Directive Regarding Use of IT Resources at Bern University of Applied Sciences[1]

The President of Bern University of Applied Sciences (BFH)

as supported by Sect. 35 Par. 2 letter h in accordance with the law of 19 June 2003 regarding the Bern University of Applied Sciences (FaG[2])

hereby decrees:

1. General Regulations

Art. 1 Purpose and Scope

[1] This directive regulates the use of IT resources by authorised users at BFH.

[2] This directive applies to all users of IT resources at BFH.

Art. 2 Terms

[1] *IT resources* are all appliances, equipment and computer programs which serve the electronic processing of information, in particular for:

- *a* Computer systems and smart devices
- *b* Peripheral devices (i.e. printers, external disk drives, storage media, etc.)
- *c* Networks (non-wireless and wireless) as well as network appliances (i.e. routers, WLAN access points, security devices, etc.) and
- *d* Software

[2] Information encompassing material and/or personal data.

[3] Marginal data cover information of the use of IT equipment.

[4] *Processing* of personal data includes any handling of personal data, such as acquiring, storing, changing, linking, disclosing or eliminating.

[5] *Disclosing* is making personal data information available for any purpose such as granting access, viewing, providing information, forwarding or publishing.

[6] IT services are offered and operated by the IT-Services Dept., which are available to all users (i.e. DNS, e-mail, registry services, etc.) as well as department-internal IT services operated by the various divisions and other services offered which those working at or for BFH may operate.

[7] IT administrators are the persons who are responsible for operating the IT services.

[8] IT resources include all IT technology, information and IT services.

[9] Users include all persons who make use of IT resources at BFH, in particular:

- *a* Affiliates of BFH according to the University of Applied Sciences statutory order[3];
- *b* Persons who are employed by organisations outside of BFH, and who have a mandate with or as partner of BFH and who conduct activities at or for BFH (i.e. research activities, support, maintenance or development work, etc.);
- *c* Affiliates of other academic facilities with which partner agreements exist;
- *d* Further persons who participate in events and who use IT resources for a specific timespan.

[1] This document is a translation. The German or French version shall prevail.
[2] BSG 435.411.
[3] BSG 436.811.

2. Use of IT means at BFH

Art. 3 IT Resources

[1]IT resources are to be utilised solely for the completion of the accruing work duties at BFH.

[2]The private, personal, non-commercial use of IT resources is permitted, as long as work and study duties as well as the daily business operations are no way impaired.

[3]The use of IT resources for the completion of daily business operations and work duties at BFH, in particular teaching and research, always has priority over other uses.

[4]Following usage types need special authorisation by the head of the department or the head of IT-Services prior to implementing:

a the use of IT resources for private purposes with commercial objectives (i.e. spin off);

b the use of IT resources for study and research purposes, which are normally prohibited in accordance with of Art. 7.

[5]The use of IT resources by organisation units not affiliated with BFH, as well as the usage based on Par. 4 let. a are classified under the claim for compensation and are regulated by special agreements.

[6]IT services which are not operated by the IT-Services Dept. and are used within the network of or for BFH are subject to the same requirements regarding data protection, usage regulations and storage of marginal data.

[7]On official BFH equipment with BFH client setup provided and maintained by BFH, no changes to settings or relevant security settings and software is to be made.

[8]The theft of IT equipment as well as additional relevant security observations in combination with IT resources must be reported immediately to the IT-Services Dept. and/or the person responsible for IT security at BFH.

[9] The disposal of information stored on data media is governed by the instruction, "Directive on the disposal of media and the prior treatment of information at the Bern University of Applied Sciences".

Art. 4 User Accounts

[1]Access to IT resources is solely possible, with a few exceptions, with a BFH user account (login name and password).

[2]The user account is personal and non-transferable.

[3]The owner of the registered user account is solely responsible for making sure that security standards are upheld in regard to all safety measures.

[4]Should the suspicion arise that a user account is being abused by unauthorised persons, the IT-Services Dept. and/or the person responsible for IT security at BFH must be informed immediately.

