Universität Zürich UZH

Executive Board of the University

Regulations on the Use of IT Tools at the University of Zurich (RUITT)

(Dated 30 November 2017)

The Executive Board of the University has resolved:

Part 1: Basic Principles

§ 1 Objective

1These Regulations are intended to ensure security in the use of information technology tools, by:

1. Determining responsibilities;
2. Setting out conditions of use; and
3. Laying down the action that will be taken to prevent and punish misuse.

2The use of IT tools at the University of Zurich is subject to the provisions laid down in these Regulations.

§ 2 Scope of Application

1These Regulations apply to the use of information technology tools at the University, whether by members of the University or by third parties. Third parties are deemed to be, for example, those attending courses or conferences, postgraduate students, users of the library, and those renting premises from the University itself or premises served by the University network.

2The UniversityHospital Zurich bears independent responsibility for issuing the corresponding regulations for its own area of authority. However, from the perspective of the IT Security Office, in the sense of the present Regulations, the UniversityHospital Zurich is treated as a user unit.

§ 3

Definitions

Use
This refers to any employment of IT tools.

IT Tools
This refers to all devices, systems and services that are used for electronic data processing, such as hardware, software, networks and network devices, the address elements (e.g. IP addresses) used for the University of Zurich, and to the stored data itself.

Members of the University
This refers to the teaching staff, mid-level academic staff, students, and administrative and technical staff, as defined in the University Act and the University Statutes.

End Users
Defines those users who use a computer but do not undertake any configuration or maintenance work on the computer system.

System Administrators
Refers to those users of a computer system who undertake configuration and maintenance work on it.

User Units
These are dean's offices, institutes, clinics, seminars, Central Services offices, libraries,

Centers of Competence, University associations and, in some cases, spin-off companies using University premises which are registered with Information Technology as purchasers of services.

Local IT Officer
This refers to the IT officers within the individual user units.

Isolation from the Network
In the sense of this document, this refers to the separation of a computer from the network, for example by disconnecting the data cable.

Strong Password
A strong password is at least eight characters long, and contains at least one of each of the following: capitals, lower-case letters, numbers, and special characters (such as punctuation marks, etc.). It may not be structured in accordance with any recognizable rule.

Personal Password
A personal password is either allocated to a given individual, or determined by them.

Group Password
This is a password which, for organizational reasons, must be known to the members of a given group.

Peer-to-Peer Programs
These are programs which serve both server and client functions.

Part 2: Organization and Responsibility

§ 4 End Users and System Administrators

1End users are responsible for the use of the IT tools and for maintaining their systems. User units may transfer responsibility for system maintenance wholly or partially from their end users to IT officers.

2These Regulations also apply to external specialists or firms engaged as system administrators.

3In the event of serious computer malfunction, end users must stop using that computer, or isolate it, and contact the system administrators for support.

4End users who do not belong to any user unit may not configure, or have configured, or operate any servers or peer-to-peer programs. They are permitted to operate only those systems which are not subject to any special security requirements, as described in §12. Information Technology may publish exceptions for peer-to-peer programs, and issue rules and regulations for their operation.

§ 5 User Units

1The user units deploy IT tools to support their end users' activities, for operational processes (e.g. printers, file servers, and research computers), and to provide general IT services (e.g. their websites).

2Each user unit is responsible for these IT tools, for technical and operational matters in connection with these IT tools, and for compliance with these Regulations. To fulfill these tasks, it must nominate a qualified IT officer, and notify Information Technology of their name.

3The guidelines for local IT officers, which are published on the internet by Information Technology, govern the rights and obligations of the IT officers, as well as their working relationship with Information Technology. On behalf of the user units, the IT officers may:

1. Monitor the network areas assigned to them, and their own computers, to ensure the proper functioning and security of these IT tools;

2. Configure servers and peer-to-peer programs, or have them configured.

4The user units' IT officers ensure that an IP address within their network area can be traced to the person who used the computer in question or, in the case of training rooms, for example, at least to the specific computer that was used. Steps must be taken to ensure that these links can be traced back over a period of six months. This rule also applies to IP addresses that are allocated temporarily and/or automatically.

5Each user unit must keep an inventory of the IT devices in operation in its particular area.

§ 6 Information Technology

1Information Technology bears sole or, in consultation with Legal Services, special responsibility for:

1. Setting up and operating central IT tools, the network, and the provision of central IT services to students and user units;
2. Providing advice and support on IT-related security matters;
3. Issuing IT security regulations for the University;
4. Issuing regulations on recording system processes (the log file policy);
5. Issuing technical implementation provisions.

2Information Technology may institute measures to restrict use of the network. In particular, it is authorized to take technical precautions to prevent unauthorized activity on the network.

3Information Technology may take appropriate action to contain misuse and malware, for example by deploying firewalls, spam filters, anti-spoofing filters, or virus protection at strategic points in the network.

§ 7 IT Security Office

1The University IT Security Office is a staff unit within Information Technology.

