**English Translation**

# Regulation (Statute) for Terms and Conditions of Use for the Communication and Data Processing Infrastructure of the University of Lübeck

of 29 November 2016 (NBl. HS MSGWG Schl.-H. p. 101)

amended by:
Statute of 29 August 2017 (NBl. HS MBWK Schl.-H. p. 76)
Statute of 14 March 2018 (NBl. HS MBWK Schl.-H. p. 18)
Statute of 13 June 2018 (NBl. HS MBWK Schl.-H. p. 43)

## Preamble

The purpose of this Regulation for Terms and Conditions of Use [hereinafter referred to as Regulation for Use] is to ensure the unhindered, secure and as trouble-free as possible use of the communication and data processing infrastructure of the University of Lübeck and its affiliated institutions, while respecting the applicable data protection regulations. The Regulation for Use safeguards the statutory functions of the University of Lübeck and its mandate to preserve academic freedom. It establishes basic rules for the proper operation of the infrastructure and thus regulates the relationship of use between the individual authorized users and the data processing infrastructure operator (hereinafter referred to as data network operator).

## § 1
## Scope of application

This Regulation for Use applies to the use of the communication and data processing infrastructure of the University of Lübeck and its affiliated institutions. The communication and data processing infrastructure consists of data processing equipment, communication systems – including telecommunications systems – and other computerized information processing equipment of the University of Lübeck and its affiliated institutions.

## § 2
## Duties and responsibilities of the data network operator

(1) The data network operator is responsible in particular for the following duties:

1. The planning, realization and operation of the communication infrastructure of the University of Lübeck for tasks in research, teaching and degree programs, administration and health care,

2. coordination of procurement of the communication infrastructure, in particular advisory opinions on investment measures, usage analysis of existing system components and requirements planning,

3. provision and maintenance of trouble-free and uninterrupted operation as much as possible of the communication infrastructure,

4. administration of address spaces and namespaces,

5. provision of communication services and central servers,

6. support of authorized users in the use of the services.

(2) To ensure proper operation of the communication infrastructure, the data network operator may issue further rules for the use of the communication infrastructure, e.g. the use of the WLAN, access to the data network via 802.1x or technical organizational standards for the operation of the communication infrastructure.

## § 3
## Authorized user

(1) Authorized to use the communication and data processing infrastructure are:

1. members and affiliates of the University of Lübeck according to § 13 HSG,

2. representatives of the University of Lübeck for the performance of their duties,

3. members and affiliates of institutions affiliated with the University of Lübeck,

4. members and affiliates of the UKSH [University Medical Center of Schleswig-Holstein],

5. members and affiliates of other institutions of higher education by special agreement,

6. other government research and educational institutions and authorities of the State of Schleswig-Holstein and the Federal Republic of Germany by special agreement,

7. and the Schleswig-Holstein student union [Studentenwerk].

(2) Other individuals and institutions may be authorized to use or to offer services for scientific purposes or to fulfil the tasks of the state institutions of higher education, provided that this does not affect the interests of authorized users referred to in paragraph 1.

(3) Contractors of the University of Lübeck (such as external companies) may be authorized to use services offered through the data network operator for the performance of their contractual obligations, provided that they do not affect the interests of the authorized users referred to in paragraph 1. Excluded hereof are private uses.

## § 4
## Authorization and use of Internet and e-mail

(1) Basically, authorization follows automatically after hiring or enrolment/matriculation. Otherwise, on application using the form „Antrag auf Zugang zur Datenverarbeitungsinfrastruktur der Universität zu Lübeck" ["Application for access to the University of Lübeck's data processing infrastructure"].

(2) Permission for use is limited to the period of academic studies, employment/activities or the proposed project at the University of Lübeck and its affiliated institutions.

(3) The authorization for the use of the communication and data processing infrastructure takes place strictly and exclusively for scientific purposes in research, teaching and academic studies, for purposes of the university administration, further education as well as for the fulfilment of other legal functions of the University of Lübeck.

(4) The private non-commercial use of Internet services is permitted by the University of Lübeck, except for the group of individuals referred to in § 3 paragraph 3, if it is insignificant and the special function of the communication and data processing infrastructure and the interests and rights of other authorized uses are not affected.

