Directive

on the Use of IT Resources at the University of Bern

Classification
For internal use
Document status
Released
The Governing Board of the University, ................................................................. 3
1. General Provisions ........................................................................................................ 3
   1.1 Aim .......................................................................................................................... 3
   1.2 Definitions ................................................................................................................ 3
2. Principles governing Use .................................................................................................. 3
   2.1 General .................................................................................................................... 3
   2.2 Processing of personal data ...................................................................................... 3
   2.3 Forwarding of personal data ................................................................................... 4
   2.4 Presentation of the University in the network ......................................................... 4
   2.5 Access to IT resources ............................................................................................ 4
   2.6 Campus account ........................................................................................................ 4
   2.7 Private or self administered devices ........................................................................ 4
3. Non-University institutes ................................................................................................ 4
4. Members of other academical institutions ...................................................................... 5
5. Misuse and Disciplinary Measures .................................................................................. 5
   5.1 Misuse ..................................................................................................................... 5
   5.2 Disciplinary measures .............................................................................................. 5
   5.3 Random checks, precautionary measures, reporting, recording .............................. 6
6. Final Provisions ................................................................................................................ 7
   6.1 Implementing provisions .......................................................................................... 7
   6.2 Commencement .......................................................................................................... 7
   6.3 Contradictory provisions ......................................................................................... 7
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).

Decrees:


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

1.2 Definitions
IT facilities are all equipment and installations, whether tangible or intangible, which enable the electronic processing, storage, transmission or destruction of information including:

- **IT facilities**
  - 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.

- **IT resources**
  - IT resources include IT facilities, information and IT services.

- **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
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.
In the event of any suspicion of a processing of such data in an Institute, an Analysis or Concept for IT security and data protection (ISDS Analysis / ISDS Concept) has to be made in accordance with the guidelines of the IT and Organisation Office of the Canton of Berne (KAIO).

2.3 Forwarding of personal data
To access applications authenticated and authorized via SWITCHaai, system-related attributes also containing personal data are transferred. This data is used exclusively for the intended purpose and serves to verify authorisations. By using applications accessed via SWITCHaai, the user consents to the data transfer.

The personal data comprises the following attributes:
- First name
- Last name
- E-mail
- Gender
- Preferred language
- Affiliation (faculty, student, staff, alum, member, affiliate, library walk-in)
- Home organization
- Type of home organization (university)

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 only possible by using a Campus account (username and password).

2.6 Campus account
The Campus account is personal and non-transferable.

The registered holder of the Campus account is responsible for the secrecy of the access data using all reasonable precautions. If there is any suspicion of the use of a Campus account by unauthorised persons, this must be reported immediately to the person responsible for IT security at the University or the person responsible for computers in the relevant Institute.

Campus accounts must be managed. In particular, the existence authorisation for the Campus accounts must be reviewed regularly. Campus accounts without this authorisation must be deleted immediately. The Management of the Institutes shall each appoint a system manager for this purpose.

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 universitärem Netzwerk“ (Available only in German)

3. Non-University institutes
The use of IT Resources 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 permitted 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 Head of IT Security together with the IT managers of the Institutes shall regularly conduct anonymous plausibility checks (random checks) to determine whether this Directive is being implemented.

In the event of any suspicion of misuse of IT resources, the Head of IT Security shall request the Governing Board of the University to authorise the announced monitoring of selected users for a specified and limited period of time. The Head of IT Security may, as a precaution, deny access to IT resources and also preserve suspicious data.

The Head of IT Security shall report immediately to the Governing Board of the University on the monitoring carried out and any precautions taken. The Head of IT Security shall recommend to the Governing Board of the University any additional measures that should be taken in order to maintain or restore lawful use of the network.

If the Head of IT Security receives any information about upload-activities of copyright protected data from the University network (e.g. using peer-to-peer-software), she/he may identify and admonish the person behind this network address, if required with the aid of the person responsible for computers in the relevant Institute. 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.

Activities carried out using the IT resources of the University of Bern, shall be recorded by the IT Services Department and retained for six (6) months as marginal data in accordance with the Federal Act of 6 October 2000 on the Surveillance of Post and Telecommunications [BÜPF; SR 780.1] and/or the Ordinance of 31 October 2001 on the Surveillance of Post and Telecommunications [VÜPF; SR 780.11].

The persons responsible for the IT resources of the Institutes are required to record and retain for six (6) months the data relating to activities carried out using their IT resources in accordance with BÜPF and or the VÜPF.

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 Commencement
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 21 January 2013.

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


On behalf of the Governing Board of the University

The Rector:

[Signature]

Prof. Dr. Christian Leumann