Regulations on the Use of the Information Processing Infrastructure of the Bauhaus-Universität Weimar

In accordance with § 5 par. 1 in connection with § 79 par. 2, no. 1 of the Thuringian Higher Education Act (ThürHG) effective 7 July 1992, and as amended by Article 1 of the Third Law amending the Thuringian Higher Education Act of 12 May 1999 (GVBI. S. 276), the Bauhaus-Universität Weimar issues the following regulations governing the use of the information processing facilities at the Bauhaus-Universität Weimar (IT infrastructure). The Senate of the Bauhaus-Universität Weimar approved these regulations on 3 November 1999.

These user regulations were presented to the Thuringian Ministry of Science, Research and Art on 10 December 1999.

- See the Announcements of the Bauhaus-Universität Weimar: *MdU 12/2000*
- Attachment 1: Regulations on the operation of web servers and information provided via web servers
- Attachment 2: Regulations of the Bauhaus-Universität Weimar governing the data communication network HABNET and the connection to wide area networks

Preamble

The purpose of these regulations is to ensure that the information processing and data communication infrastructure of the Bauhaus-Universität Weimar remains operational, accessible and secure for members, employees and guests of the university. They also serve to fulfil the legal obligations of the Bauhaus-Universität Weimar. They provide the basic rules for proper operation of the IT infrastructure and regulate user relations.

§ 1: Explanation of terms

1. The Bauhaus-Universität Weimar is referred to hereafter as the “institution”, the university’s data communication network “HABNET” as the “data communication network” and the “Service Centre for Computer Systems and Communication” as the “SCC”.

2. In the context of these regulations, the term “IT infrastructure” refers to all information processing systems (workstation computers, pool computers, central and local servers, peripheral devices, data communication network, software) and components thereof, which are owned by the institution or the state of Thuringia, or are placed at their disposal by contractual agreement.

3. The users, as referred to in these regulations, are students, employees and guests who have permission to use components of the IT infrastructure of the Bauhaus-Universität Weimar in accordance with § 4.

4. The operators of the IT infrastructure of the Bauhaus-Universität Weimar, as referred to in these regulations, are those who prepare and provide access to the IT infrastructure and carry out the respective administrative tasks in its day-to-day operation.

§ 2: Rights of use

1. The members and employees of the institution have the right to use the hardware, software, internal data communication network, the approved wide area networks and SCC services in compliance with their respective intended purposes for conducting study- and work-related tasks in research, teaching, administration, central services, education, continuing education programmes and public relations activities of the institution. Usage for purposes beyond those intended requires prior approval, insofar as it is significant, complies with § 5 and does not adversely impact the interests of other users.

2. Members of other universities, universities of applied sciences or employees of public service institutions of the state of Thuringia can also use the IT infrastructure, insofar as their usage does not significantly compromise the intended purpose of the IT infrastructure of the institution.

3. Use of the institution’s IT infrastructure by or for other individuals, companies or institutions is permissible in exceptional cases.

4. The regulations provided in Attachment 1 pertain to the operation of the web servers and the creation of web pages.

5. The “Regulations of the Bauhaus-Universität Weimar for the data communication network HABNET and the connection to wide area networks” (see Attachment 2) remain in effect.

§ 3: Application procedure

1. Applications to use the IT infrastructure are processed by the SCC.
   Members and employees of the institution are required to present appropriate identification. Students are asked to present their certificate of enrolment or proof of re-registration.

2. In accordance with §2 par. 2 and 3, applicants must submit their applications in writing to the SCC. The application must contain the objectives of usage with regard to content, the requested duration of usage, the desired services and the names of all individuals seeking authorisation. Applicants must submit a separate application to the responsible system administrator for permission to use local resources.

3. One part of the application requires that the applicant declare on record that he/she has read and will comply with the regulations on the use of the IT infrastructure and its facilities, as well as the regulations governing data protection.

§ 4: Authorisation

1. Authorisation to use the IT infrastructure is granted on the basis of available capacity.

2. Authorisation is granted on an individual basis and cannot be transferred to other persons.

3. Authorisation to use the data communication network, the central server and other services of the SCC is granted by the director of the SCC or an employee of the SCC on his/her behalf.

4. Authorisation can be denied, restricted or revoked if the conditions provided in § 2, par 1, 2 and 3 do not or no longer apply, or if such is deemed necessary with respect to the intended purpose or the required capacity exceeds the available resources of the IT infrastructure. The terms of usage may also depend on whether the user possesses relevant knowledge on how to use the desired IT systems and IT services.

5. Users receive written confirmation of authorisation for the use of the central resources with their corresponding user login data.
   The respective system administrator is responsible for issuing authorisation and configuring user access to local servers and workstation systems.

