Regulations of the Use
of the IT Facilities at the MPI for biophysical Chemistry

1. Scope
   (1) The following Regulations for Use contain general rules for the use of IT facilities at the MPI for biophysical Chemistry (hereinafter referred to as "MPI"). IT facilities include above all data processing equipment, communication systems and other facilities for computer-aided data processing, along with the attendant software.
   (2) These Regulations for Use also cover the use of privately-owned computing equipment officially approved for work purposes, as well as the use of MPI-owned computing equipment outside of the MPI.
   (3) All users of the IT facilities – irrespective of the nature of their legal relationship with the MPG – must comply with these Regulations for Use.
   (4) To the extent that legal provisions and/or (central) works agreements lay down compulsory regulations governing rights or obligations for MPG employees that diverge from these Regulations for Use, such legal provisions and works agreements shall take precedence.

2. Organisation
   (1) Each department or work group is to designate an IT administrator who is responsible for the IT infrastructure of the particular department. The IT Service, which is responsible for IT tasks regarding the entire institute, will additionally attend to tasks that cannot be resolved within the departments.
   (2) Several central IT services are provided by the “Gesellschaft für Wissenschaftliche Datenverarbeitung mbH Göttingen” (GWDG) (Society for Scientific Data Processing, Göttingen). The user regulations of the GWDG apply for the use of these services.
   (3) The IT administrators in the departments should generally be consulted first, then the IT Service. The IT Service will refer matters for which the GWDG are responsible to the GWDG.
   (4) The IT administrators of the departments are to discuss current problems or requests for change with the staff of the IT Service and the GWDG on a monthly basis. They are to prepare IT-related matters to be decided by the institute management. The results are to be recorded and forwarded to the executive director.

3. User Authorisation
   (1) Users have the right to use the IT facilities under the terms of these user regulations. They must at least have access to a computer in the institute and to an email account; however there are generally no further automatic rights such as the right to access a particular computer.
   (2) Users will receive authorisation for use of the IT facilities of the MPI and the GWDG from the IT Service only upon written application. A relevant application form must be fully completed. Users shall confirm the receipt of these Regulations for Use.
   (3) The user authorisation is generally limited to the period of employment or other contract arrangements or the length of stay as a guest. User authorisation may be granted for a limited period of time or restricted to a specific purpose. It can be denied, particularly when the user has violated his/her obligations under these regulations in the past.
(4) If a user breaches any of these terms or conditions, his/her user authorisation may be permanently withdrawn or temporarily suspended, or subsequently restricted. The relevant decision will be made by the Managing Director of the Institute. The users affected should be given the opportunity to state their own position prior to the withdrawal of the user authorisation, provided the ultimate purpose is not jeopardized as a result.

4. User Obligations
(1) Users shall refrain from any unlawful usage. Moreover, they shall refrain from any user conduct that may be detrimental to the MPG and/or harm the MPG's interests or its reputation in public.
(2) In particular, users are obliged
  1. to comply with the provisions set forth in the Regulations for Use and adhere to the restrictions of the user authorisation;
  2. refrain from any action that is detrimental to the orderly operation of the IT facilities of the MPI;
  3. to treat the entire IT facilities carefully;
  4. to work solely with the user authentication assigned to them under the terms of the authorisation;
  5. to ensure that no other persons obtain knowledge of the user passwords;
  6. to choose passwords that are difficult to guess and to change these regularly;
  7. to refrain from the unauthorised access of other users' information and from using, passing on or altering any other users' information that may have become known;
  8. to observe the MPG rules for the use of passwords;
  9. to comply with the statutory/contractual regulations for the protection of third party rights when using software, documentation and other data;
 10. to refrain from any attempts to rectify failures on their own, damage or errors in conjunction with the IT facilities, but to report the same without delay to the IT administrators;
 11. to refrain, without the express consent of the IT administrator, from interfering with the hardware and from changing the configuration of operating systems, system files, system-related user files and the network;
 12. to refrain from installing and/or using any hardware or software without the IT administrator's express consent;
 13. not to provide MPI-owned hardware and/or software to any third party for use;
 14. to return to the MPI, prior to termination of the user authorisation, all data, programmes and documentation which the MPI handed over to the user, or to which the MPI has some other contractual or legal claim in an appropriate form. Unless expressly agreed otherwise, the user shall not be permitted to retain copies of data or programmes following termination of the user authorisation;
 15. to observe the regulations of the GWDG when using IT facilities of the GWDG.

