

12.02.2008
with amend-
ments of
9.6.2009

Directive on the Use of IT Resources at the University of Bern

The Governing Board of the University,

based on Art. 3, para. 3 of the University Act of 5 September 1996 (UniG) and Art. 68, par. 2, item c of the University Statute of 17^h December 1997 (UniSt),

decrees:

I. General Provisions

Aim	Art. 1 This Directive governs the use of IT resources at the University of Bern by authorised users.
Definitions	Art. 2 IT facilities are all equipment and installations, whether tangible or intangible, which enable the electronic processing, storage, transmission or destruction of information including:
1. IT facilities	<i>a</i> computer systems and smart devices; <i>b</i> peripherals, (such as storage media, external tape and disk drives); <i>c</i> networks, both fixed and wireless, and network devices (such as routers, repeaters, security devices, wireless access points); <i>d</i> software;.
2. Information	Information is technical, administrative and personal data.
3. IT services	IT services include all central services that are made available to authorised users, such as e-mail, DNS, WWW services, digital libraries, etc.
4. IT resources	IT resources include IT facilities, information and IT services.
5. Central IT Resources	Central IT Resources include IT facilities, information and IT services that are offered by the IT Services Department throughout the University.

II. Principles governing Use

General	<p>Art. 3¹ In principle, the IT resources may be used only in order to carry out University work.</p> <p>² 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.</p> <p>³ The authorisation of the Governing Board of the University is required for:</p> <ul style="list-style-type: none">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/or research. <p>⁴ The use of IT resources for University work as well as for teaching and research has absolute priority over all other uses.</p>
Processing of personal data	<p>Art. 4¹ The processing of personal data is only permitted in conjunction with University work and subject to compliance with the data protection legislation.</p> <p>² In the event of any suspicion of a processing of such data in an Institute, an ISDS Analysis (Analysis for IT security and data protection) has to be made in accordance with the guidelines of the IT and Organisation Office of the Canton of Berne (KAIO). [amendment of 9.6.2009]</p>
Presentation of the University in the network	<p>Art. 5 The Governing Board of the University shall issue directives and recommendations on the presentation of the University on the internal and external networks.</p>
Access to IT resources	<p>Art. 6¹ Access to the Central IT Resources, which are only available to a limited group of users, is in principle only possible by using an access account (username and password, personal certificate, smart card, token, etc.).</p> <p>² Access to IT resources of Institutes of the University of Bern, which are only available to a limited group of users, is in principle only permitted by using an access account. The access accounts for the IT resources of the Institutes are set up, allocated and managed by the Institutes. If technically possible, the Institutes may use the access accounts for the Central IT Resources instead of their own access accounts.</p>
Access account	<p>Art. 7¹ The responsibility for setting up, maintaining and deleting access accounts is in principle that of:</p> <ul style="list-style-type: none">– the IT Services Department for<ul style="list-style-type: none">o matriculated studentso members of staff of the university– the Centre for University Education (Zentrum Lehre) for<ul style="list-style-type: none">o alumni

- the Management (directors of institutes, departmental heads) of the Institutes for
 - o all other groups of persons

² The access account is personal and non-transferable.

³ The registered holder of the access account is responsible for the secrecy of the access data using all reasonable precautions. If there is any suspicion of the use of an access 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.

⁴ The access accounts must be managed. In particular, the existence authorisation for the access accounts must be reviewed at least once every month. Access accounts without this authorisation must be deleted immediately. This review must also be carried out in respect of access accounts for the IT resources of the Institutes. The Management of the Institutes shall each appoint a system manager for this purpose. The system manager is also responsible for the management and the documentation relating to authorisations for the access by administrators to the systems of the Institutes.

⁵ Further regulations on the management of access accounts for the use of the Central IT Resources of the University of Bern are set out in Annex A (Provisions relating to the Management of Access Accounts for the Central IT Resources of the University of Bern).

III. Misuse and Disciplinary Measures

Misuse

Art. 8 ¹ Misuse of the IT resources is any use which

- a infringes the statutory provisions of university legislation, and in particular provisions relating to university work,
- b infringes this Directive,
- c infringes other provisions of the law
- d infringes the rights of third parties.