6. Authorisation granted to employees, who wish to use the systems or components of the IT infrastructure of the Bauhaus-Universität Weimar, automatically expires at the end of their employment contract.
   Permission to use local systems can be cancelled at an earlier date irrespective of employment status.

7. Authorisation granted to students, who wish to use the IT infrastructure, expires when they are removed from the register.

8. In accordance with §2, par. 2 and 3, the confirmation of authorisation must also include its duration of validity.

9. The usage agreement can be cancelled by the user in writing at any time.

10. With the cancellation of the usage agreement, the system operator has the right to delete all data and programs, which the user stored in specially designated storage areas on data carriers in the systems of the IT infrastructure.

§ 5: Obligations of the user

The user is obliged to:

- Observe the restrictions in the usage agreement.

- Notify the SCC regarding all changes which affect the conditions of authorisation.

- Inform the SCC in advance if the user intends to leave the institution or if a student should change his/her status to that of an employee of the Bauhaus-Universität Weimar.

- Comply with all legal provisions, these regulations and possible existing regulations on the use of central and local resources (e.g. computer-pool rules) of the institution. It is not permitted to use the IT infrastructure for criminal, terrorist, racist, discriminatory, libellous or pornographic purposes, or to post material containing propaganda for unconstitutional organisations or in any way violate the law.

- Handle the devices, systems, facilities, documentation and data carriers with care and make no attempt to technically manipulate or alter the hardware.

- Ensure that all software licenses have been legally obtained, and if not, to purchase such licences prior to using the software on computer systems of the Bauhaus-Universität Weimar.
  This does not apply to software installed in the student computer pools, or when permission is explicitly issued by the Bauhaus-Universität Weimar. The term "usage" also refers to the act of copying software.

- Refrain from making changes to or deleting provided software without the required system administrator rights. Distribution of software to third parties is not permitted, especially if prohibited explicitly in the license terms.

- Refrain from viewing, using, deleting, copying or altering system data, data in personal home folders or third-party e-mails no matter what the reason. Furthermore, users are not permitted to modify system settings (e.g. access rights) in folders and files, over which he/she has no administrative authority. The use of user login data of third parties is prohibited.

- Prevent unauthorised access to personal user login data (particularly passwords) by third parties, change passwords regularly and follow recommendations for creating secure, personalised passwords. The user is responsible for all actions and activity conducted under his/her user login with respect to the IT infrastructure – even when such actions are carried out by third parties to whom the user has intentionally or negligently provided access to his/her login data.

- Apply in writing to the institution's data protection officer for permission to store personal data in accordance with data protection regulations on workstation computers or servers of the institution.

- In public rooms where access to the IT infrastructure is offered, users are obliged to follow the operator's instructions provided by employees, student- or research assistants, who are responsible for ensuring compliance with the regulations. Users are also obliged to present proof that they indeed have permission to use the facilities.

- Comply with the house rules.

- Respect the schedules of usage times posted in the computer pools.

- Observe the fundamentals of economy and efficiency, and pay the fixed fees determined by the respective facility for consumables, rentals and leasing, etc.

- Immediately notify the responsible administrators in case of malfunctions, damages or errors in computer systems or technical equipment, and if necessary, block their further use to prevent subsequent malfunctions, accidents or fires.

- Personally safeguard self-developed or saved programmes and data, which are not protected by the security measures integral to the system in an appropriate fashion so that damage by unintended overwriting, technical malfunctions, loss or changes can be prevented.

- Immediately return user IDs, loaned documentation, hardware and software licences following their period of usage without prior request of the SCC or respective departmental unit.

- Pay for the costs of telephone and data network services accrued through accessing the data communication network from home offices, student halls of residence, approved enterprises or external institutions, insofar as the institution has not previously agreed in writing to cover such costs. Users or their respective departmental units are also obliged to cover costs accrued for services provided outside the institution, insofar as the institution has not explicitly agreed in writing to cover such costs.

§ 6: Rights of the operator of the IT infrastructure

1. Upon the user's prior consent, the operator of the institution's IT infrastructure has the right to use the user's data for internal, administrative tasks in accordance with the applicable data protection laws. The SCC as the system operator of the institution's central server has the right to publish e-mail addresses and the users' names on internal university IT systems. This right pends prior consent by the applicant. Applicants are asked to provide or deny their consent on the application form.

2. The SCC is permitted access to student files kept at the Office of Student Affairs for the purpose of approving and verifying student user status. The file only contains the student's first and last name, registration number and degree programme. The SCC is not permitted to use this data for any purpose other than those mentioned above.

3. The SCC has the right to verify and protocol data transmissions (including e-mail communication) in the data network and the use of the central system for the purpose of conducting network management tasks. This supports the SCC in the areas of:
   - Resource planning and system administration
   - Protecting the personal data of other users
   - Accounting tasks
   - Recognising and eliminating malfunctions
   - Investigating and prohibiting illegal or improper use of the IT infrastructure

   The SCC also reserves the right to conduct automatic password monitoring on the central servers in order to identify weaknesses in security. The same applies for administrators of local systems.

