



Conditions of Use
for Information-Processing Systems at DESY
dated 17 August 2006

Version 1.0

Recitals

These Conditions of Use are intended to guarantee the use of information-processing systems at DESY in a fault-free, unobstructed, lawful and secure manner. Information-processing systems cover all data processing equipment and systems and communications systems, their infrastructure, associated services and software. The Conditions of Use are based on the statutory defined objects of DESY. Subject to the IT Framework Agreement (“Rahmenvereinbarung EDV”) in the relevant applicable version¹ they outline the basic rules for the proper operation of the IT infrastructure, thereby defining the relations between individual users and central and decentral IT operations groups.

Please note: This document is based on the German document “Benutzungsordnung für Informations-Verarbeitungssysteme bei DESY vom 17. August 2006“. This translation is for information purposes only – lawfully binding is only the German version.

¹ See <http://www.desy.de/betriebsrat> under Works Agreements

Article 1 Area of Application

These Conditions of Use apply to the use of all central and decentral information-processing systems and infrastructures at DESY at the Hamburg and Zeuthen locations. For the purpose of the IT Framework Agreement, “users” are all users of information-processing systems at DESY.

Article 2 Definitions of Terms

1. A “central IT operations group” is a group which provides general IT services to the whole of DESY.
2. “Decentral IT operations groups” are groups which provide IT services only to specific areas of DESY.
3. The term “IT operations group” refers to both central and decentral IT operations groups.
4. Administrators are persons appointed within the groups to provide IT support within the groups.

All persons specified above are members of the group of responsible persons for the purposes of the IT Framework Agreement.

Article 3 Determination of Rules by IT Operations Groups

IT operations groups, if appropriate in consultation with division management and in conformity with the rights of the responsible Works Council, may issue further rules for the use of the information-processing systems assigned to the IT operations groups for the purpose of guaranteeing their proper operation.

Article 4 User permit and user licence

1. DESY may allow the following persons to use the information-processing systems:
 - a. DESY employees and employees of other research institutes on DESY premises.
 - b. Users of DESY research facilities.
 - c. Persons assigned by DESY to perform services.
 - d. Members of other research facilities under special agreements.
 - e. Other natural or legal persons under special agreements.
2. Permission is given only for scientific purposes in research and in the operation of research facilities, for teaching and study, for library purposes and administration, for further training and education and for the performance of other duties in the interests of DESY. Permission for a different type of use can be given if it is only slightly different and does not impair the interests of other users. The information-processing systems operated by DESY are available solely for official purposes.
3. Permission to use the central information-processing system is given by granting a user permit. This permit is granted by the central IT operations groups in writing or electronically on application by the user and with the prior approval of the relevant group managers or collaboration managers or their representatives.

The application must be submitted on the form prescribed by the central IT operations group and must contain the following details:

- a. Name, address and signature of the applicant and status as employee of DESY, of a collaborator or other facility, student or other user as defined in Article 4 (1);

- b. If the applicant is not a DESY employee, further contact details are required, e.g. home institute, e-mail, contact person.
- c. Name of the group or experiment belonged to.
- d. Desired IT resources.
- e. Declaration regarding the processing of personal data by the applicant and acknowledgement of the statutory data-protection provisions.
- f. Acknowledgement of these Conditions of Use or the operating rules issued as the basis for the use relations under Article 3.
- g. Consent to the relevant virus/spam-filters in application ("Regeln zur Viren- und SPAM-Filterung") at DESY².
- h. Applicant's declaration of consent to the processing of personal registration data for operating purposes, e.g. account management.
- i. Acknowledgement of the possibility of documentation of the use of IT resources and the examination of user files according to the terms of these Conditions of Use (cf. Article 7).
- j. The assurance that the user will be informed by suitable means of changes in the Conditions of Use.

4. The decentral operations groups control the licence to use the decentral information-processing systems in the same way.

5. The user permit is limited to the project applied for and is always for a limited period. It automatically extinguishes when the grounds for the permit cease to exist.

6. For the purpose of guaranteeing proper and fault-free operation, the user permit may also be issued subject to restrictions of the IT resources applied for or subject to other use-related restrictions and conditions.

7. In order to be fair to all authorised users, the operating equipment available at DESY may be subject to allocations for individual user groups by resolution of the directorate.

8. Access to the secure rooms of the computer centre requires a special permit that can be granted to a specific person on submission of an application giving the reasons and submitted to the central IT operations group by the relevant group manager.

Article 5 Users' Rights and Duties

1. The authorised users have the right to use the information-processing systems within the scope of the permit and subject to the terms of these Conditions of Use and according to the rules passed under Article 3. Any use that derogates from these types of uses requires a special permit.

