LEIBNIZ
FORSCHUNGSINSTITUT
FÜR MOLEKULARE
PHARMAKOLOGIE

IT Usage Regulations

Regulations on the Use of the IT Infrastructure at the Leibniz-Forschungsinstitut für Molekulare Pharmakologie (FMP)

Version: 2.1.6

Please note: This is a translated version for information purposes.
Only the German version is legally binding.

Preamble

The usage regulations are intended to ensure the unopposed, failure-free and secure use of the IT infrastructure of the Leibniz-Forschungsinstitut für Molekulare Pharmakologie (FMP). It establishes basic rules for the proper operation and use of the IT infrastructure and regulate the user relationships between the individual users and the FMP, as well as their rights and obligations.

§1 Scope of application

The usage regulations apply to the use of the IT infrastructure of the Leibniz- Forschungsinstitut für Molekulare Pharmakologie (FMP). The IT infrastructure consists of any data processing equipment, communication systems and other equipment for computer-assisted information processing, which are the property of the FMP and administered by the central IT or other administrators within the working groups of the FMP.

The proper setup, operation and functional monitoring of the IT infrastructure or parts of it is referred to administration and therefore of particular importance and responsibility. The corresponding paragraphs are irrelevant for users without administrative rights.

§2 Users, operators and usage

(1) The operator of the entire IT infrastructure is the Leibniz-Forschungsinstitut für Molekulare Pharmakologie (FMP). The overall responsibility for the proper and legal operation is in charge of the operator. The FMP commits all tasks needed to manage the IT infrastructure or parts of it to the administrators (in short: admins). An administrator is not a natural person, but a function or role that can be assigned to a user.

(2) The admins are technically able to view files, e-mails and network traffic of the users, as long as these items are not encrypted. However, admins are prohibited from doing so by the operator unless this is absolutely necessary for troubleshooting and to prevent fraudulent use.

(3) Administrators are:

(a) IT-Admins: the employees (members) of the central IT of the FMP - responsible for the entire central IT infrastructure;

(b) AG-Admins: the IT managers within the working groups - responsible for the dedicated decentralized IT infrastructure (including end devices)

(c) PC-Admins: every user who has an account with administrative privileges for administrative tasks on at least one end device within the IT infrastructure of the FMP.

(d) IT-Admins are usually AG- or PC-Admins, too. AG-Admins can in turn also be PC-Admins.

(4) The IT infrastructure is divided into centralized and decentralized infrastructure: The central IT infrastructure includes all systems that are maintained by the central IT (IT-Admins) of the FMP as well as services that are generally available and used by all users The decentralized IT infrastructure includes systems that are available to a limited group of users (usually work groups) and perform special tasks for users of that group. Decentralized systems are usually managed by the AG-Admins of the respective workgroups. End devices are not classified in these categories.

(5) The use of the IT infrastructure is made available to the users by the operator exclusively for official business cases in research and teaching, administration, education and training, public relations and public image of the FMP. Any deviating usage is not permitted by the operator.

Any use that overloads and/or disrupts the IT infrastructure is prohibited.

(6) The users consist of:

(a) All persons with a valid, employment or relationship contract at the FMP;

(b) Guests with a valid guest contract at the FMP;

(c) Guests without contractual obligations.

§3 Rights of use

(1) The holders of rights of use for the IT infrastructure and services of the FMP are all users described in § 2 para. 6a-b.

(2) The approval to the use of the IT infrastructure and services of the FMP is basically granted to users corresponding to §2 para.6a-b by issuing an account (user name and password).

(3) Accounts for users are always personal accounts. These accounts must only be used by the person authorized by the FMP. Handing out personal credentials to other persons or users is considered as a security breach.

(4) The user must face all the consequences if he/she has made the personal data accessible other persons.

(5) Users corresponding to §2 para.6a,b are entitled to use the central IT infrastructure once the account has been created by the central IT department.

(6) The rights of use for users corresponding to §2 para.6a,b are limited in time and ends up with the expiry of the employment relationship or the guest contract. Upon expiry of the employment relationship, the user loses the claim of an user account and the usage of services provided by the FMP.

(7) All provided services with the exception of e-mail are no longer available to the user when the contract ends up or the date of departure is arrived. The right to use his/her e-mail account can be extended one time only for furthermore 3 months. The special regulations for the e-mail accounts are only granted upon request of the user or the group leader.

