MAX PLANCK INSTITUTE
FOR MULTIDISCIPLINARY
SCIENCES

Terms of Use for the IT Services of the Max Planck Institute for Multidisciplinary Sciences (MPI-NAT)

Objective

The Institute's task is to set up and operate an efficient, reliable, secure and legally compliant IT infrastructure in the service of science. This requires the cooperation and active collaboration of all users, which is bindingly defined by these terms of use.

Scope

- The terms of use apply to the use of the IT infrastructure, consisting of network, IT systems and applications at all locations of the MPI-NAT.
- The terms of use also apply to the use of private IT devices for official purposes as well as to the use of official devices outside the institute.
- All users of the IT infrastructure - regardless of the nature of their legal relationship with the MPI-NAT - are obliged to comply with the regulations of these terms of use.
- When using services provided by other providers, such as the "Gesellschaft für Wissenschaftliche Datenverarbeitung mbH Göttingen" (GWDG), their terms of use apply in addition.
- Insofar as statutory provisions and/or Works Council agreements regulate rights or obligations for MPG employees that deviate from the present terms of use, these regulations shall take precedence.

Usage permission and admission to use

- All persons who have an ongoing employment or service contract, a guest contract with the MPI-NAT or who have any other contractual relationship with the MPI-NAT are permitted to use the facilities.
- Admission to use is granted exclusively for the fulfillment of official business or contractual duties or for scientific purposes in research, teaching and training. Any other uses are regulated by the Max Planck Society.
- Admission to use is granted upon application and simultaneous binding acceptance of the terms of use.
- Usage permission may be granted for a limited period of time and restricted to certain IT resources.
- Usage permission expires when the contractual basis expires.
- A user may have his/her permission to use the institute’s ITservices withdrawn for good cause. This decision is the responsibility of the institute's management. The user should be given the opportunity to make a statement before permissions are withdrawn, insofar as this does not jeopardize the achievement of the purpose.

User Obligations

General

- Users must refrain from any illegal or, according to generally applicable ethical standards, inappropriate usage behavior. In addition, they must refrain from any usage behavior that is likely to cause harm to the Max Planck Society or the institute or to damage the reputation or harm the interests of the Max Planck Society or the institute.
- Devices provided by the institute are to be treated with care. Changes to the equipment must be approved by the IT staff.

Reporting IT problems

- IT problems of any kind (system crashes, incorrect behavior of applications that previously ran without errors, suspicion of intrusion by unauthorized persons or malware in the system) must be reported immediately to the IT staff.

Software installation

- Only software that is licensed correctly and is required for official purposes may be installed on the institute's computers.
- The installation and execution of additional software by users is only allowed after permission has been granted.

Access control

- When leaving the workplace, the computer must be protected against unauthorized access ("locked"). Exceptions are possible if the work requires it (e.g. lab computers recording and controlling experiments) and if it is ensured by other means that no unauthorized access can take place.
- As far as technically possible, equipment must be protected against unauthorized access by password, PIN, fingerprint or other means.
- The storage of confidential or personal data on notebooks or storage media (such as USB sticks, external hard drives) is only permitted if the media or the data are encrypted.

Dealing with access data

- Secrecy: Your own secret access data (passwords, private keys) must be treated confidentially and must not be disclosed to any other person. When entering secret access data make sure nobody observes you.
- Suspicion of compromise: If there is any sign that the access data might be compromised, they must be changed immediately and the IT Service must be notified.
- Strong passwords: If passwords are used for authentication, they should be strong, i.e.
  - be sufficiently long (at least 10 digits), random and complex
  - not based on any facts that another person can easily guess or infer from personal data such as names, telephone numbers, birthdays, etc.
- Passwords should
  - not be stored or written down in plain text
  - differ for different user accounts; this is especially true for external accounts
  - be generated and managed in a password manager

  - be changed at the first login, if they are initial passwords
- If the option for 2-factor authentication exists, it should be used.

