrator is 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, store and safeguard them as evidence.

[2]In emergency cases, the director of the group “Network Security” of the ETH Zurich IT Services may also order that above measures be taken; the IT security administrator must be promptly notified and will decide whether the measures taken should remain in effect.

5. Personal Data Analysis

[1]In case of detected or suspected abuses within the meaning of Art. 19, the IT security administrator decides upon examination on recorded data in order to identify the violators according to the following principles:

a) If the **abuse** leads to **technical disruptions**, the IT security administrator may direct immediately that personal data be examined to identify the violator. If the suspected abuse could constitute a **criminal offence** pursuant to the Swiss Penal Code (e.g. within the meaning of Art. 197, Art. 259, Art. 261, Art. 261bis StGB, Art. 143bis, Art. 144bis StGB), a criminal complaint may be lodged against the violator. The decision whether to lodge such a complaint rests with the President.[19]

b) If the abuse does not cause any **technical disruption**, the direct superior (for employees) or the Rector (for students) will decide jointly with the IT security administrator, depending on the seriousness of the abuse, whether the personal data contained in the logs should be immediately examined or only if the abuse is repeated. The members of the user unit concerned will be informed in advance. If there is **a strong suspicion that an offence has**

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

taken place, a criminal complaint shall be lodged with the criminal prosecution authorities who shall conduct the personal data analysis.

c) If a technical disruption is caused **by a user's mistake**, the logs may not be examined since no abuse has occurred. Such disruptions should be prevented through appropriate protective mechanisms.

d) If an abuse pertaining to the exchange of electronic messages (e.g. e-mails) can only be investigated by reviewing the content of the messages in question, the IT security administrator must require the user concerned to reveal the content and purpose of these messages.

6. Sanctions

The responsibility for the sanctions to be imposed on violators in case of detected abuses is governed by Art. 20 of the BOT.

7. Confidentiality

[1]The data collected pursuant to point 1 must be treated in confidence; the system administrators must take the pertinent measures to prevent that members of the ETH Zurich and third parties gain unauthorized access to or knowledge of such confidential information.

[2]The results of the random checks and of the examination 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

[1]The IT security administrator shall contact the Service for Special Tasks (Dienst für Besondere Aufgaben – "DBA") to investigate offences in the context of monitoring the telecommunications network[20]. The IT security administrator and the other units of the ETH Zurich also shall promptly inform the legal department when they are contacted by the DBA or by the criminal prosecution authorities.

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

[20] Art. 28 and 29 of the Decree on Monitoring the Post and Telephone Traffic (VÜPF; SR 780.11)