User Regulations of the Centre for Information Processing and the IP Provider Units of Münster University as amended on 15 November 2010

Pursuant to Sections 2(4) and 29(2) of the North Rhine-Westphalian University Act ("Hochschulgesetz", abbr.: HG) of 31 October 2006 in conjunction with the organisational concept "The Information Processing System of Münster University" (Senate resolution of 8 July 1996, amended on 11 March 2004), the Senate of Münster University has adopted the following User Regulations for the Zentrum für Informationsverarbeitung (ZIV) and the IV-Versorgungseinheiten (IVVen) as Statutes:

Preamble

These User Regulations are intended to ensure problem-free, unhindered and secure use of the communication and information processing infrastructure (IP Infrastructure) of the ZIV and the IVVen of Münster University. They provide basic rules to ensure proper operation of the entire IP Infrastructure, thereby regulating the relationship between individual users, the ZIV and the IVVen.

§ 1
Scope of Application

These User Regulations apply to the use of the IP Infrastructure of Münster University, consisting of the data processing systems, the communication systems and other computer-based information processing resources (IP), which are under the control of the ZIV and/or the IVVen of Münster University (collectively called the "IP System"). Insofar as individual components of the IP System do not expressly fall under the control of the ZIV or an IVV, these Regulations shall apply analogously to those parts of the IP System

§ 2
Eligibility for and Admission to Use, Identity Management

(1) The following persons and bodies may be admitted to use the IP System:
    1. Members and affiliates, institutes and administrative bodies of the universities, and other organisations of the State of North Rhine-Westphalia, for which the IP System has been established in order to assist them in the performance of their duties;
    2. Members and affiliates of other universities of the State of North Rhine-Westphalia or of other state universities outside of the State of North Rhine-Westphalia on the basis of specific agreements between the universities or directives of the competent ministry;
    3. Student welfare organisations in the State of North Rhine-Westphalia;
    4. Other legal entities or natural persons if and insofar as free capacities are still available after use by the users named under No. 1 to 3, who shall have precedence in use of the IP System.

    In the case of use in connection with secondary occupations, the regulations pertaining to secondary occupations in the university sector in the State of North Rhine-Westphalia shall apply.

(2) Admission shall be granted exclusively for use in connection with or for purposes of research, teaching and study, medicine, the library and the university administration, initial and further training, and for the performance of other duties of Münster University. Any use other than the foregoing may be permitted if it is of a minor nature and does not interfere with the intended purpose of the IP System and the needs and interests of the other users. Commercial use as referred to in Para. 1 No. 4 is permitted only after prior consultation with the ZIV and/or the IVVen

for their respective areas of competence.

(3) Admission to use the equipment and services of the IP System takes place in the context of identity management by providing one or more accounts on the target system, which the user is authorized to access in accordance with his role (provisioning). Generally, all accounts of a user are identified by the same ID. In exceptional cases, the various roles of a user may require the assignment of several IDs.

a) Automatic ID Generation
Usually, IDs are generated automatically from data listed in the university facilities' registers of persons. For employees, data are transferred to the identity management system in accordance with the "Appendix Employees". For students, data are transferred to the identity management system in accordance with the "Appendix Students".

b) ID Generation on Application
In case an automatic ID generation is not possible, the ZIV may allocate an ID in response to a written application or formal online registration. The application procedure is a two-stage process:

aa) User Group
A person with responsibility for funding (university lecturer or director of an institute) must submit an application for the formation of a user group. Afterwards users can apply for admission as part of a user group. Where IVVen have their own user admission, permission is granted by the head of the relevant institution.
For purposes of admission, a description of the user group is necessary. Further specifications should be made as annexed either using a specified application form or in the course of online registrations.
Also needed:
- Signature of the user group leader
- Particulars and signature of the person responsible for funding

bb) User Application:
- Personal data according to "Appendix Employees" or "Appendix Students"
- Signature of the user
- Particulars and signature of the user group leader

c) Role Management
The roles of a user are collected separately, insofar as they are relevant to the provisioning and do not result from the data collected during ID generation.

(4) ID Activation
The users receives a password upon entry in the identity management system. In the letters sent at enrollment, students will be informed that the data stored about them constitute the basis of the usage relationship in accordance with Section 7 and with the operating rules based on Section 7(8).

(5) ID Deactivation / Grace Period
In case the user no longer holds the status or role, due to which the account has been granted, the account will be deactivated after a transition period specified in the operating rules.

