IT acceptable use policy governing the provision and use of information technology systems and processes at Friedrich-Alexander-Universität Erlangen-Nürnberg (IT-R)

Passed by the Executive Board on 25 November 2020

Table of contents

Preamble

Information technology is an essential tool for research, teaching, studying and professional development, for using the library and for numerous tasks and jobs in administration and in the technical operation of Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU). This policy is intended to facilitate the use of IT facilities, systems and processes at FAU both locally and within the network securely, without hindrance and with as little disruption as possible. It governs, in particular, the rights and obligations of users and the responsibilities, rights and obligations of the system operators.

This policy

- is based on the functions of universities as defined by law and their mandate to preserve academic freedom
- sets forth general rules for the correct operation of IT infrastructure, systems and processes
- sets out the rights of third parties which must be observed (e.g. software licences, terms and conditions of network operators, data protection and privacy)
- stipulates rules of conduct and obliges all parties to use resources efficiently.
- lists possible consequences of violations of the IT acceptable use policy at FAU.

Section 1 Scope

(1) This policy applies to the use of desktop computers, mobile devices, memory, software, cable-based and wireless data networks and other technical equipment (IT infrastructure) which is used internally at FAU or externally by third parties on behalf of FAU for electronic information processing purposes and to the systems and processes operated on the basis of this infrastructure in the area of information processing for academic and administrative purposes.

(2) This policy shall apply across the whole of FAU for all individuals and institutions entitled to use IT at the University (Section 2 (1) and (2)) and system operators (Section 5 (1)).

Section 2 Users (individuals and institutions), purpose

(1) Those entitled to use the IT infrastructure, systems and processes at FAU pursuant to Section (1) are in particular
   a) Members of FAU
   b) Members of institutes of higher education entitled to use the services provided by the Erlangen Regional Computing Centre (RRZE) within the regional concept of the RRZE
   c) Members of other institutes of higher education with respect to the high performance computing systems made available to these institutes of higher education
   d) Cooperation and contractual partners of FAU, to the extent necessary for the purposes of the collaboration or for meeting contractual obligations
   e) Legal entities governed by private law (official associations, foundations, cooperatives etc.) that have pledged in their statutes to support FAU and help it meet its legal obligations, according to the terms of an existing cooperation agreement
   f) Legal entities of which FAU is a shareholder
   g) Public institutions, in particular research and educational institutions, student services and authorities.

(2) Other individuals or academic institutions can be granted authority to use the IT services if this benefits or is closely linked to FAU tasks and provided the ability of the principal users stated in (1) to use the services is not jeopardised in any way.

(3) The IT infrastructure, systems and processes at FAU are available to the authorised individuals and institutions enabling them to carry out their tasks in research, teaching, studying and professional development, for the other tasks of institutes of higher education stated in Section (2) of the Bavarian Higher Education Act and for administrative duties.

Section 3 Authorised use

(1) Anyone who wishes to use the IT infrastructure, systems and processes at FAU requires authorisation to do so (Section 2). An application must be filed if the relevant data are not included in automated records. An exception applies to systems and services which are established for anonymous access (e.g. information services, library services, short-term guest log-in credentials for conferences).

(2) When granting authorisation, only those details which are directly required for making a decision on the application may be collected/used. In general, the following data may be collected: last name, first name, date of birth, gender, organisational unit to which the applicant belongs, description of the purpose of use, signature of applicant. Official photo ID or alternatively other official documents shall be required as proof that the personal details are correct. The system operators (Section 5 (1)) can also approve other suitable procedures for checking identity.

(3) The system operators shall decide whether to approve the application (Section 5 (1)). They may make authorisation dependent on certain criteria (evidence of a certain knowledge of how to use the services, only certain types of user, rules of use or transfer on the basis of foreign trade legislation) and impose certain requirements regarding use of the services.

(4) Authorisation shall be refused if:
   a) The requirements pursuant to Section 2 nos. 1 to 2 are not met
   b) The intended use is outside the scope described in Section 2 (3)
   c) Sufficient reason has not been given for authorisation to be granted
   d) There are reasonable grounds to believe that the applicant will not fulfil their responsibilities as a user as set out in Section 4
   e) Sufficient resources are not available for the intended purpose based on existing capacity utilisation, the resources applied for have already been reserved for special purposes or the resources are obviously unsuitable for meeting requirements
   f) The resource requirement presents a potential risk to other systems, data networks or legally protected goods of other persons (personal data, working materials, research results etc.).

