

Directives

Use of IT resources at the University of Bern

Class	For internal use
Document status	Approved

Directive

Use of IT resources at the University of Bern

The Executive Board of the University of Bern,

based on Art. 3 Para. 3 of the Law of September 5, 1996 on the University (UniG) and Art. 24 Para. 2 lit. i of the University Statute of June 7, 2011 (UniSt),

has decided as follows:

1. General provisions

1.1 Purpose

These instructions govern the use of IT resources at the University of Bern by authorized users.

1.2 Terms

IT resources	Include IT tools, information and IT services
IT tools	Are all equipment, facilities and programs of a tangible and intangible nature procured and operated by the University of Bern. This also includes private non-university IT equipment that is connected to the data network of the University of Bern. These IT tools are used to process, store, transmit or destroy information electronically, specifically: a) Computer systems (desktops, laptops, physical and virtual servers) b) Smart devices (e.g. smartphones) c) Peripheral devices (e.g. storage media) d) Networks (wired and unwired) and network devices (such as routers, repeaters, security devices, wireless access points) e) Software
Information	Is factual and personal data
IT services	Include central services that are available to authorized users (e.g. e-mail, DNS, web services, digital libraries, etc.)
Central IT resources	Comprise IT tools, information and IT services, which are offered by IT Services across the university.

2. Principles of use

2.1 General

The IT resources are used to fulfill university tasks.

The use of IT resources to fulfill university tasks as well as for teaching and research always takes precedence over any other purposes of use.

Employees of the University of Bern may only use IT resources for private purposes outside working hours, provided these instructions are complied with.

Approval from the University Executive Board is required for:

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

Directive

Use of IT resources at the University of Bern

2.2 Software license compliance

To ensure software license compliance, the technology managers shall install a corresponding agent for collecting installation data and information on software usage on each IT tool pursuant to Section 1.2 a) on which software licensed by the University of Bern is operated.

This agent must not be deactivated or uninstalled.

2.3 Processing of personal data

The processing of personal data is only permitted in the context of fulfilling university duties and in compliance with data protection legislation.

If it is known or suspected that personal data is being processed in an organizational unit within the meaning of data protection legislation, an information security and data protection (ISDS) analysis or a concept must be created.

2.4 Disclosure of data as part of the use of IT services

The University of Bern makes various applications (e.g. SWITCHaai, M365, etc.) available to authorized users. In order to access and use these applications, system-relevant attributes may be transferred, which also contain personal data (first name, surname, e-mail address, gender, preferred language, level of study, study program, installed application programs and their last time of use, etc.). A list of the attributes concerned can be viewed under the ID. This data exchange takes place exclusively:

- Between the systems and applications relevant to the studies
- To carry out the work assignment
- For the correct allocation of licenses and for ensuring software license compliance in accordance with Section 2.2

Data is disclosed solely for the specific purpose of a system and for checking access authorization.

2.5 Access to central IT resources

Access to central IT resources is only possible with a Campus Account (login name and password).

2.6 Campus Account

Your campus account is personal to you and is not transferable. The person registered in the campus account is fully responsible for all activities carried out. The campus accounts are managed by the account managers, see "Richtlinien der Informatikdienste für Konto-Verantwortliche" (Available only in German). The heads of the organizational units determine the account managers for this purpose.

The account managers regularly verify the existence entitlement and immediately delete campus accounts without such authorization. If there is any suspicion that a campus account is being used by unauthorized persons, the account manager of the responsible organizational unit must be notified immediately. If misuse is suspected, the account managers can apply to the IT Services Department to have the campus account blocked. the IT Services Department decides on the blocking and any further measures in accordance with Section 5.

Further rules for managing campus accounts can be found in the "Richtlinie zur Verwaltung und Verwendung von Campus Accounts". (Available only in German).

