Information Sheet in Using IT for Employees

1. Rights

As an employee of the University, you belong to an organizational unit of the University. Depending on your employment conditions, you may or must make use of your own IT resources, or those which are made available to you, for your work. In particular, these include the University's network and the applications that are made available. Private usage outside of actual working hours is permitted provided that it is insignificant and non-commercial. You must only operate servers or Peer-to-Peer programs on behalf of the organizational unit, for your work. By using the University's IT resources, you accept that the network is monitored and that technical measures may restrict usage to specified procedures.

2. Abuse

In connection with the University, the University's Regulations (Regulations for the Use of IT Resources at the University and Standards for the Operation of Systems at the University[1] are applicable in addition to the statutory provisions. Further provisions may be applicable in connection with your employment. Accordingly, the following are among the actions which you must not carry out with IT resources:

2.1 scanning the University's network or attempting to enter a system without authorization;

2.2 creating or distributing malicious program codes;

2.3 unlawfully downloading, copying or installing data or software;

2.4 violating the immaterial property rights of third parties (copyrights);

2.5 denigrating, damaging or harassing other persons with e-mail or web pages;

2.6 faking e-mail senders' addresses or IP addresses;

2.7 using, processing, saving or transmitting data with content which is unlawful, pornographic, racist or sexist or which extols violence.

3. Responsibility for the System

You are basically responsible for the computer system which you use in connection with the University. If a computer system is made available to you by the organizational unit, that unit will usually assume responsibility for the system which is unchanged or is operated according to local instructions.

Even if you commission someone to set up and maintain your own system, you remain responsible to the University for the said person's service and performance.

[1] See http://www.id.unizh.ch/dl/sicher/Vorschriften.html or http://www.rd.unizh.ch/rechtssammlung/richtlinien.html

4. Protection of systems against malicious programs and abuse by third parties

Computer systems may only be connected to the University's network if:

4.1 they are fully up-to-date as regards the system maintenance recommended by the manufacturer;

4.2 virus protection has been set up, which must also be kept fully up-to-date in every respect;

4.3 all user accounts that are accessible via the network are protected by a strong password or an even better procedure; and

4.4 they are free of malicious programs as far as is known.

Do not click on cross-references or open attachments whenever the content of the e-mail or website is suspicious!

5. Access protection

The password for your UniAccess account is personal and must not be made accessible to anyone else. The same applies to any other user accounts on the University's computers. You should select a password of your own. If you suspect that the password has become known to someone else, you must change it immediately. Keep your initial password in a safe place because you can use it to identify yourself to the IT Services.

Set your own PC up so that the screen is automatically locked after a maximum of 20 minutes without input. Always activate the lock manually if you leave the PC switched on in a location which is not secure. Strong passwords are also necessary to protect the PC locally.

Strong passwords are at least 8 characters long; they have at least one representative of each of the four character categories (uppercase letters, lowercase letters, numerals and punctuation characters) and they have no identifiable construction rules.

6. Data backup and availability

Check your data backup regularly and be aware of the effects that the sudden loss of your accustomed IT resources would have on your work.

7. Help

In case of any problems, contact the IT supervisor for your organizational unit or a person designated by him/her. If you discover abuses by members of the University, report them to your superior.