(5) Authorisation may be temporarily or permanently restricted or withdrawn in the event of any subsequent action that is considered sufficient reason for refusing authorisation under paragraph 4 or if the user has failed to pay any applicable usage fees for a period longer than two months.

(6) Measures that restrict the authorisation to use IT systems defined in paragraph 5 shall be applied according to the principle of proportionality. The procedure for investigating misuse set out in Section 6 must be observed. Further proceedings under criminal, disciplinary or employment law, or de-registration due to misconduct are not precluded by the refusal of authorisation.

Section 4 Rights and obligations of users

(1) Users are authorised to use the IT infrastructure, systems and processes provided by FAU only for the purposes named in Section (2)(3) and only in accordance with this policy and any other terms of use or agreements that apply in individual cases. Any form of misuse of IT systems and services at FAU is prohibited. Misuse shall be defined as using IT systems and services provided by FAU for criminal or other illegal purposes, as well as:

a) Operating unauthorised hardware within the FAU network insofar as this has not been approved by the system operator responsible (Section 5 (1))
b) Installing, operating and using systems, processes and programs which are not related to official duties
c) Installing and using software without a valid licence
d) Using IT facilities for private purposes if this exceeds marginal use, or poses a risk to the operation and security of the IT infrastructure, systems and processes or threatens a positive and cooperative working atmosphere. Altering network configurations for private purposes shall always be prohibited.

(2) Explicit reference is made to the following forms of misuse which are punishable under criminal law (German Criminal Code, StGB):

a) Data espionage (Section 202a StGB)
b) Phishing (Section 202b StGB)
c) Acts preparatory to data espionage and phishing (Section 202c StGB)
d) Handling stolen data (Section 202d StGB)
e) Data manipulation (Section 303a StGB) and computer sabotage (Section 303b StGB)
f) Computer fraud (Section 263a StGB)
g) Dissemination of pornography (Section 184 StGB), in particular dissemination, procurement and possession of child pornography (Section 184b StGB) and making pornographic content available through broadcasting or telemedia services (Section 184d StGB)
h) Dissemination of propaganda material of unconstitutional organisations (Section 86, StGB) and incitement of hatred (Section 130, StGB)
i) Insulting or defaming others (Section 185, StGB).

(3) Users are obliged to:

a) Observe copyright law (UrhG) and other legal regulations when using software, documentation and other data.

b) Not copy or distribute software, documentation and data unless explicitly authorised, or use software, documentation and data for any unauthorised purposes, in particular for commercial use. Explicit reference is made to penalties for copyright infringement, for example by making illegal copies or software or unlawfully distributing films or music (Sections 106 et seq, UrhG).
c) Permit regular inspection of software installed on devices provided by the University and comply with any requests to install auditing software for this purpose.

(4) Users are further obliged to:
a) Work only using log-in credentials which they have been explicitly authorised to use; in particular users are prohibited from using log-in credentials belonging to other users. Sharing log-in credentials with other users (for example username and password) or storing credentials in systems and devices that could be used by a third-party is prohibited (function accounts which are explicitly authorised for use by multiple users for a specific purpose are excluded from this rule; the account owner is required to maintain a record of authorised users).
b) Protect the IT infrastructure, systems and processes at FAU from unauthorised access by using a password which the user is obliged to keep secret, or a similar or superior method of authentication.
c) Take precautionary measures to prevent third parties from gaining unauthorised access to data; in particular by using a password that meets current technical requirements and logging out properly from any systems or processes or taking measures to secure their device such as locking the screen while they are absent from their workspace.
d) Immediately report any incidents that come to their attention which may be relevant to IT security to the IT officer responsible and inform the RRZE by e-mail at abuse@fau.de.

(5) Users are responsible for all actions that are performed using their log-in credentials and may also be held liable for actions performed by a third party if it can be proven that the account owner has acted negligently in allowing unauthorised access using their log-in credentials. In such cases, FAU is entitled to claim reimbursement of usage fees from a user which would have been incurred if the third party had been authorised to use the account.