2.7 Private IT equipment

The use and connection of private devices is welcomed. The corresponding framework conditions are set out in the „Weisung zur Anbindung von privaten oder selbst administrierten IT-Geräten an das allgemeine universitäre Netzwerk“. (Available only in German)

3. Non-university organizational units

For organizational units that do not belong to the University of Bern, the use of IT resources is governed by special agreements with the University of Bern.

Directive

Use of IT resources at the University of Bern

4. Members of other academic institutions

Members of other academic institutions may use the University of Bern's IT resources in accordance with mutually accepted service agreements.

5. Misuse and measures in the event of misuse

5.1 Misuse

A misuse of resources is any use of IT resources that:

- Is in contradiction to the statutory provisions of university legislation, in particular regarding the fulfillment of university duties,
- Violates these directives
- Violates other provisions of the legal system
- Infringes the rights of third-parties

The following actions in particular constitute misuse:

- a) Processing, storing or transmitting data with racist, sexist or pornographic content, subject to 2.1 Paragraph b)
- b) Unlawful copying, altering and modifying of data of any kind
- c) Creating or distributing harmful program codes (such as viruses, Trojans, worms)
- d) Hacking, specifically
 - Unauthorized intrusion or attempted intrusion into third-party computer systems
 - Taking measures to disrupt the operation of computers or networks
(*Denial of Service Attacks*)
 - Unauthenticated scanning of internal or external networks and computers for vulnerabilities
(*port scanning*)
 - Password sniffing
- e) Use of fake IP or MAC addresses (*spoofing*)
- f) Sending e-mails with fake e-mail sender addresses
- g) Modifying or extensions of network components in the university network without the express permission of the IT Services Department (in accordance with the "Weisungen über das Netzwerk der Universität Bern" (Available only in German)
- h) Mass sending of emails in the sense of unwanted and unsolicited emails
- i) Harassment of others through the use of IT resources
- j) Manipulation of university IT resources
- k) Use of IT tools in a manner that results in the infringement of intellectual property rights and fairness rights

5.2 Measures in the event of misuse

Users are personally responsible for using IT resources in compliance with the applicable legal system and these directives. In particular, the person entered in the login name is personally responsible for the consequences of using the IT resources by entering their password.

In the event of a violation of the legal system in connection with the use of university IT resources or in the event of a violation of these directives, the University Executive Board may take all measures necessary to maintain or restore the lawful state, namely:

- a) Blocking access to IT resources or other restrictions on the use of IT resources
- b) Prohibition from entering the premises
- c) Deletion of data and blocking of homepages

In addition, sanctions provided for under university or personnel law may be imposed. Criminal prosecution and the assertion of civil claims remain reserved.

Bern, December 19, 2022

Directive

Use of IT resources at the University of Bern

5.3 Random sampling, precautionary measures, reporting, logging

In cooperation with the technical officers of the university units, IT Services Department can carry out anonymous plausibility checks (random checks) in order to check that these directives are being implemented.

If there is a suspicion of misuse of IT resources, the heads of the organizational units apply to the University Executive Board via IT Services Department for the implementation of a temporary check by IT Services of a limited number of people. The IT Services Department will immediately report to the University Executive Board on the investigation carried out and any precautionary measures taken. They also apply to the University Executive Board for further measures to maintain or restore the lawful state of affairs on the Internet.

If the IT Services Department becomes aware of upload activities of copyrighted data (e.g. using peer-to-peer software) from the university network, it may identify and issue a warning to the person behind the network address, if necessary with the assistance of the technical officer of the organizational unit concerned. If upload activities are confirmed to be repeated, the person responsible in accordance with university or personnel legislation issues a reprimand. Further measures must be approved by the University Executive Board following reporting by IT Services Department.

Technical log files created by accessing the University of Bern's IT resources are stored for at least six months.

6. Final provisions

6.1 Entry into force

The present directives enter into force upon approval. They replace the directives on the use of IT resources at the University of Bern dated November 26, 2019

Bern, December 19, 2022

For the Executive Board of the University of Bern

The Rector:

Prof. Dr. Christian Leumann