Art. 4a Accessing user accounts

[1] Direct access to the contents of a user account, including a personal mailbox, by persons other than the person registered on the account is not permitted. This provision does not apply to the necessary areas of responsibility of IT administrators, whereby it is ensured, as far as possible, that personal data not be disclosed.

[2] Superiors may require employees to account for their professional electronic correspondence and, in cases where a breach of duty is suspected, enact the measures which, in terms of personnel law, make it possible to monitor a user account, while respecting the provisions set out in paragraph 6.

[3] In case of absence of a longer or unforeseeable duration, employees shall set up an automatic absence message. If this is not done, the superior is authorised to have it set up

[4] If it is presumed that professional data necessary for the lawful performance of duties are held on the user account of a former or absent employee, that person shall be contacted and asked, within a specified period, to make the data available at the BFH's usual place of work or to authorise access to the user account data.

[5] If the employee or former employee cannot be contacted or does not comply with the requests in accordance with paragraph 4, the required data may be checked by means of a substitute measure.

The person concerned must be informed of the subsequent substitute measure when the time limit is communicated. A time limit may be waived if there is imminent danger or if it is clear that the person concerned will not fulfil his or her obligation within a reasonable period of time.

.

[6] Any access to the data of a user account must be relatively proportionate and must be carried out by, or in the company of a superior person. Private and business data must be kept separate, as far as possible, so that private content is not disclosed. After access has taken place, the person concerned must be informed about the time, the procedure followed and the persons present.

Art. 5 Privately-owned and self-administrated IT equipment

[1]The use of equipment which is self-administrated by the user or the implementation of privately-owned equipment is permissible with certain restrictions.

[2]The user is solely responsible for all compliant usage of privately-owned and self-administrated equipment.

[3]Such a device may only be connected to the network (i.e. BFH LAN, BFH WLAN, VPN, etc.) when all the following conditions have been fulfilled:

- *a* The device must always be up-to-date in terms of security updates and software technical issues (system software and applications).
- *b* The installed and run software on the device must be continually provided with security updates ("End of Support/Life" software is prohibited)
- *c* All applications and installed software on the device must be legally purchased and licensed correctly. Furthermore, the licence and user agreements must be conformably implemented at all times. This applies for privately organised software as well as readily available software provided by BFH.
- *d* The device must be secured by the necessary protection measures, namely anti-virus software, malware protection, local firewall and appropriate configuration. If the operating system of the device provides a function for encrypting the data storage, this must be used in a configuration corresponding to the state of the technology.
- *e* The user actively helps in clarifying IT incidents and finding solutions where he/she or the respective device are in any way involved.

[4]The IT-Services Dept. offers "best effort" support for private or self-administrated devices. Any further, no entitlement for support exists.

[5]The use of any equipment is at the user's own risk. BFH disclaims all liability from the use of such devices.

[6]If the private or self-administrated device is given to a third party (i.e. disposal, sale, repairs, etc.) or the person leaves BFH for good, all the following conditions must be assured by the user in advance:

- *a* All saved data information on the BFH device must be returned to BFH
- *b* All saved data information on the device must be made unrecoverable and is to be deleted.
- *c* All software for which the respective license regulations explicitly prohibit further use must be uninstalled from the device.

3. Accountability and Liability

Art. 6 Compliance

[1]Every user must always adhere to the currently valid laws and regulations concerning data protection and copyright laws[4].

[2]Prior to using any kind of IT resources, in particular software, the user informs himself/herself regarding the valid license regulations and adheres to these accordingly.

[4] BSG 231.1.

[3]The processing of personal data is only permitted within the lawfully stated duties of BFH under the compliance of data privacy regulations, in particular the Cantonal Data Protection Act (CDPA)[5] and the derivative Data Privacy Regulation (DPR)[6].