4. If there is suspicion that these regulations or legal provisions have been violated, the system operator has the right to monitor the use of the IT infrastructure. The applicable data protection policies remain unaffected.

§ 7: Revocation of authorisation

1. If the SCC should discover that the user violated regulations as described in § 5 or Attachments 1 and 2, it may issue a warning or temporarily or permanently revoke or restrict authorisation. The user is given the opportunity to state his/her position orally or in writing. The user may also request that the chairperson of the SCC Advisory Board act as mediator. In any case, the user is allowed to safeguard his/her data, insofar as this does not conflict with criminal law.

2. The SCC may revoke authorisation of usage on a permanent basis or completely exclude a user from accessing the IT infrastructure only in cases of serious or repeated violations when appropriate behaviour in the future is deemed unlikely.

3. In instances of misconduct by members of the institution (students excluded), the member's supervisor is responsible for issuing warnings and restricting or revoking authorisation. In cases of student misconduct, the director of the SCC in agreement with the student's dean of studies is responsible for making a decision on courses of action. For all other users, the President is responsible for making the decision.

4. If it is not possible to come to a decision in accordance with par. 1, authorisation may be temporarily suspended until the legal circumstances or procedure is clarified. In this case, the system operator, or someone acting on his/her behalf, is responsible for making the decision. The responsible director must be immediately and fully informed of the situation.

5. The revocation of authorisation does not release the user from all or part of his/her obligations as provided by these regulations.

6. Users, whose authorisation has been revoked, are not entitled to damages incurred due to the revocation of authorisation.

7. If authorisation is revoked or restricted, the user has the right to formally contest the decision with the President of the institution. The President issues an objection notice.

§ 8: Liability

1. Users of the IT infrastructure, as well as the information providers on the web servers, are fully liable for damages deliberately or negligently caused in connection with the use of the IT infrastructure. The liability provisions applicable to public servants remain unaffected.

2. The institution and the operators of the IT infrastructure assume no liability for the consequences of computer usage, data security, deficiencies and the operability of the data communication network and functionality of the provided hardware and software.

§ 9: Equal treatment clause

Terms of status and function as applied in these regulations pertain to both sexes to an equal degree.

§ 10: Transitional and concluding provisions

1. Authorisations issued before these regulations entered into effect remain valid. Individuals, to whom these new regulations apply, shall be informed thereof by means of appropriate publications.

2. These regulations enter into effect on the first day of the month following their public announcement by the Bauhaus-Universität Weimar.
   The “Regulations for the operation of the data network HABNET” effective 14 July 1992 (Announcements by the President 6/92 p. 115) are hereby simultaneously rescinded.

Weimar, 1 November 1999
Prof. Dr.-Ing. Zimmermann
President

Attachment 1

Regulations on the operation of web servers and information provided via web servers

§ 1: Technical details

1. The SCC operates a central Internet server with the address www.uni-weimar.de.

2. The "university webmaster" is a member of the SCC who possesses all access rights to the server with the address www.uni-weimar.de and its files and who can assign temporary access rights to others. He/she is responsible for the technical availability, security and maintenance of the server.

3. Chairs and departments may set up their own web servers and appoint their own "webmasters". The SCC must be informed of the addresses of these servers if they are located outside the Bauhaus-Universität Weimar.

4. Access to publicly offered web documents must be recorded via log files. These log files are to be stored for an appropriate period of time so that they can be evaluated if necessary.

5. At the request of the information providers, webmasters can block access to certain files or folders via customised settings.

§ 2: Substantive details

1. The responsibility of the information provider, or those who allow access to information provided by external parties via the web server of the university, extends to ensuring that the information is legally unobjectionable (particularly with regard to civil, criminal, procurement, copyright, trademark and administrative laws).

2. As a rule, information offered by external parties, or links to such information, are not to be published on the web servers of the Bauhaus-Universität Weimar.
   Exceptions can be made provided that the information is closely related to the main processes of research and instruction and is presented in such a way that its relevance to the Bauhaus-Universität Weimar is recognisable. Decisions regarding such exceptions are to be made by the responsible professor or department head. Other information or links to companies, enterprises or products which do not merit exemption from this rule are only permitted on the basis of contractual agreements between the Bauhaus-Universität Weimar and the respective enterprise in agreement with the responsible webmaster.

§ 3: Additional regulations regarding web information offered via the domain www.uni-weimar.de.

1. Information provided via the domain is divided into two categories.

   - Departmental sites or web pages by members and employees of the university, for which is there is no standard layout for the information they provide. The respective information provider, who must identify himself on at least one of the web pages, bears full responsibility for the content and layout of the site. This responsibility extends to the inclusion of online links to other information providers.

