Universität Basel

Regulation on the acceptable use of university IT resources

Tuesday, 20 August 2019

With reference to §4 para 1a of the ordinance on information security of the University of Basel of 31 January 2019, the President's Board enacts the following regulation:

I. General provisions

§1. Purpose

[1] This regulation on the use of university information technology tools and services (hereinafter referred to as IT resources) governs the principles of use of the IT resources made available by the University of Basel and the secure management of information.

[2] Its purpose is to ensure correct, secure and economical use of IT resources. It further serves to protect the rights of users of IT resources at the University of Basel and personal and other confidential information.

§2. Scope

This regulation is binding for all university members and third parties (hereinafter users) who use IT resources of the University of Basel. Regulations that apply exclusively to employees are expressly designated as such.

§3. Definitions

data: information stored electronically

IT resources: devices, facilities and services used for electronic processing, storage, transfer or deletion of information, such as computer systems, data networks, software, internet access, email, VoIP, electronic locking systems

information: any records regardless of their form of representation or information medium

university/business information: information related to the activities of the University of Basel

- **personal information:** university/business information that is intended only for the user
- **confidential information:** university/business information that may be read and/or processed only by authorized individuals

private information: information that is intended only for the user and which is not university/business information

personal data: information that relates to a specific or identifiable natural person or legal entity

§4. Responsibility

Overarching responsibility for and information on correct management of IT resources for each area is borne by the head of the organizational unit at the respective hierarchical level.

II. Use of IT resources

§5. Guiding principle

[1] IT resources are generally made available for university tasks alone and must be deployed in a way that is secure, prudent and economical.

[2] The use of IT resources for secondary activities as defined by the regulations on secondary activities, agreements with third parties and the use of intellectual property is to be observed accordingly.

[3] Use of IT resources that exceeds the general, normal scope and which as such may jeopardize operations (e.g. network overload, security) is permitted only in consultation with and following approval by IT Services.

§6. Use of private IT devices

IT devices that are not made available by the University of Basel (laptops, mobile devices, etc.) may be connected to the data network of the University of Basel only in accordance with IT Services guidelines.

§7. Data protection and information security

[1] Users are responsible for ensuring that they manage their information in compliance with data protection regulations.

[2] Users must ensure that unauthorized persons do not gain access to confidential information.

[3] For security reasons it is recommended that data is stored only on the central university IT infrastructure.

[4] Users are responsible for the data security and storage of information that is not stored on the central university IT infrastructure (e.g. external backup media).

[5] Details on correct management of information at the University of Basel are governed by a separate regulation.

§8. Authentication

[1] All users receive personal user names (accounts) for access to university IT resources. Access is protected by a password to be chosen by the user and possibly other authentication methods such as PIN or token.

[2] Access data such as passwords, PINs or certificates may not be stored on systems or transferred to third parties unencrypted. Users must change their passwords if requested to do so by IT Services.

[3] Details on the correct management of user names and passwords are governed by a separate directive.

§9. Data storage and email

[1] The storage services made available by the University of Basel are generally used for the storage of university/business data.

[2] Employees are generally provided with electronic storage for personal data.

[3] With the exception of personal data, the University of Basel has access to university/business data.

[5] The university has access to emails and personal data only in exceptional cases.

[6] Details of possible access to data are governed by a separate regulation.

§10. Termination of the employment agreement

[1] On termination of the employment agreement, IT resources remain with the University of Basel.

[2] Any personal or private data on university IT resources, e.g. in the mailbox, is to be deleted by the user on departure from the University of Basel.

[3] The mailbox and personal and any private data will be deleted by the University of Basel no later than 12 months after termination of the employment agreement.

§11. Improper use

[1] Improper use refers to any use of university IT resources that infringe this regulation or which is otherwise unlawful.

[2] In particular, improper use includes:

a) violation of statutory provisions

b) retrieval, storage and/or sending of illegal content, pornography, content that glorifies violence, racist content

c) sending of offensive, derogatory or sexist content

d) violation of copyright of third parties, violation of license terms

e) violation of the personal rights of third parties

f) excessive use of IT resources for private purposes

g) establishment of direct connections to the data networks of the University of Basel not approved by IT Services (e.g. installation of wifi access points or modems)

[3] In case of doubt, the President's Board shall decide whether the usage is improper.

[4] Improper use as defined by §11 para. 2a and b does not apply to activities carried out for research purposes of which the university's Ethics Commission has granted prior approval.

§12. Measures to monitor use

[1] Use of the university network and individual IT services is logged by the service providers.

[2] For the purposes of troubleshooting and ensuring orderly operations, user-specific data may be logged, including the following: user name, network address of the accessing computer, network address accessed, time and date of access.

[3] Storage of and access to user-specific data in exceptional cases is governed by a separate regulation.

§13. Consequences of improper use

[1] In cases of improper use, the university may block access to the university infrastructure in whole or in part.

[2] Improper use by employees may result in disciplinary measures up to and including termination.

[3] Improper use by students may result in disciplinary measures up to and including deregistration in line with the student regulations.

[4] Where criminal activity is suspected, this may be reported to the appropriate authorities.

§14. Notification of security incidents

Any person who falls under the scope of these regulations is obliged to report any security-relevant incidents and security vulnerabilities of which they become aware to the information security office of the University of Basel.

§15. Final provision and effectiveness

[1] These regulations come into immediate effect on approval by the President's Board.

[2] They replace the regulations on management of university IT resources dated 11 December 2002.