2. Users are obliged,

- a. to comply with the terms of the Conditions of Use and to adhere to the limits of the user permit, in particular, the purposes of use as per Article 4 (2).
- b. to notify the responsible persons of the central user administration of any changes in important contact details, cf. Article 4 (4 b);
- c. to refrain from doing anything which disturbs the proper operation of DESY's central information-processing systems;
- d. to treat all information-processing systems and other equipment belonging to DESY with due and proper care;
- e. to use only the user codes that are permitted to be used under the permit; business-related exceptions, e.g. for system accounts are admissible under the rules passed by Computer Security Council (CSC);

² See <http://www.desy.de/rsr/intern/rsr-statements.html>

- f. to ensure that no other persons gain knowledge of user passwords and to take care to ensure that no unauthorised persons gain access to the information-processing systems, this also includes protecting access by a password that must be kept secret and which meets the requirements for DESY passwords (“DESY- Passwortregeln”)³;
- g. not to try and discover or to use third-party user codes or passwords;
- h. not to obtain unauthorised access to the information of other users and not to pass on without consent information of other users that has become known or make use of the same or modify it;
- i. to comply with the statutory requirements when using software, documentation and other data, in particular copyright protection and to observe the terms of licensing agreements under which software, documentation and data are provided by the relevant IT operations groups;
- j. not to copy the software, documentation and data provided by the relevant IT operations group nor pass on the same to third parties, unless this is expressly permitted nor use the same for any purposes other than those permitted;
- k. to provide personal websites only for official purposes and to comply with the DESY rules (“DESY-Regeln”)⁴;
- l. to follow the instructions of the personnel in the computer centres;
- m. not to eliminate faults, damage and errors on central IT equipment and data carriers themselves but to report the same to the staff of the relevant IT operations group without delay;
- n. not to interfere with any hardware installations not intended for personal use without the express consent of the relevant administrators or IT operations group (e.g. laptops etc) and not to change the configuration of the operating systems, the system files, the relevant system-based user files or the network;
- o. to refrain from connecting modems or other data communications equipment. Exceptions must be agreed with the person responsible for operations in the user groups, D4 and the corresponding IT operations group;
- p. to provide information to the management of the relevant IT operations group on demand in justified individual cases – especially for the purpose of eliminating faults or if an abuse is suspected – regarding the programs and methods used and to allow examination of the programs as necessary;
- q. to agree on the processing of personal data with D4 and the relevant IT operations group and, without prejudice to the personal data-protection obligations of the user, to comply with all data-protection and data-security precautions (“Datenschutz- und Datensicherheitsvorkehrungen”)⁵ applicable at DESY⁵;
- r. to obtain the consent of the relevant responsible for the connection of additional systems to the internal network (*segment officer* “(*Segmentbeauftragten*)”). The requirements of the CSC as per the CSC Guidelines (“RSR-Richtlinien”)⁶ must be observed;
- s. to refrain from using services and programs with file-sharing functions, e.g. Internet exchanges, for non-official purposes.

3. Special attention is drawn to the following criminal offences:

- a. Data espionage (§ 202a Criminal Code (“StGB”))
- b. Data modification (§ 303a StGB) and computer sabotage (§ 303b StGB)
- c. Computer fraud (§ 263a StGB)
- d. Dissemination of pornographic depictions (§ 184 StGB), in particular retrieval or possession of depictions of child pornography (§ 184 (5) StGB)
- e. Dissemination of propaganda materials of unconstitutional organisations (§ 86 StGB) or incitement of hatred of minority groups (§ 130 StGB)

³ See <http://www.desy.de/rsr/intern/rsr-statements.html>

⁴ See <http://www-it.desy.de/wof/documentation/www-regeln.html.de>

⁵ See <http://www.desy.de/datenschutz>

⁶ See <http://www.desy.de/rsr/intern/rsr-statements.html>

- f. Insult, slander or libel (§§ 185 ff. StGB)
- g. Punishable breaches of copyright, e.g. by reproducing software, images or sound carriers in breach of copyright (§ 106 ff. German Copyright Act (UrhG))

Article 6 Exclusion from Use

1. The user permit may be wholly or partly denied, revoked or subsequently restricted in particular if
 - a. no proper application has been made or the details in the application are not or no longer true;
 - b. the requirements for the proper use of the IT equipment are not or no longer satisfied;
 - c. the authorised user is excluded from use under Article 6 (2);
 - d. the project planned by the user cannot be reconciled with the objects of DESY and the purposes set out in Article 4 (2);
 - e. the IT components to be used are connected to a network that must satisfy particular data protection requirements and there is apparently no valid reason for the planned use;
 - f. it is to be expected that the use applied for could have an unreasonable detrimental effect on other justified projects;
 - g. there has been a breach of other provisions of these Conditions of Use or of supplementary rules.
2. Users may be temporarily or permanently given restricted access to or excluded from the use of IT resources if they deliberately breach these Conditions of Use, in particular by breaching the obligations listed in Article 5 (abusive conduct)
or
abuse the information-processing systems for criminal acts
or
DESY suffers disadvantages through unlawful user behaviour.