Art. 7 Malpractice

[1]Improper use is considered to be any use of BFH IT resources which neglects the aforementioned directive, violates the superior law or breaches the rights of third persons. Approved exceptions to the following abusive areas can be found in Sect. 3 Par. 4 of this directive:

- *a* Processing of information with illegal or immoral content, in particular scenes of violence, pornography, call to criminal activities or violence, disruption of freedom of religion and cultural affairs as well as race discrimination.
- *b* Producing instructions on how to produce or the deliberate distribution of malware programs or program parts (i.e. viruses, worms and trojans).
- *c* Unauthorised entry into database systems within or outside of BFH ("hacking"), in particular the extraction of passwords, not by IT-Services approved researching of BFH-internal and –external networks, as well as IT services on weak points (i.e. port scanning, etc.), preparation and implementation of bugs on networks and IT services (i.e. denial of service attacks).
- *d* Stealing of information as well as the unlawful processing of information, in particular copying, changing and deleting.
- *e* Publishing of content on internal BFH or external IT services if the content violates the applicable laws or damages the reputation of BFH. In particular, it is strictly prohibited to distribute copyright-protected material.
- *f* The use of IT resources of BFH with intent to violate licence agreements or copyright laws.
- *g* Purchasing, saving, installing, activating or using of any kind of illegally purchased software, licences or services.
- *h* Sending of information with faked or misleading sender information (inc. technical address) or unsolicited mass e-mails (i.e. spam mails)
- *i* Harassment or misinforming BFH employees or third parties by using IT resources (i.e. e-mail with demeaning and discriminatory content)
- *j* Extension or changing of BFH network components (i.e. modem, WLAN access points)
- *k* Use of IT resources to calculate digital payment means, such as Bitcoin.
- *l* Use of IT resources for private purposes with a commercial aim (e.g. SpinOff)

Art. 8 Consequences of Malpractice

[1]When using IT resources, in particular when implementing their personal user accounts, the users themselves are directly and personally responsible that these directives are not used for malpractice or are violating superior laws.

[2]In case of malpractice or should there be a concrete suspicion of misuse of IT resources, IT-Services has the right to take all measures necessary for restoring the IT resources to their original state, in particular:

- *a* Precautionary blocking of access to the respective IT resources.
- *b* Seizure of the improper information and securing and saving these as pieces of evidence.
- *c* Deletion of improper information in so far as security reasons necessitate this measure.
- *d* IT-Services informs the head of the affected department about the measures taken.

[3]In case of any malpractice, either personal or study legal sanctions against the user may be implemented.

[4]Criminal prosecution and charges in civil rights matters are to remain subject to the law.

Art. 9 Privacy

[1]To safeguard the implementation of the directive, anonymous plausibility controls via random sampling may be performed by IT security in cooperation with the person responsible.

[5] BSG 152.04.
[6] BSG 152.040.1.

[2]To safeguard the operation of IT services in case of failure, regular checking of the correct technical functioning is performed and data protocols are to be evaluated.

[3]In case of suspicion regarding misuse of IT resources, the head of IT makes a request to the rector for the implementation of an announced, fixed-term and person-defined restricted check.

[4]Activities undertaken using IT resources can be recorded. The marginal data generated is used to trace technical functions and secure evidence.

[5] Insofar as it is applicable, the Ordinance on Margnial Data[7] applies to the access and evaluation of marginal data containing logfiles recorded when using the electronic infrastructure.

[6] Margnial data containing personal data shall be retained for a minimum of 6 months and a maximum of 1 year. A different retention period is permissible if required by law or regulations, namely the Ordinance on Marginal Data[5], or if it is necessary to retain data as evidence. A transitional period until 31.12.2021 applies for this implementation.

Art. 10 Disclaimer

BFH does not accept liability for damages occurring as a result of defects or when using IT resources.

4 Final provisions

Art. 11 Final provisions

[1]Individual items of this directive can be further supplemented by annexes. These are to be approved in advance by the rector.

[2]The current directive replaces the version concerning the handling of IT resources at Bern University of Applied Sciences dated 13 July 2016 and is effective as of 1 January 2021.

Bern, 1 January 2021

Bern University of Applied Sciences

Prof. Dr. Sebastian Wörwag
President

[7] BSG 153.011.5.