(5) To protect the IT systems from viruses and Trojans and similar threats, it is not permitted to download, open and save files from the Internet and e-mail attachments for personal use with office devices. Internet use is forbidden for games of chance, bets and similar Internet activities, which have an addictive potential and are thus a potential health hazard for authorized users.

(6) Permission to use the Internet for private purposes in accordance with the provisions of this Regulation for Use is nevertheless granted exclusively with regard to those who have previously given their consent in accordance with Appendix 1. The submission of the declaration of consent is voluntary and freely revocable for the future. However, as long as consent has not been given, only official use for work or academic studies is permitted. Granting the potential for private use to this extent is a purely voluntary service extension of the University of Lübeck and is revocable under declaration of specific grounds. With the permission for the private use of the Internet access, no claim on the availability of the service and support is constituted.

(7) The use of e-mail accounts of the University of Lübeck is only permitted for work/academic studies-oriented purposes. Thus, it is prohibited to use the work/academic studies-oriented e-mail account for private e-mail traffic.

(8) The read/write access to a private e-mail mailbox (webmail) administered by an external service provider is permitted for the staff members/students, as long as there are no conflicts with work/student-oriented interests and no e-mail programs made available for official purposes are used.

(9) If, in the case of an incoming e-mail, the sender, the content or the attachment appears to be in doubt, the IT Service Center (ITSC) must be immediately informed. It will then decide how to further handle the situation and inform the executive committee, if necessary.

(10) An e-mail containing confidential content or personal data may only be sent externally (outside the University of Lübeck's data network) if the message is encrypted and the recipient is able to decrypt the e-mail. Other secured administrative networks (e.g. via VPN – Virtual Private Network) are considered internal in this sense.

(11) The data network operator may make the authorization dependent on the utilization of existing proficiency concerning the use of the communication and data processing infrastructure. The proficiency can be acquired at the beginning of the employment/activity period or academic studies at the University of Lübeck by attending an orientation.

(12) To ensure proper and trouble-free operation, the data network operator may also combine the permission for use with a limitation of the online time, as well as other usage-related terms and conditions.

(13) If the capacity of the communication and data processing infrastructure is insufficient to accommodate all authorized users, the resources may be appropriately allocated to each user as the authorization can only be made within the limits of available capacities.

(14) Permission for use can be completely or partially denied, revoked or subsequently restricted by the data network operator, especially if

1. there is no proper application or the information in the application is not or no longer applicable,

2. the conditions for the proper use of the communication and data-processing infrastructure do not or no longer apply,

3. the authorized person has been excluded from use according to § 7,

4. the proposed project of the authorized user is not compatible with the tasks of the University of Lübeck's communication and data processing infrastructure and the purposes set out in § 4 paragraphs 3 to 10,

5. the existing communication and data processing infrastructure is unsuitable for the requested use, or is reserved for specific purposes,

6. the capacity of the resources, the use of which is being requested, is insufficient for the planned use due to an existing degree of capacity utilization,

7. the data processing components to be used are connected to a network which must comply with special data protection requirements and no factual reason for the planned use is apparent,

8. it is to be expected that the requested use unduly interferes with other legitimate projects.

## § 5
## Use of Voice over IP (VoIP)

The VoIP system is used exclusively for message transmission. Use of the VoIP system and related communication services is regulated in the „Richtlinie über den Betrieb und die Nutzung eines auf Voice-over-IP basierenden Telekommunikationssystems der Universität zu Lübeck“ [“Policy on the operation and use of a University of Lübeck Voice-over-IP-based telecommunications system”, available in German language only].

## § 6
## Rights and obligations of the authorized users

(1) The authorized persons (authorized users) have the right to use the University of Lübeck’s communication and data processing infrastructure within the framework of the authorization and in accordance with this Regulation for Use. Any use deviating from this requires separate authorization by the data network operator.

