PAUL SCHERRER INSTITUT		Registration AW-95-06-01 Rev. 1
Title	Usage and Monitoring of IT Resources at PSI	Replaces
Authors	Tobias Marx / Werner Roser / Karsten Bugmann	Prepared 11. December 2013

Summary:

This document defines the Usage and Monitoring of all IT Resources at PSI for all users.

This directive was approved at the Direction Meeting of the 11th December 2013 and will be put into effect from the 1st February 2014.

Distributor	Debt.	Recipients	Copies	Dept.	Recipients	Copies
	PSI	Information for all PSI employees down the line and advice in PSI-Aktuell through the link in the Intranet. New employees receive the link on their first day.	1	Line management at all levels and PSI contact person	Distribution to temporary employees and staff of other companies, temporary help, trainees and guests etc.	
	User-Office	Experimenters (DUO staff) electronically			Publication in the Intranet	

	Copies
Library	3
Reserve	
Total	
Pages	4
Attachments	

Information list

D	1	2	3	4	5	8	9	A

Visum Abt.-/Laborleitung:

This directive describes the rules for dealing with IT resources at PSI. The rules are binding for all users of any of PSI's IT resources (PCs, networks, modems etc.).

1. Use of the IT resources

Every user is personally responsible for ensuring that the use of PSI's IT resources does not breach the provisions of this directive, of the legal system (e.g. criminal law, data protection etc.) and the rights of third parties (copyrights, licensing provisions, personal rights). Usage of PSI's IT resources must not damage PSI's reputation.

PSI's IT resources are primarily to be used for work. Personal use must be kept to a minimum. Private Data in this instance referring to documents of all types, including Emails and Appointments, of which have no Business use or are in any way connected to activites at PSI. Private use of PSI resources must not lead to a technical disruption, restriction or to a disproportionate demand on commonly used resources and must not pursue any commercial purpose.

Private Data must be saved onto specially desginated storage locations, in order to protect privacy. Private Data must be saved into directories/sub-directories named „privat". All other data must be saved outside of these directories.

Furthermore, no private web content may be published using PSI's IT resources. Exceptions to this are details about a person's own career experience and publications. Existing PSI-specific design samples (Corporate Design) must be used for this purpose.

In cases of longer absences or unavailability of those responsible for certain data access, as well as their deputies, impacted employees are able to petition for access to the inaccessible **duty-relevant** data via their Supervisor, of whom must then acquire approval via the Head of Human Resources and the Safety Delegate, or via their respective deputies, providing the data access reasons are justified. Duty-relevant data in this instance is data of which normally only one person is responsible for but has designated deputies whom also have access. In relation to the access to **private** data, the permission of a next-of-kin is also required.

2. Misuse

Misuse includes any use of PSI's IT resources which disregard the provisions of this directive, which are in breach of superior law or the rights of third parties.

The following actions in particular count as a misuse; some are explained in more detail in the annex to this directive:

a) The use of pornographic, sexist, racist and slanderous websites, and the storage and distribution of such content.

b) The harassment of PSI employees or of third parties through messages sent using electronic means of communication.

c) The sending of advertising emails (spam) or phishing emails.

d) The use of programs without a valid licence on PSI systems, and breaches of copyright.

e) The intentional bypassing of PSI network control mechanisms.

f) Any usage of PSI networks which has not been approved by AIT.

g) Any usage of PSI IT resources of which damages IT security, general security or other IT resources.

3. Serious Misuse

In particular, the following actions in particular are considered to be a serious misuse; they are explained in more detail in the annex to this directive:

1. Breaches of articles of the valid StGB where these occur deliberately or wilfully.
2. Repeated misuse as described in paragraph 2.
3. Any usage of PSI IT resources which damages the reputation of PSI.

Knowledge of a serious or repeated misuse obliges the direct superiors, the persons responsible for the system and the network to advise the Head of Human Resources accordingly.

