Fachhochschule Nordwestschweiz

Regulations regarding the use of the FHNW IT infrastructure (IT regulations)

Issued by the FHNW Head of Services on 12 May 2017

Approved by the FHNW President on 1 June 2017

I. General section

1. Purpose and scope of validity

1 These regulations serve the purpose of FHNW IT security and the legally permissible use of the FHNW IT infrastructure.

2 These regulations apply to all members of FHNW (staff and students) who hold a personal FHNW account.

3 These regulations form part of the FHNW Collective Labour Agreement according to Section 15.1 Collective Labour Agreement.

2. Terms

1 *FHNW IT infrastructure:* The FHNW IT infrastructure includes all IT resources which can be used to compile, process, save or present data and all IT components used for data transport. Furthermore, the FHNW IT infrastructure includes rooms, systems and installations used for operating the aforementioned IT resources and components.

2 *Methods of identification:* Methods used for the definitive identification of an individual such as requesting passwords or PIN codes or identification by means of contactless reading devices using the FH Card.

3 *Spam*: Spam is defined as unwanted messages, normally sent electronically, which are sent to a recipient without being solicited and frequently contain advertising material.

4 *Metadata*: Records concerning use of the electronic infrastructure. This includes details of the sender, recipient, time, duration and communication channel.

5 *Security measures:* Various safety functions and applications are used to protect the FHNW IT infrastructure and FHNW members' data from wrongful use, theft and damage. This is mainly carried out using antivirus protection, ad blockers, firewalls, encryption technologies, password-protected access, protocols of FHNW IT infrastructure use (recording of metadata) for the purpose of analysis and the possibility of response via remote access.

6 *Wrongful use:* Any use of the FHNW IT infrastructure is wrongful if it is in breach of these regulations or of higher-level statutory provisions or if it violates the rights of third parties (such as the processing, saving or sending of material with unlawful or indecent content, in particular representations of violence and pornography, incitement to crime or violence, interference with the freedom of religion and culture, racial discrimination).

II. Rights and responsibilities of FHNW members and their liability

3. *Rights of FHNW staff*

1 FHNW provides staff with the resources required for internal and external communication according to Section 11.7 Collective Labour Agreement. Staff are also entitled to use the FHNW IT infrastructure to carry out their work.

2 The use of FHNW IT resources is permitted for private purposes providing work performance capacity is not impaired and there is no infringement of FHNW's legitimate interests.

4. *Rights of FHNW students*

1 FHNW students are entitled to use the FHNW IT infrastructure provided for the purpose of study.

5. *Responsibilities of FHNW members*

1 Members are to use the FHNW IT infrastructure with care and in a way which is technically and legally correct.

2 Access authorisation and identification methods are individualised and therefore confidential. They may not be made accessible to third parties.

3 Passwords must be in line with the directive "Creating and using passwords for users, administrators and services".

4 The use of private devices for processing FHNW data is only permitted if the security measures defined in Section 2 Paragraph 5 are observed. FHNW can require specific security measures in justified cases. When using private devices, the responsibility for meeting security requirements lies with FHNW members.

5 Sending and forwarding spam is prohibited.

6 Expanding, altering or disrupting the FHNW IT infrastructure is prohibited. Exceptions for the purpose of teaching and research are mandated by the Director of FHNW and require prior approval by the Head of Corporate IT.

7 Analyses of the FHNW IT infrastructure in relation to IT security and architecture may only be carried out by the members of FHNW Corporate IT responsible.

8 FHNW members must immediately report any security-related incidents, unlawful behaviour or relevant security defects that become known to them to it-security@fhnw.ch or the local IT support.

6. *Liability*

1 FHNW members are liable for damages caused by grossly negligent or deliberate violation of these regulations.

2 FHNW denies any liability for damages arising from private use of the FHNW IT infrastructure.

III. Enforcement of IT security and measures in the case of wrongful use

7. Protocol analyses

1 In order to enforce IT security, the IT Security Officer (I-SIBE) regularly arranges for anonymised protocols of IT activities to be analysed. Individuals cannot be identified in this connection.

2 If there is a justified suspicion of unlawful behaviour, in particular wrongful use, the relevant information is secured and a personalised analysis is carried out. Personalised analysis involves the relevant individuals being identified.
In his function as the general director of security at FHNW, the Vice President (Head of Services) instructs personalised analyses to be carried out at the written request of the I-SIBE or a member of the FHNW Board of Directors. The Vice President decides on the involvement of the competent authority.

3 The I-SIBE informs the FHNW members involved of the personalised analysis. In cases where there is a risk of endangerment or urgency, the members can be informed after the personalised analysis has been carried out.
All personalised analyses are documented by the I-SIBE.

8. Measures in the case of wrongful use

1 If the I-SIBE ascertains wrongful use by an FHNW member based on personalised analysis, the I-SIBE secures the relevant protocols and informs the department or Programme Head/Head of Institute responsible as well as the Vice President (Head of Services).

5 In the event of wrongful use by FHNW members, the department in which the relevant individual is employed implements the measures set out in the Collective Labour Agreement.

6 In the event of wrongful use by FHNW students, the university implements the measures set out in the Course and Examination Regulations.

7 Severe misuse is reported to the law enforcement authorities.

IV. Final provisions

9. Entry into force

1 Involvement was granted to both parties according to Collective Labour Agreement Section 4.9 at the co-determination level “equal co-decision rights”.

2 These regulations come into force as of 1.6.2017 and replace the directive concerning the use of IT resources dated 1.11.2013.