UNIVERSITÄT BERN

Directive

on the Use of IT Resources at the University of Bern

Classification	For internal use
Document status	Released

Table of contents

The Governing Board of the University,

Based on Art. 3, par. 3 of the University Act of 5th September 1996 (UniG) and Art. 24, par. 2, item i of the University Statute of 7th June 2011 (UniSt),

The University Executive Board has decided the following:

1. General provisions

1.1 Purpose

This Directive governs the use of IT resources at the University of Bern by authorized users.

1.2 Terms

IT resources	IT resources include IT facilities, information and IT services.
IT facilities	are all equipment and installations, whether tangible or intangible, which enable the electronic processing, storage, transmission or destruction of information including: a) Computer systems and smart devices b) Peripherals (e.g. Storage Media), c) Networks, both fixed and wireless, and network devices (such as routers, repeaters, security devices, wireless access points) d) Software
Information	Information is technical, administrative and personal data
IT services	IT services include all central services that are made available to authorized users, such as e-mail, DNS, WWW services, digital libraries, etc.
Central IT resources	Central IT Resources include IT facilities, information and IT services that are offered by the IT Services Department throughout the University.

2. Principles governing Use

2.1 General provisions

In principle, the IT resources may be used only in order to carry out University work.

The use of the IT resources by members of staff for private purposes is only permitted outside working hours and subject to compliance with this Directive.

The authorisation of the Governing Board of the University is required for:

a) The use of the IT resources for private commercial or private advertising purposes
b) The use of data with racist, sexist or pornographic content for the purpose of teaching and research

The use of IT resources for University work as well as for teaching and research has absolute priority over all other uses.

2.2 Processing of personal data

The processing of personal data is only permitted in conjunction with University work and subject to compliance with the data protection legislation.

If it is known or suspected that personal data within the meaning of the data protection legislation are being processed in an organizational unit, an Information Security and Data Protection analysis or an Information Security and Data Protection concept must be drawn up in compliance with the guidelines of the Office for Information Technology and Organization (KAIO).

2.3 Disclosure of data while using IT services

The University of Bern makes various applications (e.g. SWITCHaai, Office365, etc.) available to authorized users. A transfer of system-relevant attributes including personal data (first name, surname, e-mail address, gender, preferred language, study level, degree program, etc.) may take place to enable access to and use of these applications. A list of the respective attributes can be viewed in the IT Services Department. This exchange of data only takes place:

- for the systems and applications relevant to studies
- to carry out work orders

Disclosure of data only takes place for the intended purpose of a system and to check access rights.

2.4 Presentation of the University in the network

The Governing Board of the University shall issue directives and recommendations on the presentation of the University on the internal and external networks.

2.5 Access to IT resources

Access to the Central IT Resources is in only possible by using a Campus account (username and password).

2.6 Campus account

The campus account is personal and non-transferable. The person registered on the campus account bears full responsibility for all activities carried out. The campus accounts are managed by the account managers (see the IT Services Department's guidelines for account managers). The organizational unit management designates the account managers for this purpose.

The account managers regularly verify the justification for existence and immediately delete campus accounts without any such justification. If it is suspected that a campus account is being used by an unauthorized user, the relevant organizational unit's account manager must be informed immediately. If misuse is suspected, account managers can apply to the IT Services Department to have the campus account blocked. The IT Services Department shall decide on the blocking of the campus account and other measures in accordance with chapter 5.

Further regulations on the management of the Campus Accounts are set out in the guidelines "Richtlinie zur Verwaltung und Verwendung von Campus Accounts". (Available only in German)

2.7 Private or self-administered devices

The Management of the University approves the use of private devices. The general framework is set out in the directive „Weisung zur Anbindung von privaten oder selbst administrierten IT-Geräten an das allgemeine universitäre Netzwerk" (Available only in German)

3. Non-University institutes

The use of IT-Ressources for Organizational units, which are not members of the University of Bern, are arranged by special agreements.

4. Members of other academical institutions

Members of other academical institutions are permited to use the IT-Ressources of the University of Bern, according bilateral agreements.