5. Rights and Obligations of the IT administrators
(1) IT administrators are those persons who are appointed by the MPI to administer the IT facilities of the institute. This includes the staff of the central IT group “IT & Electronics Service” (referred to as “IT-Service”) and the IT-administrators of the departments and groups, which have been appointed by the head of the group.
(2) The IT Service documents the user authorisations granted in a user database which is maintained in collaboration with the secretariats.
(3) Upon termination of the user authorisation, the IT administrators shall be authorized to deactivate and delete all of the user's data and programmes provided that such data will be of no further use to the institute.
(4) If so required for trouble shooting, reasons of system administration and security, as well as for the protection of user data, the IT administrators may temporarily restrict use of its resources or temporarily block individual user identifications. Wherever possible, the users affected are to be notified in advance of any such actions.
(5) According to the following rules, the IT administrators shall be authorized to document and evaluate the individual’s usage of the IT facilities, however only insofar as this is necessary
1. to ensure orderly system operation or
2. for resource planning and system administration
3. to protect the personal data of other users or
4. to account for expenses or
5. to detect and eliminate faults
(6) If there are reasonable grounds to suspect that a user is using the IT facilities in breach of the regulations as set forth under 4.1, the IT administrators may prevent any further use until the legal implications have been sufficiently clarified.
(7) Subject to the conditions set out in paragraph 6, the IT administrators shall also be authorized to inspect user files, provided this is required to correct current faults, or to clarify and prevent any form of misuse.
(8) The contents in individual users' emails or internet files may only be inspected, with the involvement the works council, where there is probable cause to suspect a relevant misuse. The logged data and/or contents will only be evaluated for the purposes of clarifying the suspicion in compliance with the legal options. The individuals affected must be notified of the inspection of their logged data and/or contents as well as of the results of the investigations as soon as this is possible without jeopardizing the investigation. The “Works Council Email and Internet Regulations” shall apply in the current version.
(9) The IT administrators shall be authorised to adopt regular measures to review the security of user passwords and user data, and to carry out necessary protection measures in order to safeguard IT resources and user data against unauthorized access by third parties. Should user-specific protection measures become necessary, the user is to be notified immediately.
(10) The IT administrators are obliged to safeguard telecommunications and data secrecy in accordance with the relevant legal provisions.

6. User Liability
(1) The liability and indemnity obligations of users who are in the employ of the MPG are subject to the general liability regulations agreed by contract of employment and to the general liability principles under labour law. Paragraphs 2 to 4 below shall apply for users who are not in the employ of the MPG.
(2) Users are liable for all damage and disadvantages arising for the MPG through improper or unlawful use of the IT facilities or owing to the users' culpable infringement of their obligations under these Regulations for Use.
(3) Users are liable for damage arising from third-party use in connection with the privileges of access and use granted to them if they are accountable for such third-party use.
(4) Users shall indemnify the MPG from all claims asserted by third parties arising from the users' culpable infringement of their obligations under these Regulations for Use.
7. Liability of the MPI

(1) The MPI provides no guarantee that the IT facilities will operate faultless at all times. Neither a possible loss of data due to system failures, nor the acquisition of confidential data through unauthorized third-party access can be ruled out.

(2) The MPI shall assume no responsibility for the accuracy of the programmes it provides. The MPI shall not be liable for the contents, in particular the accuracy, completeness and up-to-dateness, of the information to which it merely provides user access.

(3) In all other respects, the MPI shall be liable only for gross negligence or intent.

This Regulation of Use of the IT facilities replaces the User Regulations of July 15th, 2001 and will become effective on June 9th, 2008.

Göttingen, June 6th. 2008

Prof. Dr. Christian Griesinger
(Managing Director)