3. The measures described in Para. 2 shall take place only after a previous warning has been issued to no effect. The person affected must be given the opportunity to make a statement to the responsible division management. The user must always be given the opportunity to save his or her data. Temporary restrictions on use decided on by the relevant IT operations group must be cancelled as soon as proper use appears to have been guaranteed. Permanent restrictions on use or the complete exclusion of a user from all further use can be imposed only for serious and repeated breaches as defined in Para. 2 and when proper conduct can no longer be expected in the future. The decision on permanent exclusion is made by a resolution of the directorate on application by the IT operations groups and after hearing division management and, in the case of DESY employees, the responsible Works Council. This does not affect any claims of DESY arising from the user relations.

Article 7 Rights and Duties of the IT Operations Groups

1. The central IT operations groups keep a user file on the user permits issued by them in which the users, e-mail addresses, names and addresses of the permitted users are listed.
2. If necessary for the purpose of eliminating faults for system administration or extension or for reasons of system security and for the protection of user data, the IT operations groups can temporarily limit the use of their resources or temporarily disable individual user codes. Where possible, the users affected must be notified in advance.
3. If there are actual indications that a user is holding unlawful content for use, the IT operations groups in consultation with division management may prevent any further use until the legal situation has been satisfactorily clarified. If DESY employees are involved, the responsible Works Council must be notified.

4. IT operations groups are entitled to examine the security of system/user passwords and the user data by regular manual or automated measures and to perform the necessary protective measures in order to protect IT resources and user data against interference from unauthorised third parties. If there is any need to change user passwords, access rights to user files or other user-relevant protection measures, the user must be notified of the same without delay.

5. IT operations groups are entitled, under the following rules, to document the use of the information-processing systems by individual users and to evaluate the same, however, only to the extent to which this is necessary

- a. to guarantee proper system operation,
- b. for resource planning and system administration,
- c. to protect the personal data of other users,
- d. for billing purposes,
- e. for the recognition and elimination of faults and
- f. for clarification and termination of unlawful use or abuse if there is justified cause to suspect the same.

Evaluations related to persons shall be erased without delay after the purpose has been achieved.

6. Subject to the requirements of Para. 5, the IT operations groups are also entitled, while complying with data secrecy, to inspect the user files if this is necessary to eliminate current faults or to clarify or terminate misuse if there are actual grounds to suspect the same. Nevertheless, messages and e-mailboxes may only be inspected if this is unavoidable for the elimination of current faults in the message service. The inspection must be documented in each case and the user must be informed in good time⁷.

7. Subject to the requirements of Para. 5, connection data and user data in communications (especially the use of e-mail) may be documented. However, only the circumstances of telecommunications, but not the private content of the communications may be documented, processed and used.

8. The IT operations groups are obliged by the statutory provisions to protect the secrecy of telecommunications and data.

9. Administrators of the groups have the same rights and duties as the IT operations groups.

Article 8 Liability of Users

1. The user is liable for all disadvantages which are suffered by DESY as a result of the abuse or unlawful use of the information-processing systems or user permit or caused by the fact that the user, by intent or gross negligence, fails to comply with the obligations arising from these Conditions of Use.

2. The user is also liable for such damages caused by third parties within the framework of the access and use facilities, if these persons are responsible for third-party use, in particular by having passed on their *user code and password* to third parties. In this case, DESY, at its discretion, can require that the user pay a usage fee for the third-party use.

3. The user must indemnify DESY from all claims brought against DESY by third parties for compensation, forbearance or otherwise because of misuse or unlawful conduct by the user.

⁷ See <http://www.desy.de/datenschutz/Administrator.html>

Article 9 Liability of DESY

1. DESY gives no guarantee that the systems will be free of faults or operate at all times without interruption. It is impossible to exclude the possibility of data being lost due to technical faults or confidential data becoming known as a result of unauthorised interference by third parties.

2. DESY assumes no responsibility for the accuracy of the programs provided. DESY is also not liable for the content, in particular for the accuracy, completeness or up-to-dateness of the information to which it merely provides access for the purpose of use.

3. Otherwise DESY is liable only for intent or gross negligence of its employees, unless there has been a culpable breach of essential cardinal duties. In this event, DESY's liability is limited to the typical damages foreseeable at the time of establishing the use relationship, unless there is intent or gross negligence.

Article 10 Arbitration Body

The data-protection officer acts as arbitration body.

Article 11 Coming into Force

At its 1491st session on 17 August 2006, the directorate passed the Conditions of Use for Information-Processing Systems at DESY. The Conditions of Use come into force on 17 August 2006.