



Preamble

These IT usage regulations form the basis for the use of the IT services that FIAS makes available to its users. This agreement is binding and a prerequisite for use. It must be explicitly accepted. At the same time, FIAS undertakes to ensure the availability and confidentiality of the IT services and the processed data.

§1 Scope of application

This user agreement applies to the IT infrastructure operated by FIAS, hereinafter referred to as infrastructure. It applies equally to use by academic and administrative users. It is binding for internal and external IT services.

§2 Users

1. The infrastructure is available to FIAS employees, doctoral students of the graduate schools that FIAS organizes or in which it participates, as well as guests for the duration of their stay at FIAS to fulfill their tasks in research, administration and the provision of the necessary IT and communication services. Use beyond the duration of the stay for participation in a scientific project must be explicitly requested and is limited in time.
2. The term user data is used in the following for
 - a. Personal data stored in the context of access creation,
 - b. personal files (home directory), e-mail messages, databases,
 - c. files created by the system for the user.
3. Group data is shared data that is the responsibility of the respective group management.
4. Administrative data are accounting-relevant, personal and other necessary data of the FIAS administration, which are the responsibility of the management.
5. All of the above-mentioned groups of persons are users within the meaning of this agreement.

§3 Access to the infrastructure

1. Access to the non-public services (e.g. e-mail address, Internet access, use of the servers) is by means of a user ID and password and, if necessary, cryptographic keys. Setup and adjustments can be requested via the e-mail address access@fias.uni-frankfurt.de, stating
 - Surname, first name
 - Work group
 - Duration from to
 - Status (e.g. doctoral student, postdoc, administration)
 - Building and office number
2. Access must be requested via the head of the research group or the head of administration.
3. Access is restricted to the respective person. Access is only granted subject to acceptance
 - these IT user regulations
 - consent to the processing of personal data for the purpose of user administration



4. Passwords are only issued personally and may not be passed on to third parties in any form. Those technically responsible will never ask for passwords; such requests are to be regarded as an attempt to deceive.
5. Users are responsible for all actions carried out via their access.
6. Arrangements for the shared use of group data must be made in consultation with the respective group leader.
7. The access granted is limited in time and can be subsequently restricted or revoked.

§4 Obligations of the users

1. The infrastructure is used in accordance with the relevant laws and not in contravention of applicable law. Violations must be reported to FIAS immediately (see section §5).
2. Users undertake to use the infrastructure and the resources made available to them responsibly. In this context, they are liable for any damage caused by them.
3. Users shall regularly read their e-mail messages in order to be able to deal with administrative messages and inquiries in particular. If a user cannot be contacted for more than three months (non-response), it is assumed that use has ended (see section §5).
4. Commercial use of the infrastructure is excluded.
5. Private Internet and e-mail use is not permitted.
6. Devices belonging to or provided to FIAS may only be operated (i.e. installed, maintained or modified) by the central IT administration. Exceptions are installations in the user-specific file area, which are carried out in compliance with the respective license regulations, which can be requested from the IT administration.
7. Network-based services (including web services) within the infrastructure and those offered in the name of FIAS via commissioned third parties may only be operated by the central IT administration of FIAS. This excludes verifiably secure standard services that are exclusively accessible internally and serve purely group-internal or informative purposes (e.g. presence announcements) and those that are only accessible to the operating individual.
8. Electronic publications in the name of FIAS may only be made via content management systems operated by FIAS. This applies in particular to web services.
9. Deviations from point 6 are only possible via a supplementary agreement for the self-administration of devices. Deviations from 7 and 8 are only possible via a supplementary agreement for the self-administration of services.
10. In the case of publications in the form of images, sound, film and/or text, the provisions of copyright law must be observed.
11. The publication of internal FIAS information marked as confidential is prohibited.
12. The user is permitted to operate his/her own network-compatible devices within the infrastructure, provided that the devices are used in accordance with the relevant legal regulations and do not endanger the infrastructure. The respective license regulations for the installation and use of software on these devices must be complied with by the user. Point 6 and point 8 sentence 2 also apply. The devices must also be protected against attacks and misuse by using suitable technical measures (regular updates, malware scanners, firewalls, etc.) where appropriate.
13. Administrative data may not be stored on private data carriers/devices, on mobile devices only in encrypted form and on external systems (cloud or similar) only with the verifiable approval of the management.