4. Rules on monitoring and consequences

The total network traffic between the PSI networks and the Internet are monitored and recorded for the purpose of checking compliance with the usage rights. For reasons of security and quality assurance, authorised AIT staff may anonymously evaluate the recordings and monitoring protocols. Where misuse is identified or where there are grounds to suspect misuse of PSI's IT resources, a message is sent to the Head of Human Resources. This person can then request that an evaluation be made specific to a particular person. In the case of a serious misuse, the specialist for IT security is also entitled to inspect the computer systems which may have been involved in the misuse.

If the suspicion of misuse is not confirmed the evaluation of all protocols related to a specific individual will be stopped immediately and the records destroyed.

The discovery of misuse, or plausible suspicion of misuse, in accordance with these directives, can lead to administrative measures being taken and temporary loss of the right to use PSI IT resources. Systems involved in misuse can be removed from the network and only be reinstated when the security is restored and/or the misuse comes to an end.

If a criminal act is proven or suspected, PSI will secure the related protocols. PSI reserves the right to make a complaint against the persons affected. For the further assessment of legalities involved in connection with the usage of PSI's IT resources (and in particular with their misuse), Swiss Law applies.

In all cases of serious misuse the line management, the Head of Human Resources and the director together will decide on the disciplinary measures to be taken.

The costs arising from any misuse and its consequences, including clarification and sanctions (including costs of investigation, court costs and costs of lawyers) may be transferred by PSI to the fallible persons.

Annex

Notes on paragraph 2, misuse

On: d)

Breaches of copyright include the use, procurement, distribution or storage of copyright protected data and programs without appropriate approval.

On: e)

This is to be understood to include the intentional installation and use of programs/technology which allow network connections to be made from the Internet to the PSI network or network connections from the PSI network to the Internet and which thereby avoid PSI's control mechanisms (e.g. firewall).

On: f)

We consider this to include :

- Simultaneous usage of the PSI network and the guest network on the same machine. Also the simultaneous usage of the PSI network and the use of public WLANs/GPRS- and UMTS networks etc. (e.g. Swisscom). This means that all network connections with other networks must generally be deactivated when using the PSI network.
- The installation and operation of WLAN access points which have not been approved by AIT. This also applies to all WLAN components in ad hoc mode. The "ad hoc mode" permits a direct link to be made with other computer systems and in the extreme case can create access to PSI's internal network.
- The connection of private computer systems belonging to PSI staff and guests with the PSI network without adequate protective anti-virus mechanisms and all available security updates. This also applies to all PSI systems which are not maintained by AIT and to all systems which are linked with the PSI network by means of a VPN connection (e.g. PC in a private household, Notebooks etc.).
- The use of any type of peer-to-peer software (emule, edonkey, BitTorrent, etc.) for obtaining copyright-protected data (films, music files, games, software etc.), as well as material which is in breach of Art. 197 StGB.
- The passing of personal passwords to third parties to allow use of PSI's IT resources as well as the unprotected storage of written passwords and the unsecured storage of passwords within files and scripts, where the passwords allow access to PSI's IT resources.
- The publishing of PSI-internal information in the Internet without password protection.

Notes on paragraph 3, serious misuse

On: a)

Breaches of articles of the current StGB include in particular:

- Processing, acquisition, storage, transfer, offering, displaying, releasing and providing access to material such as scenes of violence or sexual behaviour in the sense of Art. 197 point 3, 3bis StGB. incitement to commit crimes or acts of violence (Art. 259 StGB), breach of freedom of belief and freedom of worship (Art. 261 StGB) or racial discrimination (Art. 261bis StGB).
- The production, advice on the production or the intentional distribution of harmful programs or program components in the sense of Art. 144bis point 2 StGB (viruses, worms, trojans, etc).
- The unauthorised entry into a data processing system (Art. 143bis StGB) (hacking), spying into passwords, the illegal acquisition of passwords, credit card numbers or bank account numbers (phishing), unauthorised searching of internal and external networks for weak points (e.g. port scanning), measures and implementing measures for disrupting networks and computers (denial of service).
- Data theft (Art. 143 StGB) and data corruption (Art. 144bis point 1 StGB).

  For the purpose of checking the security level of PSI's IT resources, the specialist for IT security may use appropriate procedures and technology.