§ 3
Mapping, Provisioning, Administration

(1) Mapping
A unique identity is assigned to each user. In order to define this unique identity, the data are

consolidated in the identity management as appropriate.

(2) Provisioning
In order to generate IDs on the supporting target systems (e.g. Active Directory Services), the following data are generally transmitted:
1. ID
2. Password
3. Roles and rights
4. First name, surname and organisational information
5. Technical information

The target systems which are currently available are administered and documented in the identity management system.
The ZIV and the IVVen can integrate further target systems into the identity management where required.
In the joint performance of duties by several universities, a data transfer from the identity management is permissible if it is necessary for the performance of duties by the transferring body or the recipient.

(3) Interface for Administrators
The administration within the provisioning system is documented in the identity management system and restricted exclusively to authorized administrators. In addition to central administrators from the administration department and the ZIV, decentralized administrators, who can provision the local target systems, may be appointed.

(4) Self-Administration
Self-administration allows the user to exercise his informational right of self-determination and inspect the data stored on him. In the context of self-administration, users can change their data independently to a specified extend. The scope of the change authorization is documented in the identity management system.

§ 4
Proper and Trouble-Free Operation

(1) User admission and access to the different target systems may be restricted and terminable.

(2) To ensure proper and trouble-free operation, the user admission may also be subject to a restriction on the computing and online time and to other use-related conditions and requirements.

(3) If the capacities of the IP resources are not sufficient to meet the needs of all eligible users, operating resources may be allocated to the individual users in accordance with the order of priority as set forth in Section 2(1).

(4) User permit and access to specific target systems may be wholly or partially refused, revoked or subsequently restricted, especially if
1. the particulars stated in the application are incorrect or are no longer correct;
2. the preconditions for proper use of the IP System do not exist or no longer exist;
3. the user has been barred from use in accordance with Section 6;
4. the project planned by the user is incompatible with the intended purposes of the IP System and the purposes as set forth in Section 2(2);
5. the available IP resources are unsuitable or insufficient for the use applied for or are reserved for special purposes;
6. the IP components intended to be used are connected to a network which must meet special data security requirements and no objective reason for the planned use can be seen;

7. it is to be expected that the intended use will unreasonably interfere with other eligible projects.

§ 5
Rights and Duties of the User

(1) The users have the right to use the resources of the IP System within the scope of their permit and in accordance with these User Regulations and any other regulations issued pursuant to Section 7(8). Any use which deviates from the above is prohibited except by special permit.

(2) The user has a duty
(General)
1. to comply with the provisions of the User Regulations and any limitations and restrictions to which the user permit is subject, and in particular to comply with the intended used and purposes as set forth in Section 2(2);
2. to take all necessary measures which have been defined by the IP Security Team in consultation with the IVVen and the ZIV and brought to the user's attention timely by e-mail and online information;
3. not to do anything which could disturb or disrupt the proper running and operation of the IP System of Münster University;
4. to treat all data processing equipment, information and communication systems and all other resources of the IP System carefully;

(Handling of user ID)
5. to work only with those user IDs which have been allocated during the admission and provisioning procedure;
6. to ensure that no other person acquires knowledge of the user passwords and to take all precautions in order to prevent unauthorised persons from accessing the IP resources of the IP System of Münster University; this also includes protecting access by a suitable password, i.e. one which cannot be guessed easily, which must be kept secret and should be changed regularly;
7. neither to identify nor to use others' user IDs and passwords;
8. not to access other users' information without authorisation nor to pass on, use or alter other users' information without their permission. This also applies to the access to IP systems of third parties via the Science Net (Wissenschaftsnetz) or the Internet. Any violation may result in individual users being barred.

(Use of software and hardware)
9. when using software, hardware, documentations and data, to comply with statutory regulations, and in particular the provisions of copyright law, and also with the terms and conditions of licences under which software, documentations and data are provided by the ZIV and the IVVen;
10. not to copy software, documentations and data provided by the ZIV or the IVVs, nor to pass it on to third parties, except where expressly permitted, nor to use it for any other than the permitted purposes;
11. when on the premises of the ZIV and the IVVen, to comply with directions of the personnel and to follow any house rules as may apply;
12. to provide evidence of user entitlement on request;
13. not to seek to remedy disturbances, damage or faults to the IP System and/or data carriers of the IP System but to report the same immediately to the personnel of the ZIV or the competent IVV;
14. except with the express consent of the ZIV or the IVVs, not to interfere in any way with the hardware installations of the IP System nor to make any changes to the configuration of the operating systems, the system files, the system-relevant user files or the network;

(Miscellaneous)
15. if so requested in specific and substantiated cases – especially on justified suspicion of misuse or for purposes of remedying faults or disturbances – to inform those in charge at the ZIV and/or the IVVen of the programs and methods being used and to allow

inspection of the programs. This provision does not apply to user data as protected by telecommunications secrecy or data secrecy, e.g. emails, personal files or the personal data of third parties (e.g. patient data).