(8) The FMP prohibits the automatic forwarding of e-mails to external accounts with the following exception: Upon request, automatic forwarding to external e-mail accounts of scientific institutions (institutes and universities) within Berlin may be approved due to close scientific cooperation. The forwarding is limited to a maximum of 3 months after the end of the user's employment with the FMP.

(9) All accounts of the user will be disabled by the IT-Admins immediately when the contract ends up or the date of departure is arrived, at the latest with the expiration of the extended usage of the e-mail account.

(10) The use of further decentralized IT infrastructure by users corresponding to §2 para.6a,b often requires the activation and/or creation of additional user accounts which are granted separately by the respective AG-Admin corresponding to §2 para.3b.

(11) Guests corresponding to § 2 para. 6c only get limited access to the IT infrastructure. Usually, they are entitled to use the guest networks. Access to other internal resources and services is prohibited. For special cases, the group leader decides whether access to these internal resources can be permitted after an individual examination. Special guest accounts are available in the workgroups for this purpose. The managers of these guest accounts maintain a list in which they write down which persons have used these accounts and during which period of time.

§4 Rights and duties of the users

(1) Users have the right to use the information and communication systems provided by the operator within the scope of the approval and in accordance with these IT usage regulations. In addition, in dealings with other operators, their supplementary usage and access guidelines apply, as these guidelines do not conflict with these usage regulations.

(2) When using the information and communication systems provided by the operator, the users are obliged:

(a) to follow the stipulations of the usage regulations and to comply with the regulations of the permission for use, in particular to comply with the purposes of use;

(b) to refrain from anything that could interfere with the proper operation of the IT infrastructure of the FMP and to use the available resources (such as PCs, printers, CPU capacity, disk storage space, bandwidth capacities, peripheral devices and consumables) responsibly, economically and ecologically;

(c) to treat the IT infrastructure of the FMP with care and consideration;

(d) to work exclusively with the user account issued to them;

(e) to ensure that no other persons gain knowledge of the accounts provided to the user and to take precautions to prevent unauthorized persons from gaining access to the IT infrastructure of the FMP; this also includes protecting the account with a strong and secure password;

(f) neither to hack nor to use third-party user accounts and / or passwords;

(g) not to take unauthorized access to information and data of other users and not to recycle, use or change information or data of other users without the permission of the operator;

(h) when using software, documents and other data, to comply with the statutory provisions, in particular those relating to copyright protection, and to observe the license conditions under which software, documentation and data are made available by the FMP;

(i) not to copy software, documents and other data provided by the operator, nor to take over or make them accessible to third parties, unless this is exclusively permitted, nor to use them for purposes other than permitted;

(j) not to supply any data/content via the IT infrastructure systems and/or to store it on IT infrastructure systems in violation of legal or licenses;

(k) not to remedy malfunctions, damage and errors in the IT infrastructure of the FMP - in particular in data processing (DP) equipment and data carriers - themselves, but to report them immediately to the IT- or AG-Admins;

(l) to immediately report the loss of IT devices and data carriers of the FMP as well as non-institutional end devices used for official purposes to the IT-Admins, the group leader and the data protection coordinator of the FMP or the data protection officer of the FVB. If a data protection violation is not reported to the supervisory authority within 72 hours, legal consequences may result;

(m) not to interfere with the IT infrastructure without the explicit consent of the operator, and in particular not to install any non-institutional systems or other access points into the IT infrastructure of the FMP without permission;

(n) to use the equipment provided by the FMP - in particular PCs and any kind of communication systems - exclusively for business purposes, not to install or use any third-party or private software, and not to make any system- or operation-relevant modifications;

(o) to provide the operator with information about programs and methods used or with access to the programs and the data collected with them in justified individual cases - in particular in case of justified suspicion of misuse-, upon request or for trouble-shooting purposes;

(p) back up all business-related data on the central network drives in order to minimize the risk of data loss;

(q) to secure their own personal data in such a way that, in the event of their loss within the IT infrastructure, no legal or financial damage is caused to the FMP.

