University of Zurich^UZH

IT Services

Standards for Systems Operation at the University of Zurich

Validity of this document

This document comprises implementation regulations for the Regulations on the Use of IT Resources at the University of Zurich (REIM) and is valid for the same individuals and applications.

If certain of these standards are not met for good reason, acceptable alternative security concepts must be presented, recorded and implemented as per REIM (§11).

Standards

1. In order to **combat abuse by third parties**, those persons who are responsible for the system are obliged to ensure that the following conditions are met:

1.1 An antivirus program is set up, and this is done in such a way that it is continuously and automatically supplied with the latest virus descriptions; if possible, it continuously checks all incoming files and can also be launched for additional in-depth checks. The range of activities of IT Services must be taken into account.

1.2 The operating system must be supported and maintained by the manufacturer or distributor.

1.3 The system is basically brought up to the current status in connection with the security updates supplied by the system manufacturer. The system manufacturer's automatic procedure should be used unless there are good reasons not to do so in individual cases.

1.4 The end users know that they must not click on cross-references, fill in forms or open attachments whenever the context of the e-mail or web site is suspicious.

1.5 Unnecessary network services that are turned on when the system is supplied must be turned off as far as possible, based on the best knowledge available.

1.6 A newly set-up system is only connected to the data network when it is well protected by a software or hardware firewall or when all service packs and updates have been installed.

2. With regard to **accessibility and confidentiality,** those individuals responsible for the system are obliged to ensure that the following conditions are met:

2.1 Individual access protection is set up, both locally and for all network connections. All users work with their own personal identification and they receive the necessary data on the basis of file authorizations.

2.2 Individual identification is implemented by means of a strong personal password or a better recognized procedure. The use of strong passwords is also stipulated in cases where a set-up with weak passwords is not technically prevented.[1]

2.3 Access protection is set up so that the system administrator is the only person who has system rights. It is ensured that only the necessary user and system accounts are set up.

2.4 Authorized individuals can protect their data individually against viewing by other authorized users who are active on the same computers. Although viewing of protected data by the system administrator is prohibited, it is not prevented by technical means.

2.5 It is recommended to set up a personal firewall such that only the necessary connections from outside are possible. If the operating system includes a personal firewall supplied with the product, either this firewall or another product must be enabled.

[1] See Regulations on the Use of IT Resources, §3.

2.6 The system is set up so that the screen is automatically locked after a maximum inactive period of twenty minutes. As a general rule, however, no special precautions are taken to prevent a person with physical access from being able to access the computer by prohibited means.

2.7 Accessibility via the network from outside the University is restricted to encrypted protocols, i.e. the IP number of the systems is in the standard class for Transistor, the University's central firewall.

2.8 In an emergency, e.g. if employment is suddenly terminated due to discord or death, the management of the organizational unit may regulate access to the organizational unit's working data by special methods. Measures necessary for this purpose, such as depositing the system administrator's password in a sealed envelope in the safe, are taken by way of precaution.

2.9 No data are kept or processed which are secret, i.e. which are subject to professional confidentiality, which represent personal data meriting special protection within the meaning of the Data Protection Act, or which are classified as secret according to the official regulations of the organizational units.

3. With regard to **data security**, those individuals responsible for the system are obliged to ensure that the following conditions are met:

3.1 End users' data stocks are backed up regularly, or the end users make use of a designated storage area on a server belonging to the organizational unit where regular data backup is carried out.

3.2 The data backup frequency is daily to weekly, but in any case often enough to enable elimination of damage generated by the loss of changes with reasonable effort by the end users.

3.3 Data backup is checked after every process change and at least once every three months.

3.4 On termination of the employment, working data are handed over to the employer.

4. With regard to **availability**, the following conditions are met:

4.1 Regular system maintenance is planned so that it can be carried out with due care, but also without unnecessarily impairing the system's fulfillment of its purpose. In cases where system maintenance is not handled by the end user himself or herself, outage times are agreed in advance.

4.2 Work with the system is planned so that no major damage is caused should an unplanned outage occur. The time and costs needed to provide a substitute solution are taken into appropriate account in this respect.

If the interpretation of the Standards for Systems Operation at the University of Zurich results in a difference due to the versions in various languages, the German version shall be authoritative.