16. to consult and agree with the ZIV and/or the competent IVV on the processing of personal data and, notwithstanding the user's own obligations under data protection law, to take the data protection and data security precautions suggested by the ZIV and/or the IVVen into account;
17. to provide content held available for others' use (e.g. web pages) with publishing details including the name and address of the person responsible for the content (Section 6 TDG [Tele-Services Act], Section 6 MDStV [Media Services State Treaty).

(3) The attention of the user is drawn in particular to the following acts which are prohibited under criminal law:

1. Eavesdropping on data (Section 202a StGB [German Criminal Code]), Interception of data (Section 202b StGB), Preparation for eavesdropping on and interception of data (Section 202c StGB)
2. The alteration of data (Section 303a StGB) and computer sabotage (Section 303b StGB)
3. Computer fraud (Section 263a StGB)
4. Dissemination of pornographic depictions (Section 184 StGB), and in particular dissemination, acquisition or possession of child pornography (Section 184b StGB) as well as dissemination of pornographic depiction via broadcasting, media or teleservices (Section 184c StGB)
5. Disseminating the propaganda of unconstitutional organisations (Section 86 StGB) and the incitement of racial hatred (Section 130 StGB)
6. Causing detriment to another's character, e.g. defamation or slander (Section 185 ff. StGB)
7. Criminal breaches of copyright, e.g. through the unauthorised reproduction of software (Section 106 ff. UrhG [German Copyright Act]).

§ 6
Exclusion from Use

(1) Users may be temporarily or permanently restricted in use of the IP resources or barred from use of them if they

1. culpably violate these User Regulations, and in particular the duties set forth in Section 5 (malconduct) or
2. misuse the resources of the IP System for criminal acts (this also applies to misuse of other facilities of the IP resources of Münster University) or
3. cause detriment to the University through other illegal user behaviour.
4. Measures pursuant to Para. 1 should only be taken after a caution has been issued with no avail. In the case of very serious breaches, the issue of a caution may be waived. The user concerned must be given the opportunity to respond. He or she may ask the chairperson of the IP Commission to act in the capacity of a mediator.

(2) Temporary restrictions on use imposed by the director of the ZIV or the competent IVV must be lifted as soon as proper use once again appears assured.

(3) A permanent restriction on use or the complete barring of a user from further use will only be considered in the event of serious or repeated violations within the meaning of Para. 1 and if proper behaviour is also not expected in future. A decision on permanent exclusion is made by the Chancellor on application of the director of the ZIV or IVV and after hearing of the IP Commission; notice of the decision must be made to the user. This shall have no effect on any claims which the ZIV or IVV may have for use of the IP System.

§ 7
Rights and Duties of the ZIV and the IVVen

(1) To the extent necessary for purposes of trouble shooting, systems administration and systems enlargement or for reasons of systems security and protection of user data, the ZIV and/or the IVVen may temporarily restrict the use or their resources or freeze individual user IDs. If possible, the users concerned should be informed accordingly in advance. This also applies to users who do not fulfill their obligation to carry out the necessary measures in accordance with Section 5(2; No. 2). These users will obtain only limited access to the network and limited options for usage of the university's resources.

(2) Should actual grounds exist for suspecting that a user is holding illegal content available on the servers of the IP System, the ZIV and/or IVVen may prevent further use until the legal situation has been clarified. This provision does not, however, cover the viewing or freezing of "normal" user data not released by the user for general access.

(3) The ZIV and/or IVVen have the right to review the security of the system/user passwords and user data through regular manual or automated measures and to undertake any protective measures, e.g. changes to passwords which could be easily guessed, as may be necessary in order to protect the resources of the IP System and user data from unauthorised access by third parties. In the event of all necessary changes to user passwords, access rights to user data and other protective measures of relevance to use, the user must be informed accordingly without delay.

(4) The ZIV and/or IVVen have the right, subject to the provisions set forth below, to document and evaluate the use of the IP System by individual users, though only to the extent necessary
   1. to ensure proper operation of the system,
   2. for purposes of resource planning and systems administration,
   3. to protect the particulars of other users,
   4. for accounting and invoicing purposes,
   5. to detect and remedy technical disturbances and faults, and
   6. to identify and prevent illegal or improper use when actual indications for such use exist. These must be documented in writing.