(3) The users must use the IT infrastructure in such a way that it does not violate applicable law. Special reference is made to the following criminal offences:

(a) Spying out of data (§ 202a StGB), interception of data (§ 202b StGB) and preparation of spying out and interception of data (§ 202c StGB);

(b) Data alteration (§ 303a StGB) and computer sabotage (§ 303b StGB);

(c) Computer fraud (§ 263a StGB);

(d) Distribution of pornographic representations (§ 184 ff. StGB), in particular distribution, acquisition and possession of child pornographic writings (§ 184b StGB);

(e) Dissemination of propaganda material of unconstitutional organisations (§86 StGB) and incitement of the people (§ 130 StGB);

(f) Offences of honour such as insult or defamation (§ 185 ff. StGB);

(g) criminal copyright infringements, e.g. by copying software in breach of copyright (§ 106 ff. UrhG);

(h) Violation of the secrecy of telecommunications (§ 206 StGB).

§5 Appointment of administrators

Each administrator (in short: admin) has to be appointed in accordance with this regulations and introduced to the central IT. This does not apply to employees of the central IT (IT-Admins), as they are directly hired by the operator for the tasks of administration. The following regulations do not apply to users who do not have administrative rights on FMP's own IT systems and therefore do not have the function of an administrator.

(1) The stipulations in §3 and §4 also apply to any admin without restrictions.

(2) Decentralized IT systems are usually controlled by individual work groups. The work

group appoints skilled users as administrators (AG-Admins) to administer these devices. Furthermore, the working group also appoints PC-Admins to do user help desk tasks within their group. Generally the appointment is done by the group leader, unless an appointment is done by superordinate instances. The appointment can be revoked at any time by the group leader or by superordinate instances. The appointment is a formless processes in text form by sending an e-mail to the central IT of the FMP.

(3) A person can only be appointed as an AG-/PC-Admin if he/she is a user according to § 2 para. 6a-b and possesses the expertise and reliability required for the fulfilment of his/her tasks. These skills should ideally be proven by experience.

(4) If centrally administered, the AG- or PC-Admin gets at least one additional, personal account (admin account) with correspondingly extended rights for the fulfilment of administrative tasks. These admin accounts must not to be used for the general use of IT systems according to §3 para.1-10.

(5) AG-/PC-Admins must be sufficiently instructed about their responsibility and obligation in accordance with these usage regulations when they are appointed. The instruction shall be taken by the respective issuing IT/AG-Admins.

(6) The FMP (in particular the appointing working group) must co-work with the AG/PC-Admin in the fulfilment of his/her tasks. This concerns in particular the provision of the resources and information necessary for the fulfilment of his/her tasks.

(7) The AG/PC-Admins do their tasks in collaboration with the IT admins.

(8) The respective responsibility of the AG-/PC-Admins depends on the needs or requirements of the workgroup. Depending on the requirements, different roles and authorizations can be assigned. In the case of end device management, this means:

(a) If the PC-Admin has only to administer one end device (e.g. notebook), he/she only gets the authorization to administer the corresponding end device.

(b) If the AG-/PC-Admin should be responsible for several or all end devices within the group, he/she gets the corresponding authorization for all named end devices.

(c) A list of the appointed AG-/PC-Admins is kept by the central IT.

§6 Rights and duties of the operator as well as IT-/AG-/PC- Admins

The following regulations do not apply to users who do not have administrative rights on FMP's own IT systems and therefore do not have the function of an administrator.

(1) The roles of the IT-/AG-/PC- administrators entail a special responsibility to use these rights carefully. In particular, all security measures (security policies) must not be circumvent. The administrative rights can also be revoked again, if the regulations are violated.

(2) The IT-Admins keep documentation on the granted user authorizations, in which the username, e-mail addresses as well as the real names of the authorized users are listed.

(3) The FMP as the operator as well as the IT-/AG-/PC-Admins contribute to the prevention or detection of misuse in all IT matters within the framework of these usage regulations.

(4) The FMP as the operator and the IT-/AG-/PC-Admins (if responsible) may temporarily restrict the use of resources or block individual usernames. Such an action may take place for troubleshooting purposes, system administration and system expansion or for validation of system security and the protection of user data. If possible, affected users

will be informed before.

(5) If there are actual indications that a user is downloading, storing or making available illegal and/or unlicensed content on the servers, clients or other data carriers of the FMP, the FMP as operator and the IT-/AG-/PC-Admins (if responsible) may block the use and access of IT systems until the legal situation has been adequately clarified.