2The IT Security Office represents the interests of the University in dealings with internet operators. To this end, user units and end users are obliged to support the IT Security Office with the processing of complaints from the internet community.

3It is responsible for the general monitoring of the University network, and for identifying security flaws in particular. It proposes security measures and also provides security recommendations.

4The IT Security Office makes complaints about security flaws and minor misuse of the system direct to the end users or IT officers responsible. If this complaint does not bring an end to the improper use of the system, the head of the user unit may be notified. The IT Security Office may involve the persons concerned and external support in order to investigate security flaws.

5The IT Security Office may order or, if necessary, force, computers to be isolated from the network.

6The IT Security Office will report severe misuse of the system to Security Services, which will take the necessary action in consultation with Legal Services.

Part 3: Use of IT Tools

§ 8 Conditions

1University IT tools, specifically including the network, must be used for University purposes. IT services which place considerable demands on the University's infrastructure services (network bandwidth, power, cooling, etc.) must be planned in cooperation with the Central Services offices responsible. Information Technology must also be notified in each case. Commercial usage for non-University purposes by tenants on University premises is permitted only with the prior written consent of the Executive Board of the University.

2The use of IT Tools for personal, non-commercial purposes is generally permitted, providing this is kept to a minimum. To ensure that individual IT tools are able to fulfill their intended purpose, the head of a user unit may draw up additional terms of use for such tools and, in particular, may limit or forbid their use for personal ends.

3It is forbidden to use IT Tools for personal, commercial purposes.

4Any form of consumption of content of an illegal, pornographic, racist, or sexist nature, or that glorifies violence, is generally prohibited. Exceptions may be made in individual cases if a legitimate requirement for appropriate purposes, e.g. for research, teaching, art, education, or official tasks, can be demonstrated. “Consumption” refers to the use, processing, storing, transferring, and/or disseminating in particular of internet services, e-mails, news communications, video or sound recordings, or other images.

5Authorization is required before any IT tools can be loaned or rented out, or sold. This authorization is granted by the head of the user unit.

§ 9 Applications Subject to Authorization

1Applications connected with the University of Zurich's public internet presence are subject to authorization. The Communications Office is responsible for granting this authorization.

The following are also subject to authorization:

1. Connections to non-University networks, such as modem lines or tunnel connections from outside the University into the University network, which do not terminate at the corresponding Information Technology service, such as a modem dial-up connection or VPN server. The IT Security Office is responsible for granting this authorization.
2. Mass e-mails to members of the University. The Executive Board of the University instructs one UZH office to handle mass mailouts. The mails approved by this office (questionnaires, University courses, etc.) are executed by Information Technology, without the e-mail addresses of the target group being passed on to those initiating the mail. Mailouts by University staff concerning matters directly related to maintaining teaching and research operations, and Central Services, are not subject to authorization.
3. The configuration of a computer with a static IP address. The user unit which oversees the local network number range is responsible for granting this authorization.

§ 10 Banned Applications

The following are forbidden:

1. The operation of mail servers which can be contacted directly from outside of the University, or which themselves directly contact mail servers outside of the University network. However, this does not apply to the continued operation of mail servers within individual user units which are already in operation and which are registered with Information Technology.

2. The operation of communication lines or tunnel connections which serve to convey traffic to the local internet at end points both within and outside the University, and thus constitute an additional data connection to the internet.
3. The continued operation of network services which are known to permit severe misuse of the University's computer systems, as well as the continued, unprotected operation of computers to which unauthorized third parties have gained administrator rights, or which such parties might otherwise misuse to disrupt or to jeopardize the University's systems.
4. The publication of websites which cause the viewer's browser to load pages or services from outside of UZH, without a conscious decision to do so on the part of the user, is generally forbidden. Specifically, no images, scripts, iframes or applets giving a foreign data source may be embedded in such websites, and neither may scripts or applets which have the same effect. Exceptions may be made only if data protection is guaranteed, in particular by concluding an agreement in this regard.
5. No websites or network services may be offered without their content being checked to ensure that they do not permit third parties to operate anonymously.

§ 11 Data Protection

1Any use of IT Tools which invades the privacy of other individuals is forbidden. Personal data may be recorded, processed, and forwarded only to the extent required to conduct the assigned task within the University. The relevant data protection and archiving provisions must be observed.

2The users of IT tools are responsible for ensuring that data cannot be misused by unauthorized third parties.

§ 12 Security Requirements

1Systems must be maintained so that they are protected as effectively as possible from misuse by third parties. In particular, maximum precautions must be taken to prevent attacks on other computers in the network, and the spread of harmful program code.

2Passwords and PINs must be kept secret. Users are responsible for the selection and quality of their passwords, and for keeping them confidential. Personal means of authentication (such as passwords, certificates, hardware tokens, and badges) and keys may not be passed on to third parties. Passwords employed by users in connection with University of Zurich systems may not be used to access other systems, such as those used for personal purposes, or for internet-based systems and services which are not connected with activities at UZH.

