Regulations on Collecting Logfiles

1. Basic Information

These regulations are an addition to the Regulations on the Use of IT Resources at the University of Zurich and are applicable to the area defined therein unless explicitly stipulated otherwise.

2. Definitions

Logfiles, Logs: electronic records of events in computer systems and networks linked with a precise indication of time.

Specialized technical terms (DHCP, VPN tunnels, ssh) are additional explanations for experts and will be understood by them.

3. Duty to record and collect

The following records must be collected and kept safely:

- all temporary or fixed assignments of IP numbers for persons (network release/clearance, VPN tunnels, ssh-tunnel service trampolin.unizh.ch) or machines (DHCP). These must be recorded so that either the person or the machine can be traced retrospectively.
- the temporary or fixed relationships between IP numbers or from IP numbers to login names of persons which are created by firewalls and servers for network address translation and by connections with forwarding servers (e.g. proxies) on a paired basis.
- the logs created for e-mail on passage through the mail servers.

As these data can be processed together with other records to create personality profiles, they are personal data in the broadest sense.

4. Purpose of logfiles

In order to fulfill the responsibility which the University has in respect of the Internet, the responsible individuals or abused machines must be traced, especially in these cases:

- dealing with complaints about the behavior of a machine or its users on the Internet.
- clarification of noticeable or disruptive behavior by machines on the Internet.
- providing information about events relating to security monitoring to the parties affected.
- ordering emergency measures or communicating individual emergency measures that have been taken in case of problems with hackers and viruses.
- In the most extreme case, the logfiles are needed to provide correct information for investigative authorities.

5. Safekeeping periods

Logfiles should be kept for half a year after assignment of the IP number. (Although the University is not a service provider within the meaning of the Federal Mail and Telecommunications Monitoring Act (BüPF), it adopts this period for practical reasons.)

It is recommended that files are kept for 4-5 weeks so that they can easily be called up by authorized staff, and for a further 22-23 weeks in an archive.

In accordance with the Data Protection Act, these data must subsequently be deleted.

6. Regulations for other logfiles

All other logfiles which allow information to be deduced about individuals' activities are also subject to the Data Protection Act. They may only be kept for as long as is necessary for a specified evaluation regarding a person, or if their deletion is unreasonable.

After half a year at the latest, files of this sort created on the machines at the University should be deleted or should be converted so that only anonymous results are then kept.

7. IT Services logfiles

The IT Services logfiles as per clause 1 must be made available to the IT Security Officer on a central system.

Network traffic may only be collected and its contents may only be analyzed by the IT Security Officer, and these activities may solely be undertaken in order to discover and/or prove the abuse of machines by unauthorized persons or programs. Other findings about activities of individuals from these data should be avoided, and are subject to absolute secrecy (telecommunications secrecy), in cases where they nevertheless come into being.

The maximum safekeeping period for network traffic data which contain more than merely the addressing elements is one week.

8. Exceptions

Logfiles on machines for which only one natural person is authorized are not subject to regulations. The collection of network traffic from such a machine by the sole party authorized to do so is also free.

Network traffic for individual machines may also be recorded to the necessary extent in order to clarify and document technical faults.

9. Further provisions

Logfiles with personal data as per clauses 1 and 4 must be treated as confidential. They may only be accessible to the group of persons who are directly involved. Third parties who are called in to assist must be selected carefully and must be obliged to maintain confidentiality.

Logfiles must contain accurate time stamps. All servers at the University should be synchronized with the University's time servers (time1.unizh.ch, time2.unizh.ch, time3.unizh.ch). All client machines should be synchronized at least each time they are started up, and at least once per day.

Extracts from logfiles and information learned from logfiles occurring in written correspondence and investigative reports may be kept for longer; the same applies to copies of delivery notes and any invoices.