² Misuse is in particular any of the following:

- a the processing, storage or transmission of data with racist, sexist or pornographic content;
- 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 of bulk emails for non-university purposes in the sense of *spamming*;
- k* using IT resources to harass others;
- l* manipulation of University IT resources;
- m* the use of IT facilities in such a way as to violate intellectual property rights and trading standards.

Disciplinary
measures

Art. 9 ¹ 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 unless it can be proven that the password was used without authorisation through no fault of the user concerned.

² 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 from the premises;
- c* delete data and block websites.

³ 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 against persons misusing IT resources is reserved.

Random checks,
precautionary
measures,
reporting, recording

Art. 10 ¹ 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.

² 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.

³ 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.

⁴ If the Head of IT Security receives any information about upload-activities of copyright protected data (e. g. using peer-to-peer-software from the University network), 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. [*amendment of 9.6.2009*]

⁵ 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].

⁶ 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.

IV. Final Provisions

Implementing-
provisions

Art. 11 ¹The Governing Board of the University may issue further implementing provisions as annexes to this Directive, providing additional detail on the articles in this Directive.

² The Commission for IT Services Department (KID) may within the scope of its authority issue further implementing provisions in the form of directives.

³ Any such implementing provisions require the approval of the Governing Board of the University.

Transitional-
provision

Art. 12 The allocation of access accounts in accordance with Art. 7 shall be implemented in phases; this provision applies only to persons who are already in possession of an access account.

Commencement

Art. 13 This Directive comes into effect on its approval by the Governing Board of the University in force. It replaces the Directive on the Use of the IT Resources at the University of Bern of 26 April 2005.

Bern, 12.02.2008

On behalf of the Governing Board of the
University

The Rector:

sig.

Prof. Dr. Urs Würgler

Amendments

Commencement

Amendment of 9.6.2009, into effect on 1.7.2009

Annex A: Provisions on the Administration of Access Accounts for the Central IT Resources of the University of Bern

Principle

The use of the Central IT Resources of the University of Bern is permitted for persons who use these IT resources for the purpose of their studies, their advanced education and training, their participation in conferences or their activity at and/or for the University of Bern.

This Annex regulates in particular the procedure for the administration of access accounts for the Central IT Resources at the University of Bern as well as the penalties for and liability of the responsible person in the event of misuse.

In addition, the regulations in this Annex are intended to ensure that only authorised persons gain access to limited resources and that no contractual conditions or legal principles are infringed.

The responsibility for setting up, maintaining and deleting access accounts is in principle that of:

- the IT Services Department for
 - matriculated students
 - members of staff of the university
- the Centre for University Education (Zentrum Lehre) for
 - alumni
- the Managements (directors of institutes, departmental heads) of the Institutes for
 - all other groups of persons

Responsibilities for the Allocation and Administration of the Access Accounts by the Managements of the Institutes

The administration of the access accounts by the Institutes themselves is the responsibility of their respective management. Access account administration may be delegated by the management of an Institute to one or more persons (e.g. the contact persons for the personnel management). Anyone with the right to carry out access account administration is referred to below as an account administrator. Written notice of any changes in the account administrators within an Institute (e.g. changes in staff, appointment of additional administrators) must be given to the IT Services Department immediately by the Institute's management. Notice of a change in the management of the Institute itself must be given to the IT Services Department by the new management.

Access Account Holder Groups administered by the Institutes

The account administrators are obliged to correctly indicate the affiliation of future holders of an access account to one of the groups listed below. The setting up of an access account for a person also includes the acceptance of that person into the partner information system of the University of Bern.

Members of an Institute who are not employed by the University of Bern

In the case of members of an Institute who are not employed by the University of Bern (project partners, guest lecturers, teaching staff not employed by the University, employees of third companies with temporary contracts for IT resources at the University of Bern, etc.) access accounts with restricted rights (e.g. online journal access, network-access, etc.) may also be set up on a temporary basis by the account administrators (for a period of up to 6 months, with further multiple 6-month extensions possible). The account administrators may if necessary also allocate e-mail-addresses at their Institute to these persons.