(2) The authorized users are obliged to,

1. comply with the requirements of this Regulation for Use,

2. refrain from anything that interferes with the proper operation of the University of Lübeck’s communication and data processing infrastructure,

3. treat all data processing systems, information and communication systems and other facilities of the communication and data processing infrastructure of the University of Lübeck and its affiliated institutions with care and respect,

4. to work exclusively with the user IDs that you have been authorized to use under the authorization process,

5. ensure that no other person gains knowledge of the user passwords and to take precautions to prevent unauthorized persons from gaining access to the University of Lübeck’s communication and data processing infrastructure; this also includes the protection of access through the use of a secret and appropriate, i.e. not easily identifiable password (see IT security policy [IT-Sicherheitsrichtlinie]),

6. neither seek nor use the user IDs and passwords of others,

7. not take unauthorized access to information of other authorized users and to not pass on, use or modify any information of other authorized users without permission,

8. to comply with the statutory provisions, in particular concerning copyright protection, when using software, documentation and other data and to observe the terms of the

license under which software, documentation and data are provided by the University of Lübeck,

9. neither copy nor to pass on the provided software, documentation and data to third parties, unless this is expressly permitted to be used for purposes other than those authorized,

10. not try to remedy malfunctions, security concerns, damages and errors in the communication and data processing infrastructure yourself, but to immediately and exclusively notify the data network operator or the responsible administrators,

11. not engage in unauthorized tampering with the hardware installation of communication and data processing infrastructure provided for use and not change the configuration of the operating systems, the system files, the system-relevant user files and the data network,

12. upon request, in justified individual cases – in particular by justified suspicion of misuse and for troubleshooting purposes – to provide, for monitoring purposes, the data network operator and the data protection officer (DPO) with information on programs and methods used, as well as access to the programs, with the exception of user data that falls under telecommunications and data secrecy,

13. to coordinate the processing of personal data with the data network operator and the DPO and – regardless of the authorized users' own data protection obligations – to strictly adhere to the data protection and data security regulations issued by the data network operator.

(3) The following offenses are particularly noted:

1. Data spying (§ 202a StGB [Strafgesetzbuch: German Criminal Code]),

2. tampering with data (§ 303a StGB) and computer sabotage (§ 303b StGB),

3. computer fraud (§ 263a StGB),

4. the dissemination of pornographic materials (§§ 184 ff. StGB), in particular the distribution, acquisition and possession of publications containing child pornography (§ 184b StGB) and the dissemination of pornographic performances by way of broadcasting, media or teleservices (§ 184c StGB),

5. the dissemination of propaganda of unconstitutional organizations (§ 86 StGB) and sedition [incitement of the people/masses] (§ 130 StGB),

6. defamation, such as libel or slander (§§ 185 ff. StGB),

7. punishable copyright infringement, e.g. violation of a copyright through the illegal reproduction of software (§§ 106 ff. UrhG [Urheberrechtsgesetz: German Copyright Act]).

(4) Furthermore, the following additional provisions are to be observed:

1. The general right of personality ([Allgemeines Persönlichkeitsrecht] APR), which is based on Article 2 paragraph 1 in conjunction with Article 1 paragraph 1 of the Basic Law [of the Federal Republic of Germany] and which provides special protection for individual, private and personal space,

2. the German Art Copyright Act ([Kunsturhebergesetz] KUG), which regulates the right to one's own image (§ 22 KUG),

3. the Act on Telemedia ([Telemediengesetz] TMG) and the Telecommunications Act ([Telekommunikationsgesetz] TKG), which set the legal framework for so-called telemedia in Germany,

4. User Regulations of the German National Research and Education Network (DFN, http://www.dfn.de) [„Benutzungsordnung des Deutschen Forschungsnetzes", available in German language only],

5. "The policy of the executive committee of the University of Lübeck concerning the use of data processing pools/computer rooms" [„Richtlinie des Präsidiums der Universität zu Lübeck zur Nutzung der EDV-Pools", available in German language only].

6. For the staff members of the university administration (ZUV, Central Facilities [Zentrale Einrichtungen]): "Occupational Accessibility Statement" [„Dienstanweisung über die Erreichbarkeit am Arbeitsplatz", available in German language only], which governs the use of electronic communication systems at the workplace.