3Any personal or group passwords that are used must be strong in nature. No other person may be told of or given access to a personal password. A password officer is to be appointed in the case of group passwords. The password officer must know all members of the group personally. They may change the password at any time, in particular when instructed to do so by the IT Security Office.

For each computer, security requirements with regard to:

1. Confidentiality and secure access;
2. Data security; and
3. Availability

must be determined, and appropriate action taken to ensure that those requirements are fulfilled.

4The standards for the operation of computing systems at the University of Zurich (*Normen für den Betrieb von Systemen an der Universität Zürich*) must be observed. Reasonable alternative security strategies must be set down in writing and implemented for systems which are subject to more stringent security requirements or which, owing to special circumstances, are unable to satisfy all points of the applicable standards. The documentation requirement set out here may be fulfilled in summary or tabular form for computers that are maintained as a group.

5 Systems may be accessed only in accordance with the access authorizations that have been granted, using the allocated means of identification and authentication. Users are responsible for their access to IT systems and applications, as well as for access by third parties that results from negligent behavior by those users. Should a user find that they have access to information that is not necessary for their work, or should they discover that their own means of identification have been misused, they must immediately notify their line manager and the IT Service Desk or IT Security Office.

§ 13 Monitoring

1The University network and individual IT services are monitored. The primary purpose of these monitoring activities is to detect the misuse of IT tools by third parties, as well as to identify needs in the interests of resource planning.

2It is not possible to designate e-mails as private, and thus to have them treated differently in the logging process. E-mails can be encrypted, however.

3The University's logfile policy, issued by Information Technology, contains further provisions in this regard.

Part 4: Misuse and the Consequences of Misuse

§ 14 Misuse

1A breach of the provisions of these Regulations, or of other University regulations as a result of the deployment or use of the University's IT tools, constitutes a case of misuse. Action may be taken against the perpetrators of such misuse.

2The following actions, in particular, are deemed to be a misuse of University IT tools:

1. The use, processing, storing, transferring, and/or disseminating of data, in particular of e-mails or websites, with content of an illegal, pornographic, racist, or sexist nature, or that glorifies violence.
2. The use of e-mail or websites to harass, denigrate, or harm other people.
3. The unlawful downloading, copying, or installation of data and software of all types.
4. The use of the IT tools in a way which breaches the intellectual property rights of third parties.
5. Failure to comply with legislation protecting personal data.
6. The production or distribution of harmful program code, such as viruses, Trojans, or worms.
7. Unauthorized scanning of the network within and outside of the University; authorization is granted only to the IT officers for the areas of the network allocated to them, and to the IT Security Office for the entire University network.
8. Any attempt to gain unauthorized access to a computer system, or to gain authorizations at a higher level than those that have been granted.
9. The use of simulated IP addresses or e-mail sender addresses.
10. The sending of mass e-mails, with the exception of the applications permitted under § 9.2.
11. Operating servers in a way that facilitates their misuse by third parties, the anonymous sending of spam e-mails, hacker attacks, or illegal data transfers.

12. The operation of hacked or infected systems within the network.

§ 15 Action in the Event of Misuse or Suspected Misuse

1The Executive Board of the University hereby notifies staff that internet access and e-mail traffic are logged. This log data may be analyzed and traced to individuals, if:

1. Significant misuses of internet access have occurred; or
2. If there are specific grounds to suspect that e-mail has been misused.

2After a written warning has been issued by the line manager, Security Services may apply to Information Technology for reports relating to the internet activity and e-mail exchanges of a specific individual or specific individuals.

3Such personal reports may cover a period of no more than three months.

4Information Technology will supply these reports to Security Services.

5If there are grounds to suspect misuse, Security Services will determine whether or not it will apply for administrative or disciplinary proceedings to be commenced against the person concerned, or only issue them with a written warning. The personal data must be destroyed if no investigation is initiated.

6Information Technology, and specifically the IT Security Office, may take all action necessary to eliminate a case of misuse and to maintain or restore the rightful state of affairs. Such action may include:

1. Reporting the breach to Security Services;
2. Investigating the cause of the malfunction in association with the IT officer or head of the user unit concerned;
3. Requesting that the responsible user rectifies the improper situation;
4. Setting deadlines for the restoration of the rightful state of affairs;
5. Blocking an account until it can be returned securely to the rightful user;
6. Blocking an account to obtain a written assurance of compliance with these Regulations.

7If there are grounds to suspect misuse, Information Technology may block connections or services, or have them blocked, on a precautionary basis. It will ensure that the data in question can be sought and saved.

8The University may block unlawful and improper data and hold it as evidence. This data will be deleted if is decided that proceedings will not be pursued, and once any such proceedings are concluded.

Part 5: Final Provision

§ 16 Entry into Force

These Regulations enter into force on 30 November 2017.

Zurich, 31 October 2017

On behalf of the Executive Board of the University of Zurich

The President: Prof. Dr. Michael Hengartner	The Secretary General: Dr. Rita Stöckli