Please note - this is an *unofficial* English translation of the German original.

RSETHZ 203.23

Standards for Responsibilities and System Maintenance

from 6 Feb 2003

The Vice President of Research and Economic Relations at ETH Zurich,

supported by Item 3 Section 2 Paragraph c Detailed Organisation Regulations ETH Zurich of 9 June 1998,

decreed:

Item 1 Purpose

This regulation aims to ensure that, in the event of an attack on or starting from a system* belonging to ETH Zurich, the person responsible for the system can be identified and contacted. Furthermore, it aims to ensure the timely removal of known weak spots, in order to reduce the vulnerability of the system as a whole.

Item 2 Policy

[1] Only devices that comply with the standards specified in these regulations may be connected to the data network at ETH Zurich.

[2] Information Technology Services (Informatikdienste) shall routinely check compliance with standards by means of spot checks.

Item 3 Responsibilities

[1] Every organisational unit shall appoint the following administrators:

a. System Administrator:
   For every device that is connected to the data network, be it inside or outside the ETH Zurich campus, there shall be an administrator. This person arranges for, among other things, the installation of the network connection, is responsible for system maintenance and data security and controls access policies so that system-related procedures can be reconstructed and attributed to a person.

* *System* includes, for example, a computer, a network component such as a router etc

b. Network administrator:
   This person
   - controls all activities relating to the connection of devices to the organisational unit's data network,
   - supplements the network guidelines provided by Information Technology Services (Informatikdienste) to suit their organisational unit and communicates these,
   - authorises devices for network connection,
   - is responsible for all network-related registrations,
   - is responsible for activation of the network connection outlets
   - administers the address ranges allocated by Information Technology Services (Informatikdienste),
   - organises network access,
   - allocates IP numbers to devices and
   - serves as the contact person within and outside the organisational unit when network problems occur.

[2] All IP addresses are to be entered by the network administrator into a central database, together with the respective responsible persons (and their email addresses). If allocation of an IP number to a system administrator is not procedurally possible, this information will be derived on a case-by-case basis from logfiles provided for the purpose.

[3] In order to guarantee they can be reached in the event of an incident, all administrators must be able to be contacted via predefined addresses. The administrators or their representatives must be reachable within one working day.

[4] The database must be accessible and readable for all members of ETH Zurich.

Item 3 System Maintenance

[1] Devices that are connected to the ETH Zurich network must be protected against known vulnerabilities.

[2] Information Technology Services (Informatikdienste) administers a constantly updated, ETH Zurich-wide list of vulnerabilities relevant for ETH Zurich, ordered by priority and urgency. Where possible, a test will be made available for the vulnerabilities listed, which can be used to check whether a given device is vulnerable. For devices that stand alone behind a firewall, the whole system, rather than just the device, will be considered.

[3] Depending on the type of vulnerability and its exploitation, the following time limits for its removal apply:
- **1 working day**: The vulnerability is being actively exploited in that other systems are being directly attacked, or there are other damaging activities emanating from it.
- **5 working days**: The vulnerability is being activity exploited, but there are no other damaging activities emanating from it.
- **20 working days**: The vulnerability is known and traceable and there are no known cases where it is actively being exploited.

The time limits listed can also be reduced in the event of an acute threat to the infrastructure.

Item 4 Measures for Non-Compliance with Standards

Should the given standards not be complied with, Information Technology Services (Informatikdienste) are obliged to disconnect the device in question from the data network, until standards are complied with.

Item 5 Entry into Force

This regulation came into force on 6 February 2003.

6 February 2003 Prof. Dr. U. Suter