## § 7
## Restriction and exclusion from use

(1) Authorized users may be temporarily or permanently restricted or excluded from using the communication and data processing infrastructure if

1. they culpably violate this Regulation for Use, in particular the obligations listed in § 4, e.g.

   a) disregard the Regulation for Use,
   b) interference with the proper operation,
   c) work with unauthorized user ID,
   d) use insufficient precautionary measures against unauthorized access to the University of Lübeck's communication and data processing infrastructure,
   e) seeking out and utilizing the user IDs and passwords of others,
   f) unauthorized access to information of other users and its further use,
   g) violation of statutory provisions, e.g. copyright protection,
   h) unauthorized use, copying and distribution of provided software, documentation and data,

i) unauthorized interference with the hardware installation as well as making changes to/in the configuration of the operating systems, the system files and the system-relevant user files of the communication and data processing infrastructure,
j) the processing of personal data without consulting with the data network operator and/or the data protection officer [DPO]

or

2. they misuse the communication and data processing infrastructure for criminal acts or

3. other unlawful user behaviour which is to the detriment of the University of Lübeck, its affiliated institutions or their affiliates or

4. they have not signed the required declaration of consent for the private use of the Internet access. In this case, private Internet use is prohibited.

(2) Measures under paragraph 1 shall be taken only after prior warning. Affected parties shall be given the opportunity to respond.

(3) Temporary restrictions on use shall be lifted as soon as proper use is again guaranteed.

(4) A permanent restriction of use or the complete exclusion of authorized users from further use shall only be considered in the event of serious or repeated violations as defined by paragraph 1. The decision on the permanent exclusion shall be made by the university management.

## § 8
## Rights and obligations of the data network operator

(1) The data network operator documents the user authorizations issued together with the e-mail addresses of the authorized users.

(2) To the extent necessary for troubleshooting, system administration and enhancement, or for reasons of system security as well as user data protection, the data network operator may temporarily restrict the use of its resources or temporarily suspend individual user identifications or network access. If possible, the affected authorized users are to be informed in advance.

(3) If there is actual evidence that authorized users have provided or are providing unlawful subject matter for use in the data network, the data network operator may prevent further use until the legal situation has been sufficiently clarified.

(4) The data network operator is entitled to monitor the security of the system/user passwords and the user data by regular automated measures and to take necessary protective measures, e.g. make changes in easily guessable passwords to protect the communication and data processing infrastructure and user data from unauthorized access by third parties. In cases of required changes to user passwords, access rights to user files and other security measures relevant to use, the authorized users must be immediately informed.

(5) The data network operator is entitled, in accordance with the following provisions, to document and evaluate the use of the communication and data processing infrastructure by the individual authorized users, but only insofar as this is necessary

1. to ensure proper system operation,

2. for resource planning and system administration,

3. to protect the personal data of other authorized users,

4. for detecting and eliminating errors as well as

5. for the clarification and prevention of unlawful or improper use.

(6) Under the conditions of paragraph 5, the data network operator is also entitled to inspect the programs and files of authorized users in accordance with data privacy provisions insofar as this is necessary to eliminate current malfunctions or to investigate and prevent misuses as long as there are actual indications of such. However, inspection of the message and e-mail mailboxes is only permissible if this is essential for the correction of current malfunctions in the messaging service. In each case, the inspection must be documented and the authorized users concerned immediately notified.

(7) Under the conditions of paragraph 5, data traffic and usage data in the communication traffic, in particular the use of e-mail, can also be documented. However, only the specific circumstances of the telecommunication – but not the non-public contents of the communication – may be collected, processes and utilized. The data traffic and usage data of online activities in the Internet and other telemedia services provided by the data network operator for use or which the data network operator grants access to the use shall be deleted as soon as possible, at the latest at the end of the respective utilization.

(8) The statutory rules according to the [European] General Data Protection Regulation (EU-GDPR) as well as according to the Schleswig-Holstein Data Protection Act for the protection of personal information (Landesdatenschutzgesetz - LDSG -) in the current version shall be complied with.

## § 9
## Logging and monitoring

(1) Logging of the uses of the use of the services (usage, traffic and content data) shall take place, if absolutely necessary

1. for reasons of data and system security,
2. for reasons of system technology (e.g. for error tracking) and
3. for reasons of work organization (e.g. to determine the nature and extent of use),
4. to monitor for misuse (if the random sampling of the data shows indications of unauthorized access or exceeding the permitted usage).