(6) The operator and the IT-Admins are entitled to check the security of system/user passwords and the data of users by means of regular manual or automated measures and to implement necessary protective measures, e.g. changes to insecure passwords, in order to protect the IT resources and user data from unauthorized access by third parties. The user must be informed immediately of any necessary changes to user passwords, access rights and other usage-relevant protective measures.

(7) In accordance with the following regulations, the operator and the IT administrators are entitled to document and evaluate individual users' of the IT infrastructure for a maximum period of 90 days, but only to the extend necessary. The data is collected by the operator for the following purposes, but in no case used for performance evaluations:

(a) to ensure proper system operation;

(b) for the detection and elimination of faults;

(c) for resource planning and system administration;

(d) for accounting purposes;

(e) to protect the personal data of other users;

(f) for the clarification and prevention of illegitimate or improper use in the event of justified suspicion.

(8) The evaluation of log data in accordance with §6 para.7e-f is done by the operator and the IT administrators exclusively in collaboration with the works council and the data protection coordinator of the FMP.

(9) The IT-/AG-/PC-Admins are obliged to maintain confidentiality.

(10) The operator and the IT-/AG-/PC-Admins are obliged to comply with the usage and access guidelines of other operators when dealing with their computers and networks.

(11) In case of troubleshooting, system administration and expansion or for reasons of system security and to protect the data of the users, the FMP as operator and the IT-/AG-/PC-Admins (if responsible) may access the IT resources provided by the FMP (in particular PCs and communication systems of any kind). The following general conditions apply:

(a) The IT-/AG-/PC-Admins (if they are responsible) have the possibility to check system processes and files on the devices and are able to initiate a remote session;

(b) The processes described under (a) are only legitimate if preceded by a malfunction report and a verbal or written order by the user;

(c) The user must agree to the connection of an IT-/AG-/PC-Admin with remote access software on the effected end device;

(d) The operator, the IT-/AG-/PC-Admins as well as all users are not allowed to connect to end devices, that are used by several persons, via remote session without the consent of the active user;

(e) The user is obliged not to leave the workstation for the duration of the remote session by the IT-/AG-/PC-Admin.

(12) The IT-/AG-/PC-Admins do all their tasks on IT systems in accordance with the needs and objectives of the FMP as operator and of the working group according to the instructions of the group leader. The IT-/AG-/PC-Admins perform their tasks to the extent granted to them in an independent manner.

(13) The IT-/AG-/PC-Admins also perform maintenance tasks on the IT systems (if not centrally controlled) within their responsibility. This includes, among other things, the installation of updates and security patches for the operating system as well as for the antivirus and other software installed on that systems.

(14) The IT-/AG-/PC-Admins are obliged to avoid security breaches by improper or negligent handling of the provided administrator account on both: the IT systems within their responsibility and on other components in the network.

(15) The IT-/AG-/PC-Admins inform the users of the effected IT systems as well as other affected persons if their working processes or other interests are affected during thier performance of tasks. They inform the users promptly about measures, if possible before the tasks will be started, so that the affected users have sufficient opportunities to exert influence.

(16) The IT-/AG-/PC-Admins undergo further trainings and inform themselves about innovations and/or problems on the IT systems to be administered so that they can always perform their tasks professionally and appropriately in accordance with the state of the art and the objectives and other requirements. The IT-/AG-/PC-Admins themselves are responsible for the professional selection of necessary further training measures.

§7 Regulations for handling end devices not belonging to the institute

(1) Users corresponding to §2 para.6a,b should always work with institute devices. Institute devices are end devices that are procured by the FMP and managed by IT-/AG-Admins. Non-institutional end devices are all other end devices.

(2) If no institute device is available, end devices not belonging to the institution may be used subject to the conditions set out in paragraphs 3-5.

(3) All users are obliged to comply with these regulations even when using end devices not belonging to the institute and are subject to all conditions, including liability regulations.

(4) The use of non-institutional end devices within the IT infrastructure of the FMP is only permitted in designated areas:

(a) For using the Internet access exclusively, the user has access to the guest networks of the FMP;

(b) Upon request, the central IT department, as the operator of the IT infrastructure systems, grants employees restricted access to internal services and resources using end devices not belonging to the institute. All communications between these end devices and the IT infrastructure of the FMP are monitored. Encrypted connections are - as far as possible - decrypted, examined and encrypted by the security gateways;

(c) Access to internal IT systems and resources with non-institutional end devices is permitted on a read-only basis. Direct interventions with more than read permissions (including transferring, writing, modifying, deleting data) with non-institutional end devices are prohibited;

(d) Data transfer from and to the institute only permitted via dedicated gateways.