(6) Users are obliged to use any IT equipment and resources provided by FAU (workstations, CPU capacity, storage, bandwidth, peripheral devices and consumables) in a responsible and economical way. Users are further obliged to avoid causing any disruption to IT operations insofar as foreseeable, and avoid to the best of their knowledge any activities that may cause damage or disruption to other users or to the IT infrastructure, systems and processes at FAU.

(7) Users may not take any of the following actions without authorisation from the system operator responsible (Section 5 (1)):
a) Modify hardware configurations or use available interfaces to alter network or system infrastructure (for example by connecting proxy servers, switches and access points).
b) Change the configuration of systems (operating systems, data networks or similar) or processes.

(8) Users must observe data protection and privacy regulations and the data protection regulations of FAU in all activities which involve the processing of personal data. This also applies if personal data is processed using IT services provided by third parties (for example cloud services).

(9) In the event of an investigation of misuse or service disruption caused by improper use, the rights of the system operator (Section 5 (1)) and the procedure set out in Section 6 must be observed immediately by users.

(10) Users are obliged to:
a) Observe all other terms of use and agreements issued by the FAU CIO committee or the system operators in addition to this acceptable use policy.
b) Comply with terms of use and access policies of other operators when using devices and networks belonging to them.

Section 5 Rights and obligations of system operators

(1) In addition to the RRZE, system operators are defined as all organisational units of FAU (faculties, schools, departments, chairs, institutes, central institutions, units and other divisions) that operate or provide IT infrastructure, systems and processes as set out in Section 1 (1) independently or with the support of internal or external service providers. If several FAU organisational units are responsible for the administrative, technical or content-related aspects of a system, they must designate a single system operator as responsible for the system within the meaning of this policy. Managers are responsible for ensuring the proper operation of IT systems as set out in this policy within their FAU organisational unit. Although operational tasks may be delegated to technical staff (administrators), managers remain ultimately responsible for the proper operation of IT systems.

(2) System operators must use the IT infrastructure, systems and processes provided at FAU exclusively in carrying out their tasks. In particular, this means that additional systems and processes may not be introduced, if an equivalent service which could be used as an alternative is already provided by FAU. This also applies if a usage fee applies for using or sharing the service. The CIO committee will decide in any case of doubt and may grant exceptions.

(3) The system operators are authorised and obliged to record and maintain appropriate proof of authorisation. The documents and information that are created or collected when applying for or extending authorisation, as well as any usage data that may arise, may be stored automatically and must be deleted when the authorisation expires. This does not apply to data to which certain retention obligations apply (e.g. accounting data).

(4) The system operator is authorised to document and monitor the utilisation of IT infrastructure, systems and processes by individual users but only to the extent that this is necessary:

a) To ensure the proper operation of IT systems and services
b) For resource planning and system administration
c) To protect the personal data of other users
d) For billing purposes
e) To detect and resolve service disruptions
f) To investigate and prevent misuse or illegal activities

(5) The system operators shall contribute in an appropriate manner, in particular in the form of regular spot checks, to prevent, resolve, or investigate misuse. System operators are authorised to check passwords and usage data and take preventative action, for example changing passwords that are easy to guess, to protect the IT infrastructure, systems, processes and usage data from unauthorised access by third parties. Users must be directly informed of any required changes to their password or any other security measures that affect their usage of IT systems and services.

(6) System operators are authorised to inspect usage data in compliance with data protection and privacy regulations and take preventative measures insofar as this is necessary to resolve service disruption or to investigate and prevent misuse. Inspecting usage data for any other purpose is not permitted.

(7) System operators are authorised and obliged to temporarily exclude users from using the IT infrastructure, systems and processes either in part or entirely and may ban users permanently in extreme cases if it can be assumed that the user will not fulfil their responsibilities as set out in Section 4. If measures that restrict use of IT systems and services are taken, the provisions set forth in Section 3 (6) and the procedural provisions in Section 6 must be observed.

(8) System operators are obliged to observe data protection and privacy regulations and the data protection regulations of FAU and to maintain confidentiality.

(9) System operators must observe agreements concluded with HR representatives. They are also obliged to support staff councils in the performance of their duties under the Bavarian Employee Representation Act (BayPVG) by providing information, making documents available and granting rights of inspection and access.