IT: Terms of use

14. In the case of data with special protection requirements (e.g. health data, highly confidential data), the person responsible for this must actively ensure the necessary protection in consultation with the IT administration and document this.

§5 Services and liability of FIAS

1. FIAS provides the best possible technical support at a reasonable cost. There is no entitlement to constant availability. FIAS will give advance notice of planned downtimes for administrative purposes. Any downtime will be kept as short as possible.
2. FIAS protects user data and data of third parties as far as possible and at least in accordance with the relevant legal regulations.
3. FIAS reserves the right to regularly check the security of accesses and systems by scanning for weak passwords, insecure keys, legal problems and technical vulnerabilities, to inform those affected and, in urgent cases, to block or decommission affected accesses and/or systems.
4. FIAS reserves the right to prevent circumvention of the provisions of this agreement by technical means. If an attempt at circumvention is detected, the access in question will be blocked immediately in consultation with the management and the data protection officer.
5. For the purpose of technical support, system maintenance or in the event of suspected misuse, the IT administration may gain access to stored data in consultation with the data protection officer.
6. FIAS uses mandatory malware scanners to protect its systems when receiving messages. Messages recognized as malicious are rejected before delivery.
7. FIAS actively operates spam analysis systems and adapts them to current requirements.
8. The FIAS ensures a regular backup of the persistent data by transferring it at least incrementally once a night in encrypted form to external storage systems and, if necessary, supplementing this with internal backup processes. Backup copies are stored for at least eight weeks and at least the last three change statuses within the scope of the backup cycles.
9. FIAS reserves the right to operate a joint infrastructure with partners for the purpose of redundancy or synergy and to use external service providers to provide its services. Both may affect the stored data within the scope of technical necessities (reliability, data backup, data processing). FIAS shall ensure that the aforementioned cooperations and commissions are carried out in accordance with this agreement.
10. FIAS reserves the right to block access in the event of non-response in accordance with §4 point 3 and in the event of breaches of the user agreement. User data available at this time and any group data will be archived and stored for a maximum of one year from this point in time. Within this period, the user can notify FIAS of a request for unblocking, data backup or data deletion, which FIAS will fulfill, provided that there are no compelling reasons (in particular according to §3) to the contrary. If no such request is made, FIAS will irretrievably delete the data at the end of the one-year period.
11. This user agreement and the associated services can be terminated by the user, the group management or the management with a notice period of three months. In this case, access, user data and, if applicable, group data will be irretrievably deleted at the agreed time.
12. If no follow-up arrangement is found after the regular end of the agreed relationship between the user and FIAS, access will continue for a further three months. Thereafter, access, user data and, if applicable, group data will be irretrievably deleted.
13. The deletion of user data and, if applicable, group data in accordance with 10, 11 or 12 may be suspended if the data may be subject to extended statutory or funding-related retention obligations. Apart from such obligations, user data will not be archived beyond the time of deletion. The user is responsible for the prior backup of his/her own data (if desired or required).
14. FIAS is not liable for any damage caused by the use of IT services.



§6 Coming into effect

These regulations enter into force on 20 February 2024 and replace the IT usage agreement dated 04 May 2022.

Frankfurt am Main, 20 February 2024

Prof. Dr. Eckhard Elsen

Scientific director

Frankfurt Institute for Advanced Studies (FIAS)

Ruth-Moufang-Straße 1

60438 Frankfurt am Main

<https://fias.institute>

Contact

Questions, concerns and messages should be addressed to the relevant department in the institute:

- IT general: it@fias.uni-frankfurt.de
- Access: access@fias.uni-frankfurt.de
- Media technology: multimedia@fias.uni-frankfurt.de

In case you need to contact the FIAS administration, please use office@fias.uni-frankfurt.de

Contact with the FIAS data protection officer is possible via datenschutz@fias.uni-frankfurt.de