(2) For the use of the Internet, the following information shall be logged:

1. Date/time,
2. source IP address,
3. destination IP address,
4. the transferred amount of data.

(3) Incoming and outgoing e-mails shall be logged with the following information:

1. Date/time,
2. sender and recipient address,
3. message ID,
4. message size,
5. event ID (e.g. redirect, transfer, receive),
6. source IP address,
7. destination IP addresses,
8. and the message info.

(4) The log data of paragraphs 2 and 3 shall be used solely for purposes of analysing and correcting technical errors, ensuring system security, network optimization and data protection control. The log data shall only be kept for as long as is necessary to achieve its purpose and shall be deleted after a maximum of 60 days. Compliance with all data protection regulations must be ensured. If there is a case of suspected misuse of the Internet or e-mail based on documented factual evidence, the log data set out in paragraphs 2 and 3 may be evaluated specific to the individual. The log data shall be deleted as soon as it is established that the suspicion has been substantiated or is unfounded, unless it is still needed for the purposes referred to in paragraph 1.

(5) Staff members who have access to the log information are cautioned to be particularly aware of the sensitivity of this data and are obligated to adhere to the data protection regulation.

(6) An evaluation of log data must take into account the principles of data protection control, in particular the principle of proportionality. The behaviour and performance monitoring of an individual by an evaluation of the log data is prohibited. As a matter of principle, evaluations of log data are to be anonymized initially.

(7) For the analysis of conspicuous, above-normal clusters in communication behaviour and/or an extensive increase of transmission volumes or particularly high transmission volumes of certain Internet or external e-mail domains the data may be inspected and evaluated by the ITSC on a monthly or ad hoc basis.

(8) Should this result in clear indications of unauthorized access or a clear violation of the permitted private use (Level 1), the affected group of authorized users must first of all, as a matter of principle, be informed of the inadmissibility of this behaviour (Level 2). At the same time, they shall be informed that, should the violations continue, targeted monitoring (Level 3)

or workplace-specific monitoring (Level 4) can take place in accordance with the procedure described in Appendix 2.

(9) Appendix 2 is part of this Regulation for Use.

## § 10
## Liability of the authorized user

(1) The authorized users shall be liable for any and all detrimental consequences, which the University of Lübeck, its affiliated institutions or their affiliates may incur due to the improper or unlawful use of the communication and data processing infrastructure and the user authorization or because the authorized users culpably fail to fulfil their obligations under this Regulation for Use.

(2) Within the context of the access and use options made available to them, authorized users are also liable for any damages incurred through third-party use, if they are responsible for such third-party use, in particular in the case of a transfer of the user ID to third parties.

(3) The authorized users shall indemnify [exempt] the University of Lübeck from all claims if third parties file a claim against the University of Lübeck for compensation for damages, injunctive relief or in any other way due to misuse or unlawful conduct on the part of the authorized users. The University of Lübeck will require the authorized users to be joined in the proceedings if third parties take legal action against the data network operator as a result of misuse or unlawful conduct on the part of the authorized users.

## § 11
## Liability of the University of Lübeck

(1) The University of Lübeck does not guarantee that the system will run error-free and at all times without interruption. The possible loss of data due to technical errors as well as the perusal of confidential data due to unauthorized access by third parties cannot be ruled out.

(2) The University of Lübeck assumes no responsibility for the accuracy of the programs provided. The University of Lübeck is also not liable for the content, in particular for the accuracy, completeness and timeliness of the information to which it merely provides access to use.

(3) Moreover, the University of Lübeck is liable only for the deliberate intention and gross negligence of its staff members unless a culpable violation of essential contractual obligations (cardinal obligation) is present. In this case, the liability of the University of Lübeck is limited to typical foreseeable damages on grounds of the user relationship, insofar as deliberate or grossly negligent actions are not present.

(4) Possible public liability claims against the University of Lübeck remain unaffected by the above provisions.

Appendix 1

**Declaration of Consent**
**to the private use of Internet access of the University of Lübeck**

I would like to make use of the offer to use the internet access to a limited extent also for private non-commercial purposes.