(10) System operators must appoint RRZE contact persons who are responsible for administrative and content-related agreements relating to the use of IT infrastructure, systems and processes in their specific capacity.

(11) System operators are obliged to:
a) Observe all other terms of use and agreements issued by the FAU CIO committee in addition to this policy.
b) Comply with terms of use and access policies of other operators when using devices and networks belonging to FAU.
c) Bring their own usage guidelines to the attention of users in a suitable form.

Section 6 Procedure for investigating misuse

(1) If there are sufficient grounds for suspecting misuse of IT infrastructure, systems and processes as defined in Section 4, the user is obliged to provide the system operator with information about installed programs and methods used and to grant access to data, insofar as this is necessary to clarify the suspicion.

(2) The FAU data protection officer must be informed by the system operator in the event of suspected misuse pursuant to paragraph 1 and can participate in the investigation at his or her discretion. If an FAU employee is suspected of misuse, Human Resources must also be involved in the event of suspicion of criminal or other unlawful actions and, while safeguarding the legitimate interests of the person concerned, the staff council responsible must be involved in the investigation. Insofar as there are no exigent circumstances, the aforementioned authorities must be involved before actual and/or legally relevant measures are taken.

(3) Users who are affected by measures investigating misuse may involve their data protection officer. Users under investigation for misuse may request involvement of the official data protection officer. If the measures refer to employees of FAU as defined in Section 4 BayPVG, the affected employee is entitled to involve not only the official data protection officer but also a representative of their staff council.

(4) Investigations according to this procedure must be documented.

Section 7 Liability of users and FAU

(1) Users shall be liable in accordance with the respective liability provisions for all damages incurred by FAU as a result of their failure to comply with their obligations under Section 4 of this policy.

(2) In accordance with the respective liability provisions, the users are also liable for damages resulting from unauthorised use by third parties if they are responsible for this third-party use due to misconduct, for example by forwarding log-in credentials.

(3) The users shall indemnify FAU against all claims asserted by third parties on the basis of misconduct as defined in paragraph 2.

(4) FAU does not warrant that its IT infrastructure, systems and processes are free from errors and available at all times without interruption. Possible loss of data due to technical faults cannot be excluded.

(5) FAU assumes no responsibility for the functionality of the programs provided. FAU is also not liable for the content, in particular for the accuracy, completeness and validity of the information to which it merely provides access.

(6) In all other respects, FAU shall only be held liable in the event of intent and gross negligence on the part of its employees, unless there is a culpable breach of material obligations, the observance of which is of particular importance for achieving the purpose of the usage agreement. In this case, FAU's liability shall be limited to typical damages which were foreseeable at the time of the establishment of the usage agreement.

(7) Possible public liability claims against FAU shall remain unaffected by the above provisions.

Section 8 Other provisions

(1) This policy may be supplemented by the system operators with further provisions appropriate for their IT infrastructure, systems and processes, provided that these do not conflict with the provisions of this policy. The FAU CIO committee must be informed about more extensive regulations. If data protection and/or employee representation issues are affected by the amendments, these are only permissible with the participation and consent of the official data protection officer and/or the staff council responsible. Regulations that exist on the date that this policy enters into force and that are compatible with its provisions shall continue to apply. Incompatible regulations will be replaced with compatible regulations and invalid regulations shall no longer apply. For the amendment of existing regulations, the procedural provisions according to sentences 2 and 3 above shall apply accordingly.

(2) Usage fees for IT infrastructure, systems and processes are available in the respective fee regulations.

(3) In the event of technical and organisational differences of opinion between users and system operators arising from the interpretation and application of this policy, an agreement shall be sought from the FAU CIO committee. If no agreement can be found, the Executive Board will reach a decision. Matters relating to legal affairs will be managed by the appropriate office in university administration.

(4) Future amendments to this policy shall be subject to consultation to the extent that they have an impact on the usage and working conditions of employees pursuant to Section 4 BayPVG.

(5) The place of jurisdiction for all legal claims arising from the user agreement is Erlangen.

Section 9 Final provisions

This policy shall enter into force on the day following its publication. It replaces the Usage Guidelines for Information Processing Systems of the University of Erlangen-Nürnberg (SEKORA regulations) of 2 June 1995.