5. Misuse and Disciplinary Measures

5.1 Misuse

Misuse of the IT resources is any use which:

- infringes the statutory provisions of University legislation, in particular provisions relating to University work
- infringes this Directive
- infringes other provisions of the law
- infringes the rights of third parties

Misuse is in particular any of the following:

a) the processing, storage or transmission of data with racist, sexist or pornographic content; (except 2.1 par. b)

b) the unlawful copying, modification or deletion of any form of data

c) the writing or spreading of harmful program codes (such as viruses, Trojan horses, or worms)

d) hacking, and in particular
   - unauthorised access, or the attempt to obtain unauthorised access to other computer systems
   - attempting to instigate the denial of service attacks
   - unauthorised searches for weaknesses in internal or external computers and networks (port scanning)
   - attempting to procure passwords without authorisation

e) feigning of IP or MAC addresses (*spoofing*)

f) sending e-mail with faked sender addresses

g) modifying or extending network components on the University network without the express permission of the IT Services Department (in accordance with the *Directive on the Network of the University of Bern*);

h) registration with external providers of non-UNIBE.CH domains with IP addresses from the University network without the express permission of the committee of the Commission for IT Services (in accordance with the *Guidelines on the Use of External Domain Names in the University of Bern*)

i) sending bulk e-mail in the sense of unsolicited and unwanted e-mails

j) using IT resources to harass others

k) manipulation of University IT resources

l) the use of IT facilities in such a way as to violate intellectual property rights and trading standards

5.2 Disciplinary measures

Users of the IT resources are personally responsible for compliance with the applicable law and this Directive. In particular, the person to whom the user name is registered is personally responsible for the consequences of the use of IT resources following the entry of his or her access password.

In the event of any violation of the law in connection with the use of University IT resources or of any breach of this Directive, the Governing Board of the University may take all steps necessary to maintain or to restore lawful usage, and in particular may:

a) suspend access to IT resources or other restrictions on the use of IT resources
b) ban those responsible form the premises
c) delete data and block websites

In addition, sanctions may be imposed as provided for in the rules and regulations of the University and under employment law. The right to prosecute or bring civil proceedings is reserved.

5.3 Random checks, precautionary measures, reporting, recording

The IT Services Department can carry out anonymous plausibility checks (spot checks) in conjunction with university units' technical managers to check the execution of this Directive.

If misuse of IT resources is suspected, the managers of the organizational units shall apply to the Governing Board of the University to have pre-announced, time-limited checks carried out by the IT Services Department in respect of a restricted group of people. The IT Services Department shall provide the Governing Board of the University with an immediate report on the investigation conducted and any precautionary measures taken. In addition, the IT Services Department shall apply to the Governing Board of the University for further measures to maintain or restore the lawful state of the network.

If the IT Services Department receives any information about upload activities of copyright-protected data from the University network (e.g. using peer-to-peer-software), it may identify and admonish the person behind this network address, if required with the aid of the relevant organizational unit's technical manager. In the affirmed case of recurrence of upload-activities, the person responsible according to the legislation of the University and the human resources reprimands the relevant person. After the report by the Head of IT security, any additional measures require the authorisation of the Governing Board of the University.

Technical log files that are created through access to IT resources at the University of Bern are stored for a minimum of six months.

6. Final provisions

6.1 Implementing provisions

The Governing Board of the University may issue further implementing provisions as annexes to this Directive, providing additional detail on the articles in this Directive.

The Commission for IT Services Department (KID) may within the scope of its authority issue further implementing provisions in the form of directives.

Any such implementing provisions require the approval of the Governing Board of the University.

6.2 Entry into force

This Directive comes into effect on its approval by the Governing Board of the University. It replaces the Directive on the Use of the IT Resources at the University of Bern of December 20, 2016.

6.3 Contradictory provisions

Existing provisions, which are contradicting this Directive, are hereby abrogated.

Bern, November 26, 2019

On behalf of the Governing Board of the University

The Rector:

Prof. Dr. Christian Leumann

This document is a translation that is provided for information purposes only. It is not legally binding. In the event of a dispute about the interpretation of an article, the text of the original German version will therefore always prevail.