   - "Official" web pages which contain central and general information in a standardised layout. The head of public relations and media of the university bears responsibility for these pages. If there is uncertainty as to which category a certain webpage belongs, the head of public relations and media must decide.

2. A university working group is responsible for determining the structure of the content and the design of the "official" web pages. This working group is comprised of the following members:

   - The head of public relations and media
   - The university webmaster
   - One member from each faculty, selected by the respective faculty deans
   - A representative of the university corporate design committee

3. The working group publishes the results of its consultation on the web server of the university in accordance with par. 4.

Attachment 2

Regulations of the Bauhaus-Universität Weimar governing the data communication network HABNET and the connection to wide area networks

§ 1: Basic conditions and subject of the regulations

1. The "operator" of the data communication network, as referred to in these regulations, is the "Service Centre for Computer Systems and Communication" (SCC) of the Bauhaus-Universität Weimar.

2. The data communication network of the institution is a centrally-operated infrastructural facility. It provides comprehensive data communication within the institution and offers access to data communication and telecommunication networks operated by external providers which are not affiliated with the institution.
   The data communication network and telephone system of the institution can jointly use and share components with one another. The necessary shared usage agreements are to be drafted and concluded by the respective providers themselves.
   All parties must comply with the existing provisions of the telephone regulations and the telecommunication service agreement.

3. In buildings with structured wiring, the data communication network ends at the data connection sockets. In buildings without structured wiring, special termination points (e.g. distribution boxes) can be installed in agreement with the operator of the data communication network and the building's IT representative. The fixed interfaces with third-party connections, or with wide area networks and the institution's telephone network, also represent termination points in the data communication network.

§ 2: Establishment, expansion, operation and use of the data communication network

1. The SCC has developed technical concepts for expanding the data communication network, taking into account requirements mandated by the executive committees of the institution, user requirements and technical innovations. These are to be realised according to the available resources and predetermined priorities. The SCC is also responsible for collaborating with the contracted providers, which have been commissioned to offer access to wide area networks at the institution.

2. Data communication at the institution is conducted on the basis of standards, or de-facto standards. The operator is responsible for deciding on authorisation of the transmission protocols in the data communication network on the basis of the user requirements. In this respect, user requirements can only be denied if:

   - There is reason to believe they will disrupt the operation of the network.
   - They would place a disproportionately high load on the network or result in high operational costs.
   - There are insufficient or no financial resources available to safeguard these transmission protocols.
   - The necessity is not justified by university administrative tasks or the demands of academic processes.

3. Only computers, transmission facilities and devices approved by the operator are permitted to connect to the data communication network.

4. Departmental units of the institution are permitted to operate logically separate subnetworks as long as a written agreement with the operator of the data communication network has been concluded, in which the interface is defined.

5. Only the operator of the data communication network and responsible telecommunication employees are permitted access to the physical systems, i.e. the system distribution switchboards.

6. Should certain data transmission protocols require freely selectable IP addresses, these addresses may only be provided by the operator. The operator can transfer the duty of issuing addresses to the departmental units of the institution for fixed subnetworks.

§ 3: Obligations of the operator of the data communication network

The operator is obliged to:

1. Ensure the secure, smooth and uninterrupted operation of the data communication network and work closely with the contracted partners entrusted with providing access to wide area networks in order to meet the respective contractual agreements.

2. Continually monitor the technical status of the data communication network and the load on specific components, and to modify the network configuration and hardware to meet changing demands. The operator is responsible for notifying the planning department with regard to budgetary requirements and apply for allocation of the necessary budgetary funding.

3. Document the expansion measures of the data communication network and inform the public on how to use the network's possibilities in an appropriate form.

4. Announce planned interruptions of operation for the purpose of maintenance, restructuring and expansion of the data communication network in an appropriate form and with advance notice, and to keep these interruptions as short as possible. If the system malfunctions, users must be informed (if possible) about usage restrictions caused by the disruption.

5. Provide assistance to users with questions regarding data protection and data security when using the data communication networks.

§ 4: Obligations of the user

The user is obliged to:

1. Contact the operator to receive the necessary addresses before connecting any devices to the data communication network if these addresses have not already been automatically assigned. The user must inform the operator of the location of the connected device and provide the name of a responsible contact partner.

2. Use only the data transmission protocols approved by the operator.

3. Make no attempt to technically manipulate, alter or carry out administrative actions on components of the data communication network without prior authorisation.

4. Use network resources in such a way that does not adversely affect other users. Transmissions, which place a disproportionate load on the network in comparison to the available access capacity, must be coordinated with the operator of the data communication network in advance.

5. Work together with the operator to localise errors if the data communication network malfunctions. If the operator discovers that the user's device is causing disruptions to the data communication network, the user must disconnect or shut down the device until the operator can ensure trouble-free operation again.