- I have read and understood the Regulation (Statute) for Terms and Conditions of Use for the Communication and Data Processing Infrastructure of the University of Lübeck, as amended, and I consent to my having limited use of the Internet for non-commercial purposes. This shall only apply if the performance of official duties/student tasks and the availability of IT systems for official/student purposes and the interests of the other authorized users are not thereby impaired.
- I agree that my private – i.e. not only the official/student – internet access within the framework of the Regulation for Terms and Conditions of Use can be processed and logged in compliance with the data protection provisions and on a person-related basis in accordance with § 9 of the Regulation for Terms and Conditions of Use.
- I also agree that the use of University of Lübeck e-mail accounts is only permitted for official/student purposes. Thus, I am prohibited from using the official/student e-mail account for private purposes. This does not apply to the use of the university e-mail address for the receipt of special student terms/conditions.

I am aware that I hereby waive the protection of telecommunications secrecy according to § 88 of the Telecommunications Act (TKG).

It is clear to me that improper or unauthorized use, in addition to legal and/or, if necessary, labour law consequences, may also have criminal consequences and, moreover, that an infringement may result in civil liability for damages.

I am aware that I can effectively revoke this consent at any time in the future, with the result that I am no longer allowed private use of the Internet from the date of revocation.

| | |
|---|---|
| Surname, given name<br>(please use block letters) | Matriculation number, if student |
| Place, date | Signature of authorized user |

Appendix 2

**Procedural description for the inspection of
the targeted (Level 3) and workplace-specific (Level 4) monitoring
in accordance with § 9 paragraph 8 of the Regulation for Use**

The responsible staff representatives/staff council, the ITSC, the official data protection officer, and, where appropriate, the equal opportunities officer and/or the representative of the severely disabled shall be involved in the determination of this procedure and the evaluation of log data. The affected authorized users must be notified of the procedure.

The inspections should be carried out at regular intervals. This is done in co-ordination with the responsible staff representatives/staff council, the ITSC, the official data protection officer, and, where appropriate, the equal opportunities officer and/or the representative of the severely disabled.

The procedure of an inspection is recommended as follows:

**Procedural description:**

1. Invitations are sent to the responsible staff representative/staff council, the official data protection officer, an ITSC representative, and, where appropriate, the equal opportunities officer and/or the representative of the severely disabled by the Executive Committee for a preparatory discussion of the inspection date.

2. On this date, three people shall be randomly selected from a list. Not all authorized users may be monitored.

3. Discourse on the suitability of the selected persons. Prohibited are evaluations, in particular of log data (usage, traffic and content data) in order to obtain information about the use of the Internet service and e-mail communication in connection with special functions to be protected (for example, staff representatives/staff council, equal opportunity representatives, representatives of the severely disabled, official data protection authorities, the personnel department).

4. Agreement on an inspection date.

5. On the date of the inspection, the selected persons are requested to allow the responsible staff representative/staff council, the official data protection officer, an ITSC representative (and, where appropriate, the equal opportunities officer and/or the representative of the severely disabled) to inspect the workstation in the workplace via the remote maintenance software.

6. The selected person is then asked to open the e-mail program and maximize a list view to hide or minimize the contents of the e-mail.

7. The subject lines shall be collectively skimmed through and examined for private features. The monitoring period of the e-mail should not exceed 3 months.

8. The inspection visitation should not take more than 10 minutes. 5 minutes for the concept and purpose of the inspection and 5 minutes for the inspection itself.

9. The results shall be made known to those affected. According to the results, the next steps should be considered:

    a) To stop the monitoring/no further control,
    b) to renew admonishment of the group of people concerned and continue the targeted monitoring or
    c) to intensify the monitoring in which the logging takes place on the workstation computer (Level 4). Workstation logging has the same requirements as Level 3, except for the notification. The staff members must be informed about this measure. If necessary, a criminal complaint can also be filed and a law enforcement agency can be called in.

10. At the end, written documentation about the inspection shall be drawn up, complete with the signatures of those who conducted the inspection.

11. Continued violations do not rule out public sector employment law or labour law-oriented measures against the staff members. If criminal offences are suspected, the evaluation of log data shall be left to the appropriate law enforcement authorities.