(5) There is no entitlement to the installation of software and licenses procured by the FMP on non-institutional end devices. The users themselves are responsible for ensuring that a legitimate license is available for the software on the non-institutional end devices used for official purposes. If special software is used on decentralised IT systems with non-institutional end devices, the responsible working group must clarify the legitimacy.

§8 Liability of users and IT-/AG-/PC-Admins

All conditions apply to both users and IT-/AG-/PC-Admins.

(1) The user is liable for the improper, abusive, illegal or unlicensed use of the provided IT services and resources and the resulting consequences, insofar as these result from culpable breach of the obligations arising from these terms of use by the user.

(2) The user is also be liable in accordance with the working rules and labour law for damage caused by third party use of resources, services and rights made available to him/her, if he/she is responsible for this third party use, in particular in the event of handing out his/her account data (user and/or admin account) to third parties.

(3) The user shall indemnify the FMP against all claims if third parties assert claims against the FMP due to abusive, illegal or unlicensed conduct on the part of the user for damages, injunctive relief or in any other manner. The FMP will take legal action against the user if third parties take legal action against the FMP on the basis of these claims.

(4) The user is liable to the FMP for any damage caused by software installed on non-institutional end devices.

§9 Liability of the FMP as operator

(1) The FMP does not guarantee that the systems will run error-free and without interruption at all times. Possible data losses as a result of technical faults, security incidents and the disclosure of confidential data by unauthorized access by third parties are minimized by using state of the art techniques, but cannot be ruled out.

(2) The FMP takes no responsibility for the correctness of the software provided. The FMP is also not liable for the content, in particular for the correctness, completeness and up-to-dateness of the information to which it merely provides access for use.

(3) The FMP takes no responsibility or liability for any improper, abusive, illegal or unlicensed use of non-institutional end-user devices, even when using it in FMP's IT infrastructure; the responsibility and liability lies solely with the user.

(4) The FMP takes no responsibility for the correct functionality and security of non- institutional end devices when it inside or outside the IT infrastructure of the FMP.

(5) As the operator of the IT infrastructure, the FMP takes no liability for the proper operation of end devices not belonging to the institute, nor is it liable for any damage caused to equipment not belonging to the institute in the course of using the IT infrastructure.

§10 Consequences of improper or unlawful use

(1) In the event of violations against legal regulations or against the provisions of these usage regulations, in particular §4 (Rights and duties of the users), the operator may restrict or completely revoke the right of use. It is irrelevant whether the violation resulted in material damage or not.

(2) Violations in the sense of §6 para.5 and §10 para.1 may result in consequences under civil service- , employment- and criminal law.

(3) The decision on a permanent restriction of use or the complete exclusion of a user's access is made by the operator. Possible claims of the FMP arising from the usage relationship remain unaffected.

§11 Legal Status and Organization of the IT of the FMP

(1) The central IT of the FMP represented by the Head of IT is subordinate to the administration and the operator. The central IT is responsible for the operation of the central IT infrastructure.

(2) The IT Commission establishes the link between the users and the central IT. It ensures an optimal flow of information, knowledge transfer and an increase in transparency in the data processing technology of the FMP:

(a) The IT Commission is an advisory committee engaged in topics of IT infrastructure and communication systems in the FMP;

(b) Each working group appoints at least one person responsible for IT related topics within that group (typically the AG-/PC-Admins), who represents the interests of the group in the IT Commission;

(c) It presents the issues discussed to the institute's management in a suitable form as information or recommendations for decision;

(d) It passes on learned IT knowledge to other users and the leaders of the working groups;

(e) The work is based on the guidelines and suggestions of the institute's management, the group leaders and the needs of the institute's users;

(f) The IT Commission meets at least once per quarter.

§12 Come into effect

These usage regulations shall come into effect on 1.1.2023.

Berlin

Prof. Dr. Volker Haucke

Managing Director of Leibniz-Forschungsinstitut für Molekulare Pharmakologie

Berlin

Dr. Nicole Münnich

Managing Director of Forschungsverbund Berlin e.V..