E-mail

- For official e-mail communication, only the use of institute's e-mail accounts is permitted.
- It must be ensured that e-mails of the institute are read regularly.
- Systematic forwarding of official e-mails to external providers or access by an external provider to the institute's e-mail account is not permitted.
- Sensitive data must not be sent unencrypted by e-mail.
- Internet links and attachments in e-mails should only be opened if their trustworthiness can be assumed from their source and context.

Data handling

- Official data must always be stored on IT systems of the institute, the GWDG or other IT systems approved by the institute. If it is necessary for business purposes and the data only require normal protection, other systems (external cloud services, private devices) may also be used.
- Data should be stored on the central file servers if possible. If they are stored locally or on other servers, it must be ensured in particular that they are backed up regularly.
- Any processing of personal data requiring high protection must be coordinated with the data protection coordinator. The user is primarily responsible for the protection of data and programs on the Institute's systems. When processing personal data, the user is obliged to implement suitable protective measures in accordance with data protection laws, whereby the Institute's IT provides suitable protective measures.
- Upon leaving the institute, all official data must be handed over to the superior in an orderly manner. In particular, compliance with "good scientific practice" must be ensured, which requires that data that form the basis of publications must be kept at the institute for at least 10 years.
- Any existing non-official data must be stored in a "PRIVATE" folder and deleted before leaving the company.

Rights of IT staff

The IT staff with extended rights are the appointed IT administrators of the "IT & Electronics Service" (hereinafter referred to as "IT Service") and the IT officers of the departments and working groups. Only they are authorized:

- to block and delete all data and programs of the user after the expiration of the usage permission, provided that the data will not be used in the institute any further.
- if it is necessary, to temporarily restrict the use of IT resources or temporarily block individual user IDs in order to rectify faults, for reasons of system administration and system security or to protect user data. If possible, the affected users should be informed of this in advance.
- to document and evaluate the use of the IT infrastructure by individual users, but only to the extent necessary
  1. to ensure proper system operation, or
  2. for resource planning and system administration or

3. to protect the personal data of other users or
4. for accounting purposes or
5. for the detection and elimination of malfunctions

The works agreement "Nutzung technischer Einrichtungen zur Überwachung von Arbeitsplatz-Computern" (Use of technical equipment for monitoring workplace computers) must be taken into account.

- to prevent further IT use if there are indications that a user is using the IT infrastructure unlawfully. However, this shall only be done until the legal situation has been sufficiently clarified.
- to inspect user data, insofar as this is absolutely necessary for the elimination of current malfunctions.

Liability of the user

- The liability and indemnity obligations of users who are employees of the MPG are subject to the general liability regulations agreed by contract of employment and to the general liability principles under labor law. For users who are not employees of MPG, the following paragraphs apply.
- Users are liable for all damages and disadvantages arising for the MPG through improper or unlawful use of the IT infrastructure or owing to the user's culpable infringement of their obligations under these Terms of Use.
- Users are liable for damages arising from third-party use in connection with the privileges of access and use granted to them if they are accountable for the third party use.
- Users shall indemnify the MPG from all claims asserted by third parties arising from the user’s culpable infringement of their obligations under these Terms of Use.

Liability of the MPI-NAT

- The MPI-NAT provides no guarantee that the IT infrastructure will operate faultless at all times. Neither a possible loss of data due to systems failures, nor the acquisition of confidential data through unauthorized third-party access can be ruled out.
- The MPI-NAT shall assume no responsibility for the accuracy of the programs provided. The MPI shall not be liable for the content, in particular for the accuracy, completeness and up-to-dateness, of the information to which it merely provides user access.
- In all other respects, the MPI-NAT shall be liable only for gross negligence or intent.

The rules of use are updated at least every 5 years or as required. They are published on the Institute's intranet.

These terms of use come into force on 1.1.2022.