(5) For any of the purposes or reasons as set forth in para. 4, the ZIV and the IVVen are also entitled, provided the regulations pertaining to data secrecy are complied with, to inspect user files to the extent necessary to remedy current faults or disturbances or to identify and prevent misuse if and insofar as actual grounds exist for suspecting such misuse.
Inspection of message and email postboxes is, however, only permissible to the extent necessary for remedying current faults and disturbances in the communications service.
Such inspection must always be documented and the user informed immediately after the intended purpose has been achieved.

(6) For any of the purposes or reasons as set forth in para. 4, the connection and utilisation data in communications traffic (especially email use) may also be documented. However, only the circumstances attendant upon the telecommunication – but not the non- public content of the communication – may be recorded, processed and used.
The connection and utilisation data of online activities on the Internet and other teleservices which are held available by the ZIV or the IVVen for use or to which they provide access must be deleted as soon as possible, except where such data is needed for accounting and invoicing purposes.

(7) In accordance with the statutory regulations, the personnel of the ZIV and the IVVen is obligated to preserve telecommunication and data secrecy.

(8) To ensure proper operation of the IP System, the directors of the ZIV and/or the IVVen may issue further regulations for the use of the IP System within their respective areas of responsibility.

§ 8
Liability of the User

(1) The user shall be liable for all detriment sustained by the University through improper or illegal use of the resources of the IP System and the user permit or through the user culpably failing to comply with his/her duties under these User Regulations.

(2) The user shall also be liable for damage caused by use by third parties within the scope of the access and utilisation possibilities provided to the user if the user is responsible for such third-party use, especially resulting from the user making his/her user ID known to such third party. In this case, Münster University may charge a utilisation fee to the user for such third- party use in accordance with the fee regulations.

(3) The user shall indemnify Münster University for all claims made on it by third parties for damages or restraint or of any other nature on account of improper or illegal use by the user. Münster University will interplead against the user should any third party bring legal action against the ZIV or the IVVen.

§ 9
Liability of the University

(1) Münster University does not warrant the trouble-free or uninterrupted operation of the IP System at all times. The loss of data through technical faults and the obtaining of confidential data through unauthorised access by third parties cannot be ruled out.

(2) Münster University does not assume any responsibility for freedom from faults of the programs made available. Nor may Münster University be held liable for the content, and in particular for the correctness, completeness or up-to-dateness of the information to which it merely provides access for use.

(3) In all other respects, Münster University may only be held liable for deliberate intent or gross negligence of its personnel, except where it culpably breaches any of its material duties. In this case, the liability of the University shall be limited to the typical damage of the kind foreseeable at the time at which the relationship relating to use was concluded between the user and the University.

(4) The foregoing shall be without prejudice to any claims against Münster University on grounds of public liability.

§ 10
Entry into Force

These User Regulations shall enter into force through publication in the Official Announcements of Münster University on the day after being posted on the bulletin board.

Issued pursuant to the resolution of the Senate of Münster University of 10 November 2010.

Münster, 15 November 2010

The Rector

Signed: Prof. Dr. U. Nelles

Appendix relating to Section 2(3) of the User Regulations of the Centre for Information Processing and the IP Provider Units of Münster University

In general, IDs are generated automatically from data listed in the university facilities' registers of persons. (Required fields are indicated by an asterisk.)

Appendix Employees

For employees, the following data are transferred to the identity management system:

- Indenture number (ID) *
- Status *
- Surname *
- First name *
- Date of birth *
- Place of birth *
- Gender *
- Title
- Street, house number
- Postcode
- Place of residence
- Country
- Personnel number *
- Category of employment *
- Finish date of the employment *
- Institution * (multivalue)
- Telephone (official) *
- Cost centre
- Bank connection
- Bank identifier code
- Account number

Appendix Students

For students, the following data are transferred to the identity management system:

- Indenture number (ID) *
- Status *
- Surname *
- First name *
- Date of birth *
- Place of birth *
- Gender *
- Title
- Street, house number *
- Postcode *
- Place of residence *
- Country *
- Telephone number (private)
- Contact email
- Matriculation number *
- Student status *
- Degree programme * (multivalue)
- Date of enrolment *

- Institution

In case of doubt about the text in this English translation the German version "Benutzungsordnung des Zentrums für Informationsverarbeitung und der IV-Versorgungseinheiten der Westfälischen Wilhelms-Universität Münster" will be the binding version.