The full requirements for the allocation and maintenance of access accounts are:

- the access account holder requires access to University of Bern IT resources in order to be able to carry out an activity at or for the benefit of the University of Bern or the visibility of the access account holder as a member of the University of Bern is clearly required for the reputation of the university (e.g. e-mail-addresses in the case of publishing academics) *and*
- the University of Bern's conditions of use in relation to IT resources are accepted and complied with (including no unlawful, commercial or private use of the access account) *and*
- the licence provisions relating to the IT resources used by the access account holder are not infringed.

In the event of any misuse of IT resources, both the access account holder and the management of the Institute shall be responsible if the access account has been set up in contravention of the rules. The practice of allocating access accounts may be audited by the IT Services Department in cooperation with the personnel section. In the event of any abuse of the practice of allocating accounts, the Institute may have its right to independently allocate access accounts revoked.

Guests, course and conference participants

The account administrator may allocate access accounts with restricted rights (in principle network access only) to guests, course and conference participants, members of companies (in connection with presentations or service contracts), etc. These access accounts are valid for a maximum period of one week and are thereafter deleted automatically. Access accounts for course and conference participants may have anonymous user names (e.g. GUEST003), but the account administrator who has allocated the access account must be able to clearly identify the account holder in the event of misuse for a period of 6 months and pass on this information to the IT Services Department.

Postgraduate students

Postgraduate students taking courses of studies worth more than 60 ECTS points are automatically registered by the Matriculation Services Department and therefore receive an access account for the duration of their course of studies. For participants in postgraduate studies worth less than 60 ECTS points, the account administrator may set up an access account with restricted rights and with an indication of the end of the postgraduate course. The account shall be permanently deleted at the end of the postgraduate course, together with any personal mailboxes, file repositories and websites.

Former members of staff in the publication process

Former members of staff of the University of Bern who are still involved in the publication process are reliant on data access and their published e-mail-address. The account administrator may arrange for their access account to be extended on expiry of their employment with the University of Bern for a further 6 months in each case, up to of a maximum period of 18 months. Simple e-mail-forwarding arrangements may continue at the justified request made to the account administrator for a maximum of 3 years. Simple e-mail-forwarding arrangements may also be made by the account administrator for other former members of staff for a duration of 1 year.

Emeritus professors and other former members of staff who have retired

For former members of staff of the university who have retired, the account administrator may set up an access account with restricted rights. Professors emeriti/ae and former members of staff are normally listed in two separate e-mail domains. If the management of an Institute so wishes, members of staff who have retired may retain their former e-mail accounts if a justified request is made to the account administrator.

Access Account Holder Groups administered by the IT Services Department

Members of staff employed by the University of Bern

In the case of future members of staff of the University of Bern, temporary access accounts with a maximum term of 2 months may be set up by the account administrator before the member of staff is registered in the PERSISKA¹-database. As soon as notice of the data has been given via PERSISKA, the access account shall be extended automatically for the duration of employment or for an unlimited duration. On expiry of the term of employment in accordance with PERSISKA, the account shall be automatically closed. 6 months after expiry of the term of employment, the account together with personal data such as mailboxes, file repositories and websites shall be deleted. Accounts set up on a temporary basis that have not been confirmed before their expiry by an acknowledgement from PERSISKA shall be automatically closed and after a further 6 months shall be deleted together with the personal mailboxes and files.

Students

Students shall be allocated an access account automatically as soon as their personal details in accordance with the advance registration form have been checked. The access account shall remain active for the duration of the course of studies. On removal

¹ PERSISKA is the cantonal salary processing system

from the register of students, the access account shall remain valid for 180 days. Thereafter it shall be deleted.

Non-university institutes

In the case of institutes that do not belong to the University of Bern, the use of the IT resources shall be regulated by special agreements with the University of Bern.

Members of other academic institutions

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

Right of amendment of the IT Services Department and Governing Board of the University

The IT Services Department reserves the right, at any time and where there is good cause, to amend these access account regulations in agreement with the Governing Board of the University.